

งานรับฟังความคิดเห็นต่อร่างมาตรฐาน  
การเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ  
ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange  
Series: Linkage Standard

TGIX



# มาตรฐานรัฐบาลดิจิทัลการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange Standard (**TGIX**)  
Series: Linkage Standard



ดร.สุพจน์ เรียมวนะ

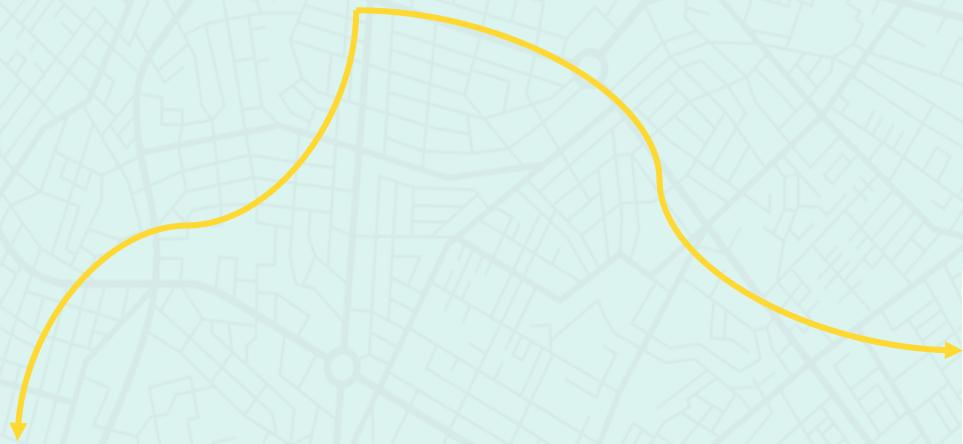
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

# มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ TGIX

มาตรฐานฯ ด้านความหมายข้อมูล

## Semantic Standard

- ข้อมูลบุคคล
- ข้อมูลนิติบุคคล
- ข้อมูลสถานที่
- ข้อมูลสิ่งของ
- อื่นๆ



You are here

## มาตรฐานฯ ด้านการเชื่อมโยงข้อมูล

### Linkage Standard

- สถาปัตยกรรมอ้างอิง
- ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน
- ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทคเคนและเชลชัน
- ข้อกำหนดด้านของความน่าเชื่อถือและความมั่นคงปลอดภัย
- ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก
- ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ

# มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล หนึ่งในกลไกหลักในการขับเคลื่อนรัฐบาลดิจิทัล

## Thailand Government Information Exchange Standard (**TGIX**) Series: Linkage Standard



ดร.สุพจน์ เรียมวนะ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล



ผศ.ดร. ณัฐวุฒิ นาพีวงศ์

อ.ประจำคณบ魏ศวกรรมศาสตร์ วิทยาลัย  
และ ประธานคณะกรรมการเทคโนโลยีด้านมาตรการเชื่อมโยง  
และแลกเปลี่ยนข้อมูลภาครัฐ



ดร.อุรัชญา เกตุพรหม

ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ  
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

# มาตรฐานรัฐบาลดิจิทัลการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange Standard (**TGIX**)  
Series: Linkage Standard



ผศ.ดร. ณัฐวุฒิ หุ่นไฟโรมัน

อ.ประจำคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย  
และ ประธานคณะกรรมการเทคโนโลยีด้านมาตรฐานการ  
เชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ

# มาตรฐานการเชื่อมโยงและ แลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government  
Information Exchange: TGIX  
(Linkage Standard)

## สาระสำคัญ

### TGIX Intra-DX

การเชื่อมโยงและการ  
แลกเปลี่ยนข้อมูลภายในกลุ่ม  
TGIX

### TGIX Inter-DX

การเชื่อมโยงและการ  
แลกเปลี่ยนข้อมูล  
ระหว่างกลุ่ม TGIX

### Federated-DX

การเชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่าง TGIX-Based  
Data Exchange กับ Data  
Exchange อื่นๆ

1

2

3

1

2

3

4

5



# มาตรฐานรัฐบาลดิจิทัลการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange Standard (**TGIX**)  
Series: Linkage Standard



นางสาวเยาวภา วงศ์มาสา

ที่ปรึกษาจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

# มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

1

## Overview

ภาพรวมของมาตรฐาน  
สถาปัตยกรรมการเชื่อมโยง  
และการแลกเปลี่ยนข้อมูล  
ภาครัฐ

2

## TGIX Intra-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภายในกลุ่ม TGIX

3

## TGIX Inter-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่างกลุ่ม TGIX

4

## Federated-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่าง TGIX-Based  
Data Exchange กับ Data  
Exchange อื่นๆ

# มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

1

## Overview

ภาพรวมของมาตรฐาน  
สถาปัตยกรรมการเชื่อมโยง  
และการแลกเปลี่ยนข้อมูล  
ภาครัฐ

2

## TGIX Intra-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภายในกลุ่ม TGIX

3

## TGIX Inter-DX

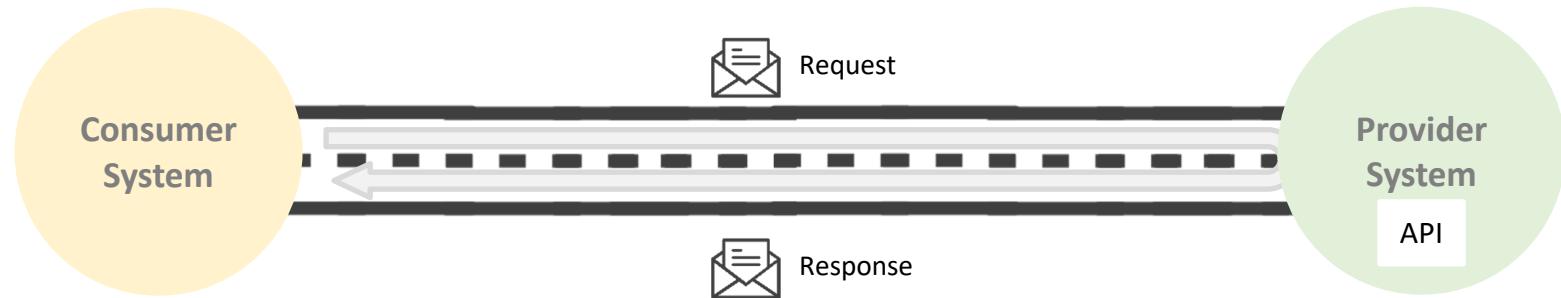
มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่างกลุ่ม TGIX

4

## Federated-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่าง TGIX-Based  
Data Exchange กับ Data  
Exchange อื่นๆ

# มาตรฐานสถาปัตยกรรม เป็นการดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูลผ่านช่องทาง **Application Programming Interface (API)**



## การเชื่อมโยงข้อมูลผ่าน API

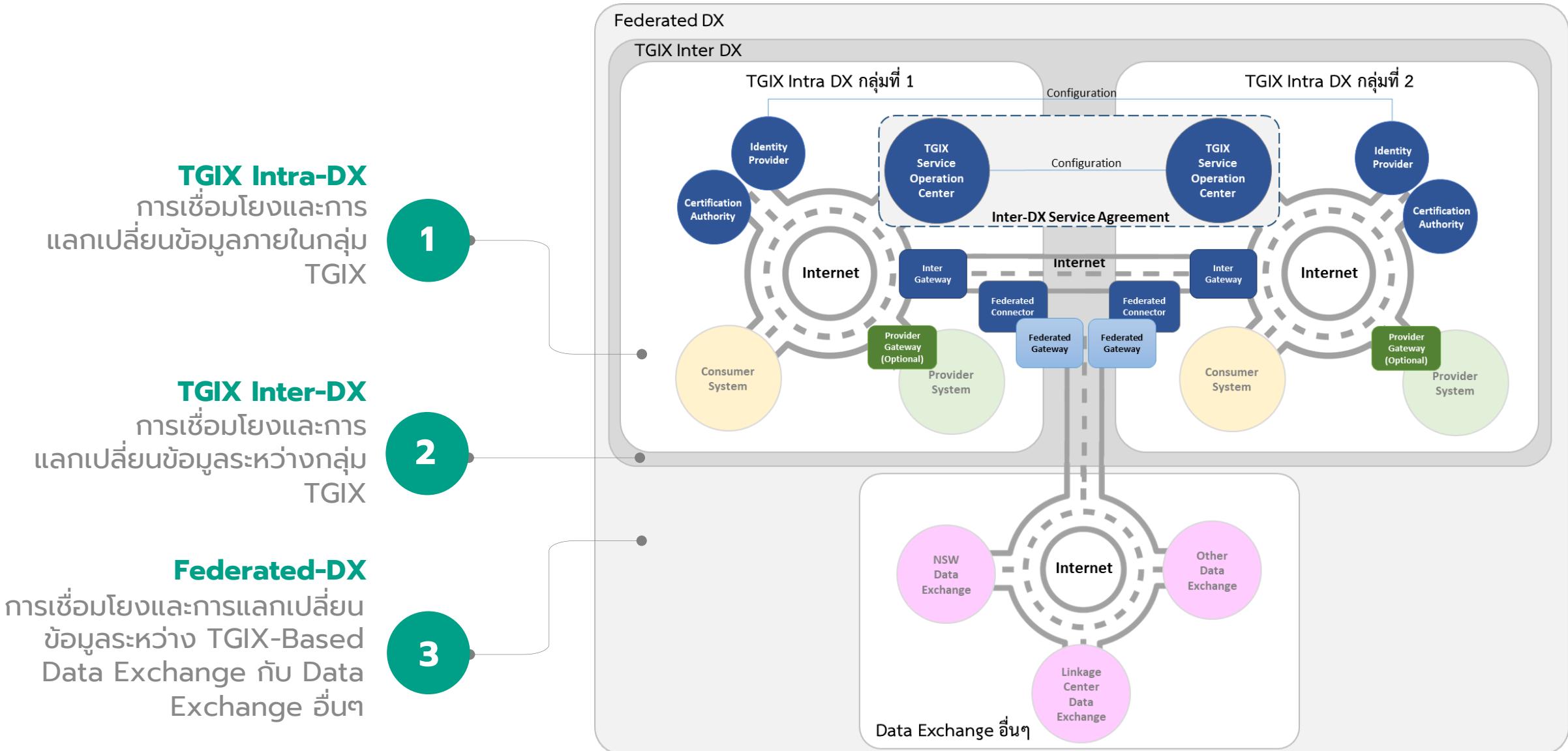
เป็นการดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูลผ่านช่องทาง Application Programming Interface หรือ API ซึ่งสร้างโดยผู้ให้บริการ API (Provider System) หน้าที่หลักของ API คือถ่ายรับคำขอ (Request) จากผู้ใช้บริการ API (Consumer System) เมื่อผู้ใช้บริการ API ส่งคำขอจากนั้น API จะรับคำขอดังกล่าว นำไปประมวลผล และสรุปเป็นข้อมูลที่ตรงกับคำขอ และส่งข้อมูลเหล่านั้นกลับไปที่ผู้ใช้บริการ API หรือเพื่อนำไปใช้งานต่อไป



## แนวคิดการเชื่อมโยงข้อมูล

เป็นขอบเขตมาตรฐานที่ระดับการเชื่อมโยงข้อมูล ซึ่งไม่ได้ครอบคลุมถึงระดับการจัดการข้อมูลทางธุรกิจของหน่วยงาน (Business Transaction Data) ที่เกิดขึ้นจากการเชื่อมโยงและแลกเปลี่ยนระหว่างกัน เปรียบเหมือนกำหนดมาตรฐานการส่งจดหมายโดยที่ไม่แตะต้องเนื้อหาข้อความในจดหมาย

# การรวมสถาปัตยกรรมเพื่อรองรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ 3 รูปแบบ



# มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

1

## Overview

ภาพรวมของมาตรฐาน  
สถาปัตยกรรมดำเนินการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภาครัฐ

2

## TGIX Intra-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภายในกลุ่ม TGIX

3

## TGIX Inter-DX

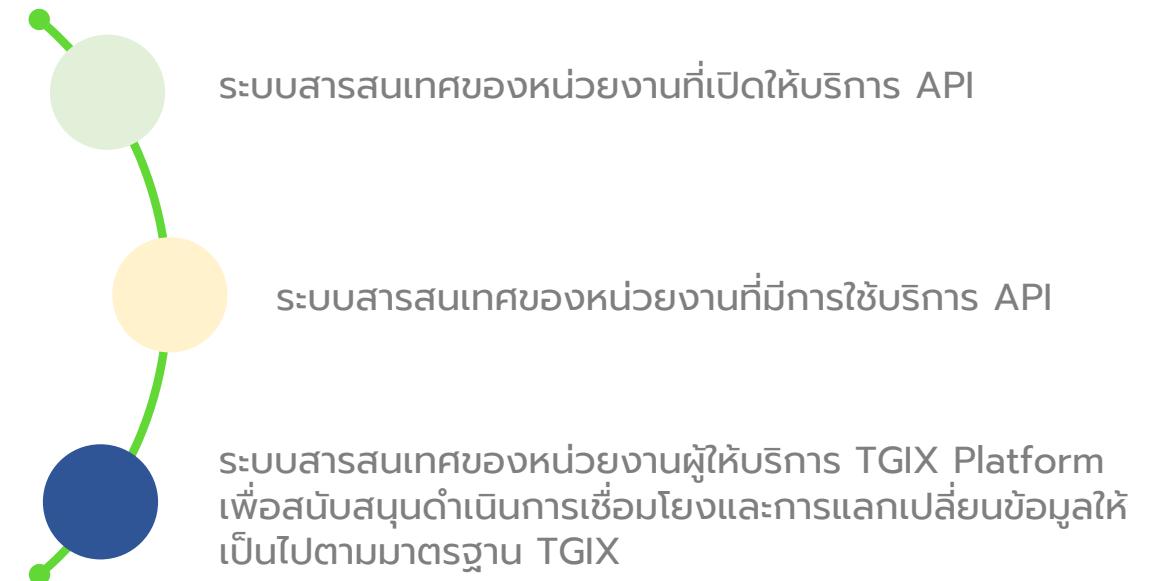
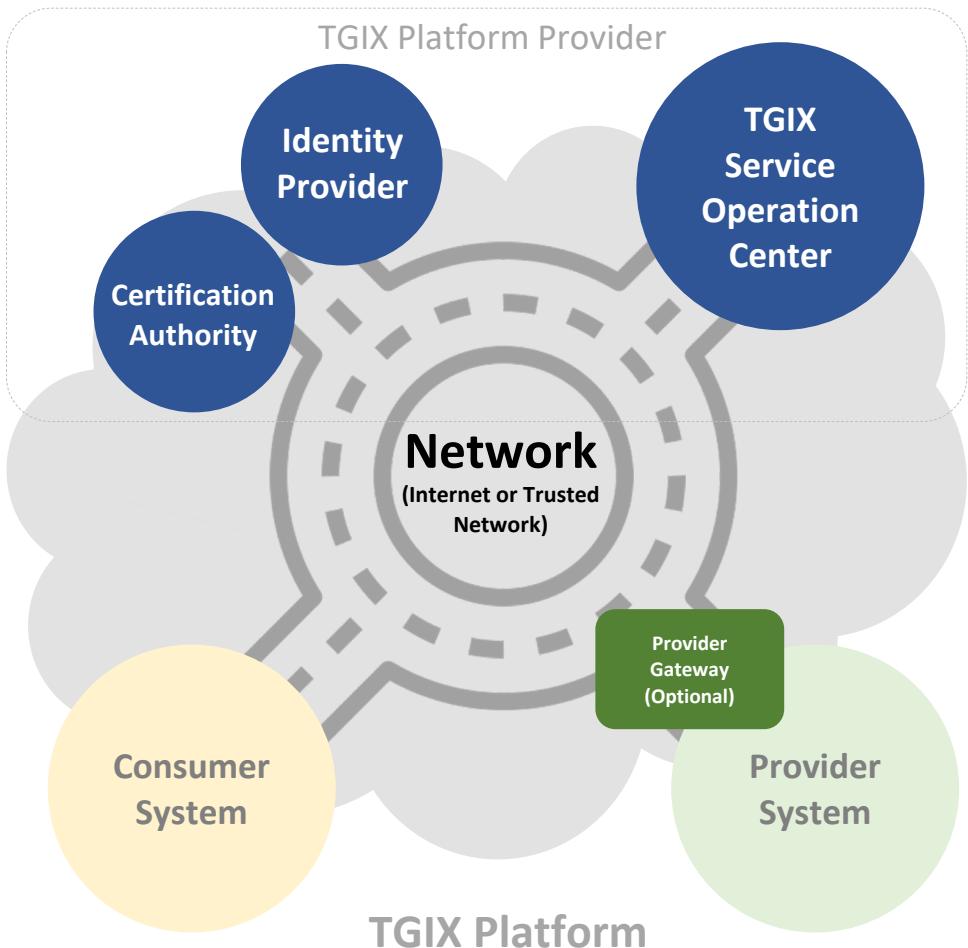
มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่างกลุ่ม TGIX

