มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. 10-2 : 2566

DGA 10-2 : 2566

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน

(THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD, SERIES: LINKAGE STANDARD, PART 2: STANDARD REGULATIONS FOR AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING)

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน

มสพร. 10-2 : 2566

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ชั้น 17 อาคารบางกอกไทยทาวเวอร์

108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400

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

ประกาศโดย

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

วันที่ 31 พฤษภาคม 2566

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

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

รองประธานกรรมการ

นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

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

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

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

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรรมการ

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

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ตามคำสั่งที่ 69/2564 ลงวันที่ 20 ตุลาคม 2564

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์
นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

คณะทำงาน

นางบุญยิ่ง ชั่งสัจจา	กรมการปกครอง
นางสาวมนทิพา เข่งพิมล	กรมพัฒนาธุรกิจการค้า
นายพงศกร ริยะมงคล	
นายกำชัย จัตตานนท์	ผู้แทนกรมศุลกากร
นางบุษยา ดวงตา	
นางสาวขนิษฐา สหเมธาพัฒน์	กรมสรรพากร
นายยุทธพล จินะสี	
นางสาวภัทราพรรณ วงศาโรจน์	ธนาคารแห่งประเทศไทย
นายยรรยง ดำรงศิริ	
นางสาวจิตสุภา วิระยะวานิช	
นายกิตติพงษ์ สุขสม	
นายพิสุทธิ นาคหมื่นไวย	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

นางศุปกิจ สกลเสาวภาคย์	กรมที่ดิน
นางตวงรัตน์ จันทรประดิษฐ์	
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายมนต์ศักดิ์ โซ่เจริญธรรม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ตามคำสั่งที่ 85/2565 ลงวันที่ 31 ตุลาคม 2565

ที่ปรึกษา

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

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

รองประธานคณะทำงาน

นางสาวยศวลัย โชติปทุมวรรณ	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คณะทำงาน

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

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน

นายเจษฎา ขจรฤทธิ์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายปราการ ศิริมา สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คำนำ

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

มาตรฐานนี้เป็นมาตรฐานลำดับที่ 2 ในกลุ่มมาตรฐานด้านการเชื่อมโยงข้อมูล และแลกเปลี่ยนข้อมูลภาครัฐ เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน ในส่วนแรกจะอธิบายถึงข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน แบบ API Key OAuth 2.0 และ Open ID Connect ในส่วนที่สองจะนำเสนอขั้นตอนในการยืนยันตัวตนด้วย API Key OAuth 2.0 และ Open ID Connect ตามลำดับ

มาตรฐานนี้ประกอบด้วยคำอธิบาย และตัวอย่างที่ใช้งานจริงเพื่อประยุกต์ใช้ในการเชื่อมโยงแลกเปลี่ยนข้อมูลกันระหว่างหน่วยงานได้อย่างมีประสิทธภาพ และมีความมั่นคงปลอดภัยของข้อมูล

สารบัญ

สารบัญรูป

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ
ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมี แนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลภาครัฐจำเป็นต้อง ขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เล็งเห็นความสำคัญในจุดนี้ จึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐเพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลภาครัฐ คือ การให้หน่วยงานของรัฐมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกัน

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ฉบับนี้ มีขอบเขตมาตรฐานที่ระดับการเชื่อมโยงข้อมูลเท่านั้น ไม่ได้ครอบคลุมถึงระดับการจัดการข้อมูลทางธุรกรรมของหน่วยงาน (Business Transaction Data) ที่เกิดขึ้นจากการเชื่อมโยงและแลกเปลี่ยนระหว่างกัน

ดังนั้น เพื่อให้บรรลุเป้าประสงค์หลักดังกล่าว เอกสารฉบับนี้จึงนำเสนอข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน สำหรับประกอบเอกสารว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของประเทศไทยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งานที่ใช้ในเอกสารฉบับนี้มีดังนี้

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

2.2 ผู้ให้บริการ (Provider) หมายความว่า หน่วยงานที่เปิดให้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.3 ระบบผู้ให้บริการ (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.4 ผู้ใช้บริการ (Consumer) หมายความว่า หน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.5 ระบบผู้ใช้บริการ (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.6 แพลตฟอร์มมาตรฐาน TGIX-based Data Exchange Platform หมายความว่า ระบบสารสนเทศการเชื่อมโยงและแลกเปลี่ยนข้อมูลกลางที่มีมาตรฐานตาม TGIX โดยเรียกแบบย่อว่า TGIX Platform

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

2.8 การยืนยันตัวตน (Authentication) หมายความว่า กระบวนการที่ผู้ใช้บริการ API ยืนยันตัวตนกับ ผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน

2.9 การยืนยันตัวตนด้วยวิธีการใช้ API Key (API Key Authentication Method) หมายความว่า กระบวนการยืนยันตัวตนด้วยวิธีการใช้ API Key ซึ่งเป็นค่าที่สร้างขึ้นแบบไม่ซ้ำกันโดยระบบผู้ให้บริการ (Provider System) แล้วส่งมอบให้ระบบผู้ใช้บริการ (Consumer System) เก็บไว้ใช้ในการยืนยันตัวตนระหว่างเรียกใช้งานบริการแบบ REST API ของระบบผู้ให้บริการ (Provider System)

2.10 การยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0 หมายความว่า กระบวนการยืนยันตัวตนด้วยวิธีการใช้ OAuth 2.0 ซึ่งระบบผู้ใช้บริการ (Consumer System) ดำเนินการยืนยันตัวตนก่อนรับบริการ API จากระบบผู้ให้บริการ (Provider System) ตามมาตรฐาน TGIX

2.11 การยืนยันตัวตนด้วยมาตรฐาน Open ID Connect หมายความว่า กระบวนการยืนยันตัวตนด้วยวิธีการใช้ Open ID Connect ซึ่งระบบผู้ใช้บริการ (Consumer System) ดำเนินการยืนยันตัวตนก่อนรับบริการ API จากระบบผู้ให้บริการ (Provider System) ตามมาตรฐาน TGIX

2.12 ประเภทการให้สิทธิ์ (Grant Type) หมายความว่า ประเภทการให้สิทธิ์ระหว่างระบบผู้ใช้บริการ (Consumer System) และผู้พิสูจน์และยืนยันตัวตน (Identity Provider) เมื่อมีการเลือกใช้มาตรฐาน OAuth 2.0 ในการยืนยันตัวตนก่อนเรียกใช้บริการ API ไปยังระบบผู้ให้บริการ (Provider System)

2.13 การให้สิทธิ์ (Authorization) หมายความว่า กลไกที่ระบบให้สิทธิ์หรือเพิกถอนสิทธิ์ในการเข้าถึงข้อมูลหรือดำเนินการบางอย่างในระบบ เช่นผู้ใช้งานจะต้องดำเนินการยืนยันตัวตนก่อนจึงจะเข้าถึงข้อมูลของระบบได้ เป็นต้น

2.14 การควบคุมสิทธิ์ (Access Control) หมายความว่า กลไกที่ระบบควบคุมสิทธิ์และตรวจสอบสิทธิ์ตามบทบาทและหน้าที่ของผู้ใช้งาน

2.15 การควบคุมสิทธิ์ในการเข้าถึง API (API Access Control) หมายความว่า การควบคุมสิทธิ์ในการเข้าถึง API ด้วยวิธีการควบคุมสิทธิ์และการตรวจสอบสิทธิ์ตามบทบาทและหน้าที่ของผู้ใช้งาน API โดยวิธีที่แนะนำคือ Role-Based Access Control (Role-Based Access Control) อ้างอิงจาก INCITS 359-2012 [R2017]