4

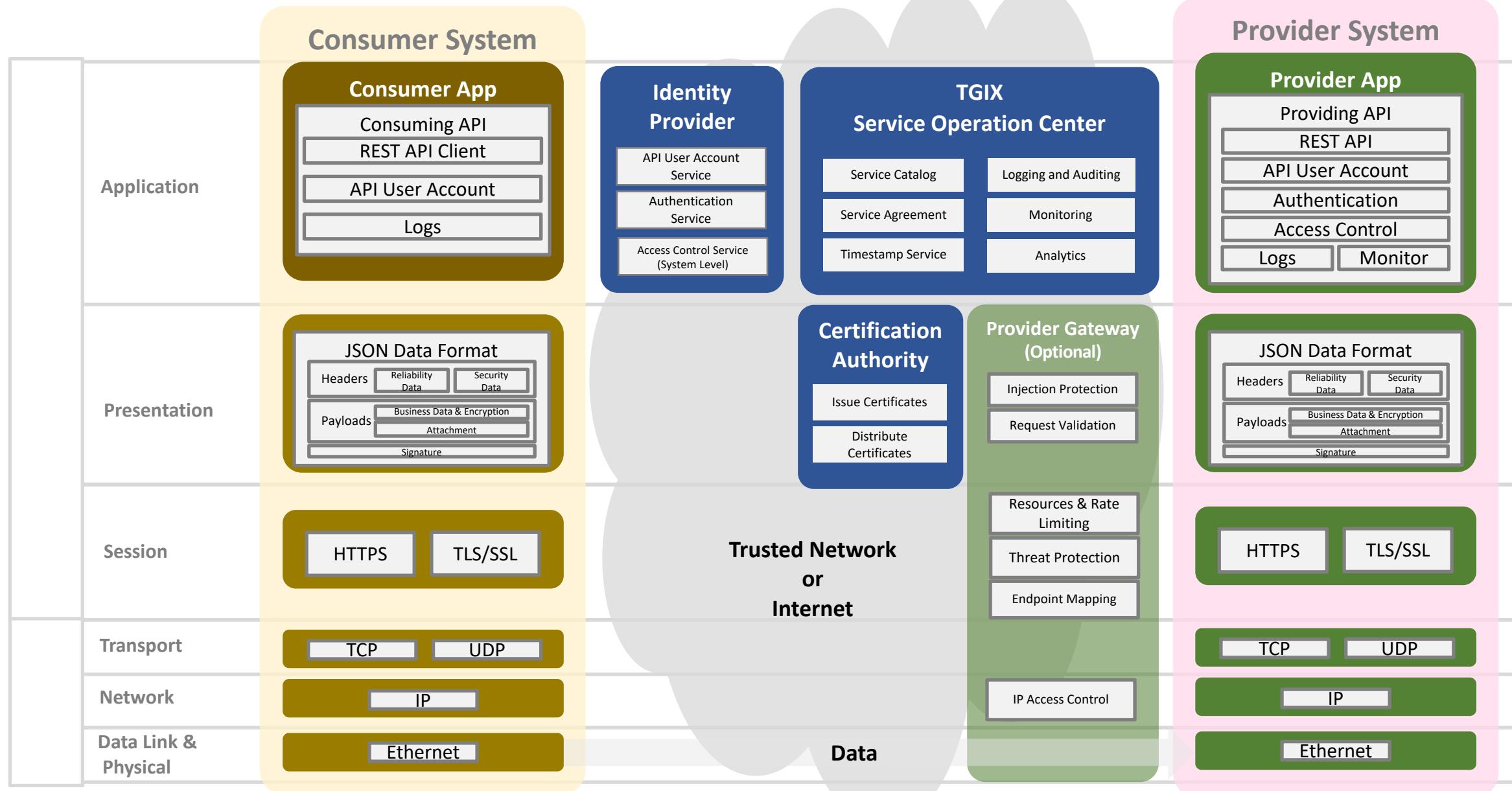
## Federated-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่าง TGIX-Based  
Data Exchange กับ Data  
Exchange อื่นๆ

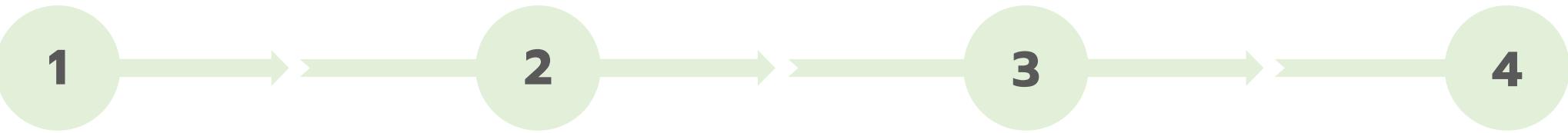
# องค์ประกอบของการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX-based Data Exchange (TGIX Intra-DX)



# รายละเอียดองค์ประกอบของการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX-based Data Exchange (TGIX Intra-DX)



# แนวทางดำเนินการของผู้ให้บริการ API (Provider System)



## พัฒนา REST API

ดำเนินการพัฒนา API ประเภท Representational State Transfer (REST API หรือ RESTful API) ใช้สำหรับเชื่อมโยงและการแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX ด้วยลักษณะโครงสร้าง JavaScript Object Notation (JSON) ของ TGIX JSON Data Format

ผู้ให้บริการสามารถเลือกดำเนินการตามประเภทข้อมูล ได้แก่

- แลกเปลี่ยนข้อมูลเชิงธุรกรรม
  - ข้อมูลเชิงธุรกรรม ที่ Payload เป็น JSON
  - ข้อมูลเชิงธุรกรรม ที่ Payload ไม่ได้เป็น JSON
- แลกเปลี่ยนข้อมูลที่เป็น File
  - File ขนาดไม่เกิน 5 MB
  - File ขนาดใหญ่เกิน 5 MB

## พัฒนา ส่วนประกอบอื่นๆ ของ API

ดำเนินการพัฒนาส่วนประกอบอื่นๆ ของ API ตามเอกสารมาตรฐานดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาคครัว ด้านการเชื่อมโยงข้อมูล เรื่องต่อไปนี้

- ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน
- ข้อกำหนดของโปรโตคอลระดับแอปพลิเคชัน เช่นพ้อยน์ การจัดการโทken และเซสชัน
- ข้อกำหนดของการกำหนดชื่อและเนมสเปช
- ข้อกำหนดของการตรวจสอบระบบและการลงบันทึก็อค
- ข้อกำหนดของความน่าเชื่อถือและความมั่นคง ปลอดภัย

## ลงทะเบียน API

ดำเนินการลงทะเบียน API พร้อมสร้างคู่มือการเรียกใช้งาน API ไว้ที่ Service Catalog ของ TGIX Service Operation Center (SOC) ซึ่งดูแลโดยผู้ให้บริการ TGIX Platform



## จัดการด้านความมั่นคง ปลอดภัยทางไซเบอร์ของ API

ดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ของระบบสารสนเทศผู้ให้บริการ API โดยเฉพาะเกี่ยวกับการป้องกันการโจมตี API แบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS) จากผู้ใช้บริการที่ไม่พึงประสงค์ เช่น

- ดำเนินการป้องกันไม่ให้มีการโจมตี API จากผู้ใช้งานที่ไม่พึงประสงค์ ก่อนที่คำขอ ไปถึงยังระบบสารสนเทศที่ให้บริการ API
- ดำเนินการกำหนดจำนวนคำขอที่จะเรียกใช้ API โดยผู้ใช้บริการ API เพื่อป้องกันการโจมตีจากผู้ใช้บริการที่ไม่พึงประสงค์และลดโหลดของระบบสารสนเทศที่ให้บริการ API

หน่วยงานผู้ให้บริการ API สามารถพิจารณาทำ API Gateway เข้ามาช่วยดำเนินการในข้อนี้ได้ หรือสามารถร่วมมือกับหน่วยงานผู้ให้บริการ TGIX Platform ใน การช่วยดำเนินการตามข้อกำหนด

# แนวทางดำเนินการของผู้ให้บริการ API (Provider System) (ต่อ)



รายละเอียดเพิ่มเติม  
ของการพัฒนา  
REST API

## TGIX JSON Data Format ឧរោកទី 1

เป็น Content Type ประเภท JSON កំង Message ដែលងាយស្រួលប្រើប្រាស់

```
1 // =====
2 // Request Header
3 // =====
4 [POST, GET, DELETE, PUT, OPTIONS, PATCH] https://oneweb.tgix.com/api/v1/sendmessage HTTP/1.1
5 Authorization: Bearer [YOUR_AUTH_TOKEN]
6 Accept-Encoding: [Accept Encoding]
7 Accept-Language: [Language]
8 Accept: [Mime Type]
9 Host: [Domain Name]
10 Cache-Control: no-cache
11 Connection: keep-alive
12 Content-Type: application/json; charset=UTF-8
13 Content-Length: [Number of bytes in entire request body]
14 Origin: [URL: Domain name]
15
16 // =====
17 // Message: TGIX-Object
18 // =====
19
20
21
22 {
23     "TGIXHeader": {
24         "messageVersion": "", //Require: Message specification version: V1.0
25         "MessageId": "", //Require: Generated for each message using UUID V1
26         "Timestamp": "", //Require: Time stamp was from source system: UTC format: 2021-09-28T08:10:12.44+07:00.
27         "clientId": "", //Require: Reference to unique client
28         "event": "", //Require: Description for explain action
29         "expirationTime": "", //Optional: When the message should expire: millisecond
30         "apiKey": "", //Optional: key for access API
31         "RequestId": "", //Optional: Assigned by the request client, and automatically copied by the Respond methods to correlate responses to the original request.
32         "Headers": "", //Optional: Additional headers, which can be added by the user, middleware, or diagnostic trace filters.
33         "ConversationId": "", //Optional: Assigned when a set of messages is sent or published and no consumed message is available, ensuring that a set of messages within the same conversation have the same identifier.
34         "attachments": { //Optional: only case attach file or XML message
35             "mimeType": "", //Require: Mimetype of media
36             "contentId": "", //Require: reference to part content data
37             "name": "", //Require: name of media
38             "referenceId": "", //Require: reference from source system
39             "description": "", //Optional: Information of media
40             "sequence": "" //Optional: Sequence or Order of media
41         },
42         "messageStatus": // Require: only response message.
43         {
44             "status": "", // Require: (HTTP status: 200,401,... other code)
45             "description": "", // Require: Description or information for status
46             "error": { // Require: only provider return error
47                 "code": "", // Require: Reference error code
48                 "message": "" // Require: Error message
49             }
50         }
51     },
52     "TGIXPayload": { // Message payload
53         // =====
54     },
55     "TGIXSignature": { // Signature
56         "alg": "RS256", //Require: Algorithm
57         "cert": "<>public key of signer Alice<>", //Require: Public key "Alice"
58         "sigValue": "<>signature Alice<>" //Require: Signing value from "Alice"
59     }
60 }
61 // =====
62 }
```

TGIX Message Header

TGIX Message Payload

TGIX Message Signature

HTTP Header

HTTP Body

# แนวการดำเนินการของผู้ให้บริการ API (Provider System) (ต่อ)

## TGIX JSON Data Format ประเภทที่ 2

โดย Default เป็น Content Type ประเภท JSON แต่ผู้ใช้งานสามารถเลือกเปลี่ยนเป็น Multipart ได้ เพื่อรองรับ XML Message หรือการแนบ File ขนาดไม่เกิน 5 MB

รายละเอียดเพิ่มเติม  
ของการพัฒนา  
REST API

TGIX Message Header

TGIX Message Payload

TGIX Message Signature

```
1 // Request Header
2 // =====
3 // [POST, GET, DELETE, PUT, OPTIONS, PATCH] https://oneweb.tgix.com/api/v1/sendmessage HTTP/1.1
4 Authorization: Bearer [YOUR_AUTH_TOKEN]
5 Accept-Encoding: [Accept Type]
6 Accept-Language: [Language]
7 Accept: [Mime Type]
8 Host: [Domain Name]
9 Cache-Control: no-cache
10 Connection: keep-alive
11 Content-Type: [ application/json; charset=UTF-8 or
12           multipart/related; boundary=tgix_message ] //Default: Standard message
13           //Exception case: Attach file and Support XML message
14 Content-Length: [Number of bytes in entire request body]
15 Origin: [URL: Domain name]
16
17
18 // Message: TGIX-Object
19 // =====
20 {
21
22   "TGIXHeader": {
23     "messageVersion": "", //Require: Message specification version: V1.0
24     " messageId": "", //Require: Generated for each message using UUID V1
25     "timestamp": "", //Require: When the message was sent from source system: UTC format: 2021-09-28T08:10:12.44+07:00.
26     "clientId": "", //Require: Reference to unique client
27     "event": "", //Require: Description for explain action
28     "expirationTime": "", //Optional: When the message should expire: millisecond
29     "apiKey": "", //Optional: Key for access API
30     "requestId": "", //Optional: Assigned by the request client, and automatically copied by the Respond methods to correlate responses to the original request.
31     "Headers": "", //Optional: Additional headers, which can be added by the user, middleware, or diagnostic trace filters.
32     "ConversationId": "", //Optional: Assigned when the first message is sent or published and no consumed message is available
33     // ensuring that a set of messages within the same conversation have the same identifier.
34     "Attachments": [
35       {
36         "mimeType": "", //Require:MimeType of media
37         "contentId": "", //Require: reference to part content data
38         "name": "", //Require: name of media
39         "referenceId": "", //Require: reference id from source system
40         "description": "", //Optional: Information of media
41         "sequence": "" //Optional: Sequence or Order of media
42       }
43     ],
44     "messageStatus": { // Require: only response message.
45       "status": "", // Require: [HTTP status: 200,401,...other code]
46       "description": "", // Require: Description or information for status
47       "error": { // Require: only provider return error
48         "code": "", // Require: Reference error code
49         "message": "" // Require: Error message
50       }
51     }
52   },
53   "TGIXPayload": { // =====
54     // Message payload
55     // =====
56   },
57   "TGIXSignature": { // =====
58     "alg": "RS256", //Require: Algorithm
59     "cert": "<>public key of signer Alice><>", //Require: Public key "Alice"
60     "sigValue": "<>signature Alice><>" //Require: Signing value from "Alice"
61   }
62 }
63
64
65
66
67
68 }
```

HTTP Header

HTTP Body

# แนวการดำเนินการของผู้ให้บริการ API (Provider System) (ต่อ)

## TGIX JSON Data Format ประเภทที่ 3

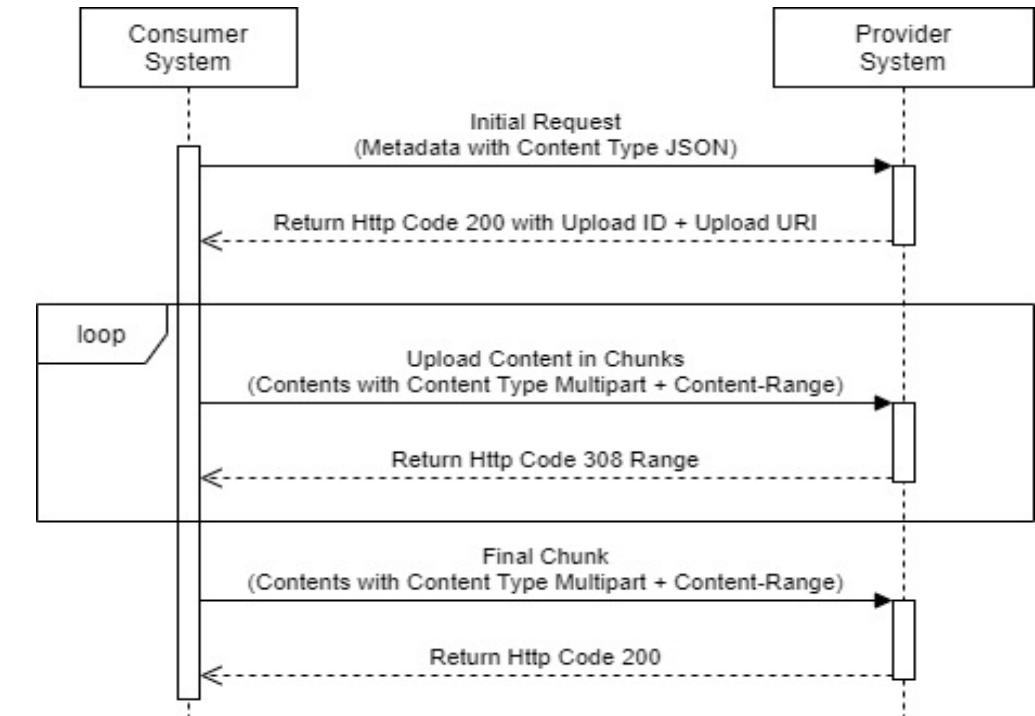
รองรับ File ขนาดใหญ่เป็นการผสมผสานระหว่าง TGIX JSON Data Format ประเภทที่ 1 และ ประเภทที่ 2 เข้าด้วยกัน

รายละเอียดเพิ่มเติม  
ของ การพัฒนา  
REST API

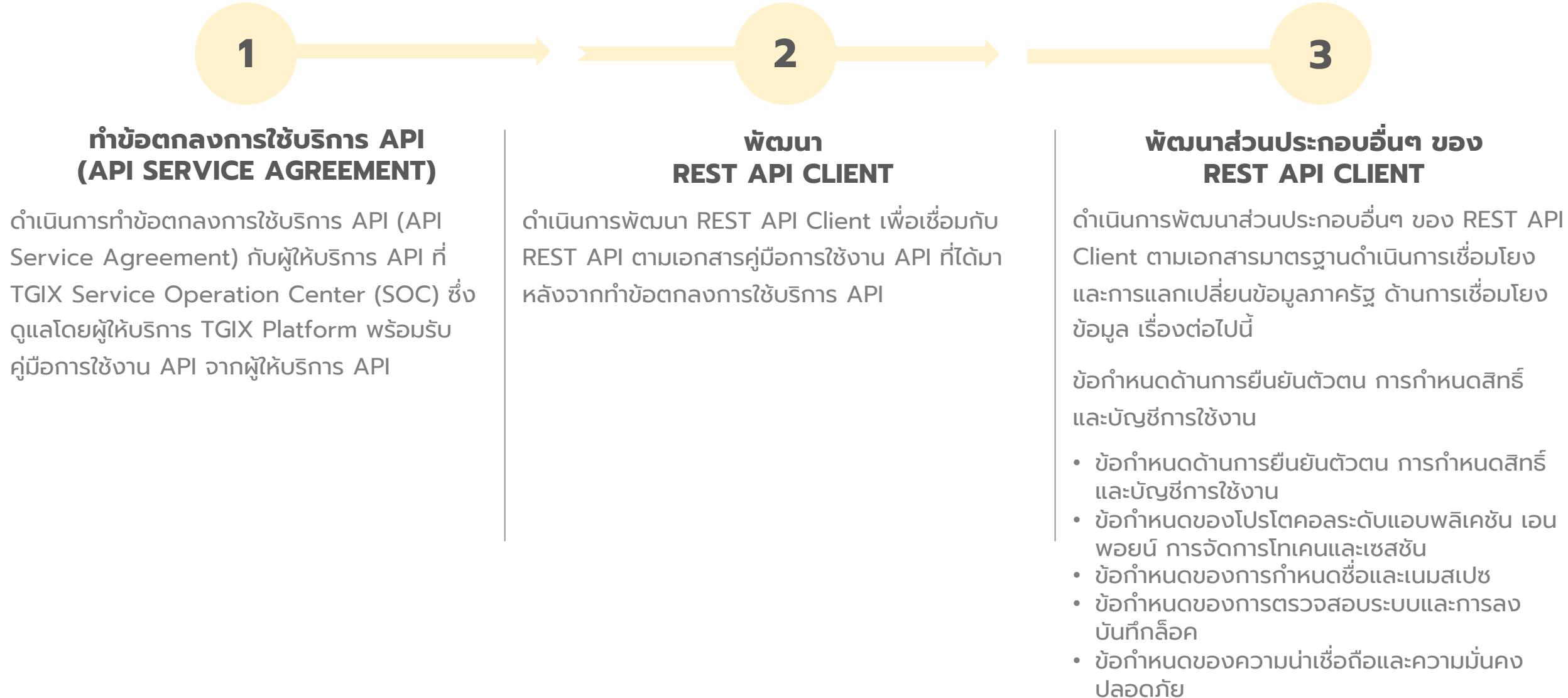
### การทำงานคือ

1. Consumer System ส่ง Request ไปแจ้งว่าจะมีการ Upload File พร้อมแจ้งขนาดและจำนวน Chunk กี่จังหวะ แล้ว Provider ส่ง Upload ID และ URI กลับ
2. Consumer System แบ่ง File ออกเป็น Chunk ย่อยๆ แล้วทยอย Upload ทีละ File จนสำเร็จ
3. ถ้ามี Chunk ใดมีปัญหาสามารถเลือกให้มีการ Resume ได้

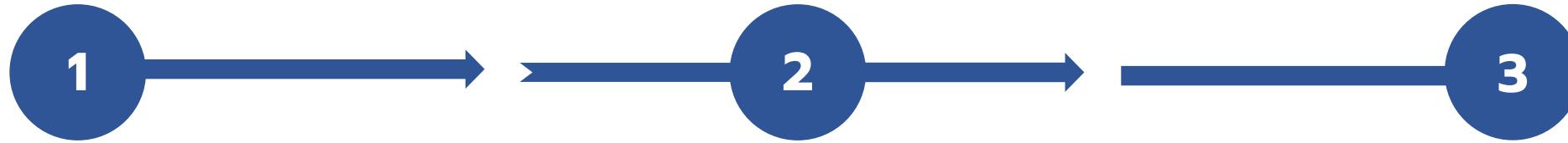
```
PATCH /document HTTP/1.1
Content-Type: multipart/byteranges; boundary=THIS_STRING_SEPARATES
--THIS_STRING_SEPARATES
Content-Type: text/plain
Content-Range: bytes 10-21/22
1234567890
--THIS_STRING_SEPARATES--
```



# แนวการดำเนินการของผู้ใช้บริการ API (Consumer System)



# แนวทางดำเนินการของผู้ให้บริการ TGIX Platform (TGIX Platform Provider)



## ดำเนินการให้มีบริการพิสูจน์และยืนยันตัวตน (IDENTITY PROVIDER: IDP)

- บริการกำหนดบัญชีรายชื่อผู้ใช้งาน (API User Account Service)
- บริการยืนยันตัวตนผู้ใช้บริการ API (Authentication Service) รองรับมาตรฐาน OAuth 2.0 หรือ Open ID Connect
- บริการตรวจสอบสิทธิ์ของผู้ใช้บริการ API เพื่อบุคลากรให้เข้าถึง API (Access Control Service (System Level)) รองรับมาตรฐาน OAuth 2.0 หรือ Open ID Connect

## ดำเนินการให้มีศูนย์ปฏิบัติดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูล (SERVICE OPERATION CENTER: SOC)

- บริการรายชื่อของ API (Service Catalog) สำหรับแลกเปลี่ยนข้อมูลที่พร้อมใช้งานภายใต้แพลตฟอร์ม
- บริการจัดทำข้อตกลง (Service Agreement) หรือสัญญา (Service Contract) ระหว่างผู้ให้บริการ (Provider) และผู้ใช้บริการ (Consumer) ซึ่งประกอบด้วยเอกสารต่างๆ ที่เกี่ยวกับการใช้งาน API ที่ผู้ใช้บริการสามารถนำไปพัฒนาเป็น API Client ได้
- บริการเชื่อมต่อ กับ Time Stamping Authority (TSA) (Timestamp Service) เพื่อใช้ประทับรองเวลาอิเล็กทรอนิกส์ ใช้ในการลงลายมือชื่อดิจิตอล (Digital Signature) รวมทั้งเพื่อสร้างความเชื่อมั่นและรับรองในเวลาในการเชื่อมโยงและแลกเปลี่ยน
- บริการจัดเก็บ Log (Logging and Auditing) ที่เกิดจากดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูลของกลุ่ม
- บริการตรวจสอบและวิเคราะห์ผลการตรวจสอบระบบ (Monitoring and Analytics)

## ดำเนินการให้มีบริการออกใบรับรอง (CERTIFICATION AUTHORITY: CA)

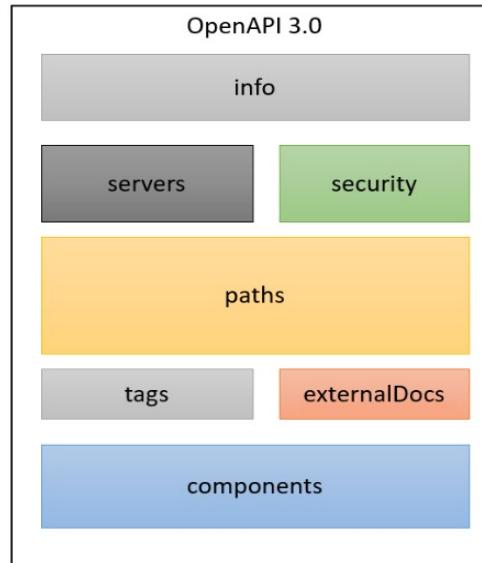
- บริการออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เป็นบริการออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ให้แก่สมาชิกในกลุ่ม TGIX เพื่อ
  - ใช้ในการลงลายมือชื่อดิจิตอล (Digital Signature) หรือ การเข้ารหัส (Encryption) และ
  - ใช้เป็น Server Certificate (SSL) หรือ ใบรับรอง อิเล็กทรอนิกส์สำหรับเครื่อง Server เพื่อให้สามารถใช้งานการเชื่อมต่อได้อย่างปลอดภัย
- บริการส่งใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อ ส่งใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ส่งให้แก่ สมาชิกในกลุ่มแบบอัตโนมัติหรือส่งผ่านช่องทางอื่นๆ ตามที่ตกลงกัน

## แนวการดำเนินการของ

# ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) (ต่อ)

รายละเอียดเพิ่มเติมของบริการจัดทำข้อตกลง (SERVICE AGREEMENT) ใน SOC

ตัวอย่างข้อตกลงการบริการจาก SwaggerHub ที่ใช้มาตรฐาน OpenAPI Specification Version 3.0 (OAS 3.0)



The screenshot shows the "Audit Service" API documentation on SwaggerHub. The top header includes the service name, version (1.0.0), and OAS3 compliance.

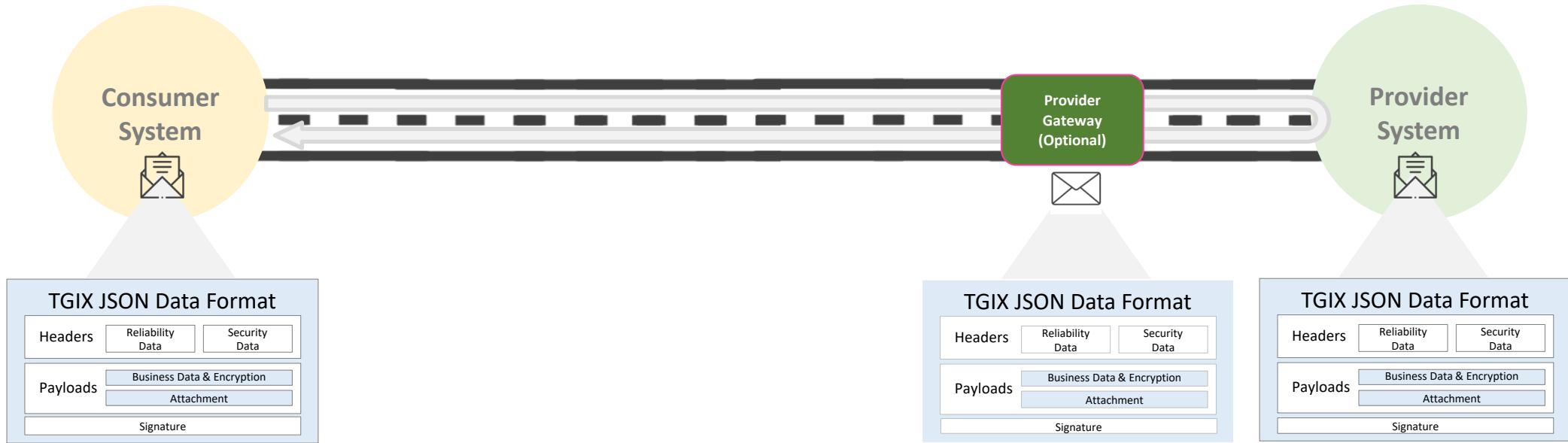
The main content area displays the API structure:

- authentication**: Token calls
- organization**: Secured Organization calls
- user**: Secured User calls
- role**: Secured Role calls
- health-check**: Checks server health

Below the API structure is a green button labeled "Authorize" with a lock icon. To the right of the API sections are collapse/expand arrows (^ and v). At the bottom right is a lock icon.

At the very bottom of the screenshot, there is a green bar containing the text "POST /health-check checks server health".

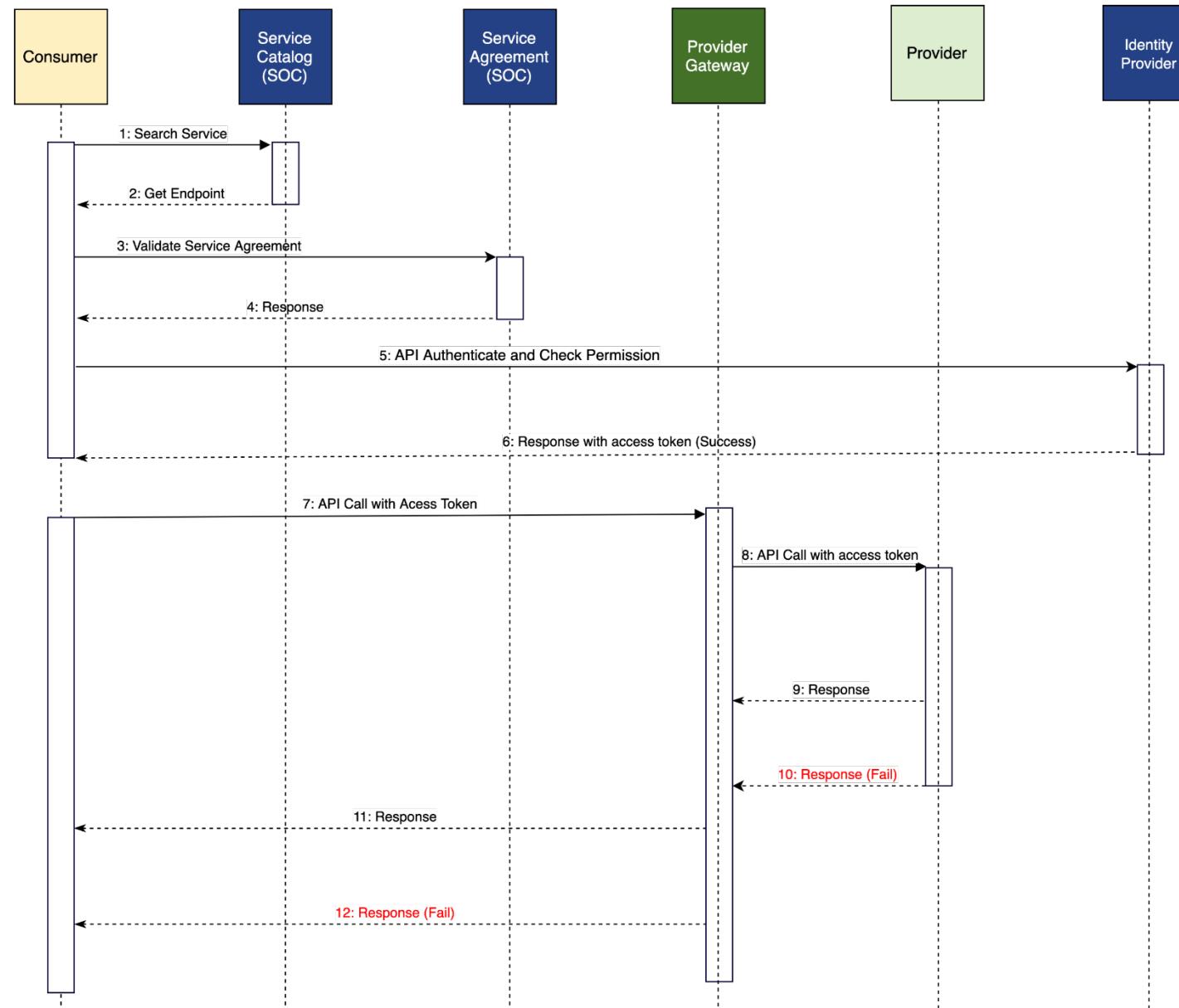
# ลักษณะ Data Format ในการแลกเปลี่ยนข้อมูลภายในบุคลุ่ม TGIX-based Data Exchange



“ใช้ลักษณะ Data Format เป็น TGIX JSON Data Format เดียวกัน  
ทั้ง Provider System และ Consumer System”

# ขั้นตอนการทำงานในกลุ่ม

## TGIX-based Data Exchange



# มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

1

## Overview

ภาพรวมของมาตรฐาน  
สถาปัตยกรรมดำเนินการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภาครัฐ

2

## TGIX Intra-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภายในกลุ่ม TGIX

3

## TGIX Inter-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่างกลุ่ม TGIX

4

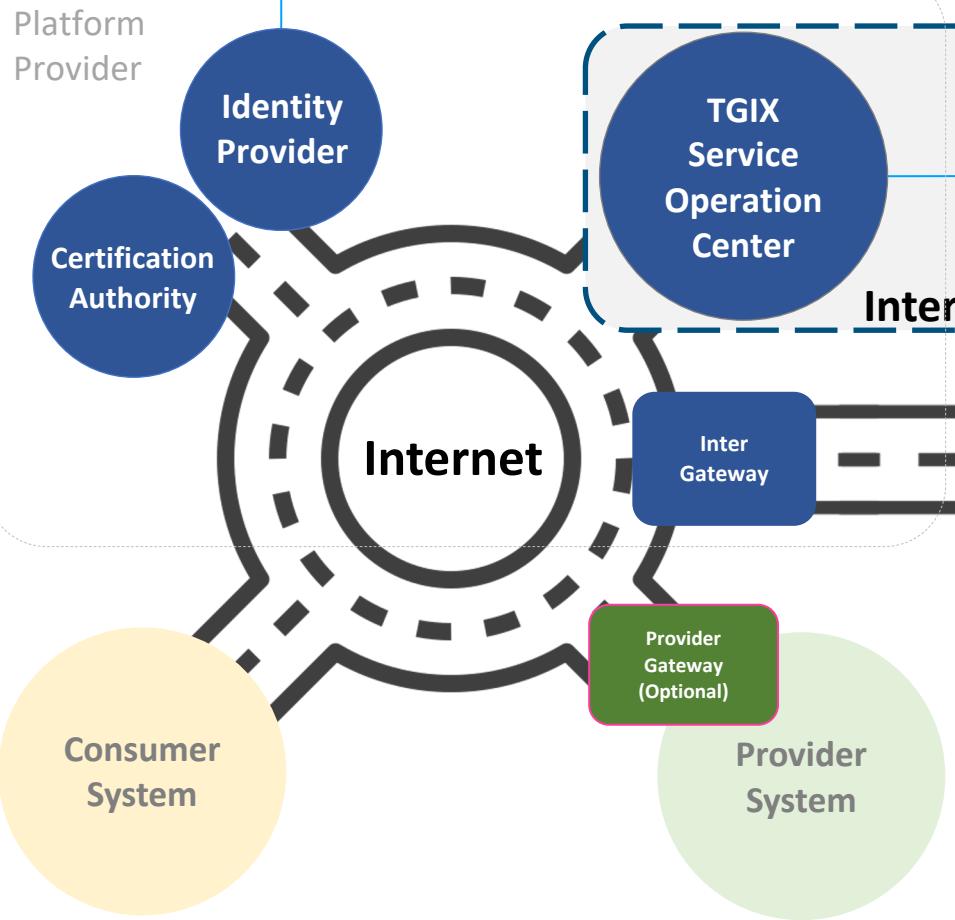
## Federated-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่าง TGIX-Based  
Data Exchange กับ Data  
Exchange อื่นๆ