2.16 การบริหารจัดการบัญชีผู้ใช้งาน API (API User Account) หมายความว่า ระเบียบปฏิบัติในการที่ระบบผู้ใช้บริการ (Consumer System) ใช้สำหรับยืนยันตัวตนเพื่อใช้บริการ API ของระบบผู้ให้บริการ (Provider System) แบ่งประเภทบัญชีได้ตามประเภทการยืนยันตัวตนได้ 3 ประเภทบัญชี คือ บัญชีใช้งานประเภท API Key ใช้สำหรับการยืนยันตัวตนด้วย API Key บัญชีใช้งาน Identity Provider ที่รองรับมาตรฐาน OAuth 2.0 และบัญชีใช้งาน Identity Provider ที่รองรับมาตรฐาน Open ID Connect

2.17 ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) หมายความว่า ระบบสารสนเทศของหน่วยงานหรือของผู้ให้บริการแพลตฟอร์ม TGIX สำหรับผู้รับลงทะเบียนและผู้พิสูจน์ตัวตน และการบริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการโดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้

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

2.19 ต้อง (Must) หมายความว่า ผู้ดำเนินการต้องทำตามข้อกำหนดในมาตรฐานฯ

2.20 ควร (Should) หมายความว่า ผู้ดำเนินการควรทำตามข้อกำหนดในมาตรฐานฯ

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

3.1 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 [6]

มาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชน ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอ ที่จะเกิดการบูรณาการร่วมกัน

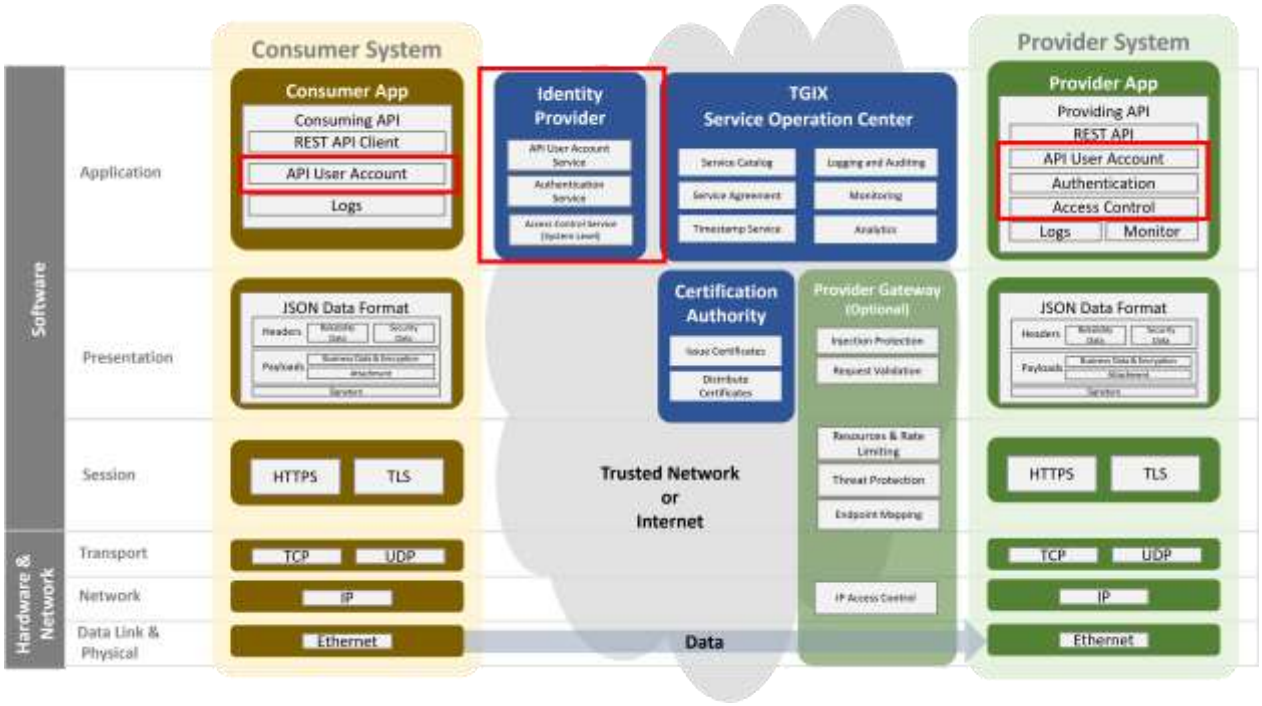
มาตรา 15 ระบุว่า ให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ
(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด
(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล
(4) เรื่องอื่นๆ ตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลมอบหมาย

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

4. ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์ และบัญชีการใช้งาน

การยืนยันตัวตน (Authentication) การควบคุมสิทธิ์ (Access Control) และบัญชีการใช้งาน (Accounting) เป็นองค์ประกอบสำคัญของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ดังรูปที่ 1 องค์ประกอบเหล่านี้ช่วยให้ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) เชื่อมโยงและแลกเปลี่ยนข้อมูลได้อย่างปลอดภัย



รูปที่ 1 ภาพรวมองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

4.1. การยืนยันตัวตน (Authentication)

การยืนยันตัวตนเพื่อขอใช้บริการการแลกเปลี่ยนข้อมูล หมายถึง กระบวนการที่ระบบผู้ใช้บริการ (Consumer System) ทำการยืนยันตัวตนเพื่อขอใช้บริการ API ของระบบผู้ให้บริการ (Provider System) ที่เป็น REST API แนวทางในการยืนยันตัวตนตามมาตรฐานฯ มี 3 วิธีคือ API Key, OAuth 2.0 และ Open ID Connect ซึ่งหน่วยงานที่เกี่ยวข้องสามารถพิจารณาเลือกตามความเหมาะสมของความต้องการในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

อย่างไรก็ตามหน่วยงานสามารถพิจารณาเลือกใช้มาตรฐานรูปแบบอื่นๆ ที่อยู่นอกเหนือมาตรฐานฯ เช่น 2-Factor Authentication, แบบ Multi-Factor Authentication เป็นต้น รวมทั้งสามารถพิจารณาดำเนินการตามมาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ

4.2. การยืนยันตัวตนด้วย API Key

API Key ใช้เพื่อยืนยันว่าระบบผู้ใช้บริการ (Consumer System) ต้องการขอเข้าถึง API แบบ REST API ของระบบผู้ให้บริการ (Provider System) แต่ไม่ได้ต้องการการยืนยันตัวตนระดับผู้ใช้งาน ของระบบผู้ใช้บริการ (Consumer System) ดังนั้น ในด้านความปลอดภัยจะเพียงพอสำหรับการเข้าถึง API ที่เป็นบริการ API ทั่วไปในหน่วยงานของระบบผู้ให้บริการ (Provider System) โดยข้อมูลเหล่านั้นสามารถเข้าถึงด้วย API โดยที่ไม่ต้องยืนยันตัวตนระดับบุคคลหรือองค์กร

ในกรณีที่ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) พิจารณาเลือกการยืนยันตัวตนด้วย API Key สามารถดำเนินการการตามขั้นตอนในภาคผนวก ก.1 ขั้นตอนการยืนยันตัวตนด้วย API Key