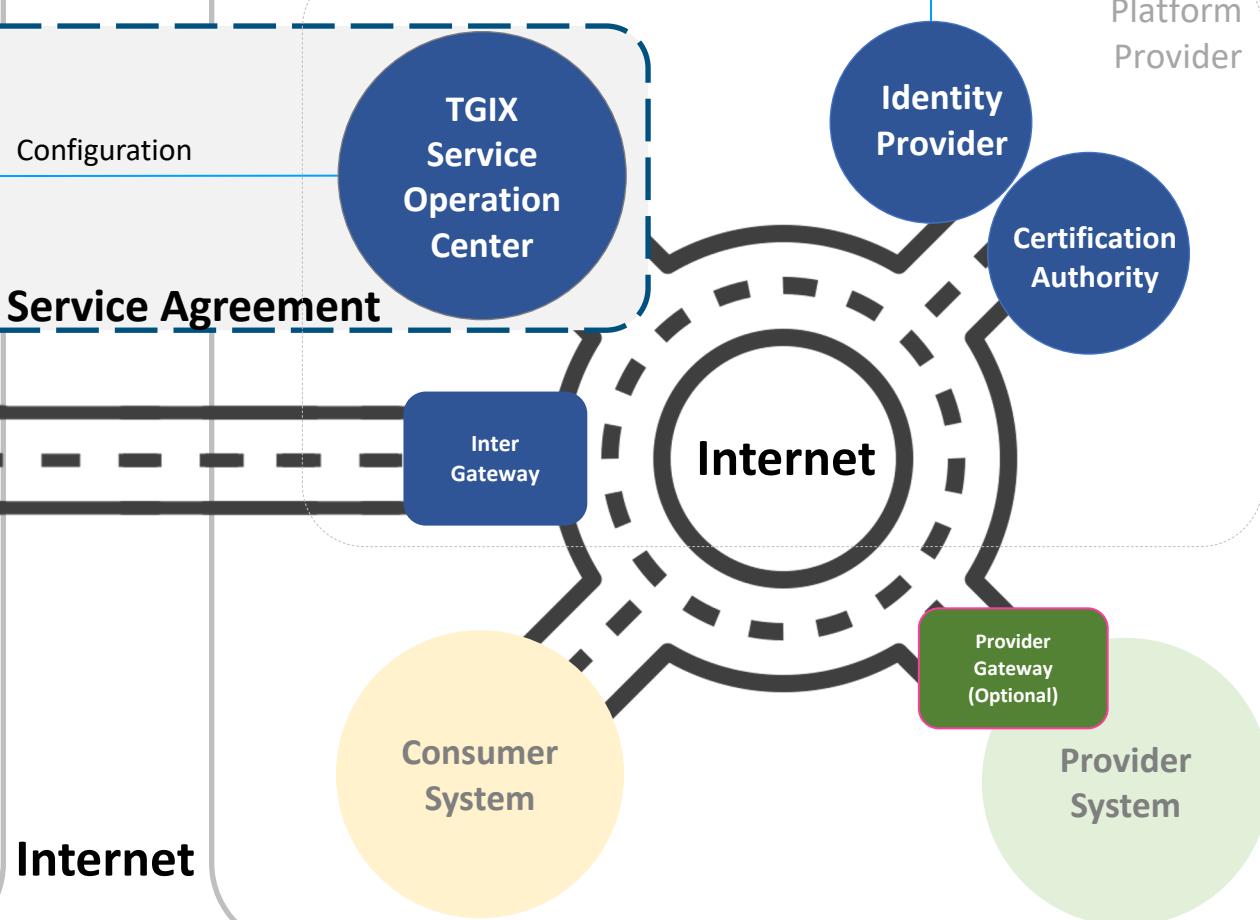
ອົນຄປະກອບຂອງການແລກປ່ຽນຂ້ອມູລະຫວ່າງກລຸມ

## TGIX-based Data Exchange (TGIX Inter-DX)

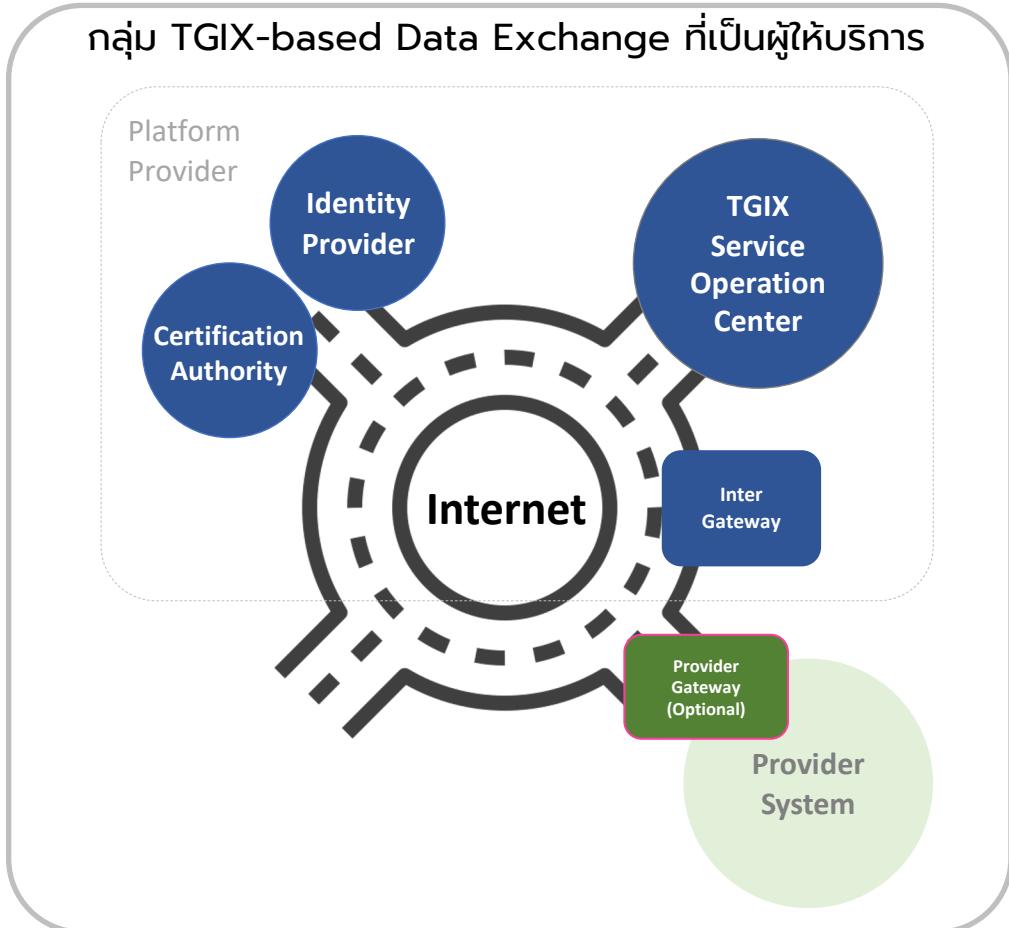
TGIX-based Data Exchange 1



TGIX-based Data Exchange 2



# แนวทางดำเนินการของกลุ่ม TGIX-based Data Exchange ที่เป็นผู้ให้บริการ API



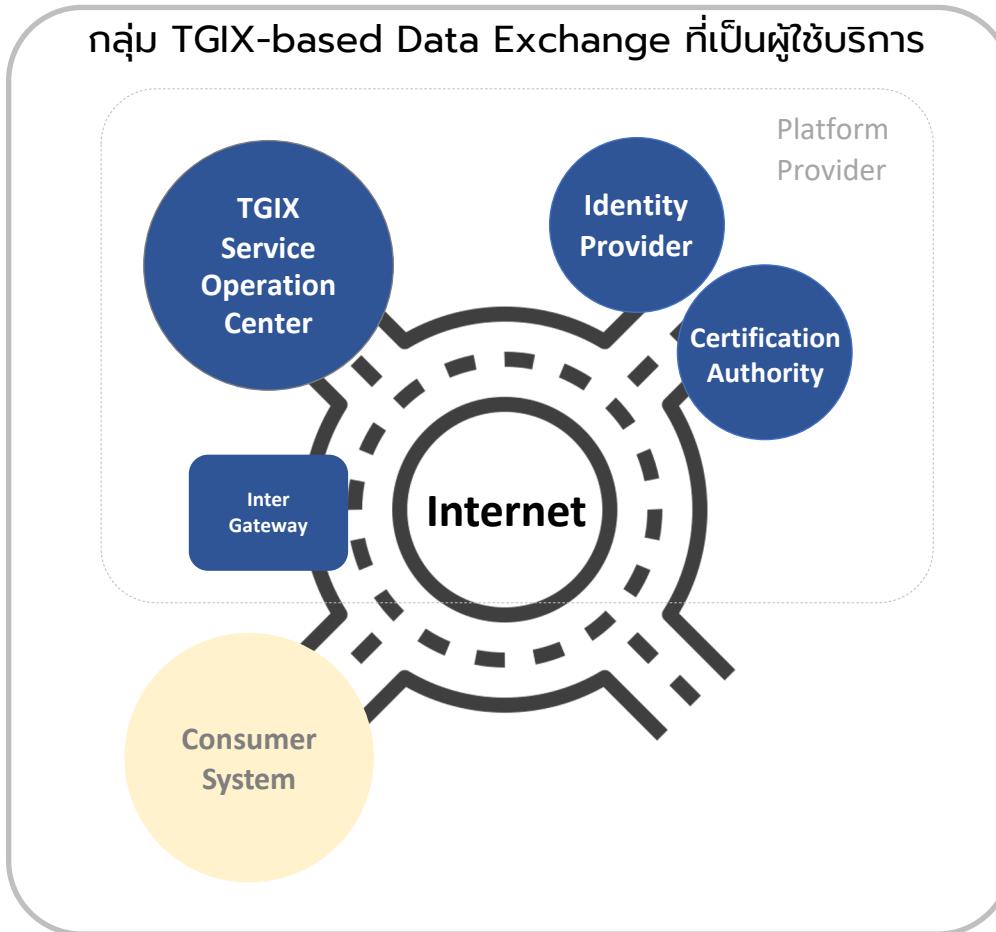
## แนวทางดำเนินการของผู้ให้บริการ TGIX Platform

- 1 มีบริการขั้นพื้นฐาน  
มีบริการขั้นพื้นฐานเหมือนเช่น TGIX Intra-DX
- 2 มีบริการยืนยันตัวตน  
สำหรับการเชื่อมโยงและ  
แลกเปลี่ยนข้อมูลระหว่าง  
กลุ่ม
  - กรณีที่ยืนยันตัวตนระดับกลุ่มให้หน้าที่การตรวจสอบ Access Token ที่ได้จากการยืนยันตัวตนที่ Identity Provider ของกลุ่มผู้ใช้บริการ เป็นหน้าที่ของ Inter Gateway
  - กรณีที่ยืนยันตัวตนที่ระดับรายบุคคลของระบบผู้ใช้บริการ ควรพิจารณาเพิ่มศักยภาพของ Identity Provider ให้รองรับการยืนยันตัวตนจากผู้ใช้งานทั้ง 2 กลุ่ม ในลักษณะ Federated Identity Provider
- 3 มีบริการป้องกันการโจมตี  
API จากผู้ที่ไม่พึงประสงค์  
จากภายนอกกลุ่ม  
(บริการ INTER API  
GATEWAY หรือเทียบเท่า)
  - การตรวจสอบ Access Token ที่ได้จากการยืนยันตัวตนที่ Identity Provider ของกลุ่มผู้ใช้บริการ
  - ป้องกันการโจมตี API จากผู้ที่ไม่พึงประสงค์จากภายนอกกลุ่ม

## แนวทางดำเนินการของผู้ให้บริการ API (Provider System)

- 1 พัฒนา API  
ดำเนินการพัฒนา API ตาม  
ขั้นตอนของ TGIX Intra-DX
- 2 ลงทะเบียน API  
ดำเนินการลงทะเบียน API พร้อมกับ  
อนุญาตให้สามารถเรียกใช้งานจาก  
กลุ่ม TGIX-based Data  
Exchange ที่เป็นผู้ใช้บริการ API  
พร้อมกับสร้างคู่มือการเรียกใช้งาน  
API ไว้ที่ Service Catalog ของ  
TGIX Service Operation  
Center (SOC) ซึ่งถูกโดยผู้  
ให้บริการ TGIX Platform
- 3 กำหนดกล่องบริการ  
ระหว่างกลุ่ม  
ดำเนินการกำหนดกล่องบริการระหว่าง  
กลุ่ม TGIX (Inter-DX Service  
Agreement) กับกลุ่ม TGIX-  
based Data Exchange ที่เป็น  
ผู้ใช้บริการ API

# แนวทางดำเนินการของกลุ่ม TGIX-based Data Exchange ที่เป็นผู้ใช้บริการ API



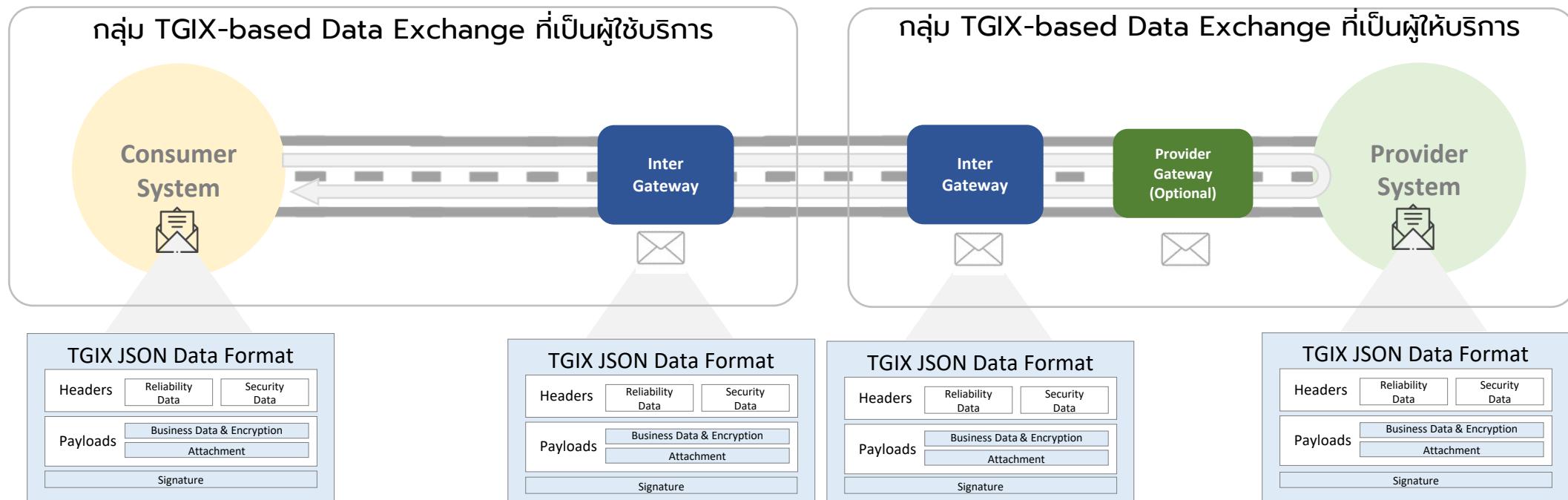
## แนวทางดำเนินการของผู้ให้บริการ TGIX Platform

- 1 มีบริการขั้นพื้นฐาน  
มีบริการขั้นพื้นฐานเหมือนเช่น TGIX Intra-DX
- 2 มีบริการยืนยันตัวตน  
สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกลุ่ม
  - กรณีที่ยืนยันตัวตนที่ระดับรายบุคคลของระบบผู้ใช้บริการ ควรพิจารณาเพิ่มศักยภาพของ Identity Provider ให้รองรับ การยืนยันตัวตนจากผู้ใช้งานทั้ง 2 กลุ่ม ในลักษณะ Federated Identity Provider
- 3 มีบริการป้องกันการโจมตี API จากผู้ที่ไม่พึงประสงค์  
จากภัยนอกรุ่ม
  - (บริการ INTER API GATEWAY หรือเทียบเท่า)
    - ดำเนินการ Map Endpoint ของผู้ให้บริการ API ให้ผู้ใช้บริการ API เรียกใช้งาน
    - ดำเนินการอุปกรณ์ให้เฉพาะบางผู้ใช้บริการ API หรือ เอพะ: IP Address หรือ Domain เท่านั้นที่เรียกใช้ API ได้
    - ดำเนินการป้องกันไม่ให้มีการโจมตี API จากผู้ใช้งานที่ไม่พึงประสงค์ ก่อนที่คำขอ ไปถึงชั้น ระบบสารสนเทศที่อยู่ในกลุ่ม

## แนวทางดำเนินการของผู้ใช้บริการ API (Consumer System)

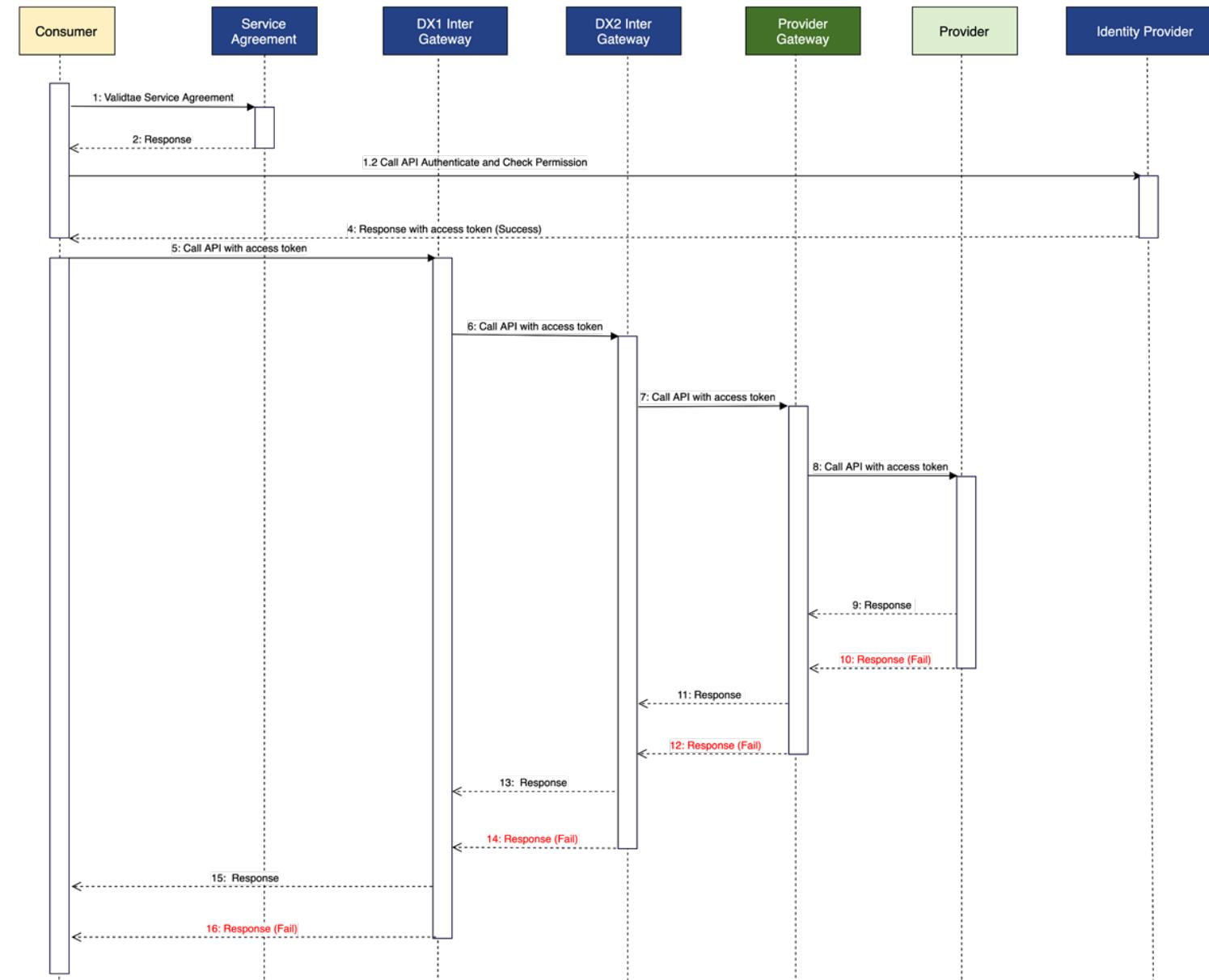
- 1 ทำข้อตกลงบริการ  
ระหว่างกลุ่ม TGIX
  - ดำเนินการทำข้อตกลงบริการระหว่างกลุ่ม TGIX (Inter-DX Service Agreement) กับกลุ่ม TGIX-based Data Exchange ที่เป็นผู้ให้บริการ API พร้อมกับรับคู่มือการใช้งาน API
- 2 พัฒนา API CLIENT
  - ดำเนินการพัฒนา API Client ตามขั้นตอนเหมือน TGIX Intra-DX

# ลักษณะ Data Format ในการแลกเปลี่ยนข้อมูลระหว่างกลุ่ม TGIX-based Data Exchange (TGIX Inter-DX)



“ใช้ลักษณะ Data Format เป็น TGIX JSON Data Format เดียวกันกับ 2 กลุ่ม”

# ขั้นตอนการทำงานระหว่างกลุ่ม TGIX-based Data Exchange



# มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

1

## Overview

ภาพรวมของมาตรฐาน  
สถาปัตยกรรมดำเนินการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภาครัฐ

2

## TGIX Intra-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลภายในกลุ่ม TGIX

3

## TGIX Inter-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่างกลุ่ม TGIX

4

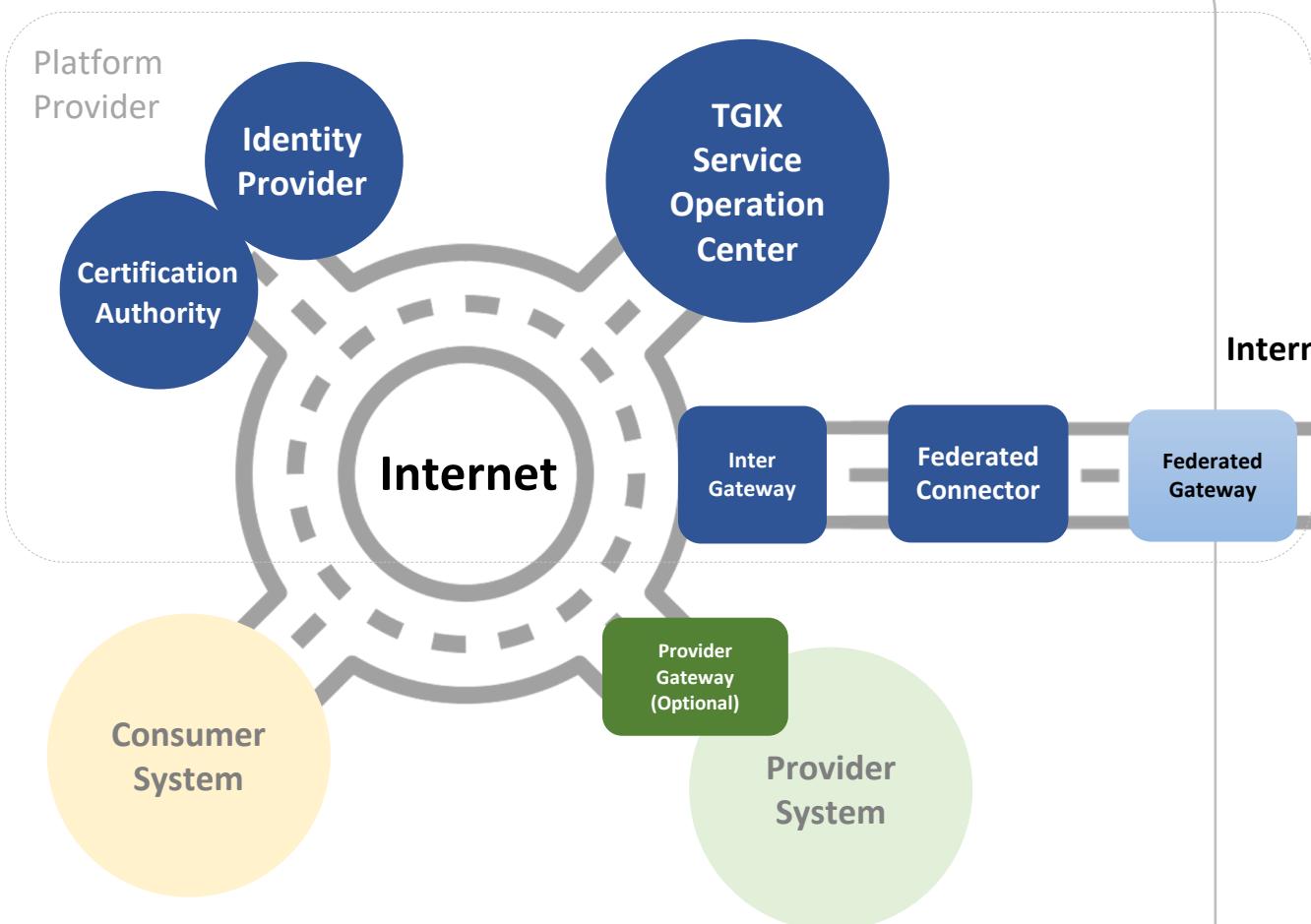
## Federated-DX

มาตรฐานสถาปัตยกรรมการ  
เชื่อมโยงและการแลกเปลี่ยน  
ข้อมูลระหว่าง TGIX-Based  
Data Exchange กับ Data  
Exchange อื่นๆ

# องค์ประกอบของการแลกเปลี่ยนข้อมูลระหว่างกลุ่ม

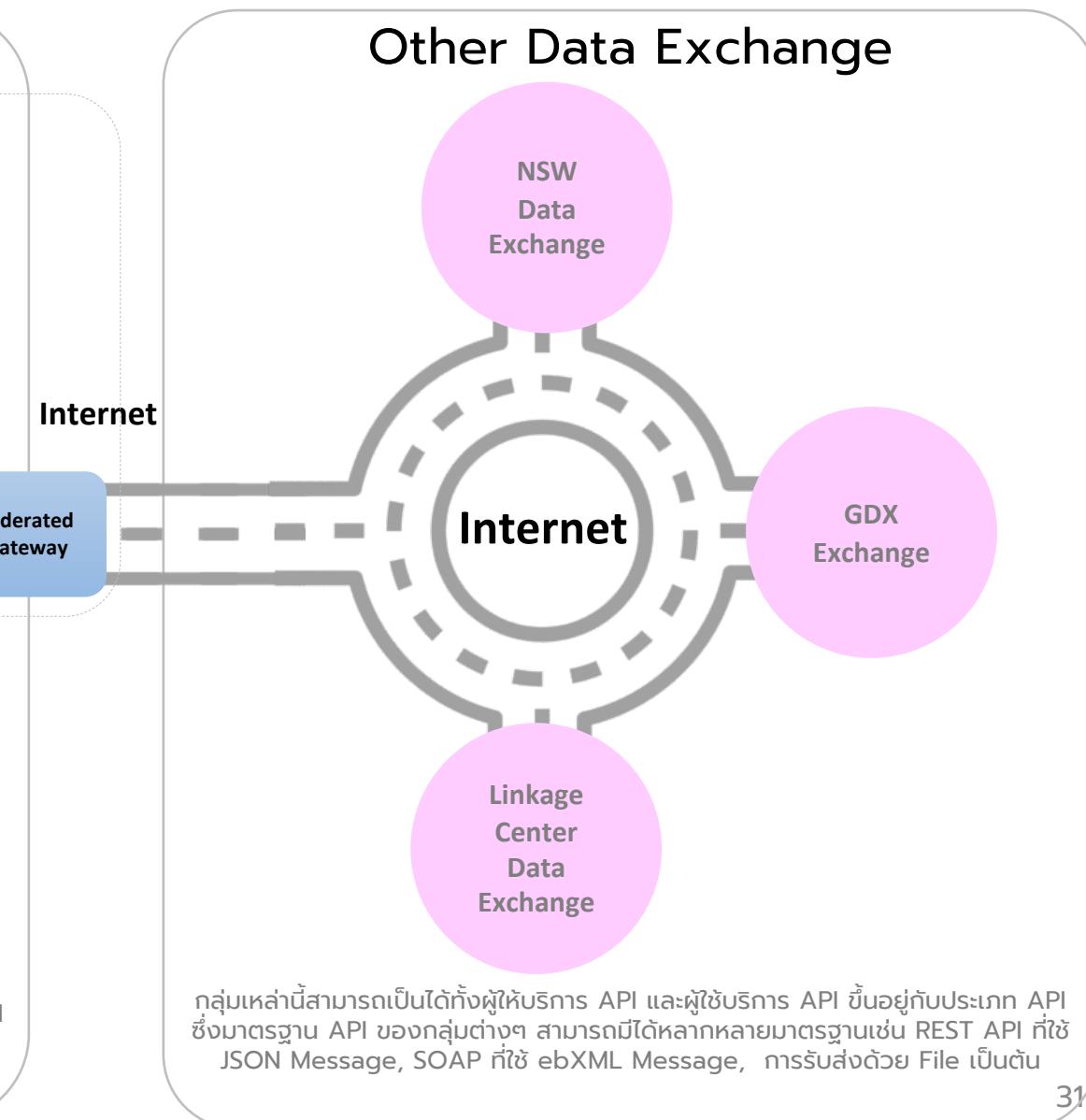
## TGIX-based Data Exchange กับ Data Exchange อื่นๆ (Federated-DX)

### TGIX-based Data Exchange



เป็นกลุ่ม TGIX-based Data Exchange ที่ดำเนินการตามมาตรฐาน TGIX มีได้กั้งผู้ให้บริการ API และผู้ใช้บริการ API ขึ้นอยู่กับประเภท API

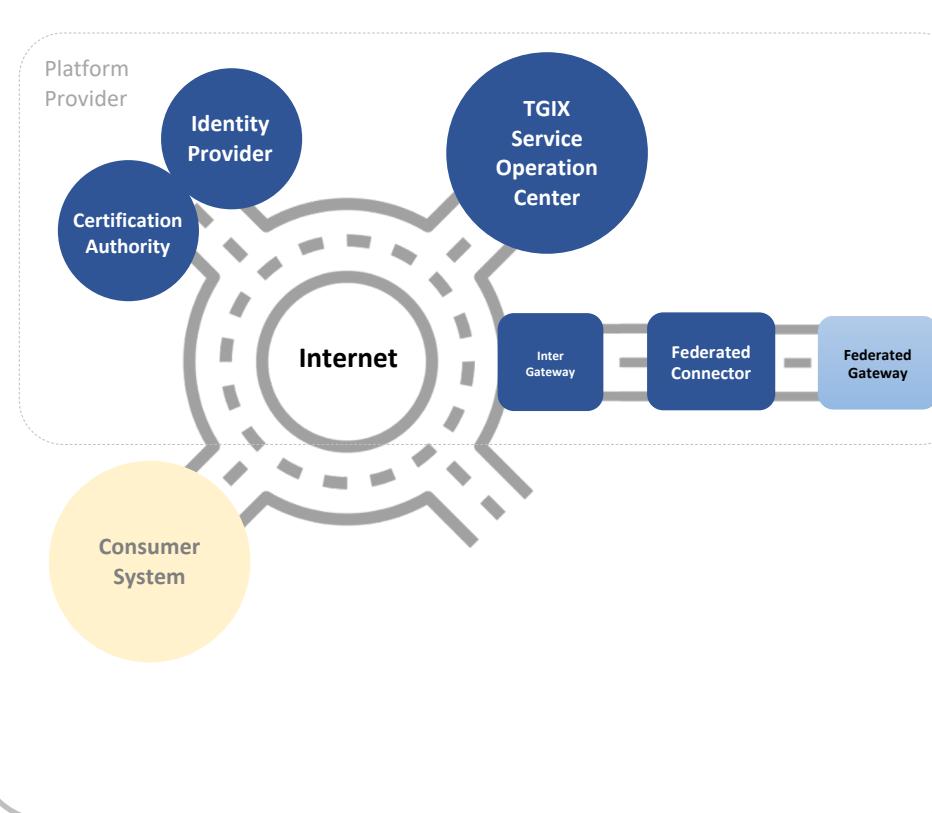
### Other Data Exchange



กลุ่มเหล่านี้สามารถเป็นได้กั้งผู้ให้บริการ API และผู้ใช้บริการ API ขึ้นอยู่กับประเภท API ซึ่งมาตรฐาน API ของกลุ่มต่างๆ สามารถมีได้หลากหลายมาตรฐาน เช่น REST API ที่ใช้ JSON Message, SOAP ที่ใช้ ebXML Message, การรับส่งด้วย File เป็นต้น

# แนวทางดำเนินการของ TGIX-based Data Exchange ที่เป็นผู้ใช้บริการ API ของ Federated DX

## กลุ่ม TGIX-based Data Exchange ที่เป็นผู้ใช้บริการ



## แนวทางดำเนินการของผู้ให้บริการ TGIX Platform

### 1 มีบริการขั้นพื้นฐาน

มีบริการขั้นพื้นฐานเหมือนกลุ่ม TGIX-based Data Exchange ที่เป็นผู้ใช้บริการ API ของ TGIX Inter-DX

### 2 มีบริการตัวกลาง (FEDERATED CONNECTOR) เพื่อเชื่อมโยงและแลกเปลี่ยนระหว่างกลุ่ม TGIX และกลุ่ม DATA EXCHANGE ที่ใช้มาตรฐานอื่นๆ

- ดำเนินการสร้าง Endpoint URL ที่เป็น REST API ตามมาตรฐาน TGIX และลงทะเบียนไว้ที่ Service Catalog เพื่อให้ผู้ใช้บริการในกลุ่ม TGIX-based Data Exchange สามารถเรียกใช้บริการด้วย REST API ตามมาตรฐาน TGIX ได้
- ดำเนินการแปลง Message จาก TGIX Message ที่รับมาจาก Endpoint URL เป็นรูปแบบอื่นๆ เช่น JSON, ebXML หรือ File ที่ผู้ให้บริการต้องการ
- ดำเนินการแปลงประเภท API ไปเป็นรูปแบบที่ผู้ให้บริการต้องการ เช่น SOAP เป็นต้น และเรียกไปยังผู้ให้บริการที่อยู่ในกลุ่ม Data Exchange อื่นๆ

### 3 มีบริการป้องกันการโจมตี API จากผู้ที่ไม่พึงประสงค์จากภายนอกกลุ่ม (บริการ FEDERATED GATEWAY หรือ เทียบเท่า)

## แนวทางดำเนินการของผู้ใช้บริการ API (Consumer System)

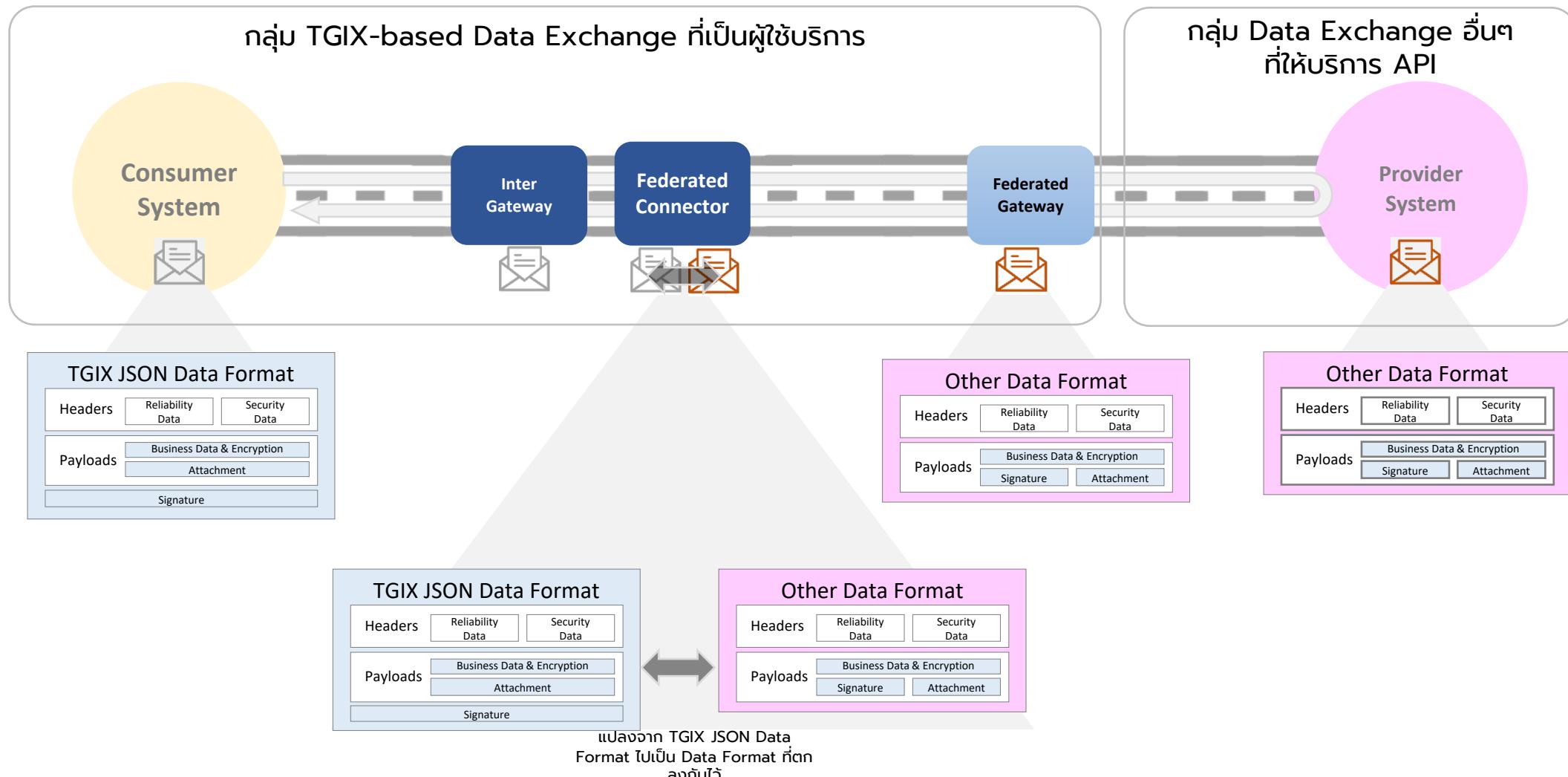
### 1 ทำข้อตกลงบริการระหว่างกลุ่ม TGIX

ดำเนินการทำข้อตกลงบริการ Endpoint URL ของ Federated Connector กับผู้ให้บริการ TGIX Platform พร้อมกับรับคู่มือการใช้งาน API