4.3. การยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0

OAuth 2.0 เป็นการรวมกระบวนการยืนยันตัวตนและจัดการสิทธิ์ให้เข้าถึงข้อมูลเข้าด้วยกัน ตามมาตรฐาน The OAuth 2.0 Authorization Framework: Bearer Token Usage: RFC-6749 [1] , RFC-6750 [2] มาตรฐาน OAuth 2.0 สามารถใช้ยืนยันตัวตนระดับผู้ใช้งานระบบได้ ดังนั้นจึงเหมาะสมในการเข้าถึง API ที่เป็นบริการเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลสำคัญของระบบผู้ให้บริการ (Provider System) รวมทั้ง API เชิงธุรกรรมประเภทที่เป็นการสร้าง ลบหรือแก้ไขข้อมูล โดยหลักการของ OAuth 2.0 จะเป็นการยืนยันตัวตนผู้ใช้งานในระบบ (End User) ของระบบผู้ใช้บริการ (Consumer System) กับระบบพิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับ OAuth 2.0 เพื่อให้ได้ Access Token ซึ่งกระบวนการดังกล่าวเรียกว่าการยืนยันตัวตนและให้สิทธิ์ (Grant Type) หลังจาก ระบบผู้ใช้บริการ (Consumer System) ได้รับ Access Token แล้วจะนำมาใช้ในการเข้าถึง API ของระบบผู้ให้บริการ (Provider System)

ในกรณีที่ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) พิจารณาเลือกการยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0 สามารถดำเนินการการตามขั้นตอนในภาคผนวก ก.2 ขั้นตอนการยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0

4.4. ขั้นตอนการดำเนินการเพื่อยืนยันตัวตนด้วยมาตรฐาน Open ID Connect

Open ID Connect (OIDC) เป็นมาตรฐานการยืนยันตัวตนที่ทำงานอยู่บนมาตรฐาน OAuth 2.0 โดยมีจุดเด่นคือการให้ระบบงานใช้ยืนยันตัวตนของผู้ใช้งานเพียงครั้งเดียวแล้วสามารถเข้าไปใช้งานระบบอื่นๆ ได้หลายระบบ (Single Sign On) พร้อมทั้งสามารถบริหารจัดการข้อมูลผู้ใช้งานโดยใช้ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับมาตรฐาน Open ID Connect ในขณะที่มาตรฐาน OAuth 2.0 จะเน้นการยืนยันตัวตนเพื่อให้สิทธิ์ในการเข้าถึงทรัพยากรต่างๆ เช่น API เป็นต้น

ดังนั้น ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) ที่ใช้มาตรฐาน TGIX แล้วมีความต้องการยืนยันตัวตนผู้ใช้งานเพียงครั้งเดียวแล้วสามารถเข้าไปใช้งานระบบของหน่วยงานอื่นๆ ในกลุ่มได้หลายระบบ (Single Sign On) สามารถเลือกยืนยันตัวตนสำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลผ่าน API ด้วยผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับมาตรฐาน Open ID Connect ด้วยเช่นกัน ซึ่งมีขั้นตอนการดำเนินการเดียวกันกับที่ใช้ในมาตรฐาน OAuth 2.0 ตามที่กล่าวในหัวข้อก่อนหน้านี้

สิ่งที่แตกต่างกับมาตรฐาน OAuth 2.0 ที่เพิ่มขึ้นมาในมาตรฐาน Open ID Connect คือระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) สามารถเรียกดูข้อมูลพื้นฐานของผู้ใช้งานด้วย ID Token ซึ่งเป็น Token ที่ผ่านการเข้ารหัสด้วย JSON Web Tokens (JWT) ทั้งนี้ขึ้นอยู่กับ ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ที่สมาชิกในกลุ่มเลือกใช้ดำเนินการ เช่น ID Token ที่เข้ารหัสด้วย JSON Web Token (JWT) ของ Microsoft Identity Platform [3]

eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJsd2VDYWhsVWpPTklwaTRqSmdZd29jTHBH
UnZHQk9uNThUSE1UeUJ5RUNrIn0.eyJleHAiOjE2NzkzOTkxNTYsImlhdCI6MTY3OTM5ODg1Niwian
RpIjoiMTJmNTc2M2EtZTMwYi00NjhkLWFlODYtMDFmNjljNTczMmQ3IiwiaXNzIjoiaHR0cHM6Ly90
Z2l4aWRwLXNhbmRib3guZGdhLm9yLnRoOjg0NDMvcmVhbG1zL3RnaXgiLCJzdWIiOiIyMTBjZGI1
Zi1kNTg5LTQyM2UtOTk1ZC0xZTE2YjBjM2VkOWQiLCJ0eXAiOiJCZWFyZXIiLCJhenAiOiJ0ZXN0X2
NsaWVudCIsInNlc3Npb25fc3RhdGUiOiJiMTA2NGM2Mi1hMTFiLTQ0YzQtYTAxOS1mYWYzZDFjZjFk
MGQiLCJhbGxvd2VkLW9yaWdpbnMiOlsiaHR0cHM6Ly90Z2l4YzAxLXNhbmRib3guZGdhLm9yLnR
oIiwidGdpeGMwMS5vbmV3ZWIudGVjaDo5NDQzIiwiaHR0cDovL3RnaXhjMDEtc2FuZGJveC5kZ2E
ub3IudGgiLCJodHRwOi8vbG9jYWxob3N0IiwiaHR0cDovL2xvY2FsaG9zdDozMDAwIl0sInNjb3BlIjoic
HJvZmlsZSBlbWFpbCIsInNpZCI6ImIxMDY0YzYyLWExMWItNDRjNC1hMDE5LWZhZjNkMWNmMW
QwZCJ9.NieEn-1JxRGlAM2FTHkVKXwiuflkZMBoUjKxKNS4kZu-
7BGKdkbe_UPJzgUWX8aqpGlv8Qu3J58VhewtDb1IkwRqDkpCFQI8Im6HUukouepUYK0rqvAphptr
QU2ynuGGsgZRmCPPP8okx-piXQh5PCcK3JqVFxCquySXYSr2_hGRACaT3-
HYBf1hiphVqwj5o3PVa3jJav8ZjEpvq7r5QdMXEUznLTDDavNcY_vPpyISJps5rn6uvWKcP2pvxpgow
F43vtIufQrCnAZ-
rMEb3LsV1MN3MYWujpRgDaY0gZZ2ANDDEhdxEemAk03vOoIfPiXlUzL72X8qasefhwrkBQ

เมื่อถอดรหัสแล้วจะมีข้อมูลคือ


```
{
  "alg": "RS256",
  "typ": "JWT",
```

```
  "kid": "lweCahlUjONIpi4jJgYwocLpGRvGBOn58THMTyByECk"
}.{
  "exp": 1679399156,
  "iat": 1679398856,
  "jti": "12f5763a-e30b-468d-ae86-01f69c5732d7",
  "iss": "https://tgixidp-sandbox.dga.or.th:8443/realms/tgix",
  "sub": "210cdb5f-d589-423e-995d-1e16b0c3ed9d",
  "typ": "Bearer",
  "azp": "test_client",
  "session_state": "b1064c62-a11b-44c4-a019-faf3d1cf1d0d",
  "allowed-origins": [
    "https://tgixc01-sandbox.dga.or.th",
    "tgixc01.oneweb.tech:9443",
    "http://tgixc01-sandbox.dga.or.th",
    "http://localhost",
    "http://localhost:3000"
  ],
  "scope": "profile email",
  "sid": "b1064c62-a11b-44c4-a019-faf3d1cf1d0d"
}.[Signature]
```


การเข้ารหัสด้วย JSON Web Token (JWT) มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน

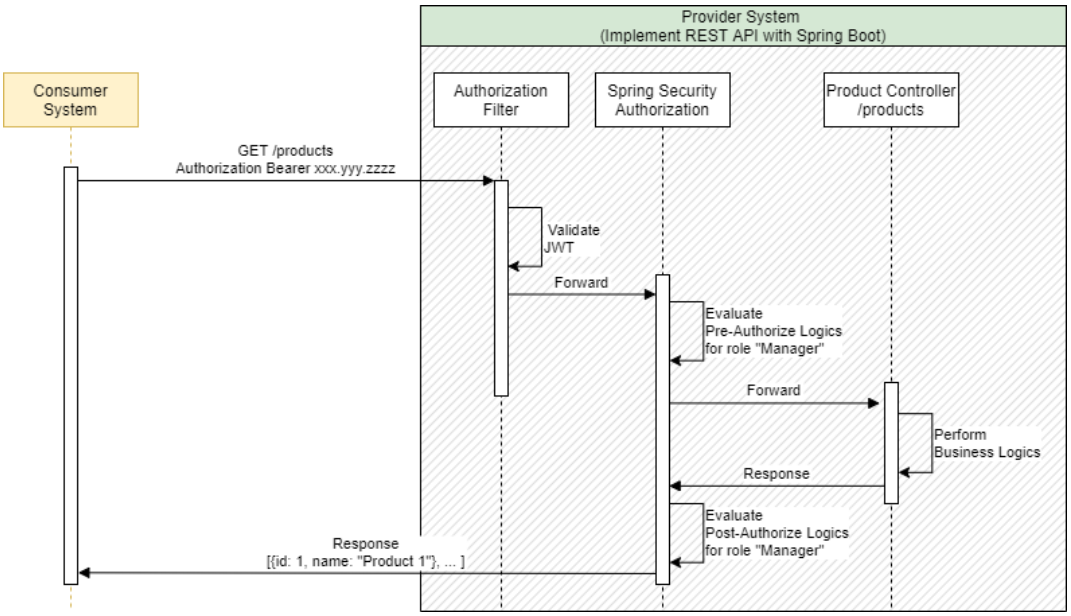
4.5. การควบคุมสิทธิ์ในการเข้าถึง API (API Access Control)

การควบคุมสิทธิ์ในการเข้าถึง API ตามมาตรฐาน TGIX มีจุดประสงค์เพื่อให้ระบบผู้ให้บริการ (Provider System) มั่นใจว่าเฉพาะระบบหรือบุคคลที่ได้รับอนุญาตเท่านั้นถึงจะเข้าถึง API ได้ มีข้อกำหนดดังต่อไปนี้

(1) ระบบผู้ให้บริการ (Provider System) ต้องตรวจสอบว่า มีเฉพาะระบบผู้ใช้บริการ (Consumer System) ที่ผ่านการยืนยันตัวตนเท่านั้นที่มีสิทธิ์เข้าถึง API ของระบบผู้ให้บริการ (Provider System) ตามรายละเอียดการยืนยันตัวตน

(2) ระบบผู้ให้บริการ (Provider System) ควรออกแบบและพัฒนาการควบคุมสิทธิ์และการตรวจสอบสิทธิ์ตามบทบาทและหน้าที่ของผู้ใช้งาน API ด้วยวิธี Role-Based Access Control (RBAC) อ้างอิง

จาก INCITS 359-2012[R2017] Information technology - Role Based Access Control [4] ผู้ใช้งาน API ที่กล่าวถึงนั้นสามารถเป็นระดับของระบบผู้ใช้บริการ (Consumer System) หรือระดับบุคคลผู้ใช้งาน (End User) ในระบบของระบบผู้ใช้บริการ (Consumer System) ทั้งนี้ขึ้นอยู่กับความต้องการทางธุรกิจ (Business Requirement) ของ API และภาษาโปรแกรมที่ใช้พัฒนา API ดังตัวอย่างขั้นตอนตรวจสอบสิทธิ์แบบ Role-Based Access Control (RBAC) ของ REST API ด้วยภาษาจาวาโดยใช้ Spring Boot และ JWT



รูปที่ 2 ตัวอย่างขั้นตอนตรวจสอบสิทธิ์ภาษาจาวาโดยใช้ Spring Boot และ JWT

ในตัวอย่างข้างต้น เมื่อระบบผู้ใช้บริการ (Consumer System) เรียกใช้ API GET /products ระบบผู้ให้บริการ (Provider System) จะตรวจสอบสิทธิ์แล้วพบว่าเป็น Role ชื่อ Manager จึงดำเนินการตามเงื่อนไขทางธุรกิจแล้วส่งข้อมูลกลับไปให้ระบบผู้ใช้บริการ (Consumer System)

4.6. การบริหารจัดการบัญชีการใช้งาน (API Accounting)

บัญชีการใช้งานหมายถึงบัญชีที่ระบบผู้ใช้บริการ (Consumer System) ใช้สำหรับยืนยันตัวตนเพื่อใช้บริการ API ของระบบผู้ให้บริการ (Provider System) แบ่งประเภทบัญชีได้ตามประเภทการยืนยันตัวตนได้ 3 ประเภทบัญชี คือ

4.6.1 บัญชีใช้งานประเภท API Key ใช้สำหรับการยืนยันตัวตนด้วย API Key

เมื่อระบบผู้ให้บริการ (Provider System) กำหนดให้ API มีการยืนยันตัวตนด้วยบัญชีการใช้งานประเภท API Key ทั้งระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) ต้องดำเนินการ

บริหารจัดการบัญชีการใช้งานให้มีความปลอดภัย ทั้งระหว่างการจัดเก็บและการรับส่งข้อมูล API Key โดยมีแนวทางปฏิบัติดังนี้

(1) ระบบผู้ให้บริการ (Provider System) ต้องเก็บรักษา API Key ไว้ในที่ปลอดภัย เช่น เก็บไว้ฐานข้อมูลโดยทำการใส่ Prefix และ Hash ค่าของ API Key ดังที่กล่าวไว้ในข้อ ก.1 ขั้นตอนการยืนยันตัวตนด้วย API Key

(2) ระบบผู้ใช้บริการ (Consumer System) ไม่ควรกำหนด API Key ไว้ใน Source Code ซึ่งอาจจะเกิดความผิดพลาดขณะแชร์ Source Code ให้กับบุคคลอื่นได้ ให้เก็บไว้ใน Environment Variable หรือ File หรือที่อื่นๆ ที่ไม่อยู่ใน Source Code หลัก รวมทั้งทำการ Hash ของมูล API Key ก่อนเก็บเสมอ

(3) ระบบผู้ให้บริการ (Provider System) ควรออกแบบและพัฒนา API ให้สามารถกำหนด Access Control ของแต่ละ API Key ที่มอบให้แก่ผู้ขอใช้บริการ API ได้

(4) ระบบผู้ให้บริการ (Provider System) ควรออกแบบและพัฒนา API ให้สามารถกำหนดวันหมดอายุของ API Key ได้

(5) ระบบผู้ให้บริการ (Provider System) ควรใช้ API Key ใน API ประเภทที่เป็นการอ่านข้อมูลเท่านั้น เนื่องจาก API Key ส่วนข้อมูลประเภทที่เป็นการสร้าง ลบหรือแก้ไขข้อมูล ควรใช้การยืนยันตัวตนระดับบุคคลหรือองค์กรร่วมด้วย เช่น OAuth 2.0 เป็นต้น