### 2 พัฒนา API CLIENT

ดำเนินการพัฒนา API Client ตามขั้นตอนเหมือน TGIX Intra-DX

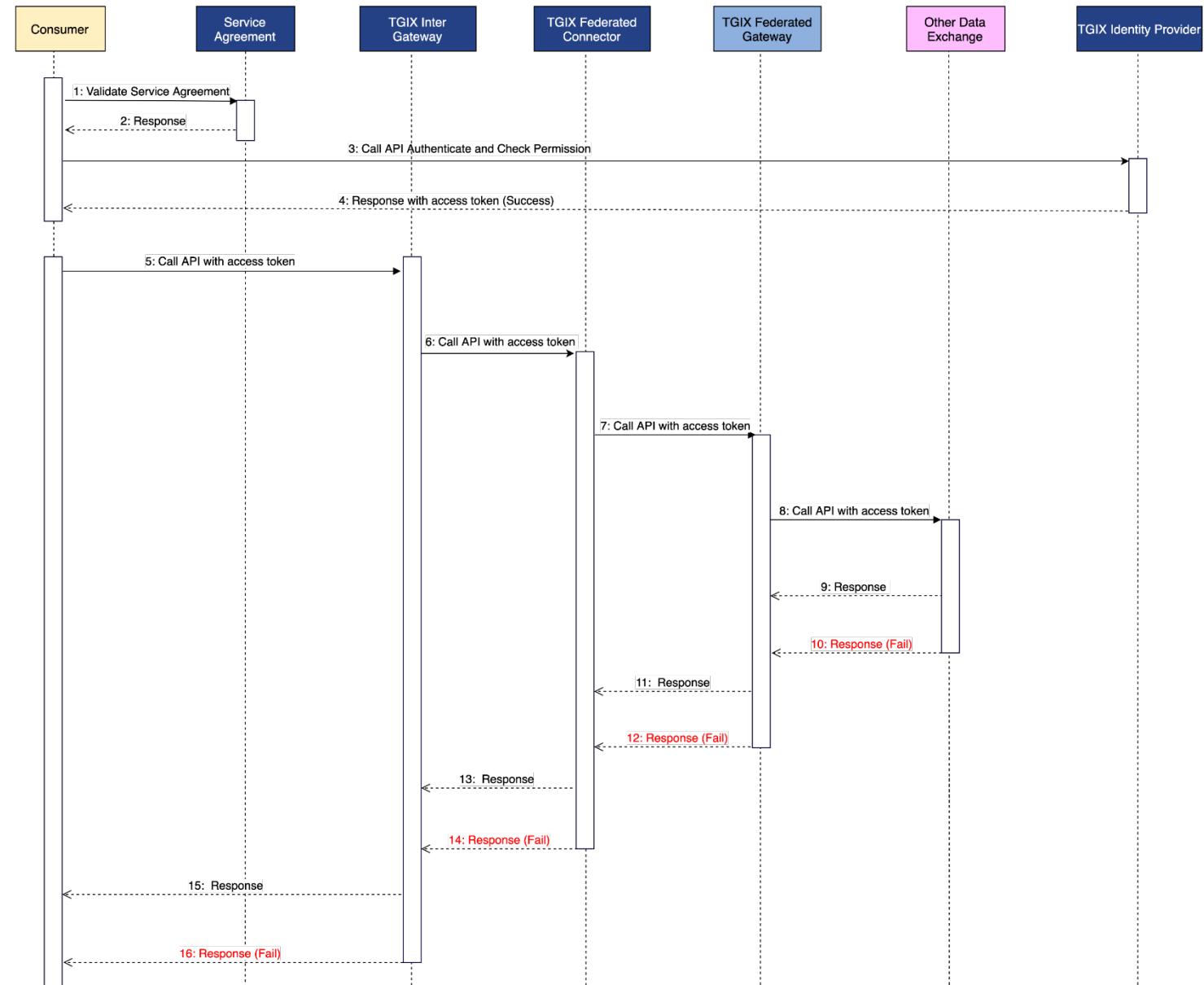
# แนวการดำเนินการของ TGIX-based Data Exchange ที่เป็นผู้ใช้บริการ API ของ Federated DX



"ลักษณะข้อมูลที่ใช้แลกเปลี่ยนจะถูกกำหนดไว้เป็นมาตรฐานด้วยแบบ TGIX JSON Data Format และสามารถแปลงไปเป็นรูปแบบที่ตกลงร่วมกันโดยใช้ Federated Connector"

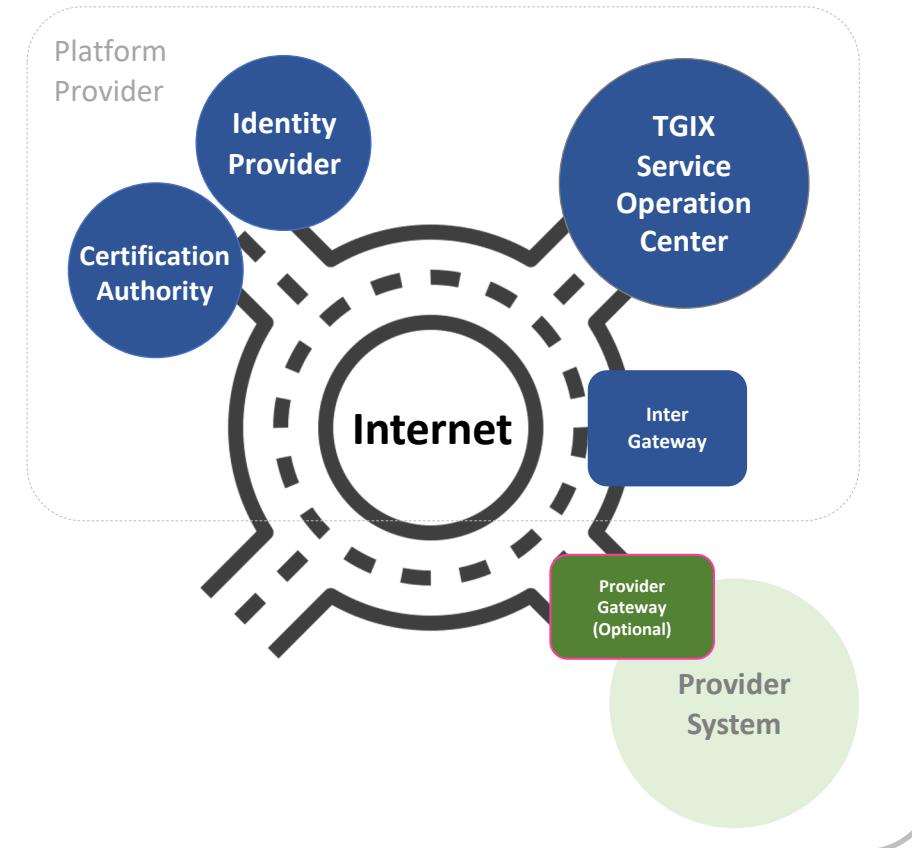
# ขั้นตอนการทำงานระหว่างกลุ่ม

## TGIX-based Data Exchange ที่เป็นผู้ใช้งาน API ของ Federated DX



# แนวทางดำเนินการของ TGIX-based Data Exchange ที่เป็นผู้ให้บริการ API ของ Federated DX

กลุ่ม TGIX-based Data Exchange ที่เป็นผู้ให้บริการ



“ในกรณีที่กลุ่ม TGIX-based Data Exchange เป็นผู้ให้บริการ API แก่ผู้ใช้บริการ API ในกลุ่ม Data Exchange อื่นๆ นั้น กำหนดให้ใช้ REST API ตามมาตรฐาน TGIX ดังนั้นสามารถใช้แนวทางดำเนินการของกลุ่ม TGIX-based Data Exchange ที่เป็นผู้ให้บริการ API”

# มาตรฐานรัฐบาลดิจิทัลการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange Standard (**TGIX**)  
Series: Linkage Standard

## Q&A

# มาตรฐานรัฐบาลดิจิทัลการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange Standard (**TGIX**)  
Series: Linkage Standard



นายวิชญะ เจริญรัตนวัฒน์

ที่ปรึกษาจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

- 1 มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting
- 2 มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session
- 3 มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล
- 4 มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)
- 5 มาตรฐานองค์ประกอบด้าน การบันทึก.log (Logging) และการ ติดตาม (Monitoring)
- 6 มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

1

มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting

2

มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session

3

มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล

4

มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)

5

มาตรฐานองค์ประกอบด้าน การบันทึกล็อก (Logging) และการ ติดตาม (Monitoring)

6

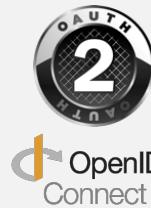
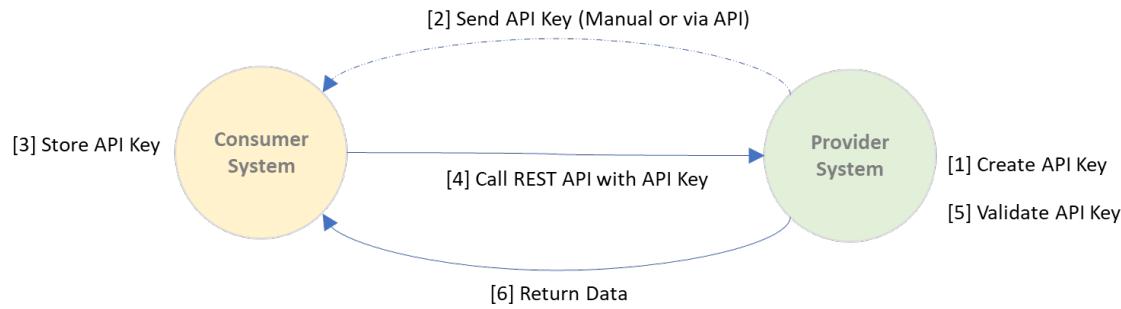
มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# การบริหารการยืนยันตัวตน และ การบริหารจัดการบัญชีผู้ใช้งาน API (API Authentication and Accounting)



## การบริหารจัดการ API Authentication และ Accounting ด้วย API Key

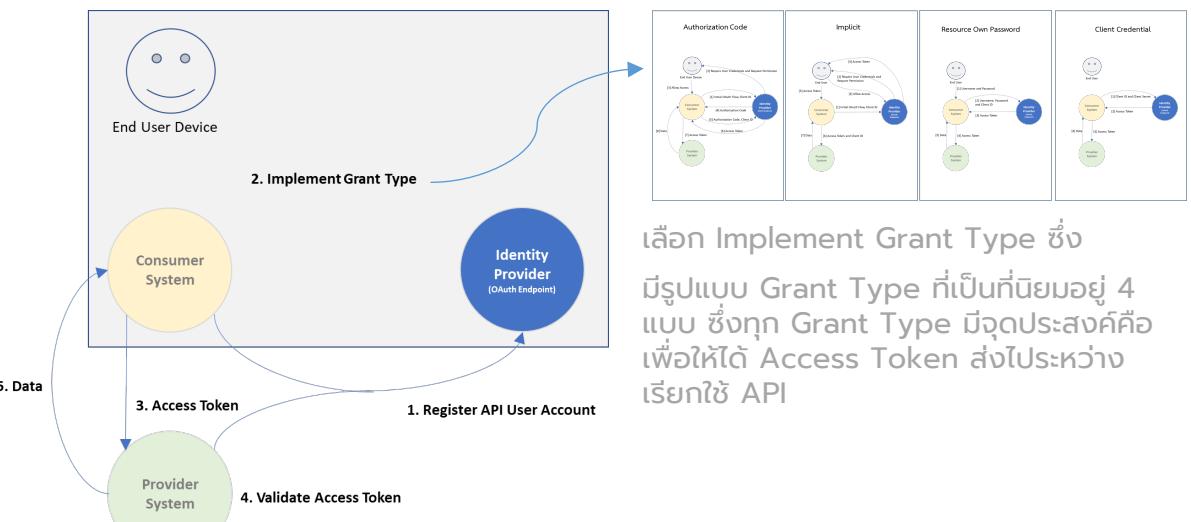
API Key ใช้เพื่อยืนยันว่าผู้ใช้บริการ API (Consumer System) ต้องการขอเข้าถึง API แบบ REST API ของผู้ให้บริการ API (Provider System) แต่ไม่ได้ต้องการการยืนยันตัวตนดับตัวบุคคลที่ใช้งานในระบบของผู้ใช้บริการ API (Consumer System)



## การบริหารจัดการ API Authentication และ Accounting ด้วย OAuth 2.0/Open ID Connect

OAuth 2.0 เป็นการรวมกระบวนการยืนยันตัวตนและจัดการสิทธิ์ให้เข้าถึงข้อมูลเข้าด้วยกัน มาตรฐาน OAuth 2.0 สามารถใช้ยืนยันตัวตนระดับผู้ใช้งานระบบได้ ดังนั้นจึงเหมาะสมในการเข้าถึง API ที่เป็นบริการเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลสำคัญของผู้ให้บริการ API (Provider System)

Open ID Connect (OIDC) เป็นมาตรฐานการยืนยันตัวตนที่ทำงานอยู่บนมาตรฐาน OAuth 2.0 โดยมีจุดเด่นคือการให้ระบบงานใช้ยืนยันตัวตนของผู้ใช้งานเพียงครั้งเดียวแล้วสามารถเข้าไปใช้งานระบบอื่นๆ ได้หลายระบบ (Single Sign On)



เลือก Implement Grant Type ซึ่ง

มีรูปแบบ Grant Type ที่เป็นที่นิยมอยู่ 4 แบบ ซึ่งทุก Grant Type มีจุดประสงค์คือ เพื่อให้ได้ Access Token ส่งไประหว่าง เรียกใช้ API

# การควบคุมสิทธิ์ในการเข้าถึง API (Access Control)



## การควบคุมสิทธิ์ในการเข้าถึง API ด้วย Role-Based Access Control (RBAC)

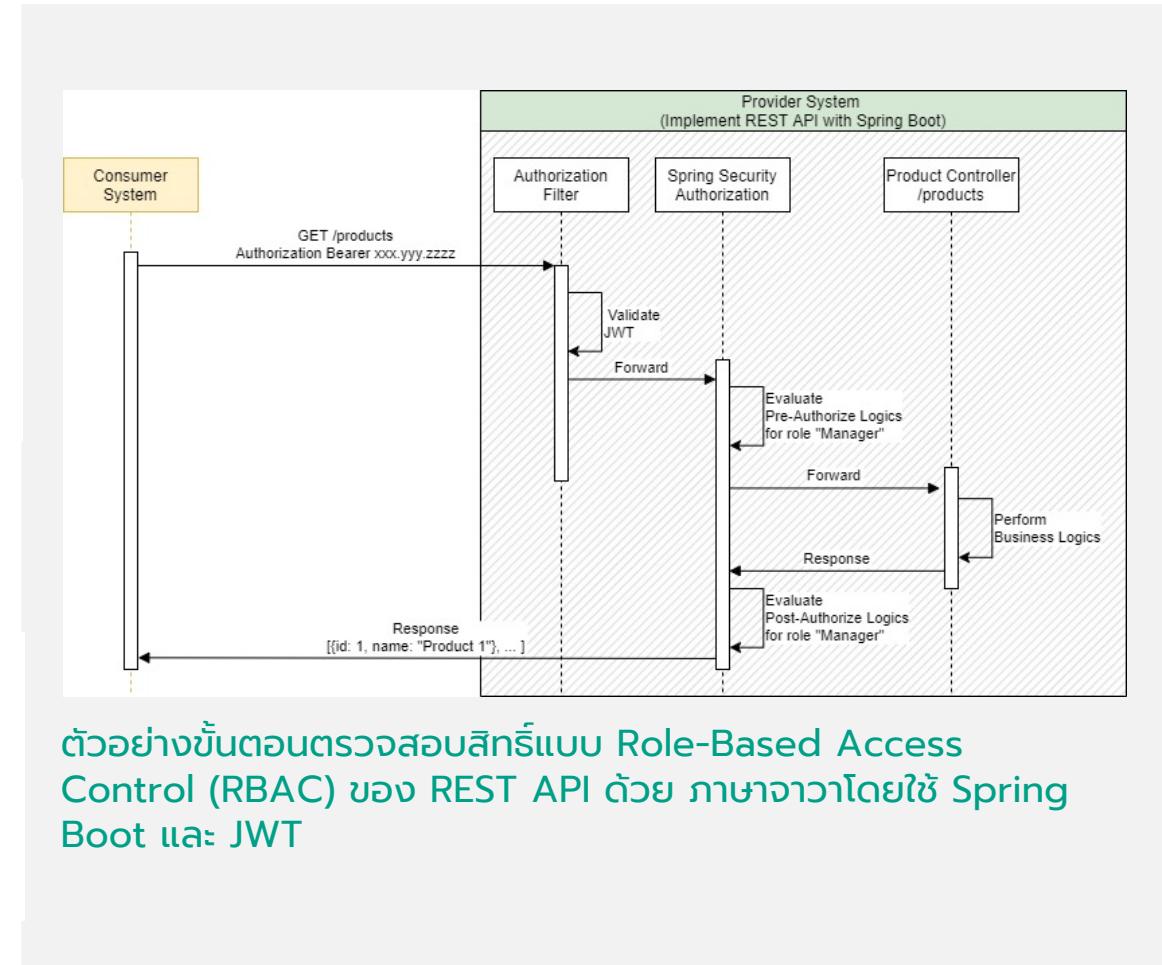
ผู้ให้บริการ API (Provider System) ควรออกแบบและพัฒนาการกำหนดสิทธิ์และการตรวจสอบสิทธิ์ตามบทบาทและหน้าที่ของผู้ใช้งาน API ด้วยวิธี Role-Based Access Control (RBAC) อ้างอิงจาก INCITS 359-2012[R2017] Information technology - Role Based Access Control