(6) ระบบผู้ให้บริการ API ควรให้บริการ REST API ผ่าน HTTPS (TLS) เท่านั้น

(7) ทั้งระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) ควรมีการทดสอบความปลอดภัยของระบบเพื่อหาช่องโหว่ที่เกิดจากการใช้ API Key ก่อนการใช้งานจริง เช่น ทดสอบเจาะระบบตามหัวข้อของ OWASP API Security [5]

4.6.2 บัญชีใช้งาน Identity Provider ที่รองรับมาตรฐาน OAuth 2.0

เมื่อระบบผู้ให้บริการ (Provider System) กำหนดให้ API มีการยืนยันตัวตนด้วยบัญชีการใช้งานประเภท OAuth 2.0 ทั้งระบบผู้ให้บริการ (Provider System) ระบบผู้ใช้บริการ (Consumer System) และหน่วยงานผู้บริการ TGIX Platform เพื่อเชื่อมโยงและแลกเปลี่ยนข้อมูล จะต้องดำเนินการดังต่อไปนี้

(1) หน่วยงานผู้บริการ TGIX Platform ดำเนินการจัดเตรียมระบบพิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับมาตรฐาน OAuth 2.0

(2) หน่วยงานผู้บริการ TGIX Platform ดำเนินการรับลงทะเบียนบัญชีผู้ใช้งาน

(3) ผู้ให้บริการ API (Provider System) ต้องให้บริการ REST API ผ่าน HTTPS (TLS) เท่านั้น

(4) Access Token ควรมีระยะเวลาการใช้งานได้จำกัด ซึ่งผู้ขอใช้บริการ API จะต้องเรียกใช้บริการ API ก่อนที่ Access Token จะหมดอายุ มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยน

ข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

(5) เมื่อ Access Token ใกล้หมดอายุผู้ให้บริการ API สามารถเรียก Refresh Token เพื่อขอต่ออายุ Access Token ได้ มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

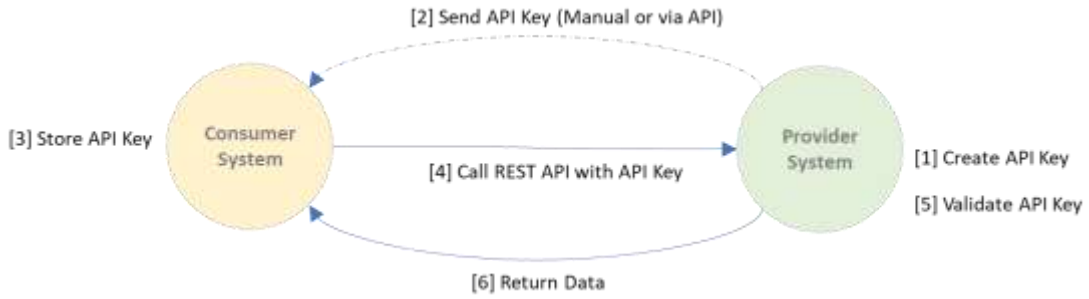
4.6.3 บัญชีใช้งาน Identity Provider ที่รองรับมาตรฐาน Open ID Connect

กรณีที่ระบบผู้ให้บริการ (Provider System) กำหนดให้ API มีการยืนยันตัวตนด้วยบัญชีการใช้งานประเภท Open ID Connect ทั้งระบบผู้ให้บริการ (Provider System) ระบบผู้ใช้บริการ (Consumer System) และหน่วยงานผู้บริการ TGIX Platform จะมีการดำเนินการเหมือนกับใช้มาตรฐาน OAuth 2.0

ภาคผนวก ก ขั้นตอนการยืนยันตัวตน

ก.1 ขั้นตอนการยืนยันตัวตนด้วย API Key

ในด้านเทคนิคนั้น API Key เป็นค่าที่สร้างขึ้นแบบไม่ซ้ำกันโดยระบบผู้ให้บริการ (Provider System) แล้วส่งมอบให้ระบบผู้ใช้บริการ (Consumer System) เก็บไว้ใช้ในการยืนยันตัวตนระหว่างเรียกใช้งาน REST API ของระบบผู้ให้บริการ (Provider System) ดัง**รูปที่ 3**



รูปที่ 3 ขั้นตอนการดำเนินการเพื่อยืนยันตัวตนด้วย API Key

ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) มีขั้นตอนการดำเนินการดังต่อไปนี้

ขั้นตอนที่ ก.1.1: การสร้าง API Key (Create API Key)

ในขั้นตอนนี้ ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการสร้าง API Key ดังรูปที่ 3 ซึ่งในแต่ละ API นั้น ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการสร้าง API Key ให้มีค่าไม่ซ้ำกัน โดยวิธีการที่แนะนำคือการสุ่มด้วยวิธีการ Secure Random จากภาษาโปรแกรมที่ใช้พัฒนาระบบ เช่น โปรแกรมภาษา Java ดังนี้

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;
import org.apache.commons.codec.binary.Base64; public class SampleGenerateAPIKey {
    public static void main(String[] args) {
        try {
            SampleGenerateAPIKey s = new SampleGenerateAPIKey();
            String prefix = SampleGenerateAPIKey.getSecureRandom(32).substring(0,7),key =
SampleGenerateAPIKey.getSecureRandom(32);
            System.out.println("API key: " + s.genAPIKey(prefix, key));
        } catch (NoSuchAlgorithmException e) {
        }
    }

    public static String filter(String source) {
        return source.replaceAll("/", "").replaceAll("\\+", "").replaceAll("=", "").replaceAll("\\\\", "");
    }
```

```
    public static String getSecureRandom(int bytesLength) throws NoSuchAlgorithmException{
        byte[] sRandomBytes = new byte[bytesLength];
        SecureRandom.getInstance("SHA1PRNG").nextBytes(sRandomBytes);
        return filter((new Base64()).encodeToString(sRandomBytes));
    }

    public String genAPIKey(String prefix, String key) throws NoSuchAlgorithmException{
        return prefix + "." + filter(
                (new Base64())
                        .encodeToString(MessageDigest
                                .getInstance("SHA-256")
                                .digest((prefix + key)
                                        .getBytes(StandardCharsets.UTF_8))));
    }
}
```

ผลลัพธ์ที่ได้จากตัวอย่างข้างต้นคือ API Key ที่มีค่าดังนี้

API Key : Lhyz7fW.0MFHlBmWWVhoLZWSmNXBW8lugbOwkTtHy76BEQ ซึ่งประกอบด้วย Prefix คือ Lhyz7fW และ Key คือ 0MFHlBmWWVhoLZWSmNXBW8lugbOwkTtHy76BEQ

หลังจากได้ค่า API Key แล้ว ระบบผู้ให้บริการ (Provider System) ควรเก็บรักษา API Key ไว้ในที่ปลอดภัย เช่น เก็บไว้ในฐานข้อมูลโดยทำการใส่ Prefix และ Hash ค่าของ API Key ด้วยภาษาโปรแกรมที่ใช้พัฒนาระบบ ดังนี้

API Key : {prefix}.{hash_of_whole_api_key}

นอกจากนี้ ระบบผู้ให้บริการ (Provider System) ควรระบุได้ว่ามีการส่งมอบ API Key ให้กับระบบผู้ใช้บริการ (Consumer System) ใดแล้วบ้าง พร้อมทั้งมีการกำหนดวันหมดอายุของ API Key สามารถกำหนดค่าตั้งต้นให้ไม่มีวันหมดอายุ แต่ควรสามารถปรับเปลี่ยนให้มีวันหมดอายุตามความเหมาะสมของ API ได้ นอกจากนี้ ควรสร้าง API Key ได้ใหม่เมื่อมีการร้องขอจากระบบผู้ใช้บริการ (Consumer System)

ขั้นตอนที่ ก.1.2: การส่งมอบ API Key (Send API Key)

ในขั้นตอนนี้ ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการส่งมอบ API Key ให้กับระบบผู้ใช้บริการ (Consumer System) ดังรูปที่ 3 ซึ่งการส่งมอบ API Key นั้น เกิดขึ้นหลังจากระบบผู้ให้บริการ (Provider System) ทำข้อตกลงเพื่อใช้บริการ API (Service Agreement) กับระบบผู้ใช้บริการ (Consumer System) ที่ TGIX Service Operation Center ซึ่งดูแลโดยหน่วยงานผู้บริการ TGIX Platform เรียบร้อยแล้ว โดยมีรายละเอียดตามมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการ

เชื่อมโยงข้อมูล ซึ่งระบบผู้ให้บริการ (Provider System) สามารถเลือกดำเนินการส่ง API Key ผ่านช่องทางต่างๆ ได้ตามความเหมาะสมและงบประมาณของหน่วยงาน เช่น

- ส่งผ่านอีเมล
- สร้าง API สำหรับส่ง API Key
- พัฒนาหน้าจอสำหรับให้ระบบผู้ใช้บริการ (Consumer System) มารับ API Key

ขั้นตอนที่ ก.1.3: การเก็บรักษา API Key (Store API Key)

ในขั้นตอนนี้ ระบบผู้ใช้บริการ (Consumer System) ต้องดำเนินการเก็บรักษา API Key ดังรูปที่ 3 ซึ่งหลังจากได้รับมอบ API Key แล้วนั้น ระบบผู้ใช้บริการ (Consumer System) ควรเก็บรักษา API Key ไว้ในที่ปลอดภัย ไม่ควรกำหนด API Key ไว้ใน Source Code ซึ่งอาจจะเกิดความผิดพลาดขณะแชร์ Source Code ให้กับบุคคลอื่นได้ ระบบผู้ใช้บริการ (Consumer System) ควรเก็บ API Key ไว้ใน Environment Variable หรือ File หรือที่อื่นๆ ที่ไม่อยู่ใน Source Code หลัก รวมทั้งทำการ Hash ของข้อมูล API Key ก่อนเก็บเสมอ

ขั้นตอนที่ ก.1.4: การยืนยันตัวตนและเรียก API ด้วย API Key (Call REST API with API Key)

ในขั้นตอนนี้ ระบบผู้ใช้บริการ (Consumer System) ต้องดำเนินการการยืนยันตัวตนเพื่อเรียกใช้บริการ REST API ด้วย API Key ดังรูปที่ 3 ซึ่งเกิดขึ้นเมื่อได้รับ API Key แล้วระบบผู้ใช้บริการ (Consumer System) จะต้องดำเนินการส่งข้อมูล API Key เพื่อยืนยันตัวตนระหว่างเรียกใช้บริการ REST API ไปยังระบบผู้ให้บริการ (Provider System) โดยระบบผู้ใช้บริการ (Consumer System) สามารถดำเนินการตามที่ได้ตกลงไว้กับระบบผู้ให้บริการ (Provider System) จากวิธีต่อไปนี้

(1) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Authorization Header ขณะเรียกใช้ REST API ตัวอย่างเช่น

```
Authorization: Apikey 1234567890abcdef
```

(2) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Basic Authentication ของ REST API ตัวอย่าง Curl Command เช่น

```
curl -X GET \
  'https://provider_server/endpoint/' \
-H 'authorization: Basic 1234567890abcdef '
```

(3) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Body Data ขณะเรียกใช้ REST API ตัวอย่างเช่น

```
curl -X POST \
```

```
"https://provider_server/endpoint/" \
-H 'content-type: application/json' \
-d '{
        "api_key": "1234567890abcdef "
         }'
```

(4) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Query String ขณะเรียกใช้ REST API ตัวอย่างเช่น

```
curl -X GET "https://provider_server/api_endpoint/?api_key=1234567890abcdef '
```

ขั้นตอนที่ ก.1.5: การตรวจสอบความถูกต้องของ API Key (Validate API Key)

ในขั้นตอนนี้ ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการตรวจสอบความถูกต้องของ API Key ดัง**รูปที่ 3** ซึ่งเกิดขึ้นเมื่อระบบผู้ให้บริการ (Provider System) ได้รับการขอใช้บริการ API พร้อมด้วย API Key หลังจากนั้น ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการตรวจสอบความถูกต้องแล้วดำเนินการให้บริการ API ตามข้อมูลที่ถูกร้องขอ หรือปฏิเสธการให้บริการหาก API Key ไม่ถูกต้อง ซึ่งขั้นตอนนี้ผู้ให้บริการ API สามารถดำเนินการได้ตามความเหมาะสมของภาษาโปรแกรมที่ใช้พัฒนาระบบ

ขั้นตอนที่ ก.1.6: การตอบกลับผลการให้บริการ API (Return Data)

ในขั้นตอนนี้ ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการตอบกลับผลการให้บริการ API ดังรูปที่ 3 ซึ่งเกิดขึ้นเมื่อระบบผู้ให้บริการ (Provider System) ตรวจสอบความถูกต้องของ API Key แล้วดำเนินการให้บริการ API ตามข้อมูลที่ถูกร้องขอสำเร็จ ควรตอบกลับด้วย HTTP Code 200 ตามตัวอย่างนี้ หรือ HTTP Code อื่นๆ ตามความเหมาะสม

```
        “messageStatus": {
         “status": “200",
         “description": " REST API successfully carried out the client requested"
}
```

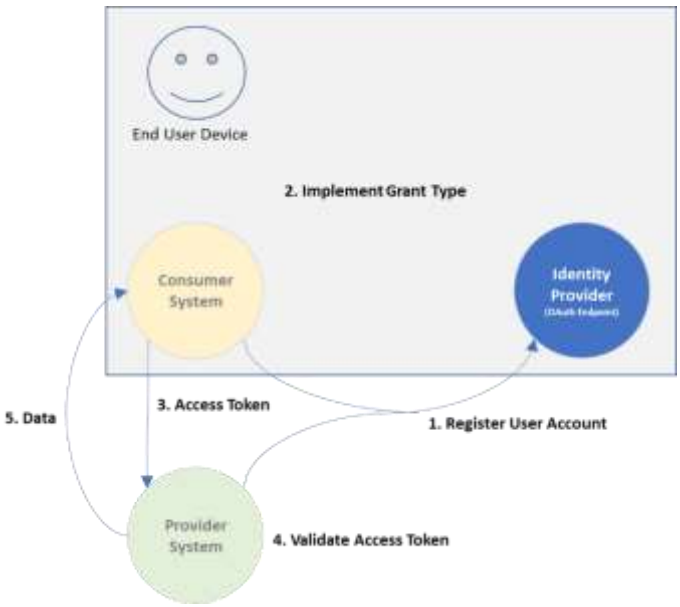
กรณีต้องการปฏิเสธการให้บริการ เนื่องจาก API Key ไม่ถูกต้อง ควรตอบกลับด้วย HTTP Code 401 ตามตัวอย่างต่อไปนี้

```
“messageStatus": {
        “status": “401",
        “description": " Unauthorized - ApiKey invalid or ApiKey not found"
```