## ระดับของการควบคุมสิทธิ์ในการเข้าถึง API

การควบคุมสิทธิ์ในการเข้าถึง API สามารถแบ่งเป็น

- ระดับระบบผู้ใช้บริการ API (Consumer System) หรือ
- ระดับบุคคลผู้ใช้งานในระบบผู้ใช้บริการ API (Consumer System) ตามความเหมาะสมของความต้องการทางธุรกิจ (Business Requirement) และภาษาโปรแกรมที่ใช้พัฒนา API



ตัวอย่างขั้นตอนตรวจสอบสิทธิ์แบบ Role-Based Access Control (RBAC) ของ REST API ด้วย ภาษา Java โดยใช้ Spring Boot และ JWT

# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

- 1 มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting
- 2 มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session
- 3 มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล
- 4 มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)
- 5 มาตรฐานองค์ประกอบด้าน การบันทึกล็อก (Logging) และการ ติดตาม (Monitoring)
- 6 มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# การบริหารจัดการ Token

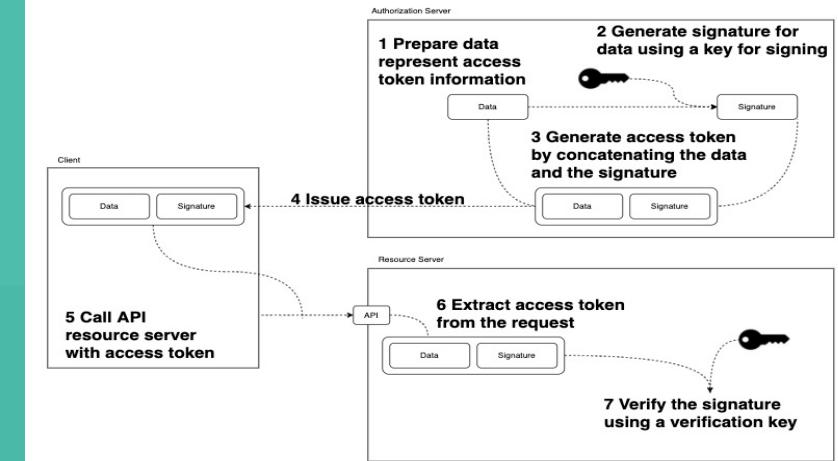


JSON Web Tokens หรือที่เรียกว่า JWTs RFC 7519 เป็นโทคีนการรักษาความปลอดภัยที่ใช้ JSON ที่ปลอดภัยสำหรับ URL

JWT มีชุดการอ้างสิทธิ์ที่สามารถเชื่อมต่อและ/หรือเข้ารหัสได้ ข้อมูลจำเพาะของ JWT ได้รับการนำไปใช้อย่างรวดเร็ว เนื่องจากได้รวมเอาข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยไว้ในที่เดียว จ่ายต่อการปกป้อง ตำแหน่ง และเนื่องจากง่ายต่อการใช้งานโดยใช้เครื่องมือที่หาได้ทั่วไป

พื้นที่แอปพลิเคชันหนึ่งที่ JWT มักใช้คือการแสดงข้อมูล Digital Identity เช่น OpenID Connect id\_tokens OpenID.Core และ OAuth 2.0 RFC 6749 access\_tokens และ refresh\_token ซึ่งมีรายละเอียดเฉพาะสำหรับการปรับใช้

## การตรวจสอบ Token



## ตัวอย่างการใช้งาน JWT Token

```
{  
  "alg": "RS256",  
  "typ": "JWT",  
  "kid": "73b21ab8-20f8-11ec-9621-0242ac130002"  
}  
  
{  
  "iss": "http://example.org",  
  "aud": "http://example.com",  
  "iat": 1632901338586,  
  "exp": 1632901340586,  
  "nbf": 1632901338586,  
  "nonce": "n-0S6_WzA2Mj",  
  "at_hash": "eyJ0eXAiOiJKV1QiLCJhbGciOiJ...",  
  "c_hash": "eyJ2ZXIiOiIyLjAiLCJpc3MiOiJ0...",  
  "auth_time": "2021-09-29T08:10:12Z",  
  "sub": "Sample payload JWT",  
  "jti": "73b21ab8-20f8-11ec-9621-0242ac130002",  
  "client_id": "s6BhdRkqt3"  
}
```

The diagram shows the structure of a JWT token. It is divided into three main sections: Headers, Claims, and a Signature (represented by a large redacted area). The Headers section contains the algorithm ("alg: RS256"), token type ("typ: JWT"), and kid (key identifier). The Claims section contains various data points such as issuer ("iss: http://example.org"), audience ("aud: http://example.com"), and timestamps for issuance, expiration, and not before. Other claims include a nonce, authentication hash, client ID, and a subject.

# การบริหารจัดการ Session



เซสชัน (Session) จะเกิดขึ้นเมื่อมีความต้องการในการสื่อสารกับบันเครือข่ายระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง



เซสชันจะ:

- เริ่มต้นเมื่ออุปกรณ์รับส่งสัญญาณของสองเครื่องเริ่มทำการเชื่อมต่อจะสร้างเซสชันสำหรับการรับส่งข้อมูลขึ้นและ
- สิ้นสุดเมื่ออุปกรณ์ทั้งสองได้รับข้อมูลตามที่ต้องการครบแล้ว และส่งข้อความ "เสร็จสิ้น" จะเป็นการยกเลิกการเชื่อมต่อ ในบริบทของการเข้ารหัส TLS อุปกรณ์ทั้งสองจะต้องแลกเปลี่ยนข้อมูลและสร้างคีย์เซสชันใหม่เพื่อเปิดการเชื่อมต่อ



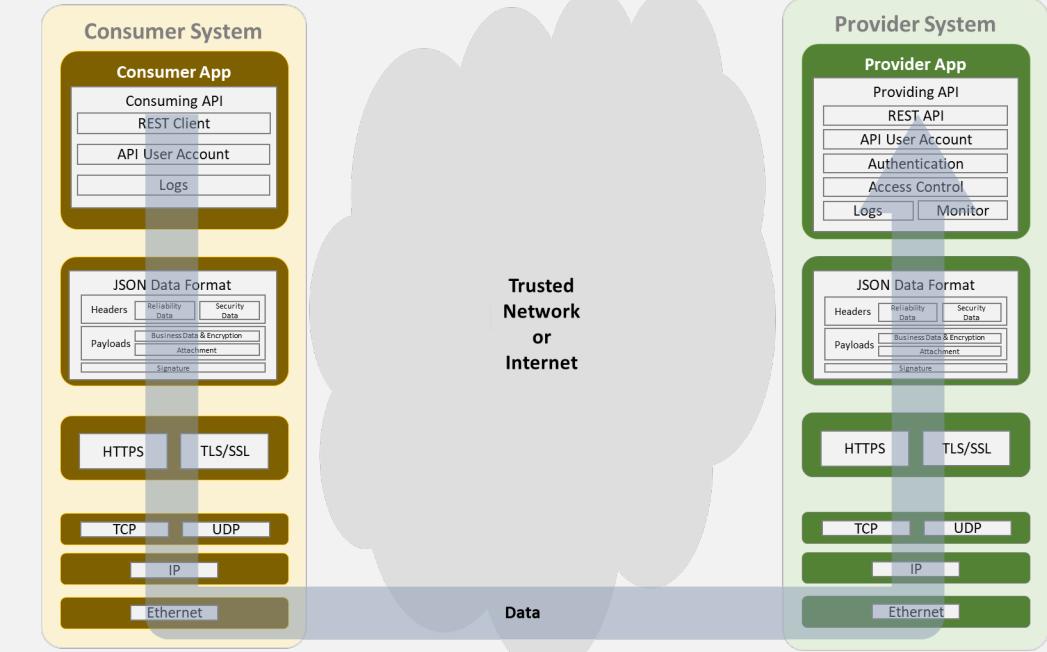
HTTPS ซึ่งเป็น HTTP ที่มีโปรโตคอลการเข้ารหัส TLS ใช้การเข้ารหัสทั้งสองประภาค การสื่อสารทั้งหมดผ่าน TLS เริ่มต้นด้วยขั้นตอนการทำแอนด์เชค TLS จะใช้การเข้ารหัสแบบสมมาตรสำหรับการทำให้ TLS แอนด์เชคทำงานได้ ในระหว่างการแอนด์เชค TLS อุปกรณ์สื่อสารทั้งสองจะสร้างคีย์เซสชัน และจะใช้สำหรับการเข้ารหัสแบบสมมาตรสำหรับเซสชัน โดยปกติอุปกรณ์สื่อสารทั้ง 2 เครื่อง คือ คลาวด์ และเซิร์ฟเวอร์



คลาวด์ และเซิร์ฟเวอร์ ในที่นี้คือ Consumer System และ Provider System นั้นเอง

## การสร้าง Session ระหว่าง

### Consumer System และ Provider System



# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

- 1 มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting
- 2 มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session
- 3 มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล
- 4 มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)
- 5 มาตรฐานองค์ประกอบด้าน การบันทึกล็อก (Logging) และการ ติดตาม (Monitoring)
- 6 มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# ໂປຣໂຕຄອລ (Protocol) ສໍາຮັບການເຊື່ອມໂຍງແລກປ່ຽນຂ້ອມູລ



ກຳຫົດໃຫ້ການເຮັດໃຊ້ງານ Endpoint URL ຕ້ອງດໍາເນີນການຜ່ານ  
HTTPS ເກົ່ານັ້ນ



ກຳຫົດໃຫ້ມີການໃຊ້ TLS version 1.2 ເປັນອຍ່າງນ້ອຍສໍາຮັບ TLS/SSL



ກຳຫົດໃຫ້ການໃຊ້ງານ Transmission Control Protocol (TCP) ຕ້ອງກຳຜ່ານ TLS/SSL  
ເກົ່ານັ້ນ

# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

- 1 มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting
- 2 มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session
- 3 มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล
- 4 มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)
- 5 มาตรฐานองค์ประกอบด้าน การบันทึกล็อก (Logging) และการ ติดตาม (Monitoring)
- 6 มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)



## HTTPS

การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย



## ห้ามเปลี่ยนเส้นทางจาก HTTP ไป HTTPS

ห้ามทำการเปลี่ยนเส้นทาง HTTP ไปยัง HTTPS โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกรูปแบบ



## ใบรับรอง (Certificates)

ใบรับรอง (Certificates) จะต้องมีการเข้ารหัส เช่น SHA-2 (Secure Hash Algorithm 2) และต้องมีขนาด秘钥 (Key size) อย่างน้อย 2048



## HTTP Method

ให้ปิดการใช้งานเมื่อ遇到 HTTP Method ที่ไม่ได้ใช้งานและส่งคืนค่า HTTP 405



## ใบรับรองจากหน่วยงานที่ได้รับอนุญาต

ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต



## การตรวจสอบ

ต้องมีการตรวจสอบ (Validate) ทุก ๆ การเรียกใช้งาน (Request)

# ข้อกำหนดด้านความปลอดภัยของการเข้ารหัส (Encryption)



## Encryption

สำหรับการส่งข้อมูลที่สำคัญหรือเป็นความลับที่ต้องการการเข้ารหัสจะต้องใช้การเข้ารหัสแบบสมมาตร (Symmetric Encryption) และ

- AES (Advanced Encryption Standard) โดยมีความยาวของกุญแจอย่างน้อย 128 bits (AES-128)



## Digital Signature

สำหรับการลงลายมือชื่อแบบดิจิทัลเพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้อัลกอริธึมแบบใดแบบหนึ่งดังต่อไปนี้

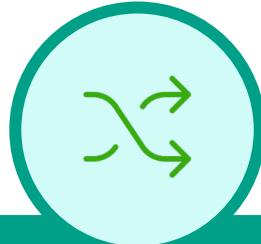
- DSA (Digital Signature Algorithm)
  - มีขนาดอย่างน้อย 112 bits
  - Domain Parameter อย่างน้อย  $(L, N) = (2048, 224)$
- ECDSA (Elliptic Curve-based Digital Signature)
  - มีขนาด อย่างน้อย 112 bits
  - Domain Parameter อย่างน้อย 224 bits
- RSA (Rivest-Shamir-Adelman algorithm)
  - มีขนาดอย่างน้อย 112 bits
  - Domain Parameter อย่างน้อย 2048 bits



## Hash functions

สำหรับการสร้างหรือตรวจสอบลายมือชื่อแบบดิจิทัลโดยใช้ฟังก์ชันแฮช (Hash Function) จะต้องใช้ฟังก์ชันแบบใดแบบหนึ่งดังต่อไปนี้

- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 และ SHA-512/256)
- SHA-3 (SHA3-224, SHA3-256, SHA3-384 และ SHA3-512)



## Random Bit Generation

สำหรับการสร้างตัวเลขแบบสุ่ม (Random Bit Generation) เพื่อจุดประสงค์ต่าง ๆ เช่นการสร้างกุญแจ (keys) ตัวเลขแบบใช้ครั้งเดียว (Nonces) และ ค่าสุ่มเพื่อการยืนยันตัวตน (Authentication Challenges) จะต้องใช้อัลกอริธึมแบบใดแบบหนึ่งดังต่อไปนี้

- Hash\_DRBG และ HMAC\_DRBG
- CRT\_DRBG โดยใช้ AES-128, AES-192 และ AES-256

# ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit)



## Request Limit

สามารถจำกัดจำนวนการร้องขอบริการต่อผู้ใช้บริการหรือบริการได้ (Number of requests per client/resource) โดยผู้ให้บริการทำการประเมินจากทรัพยากรและประสิทธิภาพที่จะให้บริการได้กับความต้องการใช้บริการของผู้ใช้บริการ

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



<https://konghq.com/blog/how-to-design-a-scalable-rate-limiting-algorithm/>

The screenshot shows the Red Hat 3Scale API Management interface. The left sidebar has 'Overview', 'Analytics', 'Applications' (which is selected and highlighted with a red box), 'Subscriptions', 'ActiveDocs', and 'Integration'. The main area is titled 'Metrics, Methods, Limits & Pricing Rules' under 'Metric or Method (Define)'. It shows 'Hits' and 'Pricing (0)', 'All Limits (0)', and a 'New usage limit' button. Below this is a table for 'Usage Limits' with columns 'Period' and 'Value'. One row shows 'foo' with 'Pricing (0)' and 'All Limits (0)'.

[https://access.redhat.com/documentation/en-us/red\\_hat\\_3scale\\_api\\_management/2.4/html/access\\_control/rate-limits](https://access.redhat.com/documentation/en-us/red_hat_3scale_api_management/2.4/html/access_control/rate-limits)

# ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (ต่อ) (Resource and Rate Limit)



## Execution timeouts

สามารถจำกัดเวลาการทำงานของบริการได้ (Execution timeouts) โดยควรกำหนดค่าตั้งต้นของขนาดสูงสุดของเวลาการทำงาน (Execution timeout) ไว้ที่ 60 วินาที หรือสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการให้บริการ โดยสามารถเลือกดำเนินการได้จาก

- การพัฒนาด้วยภาษาโปรแกรมของ Provider System
- การระบุไว้ที่ Web Server หรือ Application Server ของ Provider System
- การใช้ API Gateway เข้ามาช่วยดำเนินการ
- อื่น ๆ ตามความเหมาะสม



## Limit request payload size

สามารถจำกัดขนาดของข้อความในการร้องขอบริการได้ (Request payload size) โดยควรกำหนดค่าตั้งต้นของขนาดสูงสุดของข้อความร้องขอบริการ (Request payload size) ไว้ที่ 128 MB (Megabytes) หรือสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการให้บริการ โดยสามารถเลือกดำเนินการได้จาก

- การพัฒนาด้วยภาษาโปรแกรมของ Provider System
- การระบุไว้ที่ Web Server หรือ Application Server ของ Provider System
- การใช้ API Gateway เข้ามาช่วยดำเนินการ
- อื่น ๆ ตามความเหมาะสม

# ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (ต่อ) (Resource and Rate Limit)



## Limit response records

สามารถจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ร้องขอการในหนึ่งการร้องขอและตอบกลับ (Number of records per page to return in a single request response)

### จุดประสงค์เพื่อ

- ให้การตอบกลับของ API ใช้เวลาอย่างเช่น < 2 วินาที เป็นต้น
- ต้องการให้จำนวนข้อมูลที่ส่งกลับใน Payload มีความเหมาะสม เช่น < 500kb เป็นต้น

### ตัวอย่างการใช้ Pagination เช่น

Page 1: /customers?page=1&limit=10

Page 2: /customers?page=2&limit=10

...