```
}
```

ก.2 ขั้นตอนการยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0

ระบบพิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับ OAuth 2.0 ระบบผู้ใช้บริการ (Consumer System) และระบบผู้ให้บริการ (Provider System) มีขั้นตอนการดำเนินการดังนี้



รูปที่ 4 ภาพรวมของการยืนยันตัวตนด้วย OAuth 2.0

ขั้นตอนที่ ก.2.1 การลงทะเบียนบัญชีผู้ใช้งาน (Register User Account)

ในขั้นตอนนี้ ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) ดำเนินการแจ้งความประสงค์ขอลงทะเบียนบัญชีใช้งานที่ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ซึ่งดูแลโดยหน่วยงานผู้บริการ TGIX Platform ดังรูปที่ 4 ขั้นตอนนี้จะเกิดขึ้นหลังจากที่ระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) ทำข้อตกลงเพื่อใช้บริการ API (Service Agreement) ไว้ที่ TGIX Service Operation Center เรียบร้อยแล้ว

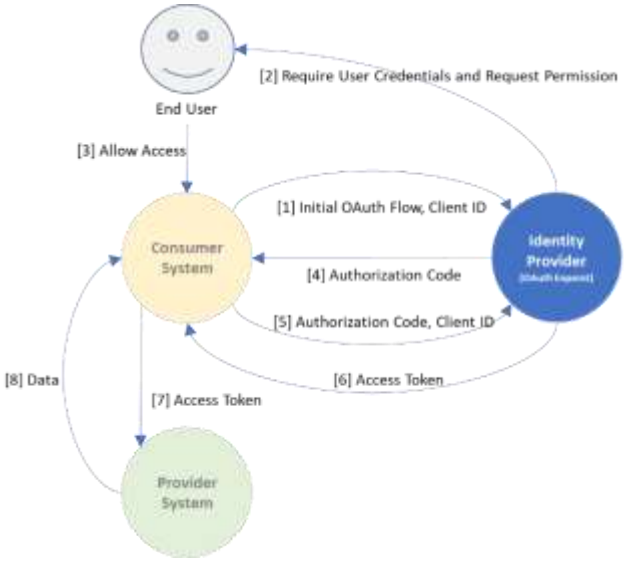
วิธีดำเนินการในขั้นตอนนี้ขึ้นอยู่กับ Identity Provider ที่สมาชิกในกลุ่ม TGIX และหน่วยงานผู้บริการ TGIX Platform ตกลงกันเลือกใช้ดำเนินการเพื่อบริหารจัดการบัญชีผู้ใช้งาน

ขั้นตอนที่ ก.2.2: การยืนยันตัวตนเพื่อให้ได้ Access Token (Implement Grant Type)

ขั้นตอนนี้ ระบบผู้ใช้บริการ (Consumer System) ต้องดำเนินการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (Identity Provider) เพื่อให้ได้ Access Token ดังกรอบสีเทาในรูปที่ 4 ซึ่งในมาตรฐาน OAuth 2.0 มีประเภทการยืนยันตัวตนและให้สิทธิ์ (Grant Type) ซึ่งระบบผู้ใช้บริการ (Consumer System) สามารถเลือกดำเนินการได้ตามความเหมาะสมของภาษาโปรแกรมที่ใช้พัฒนาและงบประมาณที่มี โดยเลือกได้จาก 4 ประเภท ได้แก่

(1) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Authorization Code

Authorization Code เป็น Grant type ประเภทที่ระบบผู้ใช้บริการ (Consumer System) ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (Identity Provider) โดยนำ Authorization Code มาแลกเปลี่ยนเป็น Access Token

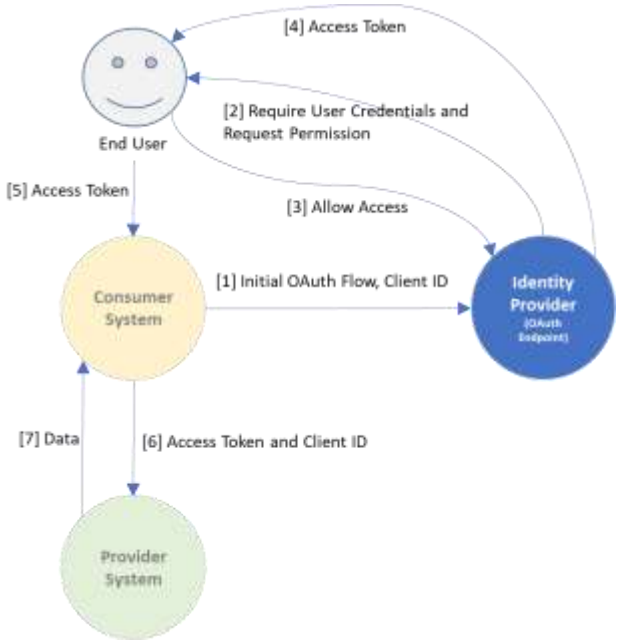


รูปที่ 5 ขั้นตอนการยืนยันตัวตนด้วย Grant Type ประเภท Authorization Code

จากลำดับที่ [1] – [6] ในรูปที่ 5 นั้นระบบผู้ใช้บริการ (Consumer System) สามารถเลือกดำเนินการเพื่อให้ได้ Access Token ตามหลักการใน OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.1 [6]

(2) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Implicit

Implicit จะมีความคล้ายกับแบบ Authorization Code แต่ต่างกันที่ระบบผู้ใช้บริการ (Consumer System) ไม่ต้องดำเนินการส่ง Authorization Code แล้วไปขอ Access Token อีกที แต่จะได้ Access Token กลับมาผ่านทาง Query String จากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ในคราวเดียว

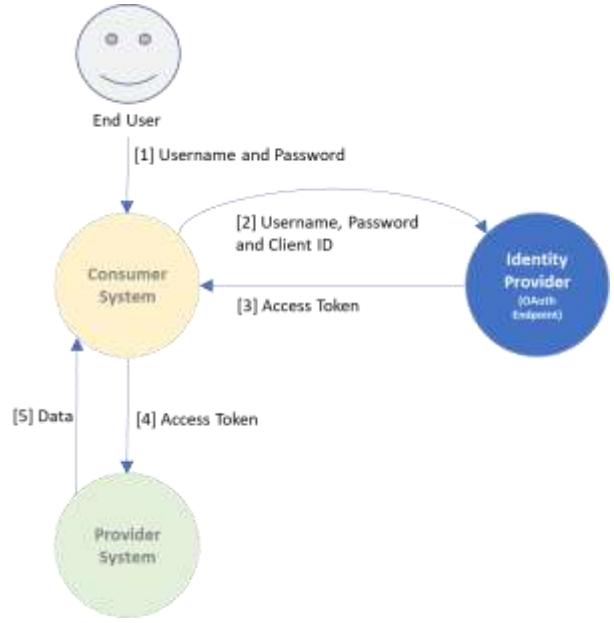


รูปที่ 6 ขั้นตอนการยืนยันตัวตนด้วย Grant Type ประเภท Implicit

จากลำดับที่ [1] – [5] ในรูปที่ 6 นั้นระบบผู้ใช้บริการ (Consumer System) สามารถเลือกดำเนินการเพื่อให้ได้ Access Token ตามหลักการใน OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.2 [7]