Page 50: /customers?page=50&limit=10

หมายเหตุ

- Page คือเลขที่หน้า
- Limit คือจำนวนแถวที่ส่งกลับของหน้านั้นๆ

# ข้อกำหนดการจัดการความผิดพลาด (Error handling)



## Do not return call stacks

บริการจะต้องไม่ส่งรายละเอียดข้อผิดพลาดทางเทคนิคไปยังผู้ขอใช้บริการ เช่น ไม่ควรแสดงข้อความข้อผิดพลาดของลำดับการเรียกของระบบ (Call stacks) หรือข้อความข้อผิดพลาดของคำสั่งเรียกฐานข้อมูล



## Return only HTTP status responses

บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) เช่น ไม่ควรแสดงข้อมูลระดับระบบ (System level) ไปในข้อผิดพลาดที่ตอบกลับ

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

<https://datatracker.ietf.org/doc/html/rfc7231>

# ข้อกำหนดการจัดการความผิดพลาด (Error handling)



## Validation first

การตรวจสอบข้อมูลนำเข้าควรจะกระทำเป็นลำดับแรกสุดเก่าที่จะทำได้นับตั้งแต่ได้รับข้อมูลเข้ามาจากระบบภายนอก



## Logging input validation

ตรวจสอบบันทึกกิจกรรมและข้อมูลราชคุมพิวเตอร์ที่ไม่ผ่านการตรวจสอบข้อมูลนำเข้า (Logging input validation)



## Verify input

ตรวจสอบข้อมูลนำเข้า โดยตรวจสอบ เช่น ขนาดความยาว ช่วงของข้อมูล รูปแบบข้อมูล และประเภทข้อมูล ให้ตรงตามข้อกำหนดทางเทคนิคของบริการนั้นที่กำหนดไว้



## Limit input size

กำหนดการจำกัดขนาดของข้อมูลนำเข้าที่เหมาะสมและปฏิเสธข้อมูลนำเข้าที่มีขนาดเกินที่กำหนดไว้



## Regular Expression

จำกัดข้อมูลนำเข้าให้อยู่ในรูปแบบที่เหมาะสมกับประเภทข้อมูลตามข้อกำหนดทางเทคนิคของบริการนั้นด้วยการตรวจสอบด้วยนิพจน์ปกติ (Regular Expression)

เมื่อดำเนินการตรวจสอบแล้วพบข้อผิดพลาด ควรแจ้งให้ผู้ใช้บริการทราบตามตัวอย่างนี้

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

# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

- 1 มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting
- 2 มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session
- 3 มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล
- 4 มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)
- 5 มาตรฐานองค์ประกอบด้าน การบันทึกล็อก (Logging) และการ ติดตาม (Monitoring)
- 6 มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# การบันทึกЛОГ (Logging)

มีแนวทางการบันทึกЛОГแบ่งเป็น 2 กลุ่มคือ

{Header}

ตัวอย่างการบันทึกข้อมูลเชิงเทคนิค  
(Technical logs) ในส่วน TGIX Message Header

```
{  
    "messageVersion": "V1.0.0",  
    "MessageId": "M1633151789",  
    "Timestamp": "2021-10-08T08:10:12.24+07:00",  
    "clientId": "452435",  
    "event": "SendMessage",  
    "RequestId": "423984729387",  
    "Host": "localhost",  
    "InitiatorId": "",  
    "ConversationId": "1",  
    "SourceAddress": "http://localhost:8081/callService",  
    "DestinationAddress": "http://localhost:8080/xmlService",  
    "ResponseAddress": "",  
    "ExpirationTime": "1643151789",  
    "SentTime": "  
}  
)
```

{Full}

ตัวอย่างบันทึกข้อมูลเชิงธุรกรรม (Transaction logs) กั้งที่เป็น JSON Message และ ไปใช้ JSON Message

```
"Action": {  
    "Protocol": "http",  
    "Method": "POST",  
    "Path": "/searchJuristic",  
    "URL": "http://localhost:8081"  
},  
"TGIXPayload": {  
    "JuristicID": "0133552005772"  
}
```

JSON Message

```
"attachMents": [  
    {  
        "mimeType": "text/xml",  
        "contentId": "0",  
        "name": "Screen Shot 2564-10-08 at 10.41.34.png",  
        "referenceld": "170e80bc-281e-11ec-9621-0242ac130000",  
        "sequence": "1"  
},  
    {  
        "mimeType": "image/jpeg",  
        "contentId": "1",  
        "name": "Screen Shot 2564-10-08 at 10.07.10.png",  
        "referenceld": "170e80bc-281e-11ec-9621-0242ac130001",  
        "sequence": "1"  
}  
]
```

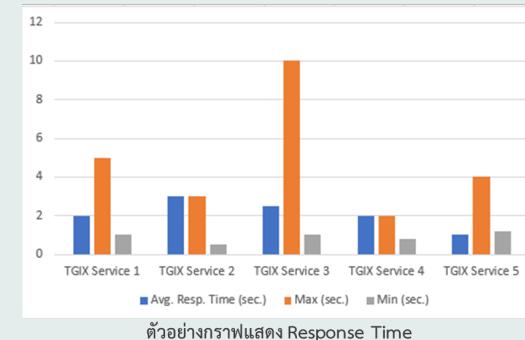
Message ประเภทอื่นๆ

# การติดตาม (Monitoring)

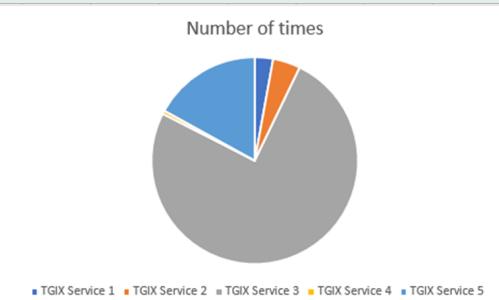
การติดตามด้านการปฏิบัติงาน จะใช้ข้อมูลจากการบันทึกข้อมูลเชิงเทคนิค และบันทึกข้อมูลเชิงธุรกรรม มาติดตามการทำงานสัดสี่แนวทางการดำเนินการการติดตาม (Monitoring) สามารถเลือกได้จากการเลือกต่อไปนี้

## Programming

พัฒนาด้วยภาษาโปรแกรมของ Provider System



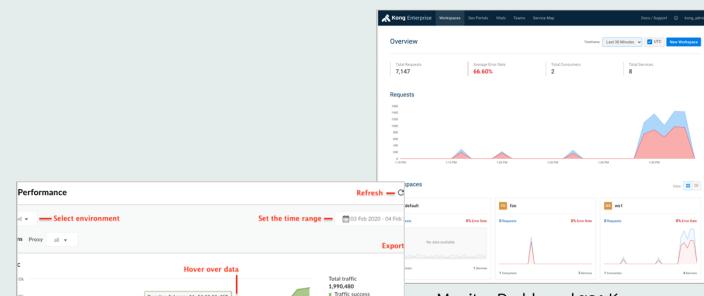
ตัวอย่างกราฟแสดง Response Time



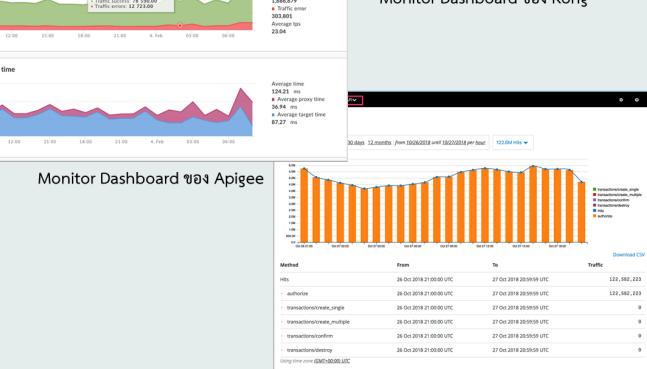
ตัวอย่างกราฟแสดงจำนวนครั้งในการเรียกใช้งาน

## API Gateway

ใช้เครื่องมือ API Gateway Monitoring เช่น Kong, 3Scale, Apigee เป็นต้น



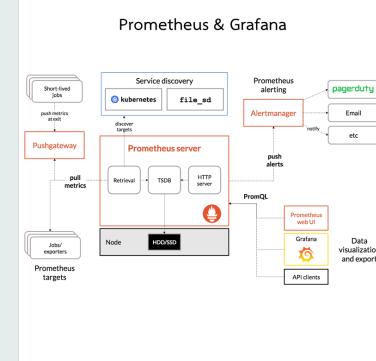
Monitor Dashboard ของ Kong



Monitor Dashboard ของ 3Scale

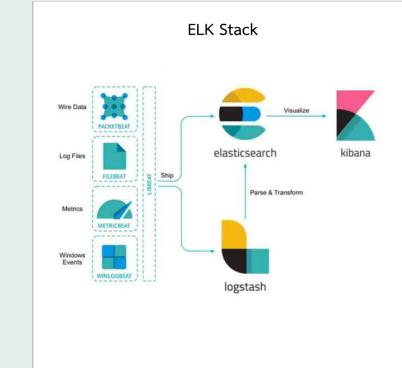
## Monitoring tools

ใช้ Monitoring Solution อื่น ๆ ที่เป็นที่นิยม เช่น Prometheus Grafana, ELK Stack เป็น



<https://prometheus.io/docs/introduction/overview/>

ELK Stack



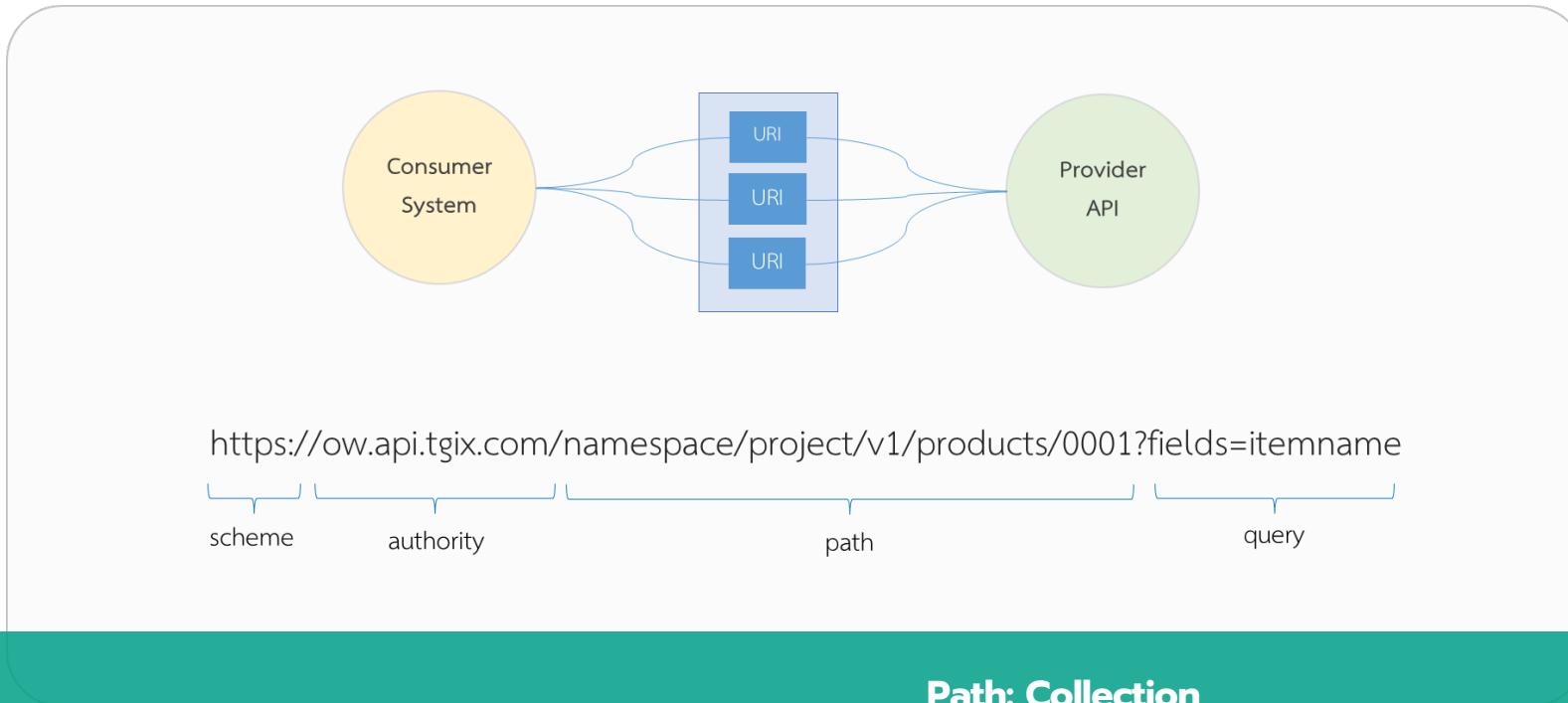
<https://www.elastic.co/what-is/elk-stack/>

# มาตรฐาน องค์ประกอบการ เชื่อมโยงและ แลกเปลี่ยนข้อมูล ภาครัฐ ด้านการเชื่อมโยง ข้อมูล

- 1 มาตรฐานองค์ประกอบด้าน Authentication Access Control และ Accounting
- 2 มาตรฐานองค์ประกอบด้าน การบริหารจัดการ Token และ Session
- 3 มาตรฐานองค์ประกอบด้าน โปรโตคอล (Protocol) สำหรับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล
- 4 มาตรฐานองค์ประกอบด้าน ความมั่นคงปลอดภัย (Security) และ การเข้ารหัสข้อมูล (Encryption)
- 5 มาตรฐานองค์ประกอบด้าน การบันทึกล็อก (Logging) และการ ติดตาม (Monitoring)
- 6 มาตรฐานองค์ประกอบด้าน การกำหนด Namespace ของระบบ

# หลักการกำหนด Namespace ของระบบตามมาตรฐาน TGIX

การกำหนดโครงสร้างของ URI (Uniform Resource Identifiers) เป็นการระบุที่อยู่ของทรัพยากร (Resource) ที่ให้บริการ



## Scheme

เป็นการกำหนด Protocol สำหรับเรียกใช้งาน API เช่น http://

## Authority

เป็นการกำหนด Domain ของผู้ให้บริการตามมาตรฐานที่กำหนด เช่น ow.api.tgix.com

## Path: API

เป็นการกำหนดชื่อการให้บริการ เช่น /namespace/project

## Path: Version

เป็นการกำหนดเวอร์ชันของการให้บริการ เช่น /v1

## Path: Collection

เป็นการกำหนดรูปแบบสำหรับการเข้าถึงข้อมูลหลายชุดพร้อมกัน เช่น /products

## Path: Resource

เป็นการกำหนดรูปแบบสำหรับการเข้าถึงข้อมูลชุดเดียว กัน เช่น /products/0001

## Query

เป็นการกำหนดเงื่อนไขการแสดงข้อมูล เช่น fields=itemname

# การกำหนดรูปแบบ Resource Names และ Query

## สามารถกำหนดรูปแบบ Resource Names ซึ่งมีแนวทางในการกำหนดดังนี้

- ควรเป็นคำนาม โดยห้ามใช้คำกริยาในการอธิบาย
- ควรเป็นเอกพจน์สำหรับแบบ Instance Resource
- ควรเป็นพหุพจน์สำหรับแบบ Collection Resource
- ควรเป็นตัวพิมพ์เล็ก (Lower-case) และมีเครื่องหมาย - (Hyphen) สำหรับคั่นคำ



/employees

ใช้คำพหุพจน์ในการตั้งชื่อ Resource และ Collections



/get-employee

ใช้คำกริยา

/sea-cargo

ใช้คำนาม

/products

ใช้คำพหุพจน์ในการตั้งชื่อ Resource และ Collections

## สามารถกำหนดรูปแบบ Query ซึ่งมีแนวทางในการกำหนดดังนี้

- ควรใช้ \_ (Underscore) สำหรับคั่นคำ
- ควรเป็นตัวพิมพ์เล็กทั้งหมด (Lower-case)
- ควรใช้เท่ากับจำเป็น เช่น การ Filters และ Sorting
- ไม่ควรใช้ตัวอักษรที่เป็นข้อมูล Sensitive



?first\_name=Verawat&date\_of\_birth=2021-10-31

ใช้ \_ (Underscore) สำหรับคั่นคำ

?sort-asc&sort\_fields=name,last\_modified

ใช้ตัวพิมพ์เล็กทั้งหมด



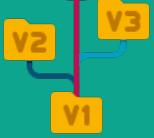
?First\_Name=Verawat&date\_of\_birth=2021-10-31

ใช้ตัวพิมพ์ใหญ่/ผสมตัวพิมพ์เล็ก

/products/1234/desc

กำหนดวิธีการแสดงผลเข้าไปเป็นส่วนหนึ่งของ URI

# การกำหนดรูปแบบ Version



การปรับเปลี่ยนเวอร์ชันจะเปลี่ยนเมื่อมีการอัพเกรดของ API และเป็นการป้องกันการเกิดการหยุดการทำงานของ API ให้บริการ (Breaking API) โดยที่ไม่ต้องแจ้งผู้ใช้บริการให้ทราบล่วงหน้า โดยเวอร์ชันจะกำหนดเป็นส่วนหนึ่งใน URI

## ตัวอย่าง

```
GET /namespace/v1/  
//HTTP 200 OK  
{  
    "api_name": "namespace",  
    "api_version": "1.0.3"  
    "api_released": "2021-08-10"  
    "api_documentation": "https://tgix.api.com/namespace/v1/docs"  
    "api_status": "active"  
}
```

# มาตรฐานรัฐบาลดิจิทัลการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

Thailand Government Information Exchange Standard (**TGIX**)  
Series: Linkage Standard

## Q&A

# ช่องทางการเสนอความคิดเห็น



มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

ขอเชิญแสดงความคิดเห็นต่อร่างมาตรฐานรัฐบาลดิจิทัล ว่าด้วย (ร่าง) มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

ขอเชิญเข้าร่วมงานรับฟังความคิดเห็นต่อร่างมาตรฐาน  
วันพุธที่ 6 มกราคม พ.ศ. 2565 เวลา 13.00 - 16.30 น.

ผ่านทางช่องทาง



ขอความกรุณารอตัวบ่งชี้ความคิดเห็นกลับมาภายใน  
**วันศุกร์ที่ 21 มกราคม พ.ศ. 2565**

>>> คลิกเพื่อลองลงทะเบียนหน่วยงาน

>>> คลิกเพื่อใส่ข้อเสนอแนะต่อร่างมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องสภากาชาดไทยกรณีว่างอิง

>>> คลิกเพื่อใส่ข้อเสนอแนะต่อร่างมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนด 5 ด้าน

>>> คลิกเพื่อดownload ไฟล์ร่างมาตรฐาน ไฟล์แบบสอบถาม และเอกสารที่เกี่ยวข้อง

## ช่องทางการติดต่อ

ฝ่ายมาตรฐานดิจิทัลภาครัฐ กีมมาตรฐานดิจิทัลภาครัฐ 3



เบอร์โทรศัพท์ติดต่อ

08 0045 3484 (ปราการ)

08 0045 3422 (เจชฎา)

09 4662 9461 (พญขันพร)