(3) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Resource Owner Password

เป็นการยืนยันตัวตนและขอสิทธิ์โดย ผู้ใช้งานระบบของระบบผู้ใช้บริการ (Consumer System) จะให้ Username และ Password กับระบบผู้ใช้บริการ (Consumer System) โดยตรง เพื่อนำไปขอ Access Token จากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ดังนี้

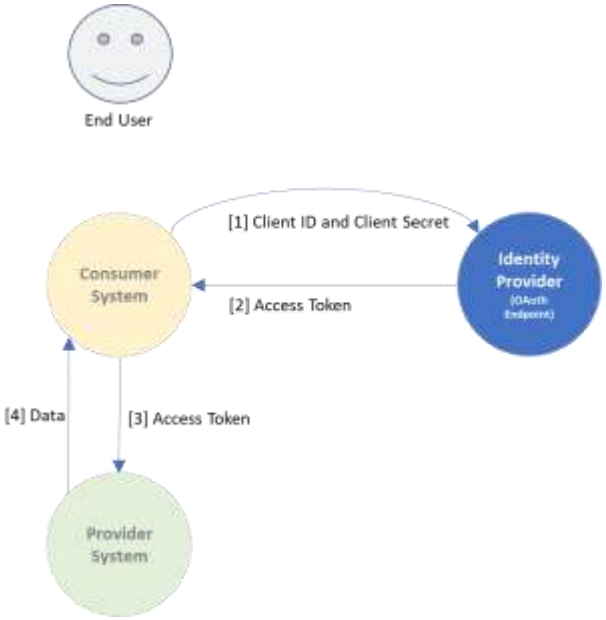


รูปที่ 7 ขั้นตอนการยืนยันตัวตนด้วย Grant Type ประเภท Resource owner password

จากลำดับที่ [1] – [3] ในรูปที่ 7 นั้นระบบผู้ใช้บริการ (Consumer System) สามารถเลือกดำเนินการเพื่อให้ได้ Access Token ตามหลักการใน OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.3 [8]

(4) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Client Credentials

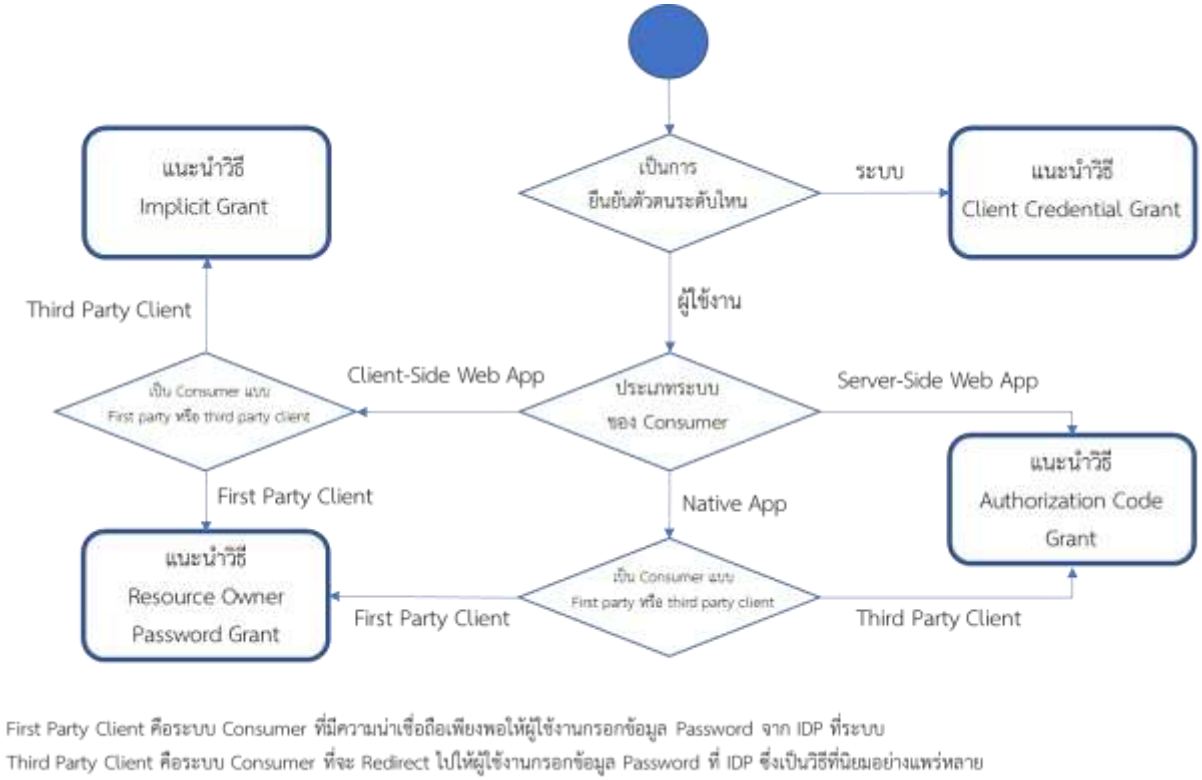
เป็นการยืนยันตัวตนและขอสิทธิ์โดยระบบผู้ใช้บริการ (Consumer System) จะใช้ Client ID และ Client Secret ในการส่งไปขอ Access Token ที่ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) โดยจะเป็นการขอระหว่าง Server ไปยัง Server โดยตรง



รูปที่ 8 ขั้นตอนการยืนยันตัวตนด้วย Grant Type ประเภท Client Credentials

จากลำดับที่ [1] – [2] ในรูปที่ 8 นั้นระบบผู้ใช้บริการ (Consumer System) สามารถเลือกดำเนินการเพื่อให้ได้ Access Token ตามหลักการใน OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.4 [9]

แนวทางในการเลือกประเภท Grant Type ขึ้นอยู่กับประเภทข้อมูลต่างๆ ของระบบผู้ใช้บริการ (Consumer System) ได้แก่ ผู้ถือข้อมูลการยืนยันตัวตน และลักษณะ Application ของระบบผู้ใช้บริการ (Consumer System) เป็น Web Application หรือ Native Application ดังรูปที่ 9



รูปที่ 9 แนวทางการเลือกดำเนินการ Grant Type

เมื่อระบบผู้ใช้บริการ (Consumer System) ดำเนินการเสร็จเรียบร้อย ผลลัพธ์ที่ระบบผู้ใช้บริการ (Consumer System) ได้รับคือ Access Token ที่ได้รับการเข้ารหัสด้วย JSON Web Tokens (JWT) เพื่อใช้ส่งให้กับระบบผู้ให้บริการ (Provider System) ในขณะเรียกใช้บริการ REST API ของระบบผู้ให้บริการ (Provider System) ตัวอย่าง Access Token ดังนี้

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token":"
eyJhbGciOiJIUzIINiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiodHRwOi8vbXktZG9tYWluLmF1dGgwLmNvSl
sInN1Yil6ImF1dGgwfDEyMzQ1NilsimF1ZCI6IjEyMzRhYmNKZWYiLCJleHAiOjEZMTEyODESNzAsIm
lhdCIGMTMxMTI4MDk3MCwibmFtZS|6lkphbmUgRGOlliwiZ2|2ZW5fomFtZS|6lkphbmUiLCJmYW
pbHfomFtZSI6IkRvZSJ9.bqljxtG9B_bielkqOnjTY9DI9FilFb6IMQINXoYs",
   "token_type":"example",
   "expires_in":3600,
```

```
"example_parameter":"example_value"
```

การดำเนินการแบบละเอียดเกี่ยวกับ JSON Web Tokens (JWT) มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

ขั้นตอนที่ ก.2.3: การเรียกใช้ REST API ด้วย Access Token (Call API with Access Token)

ขั้นตอนนี้ ระบบผู้ใช้บริการ (Consumer System) ต้องดำเนินการเรียกใช้บริการ REST API ของระบบผู้ให้บริการ (Provider System) ด้วย Access Token ดังรูปที่ 4 ซึ่งขั้นตอนนี้เกิดขึ้นหลังจากที่ระบบผู้ใช้บริการ (Consumer System) ได้รับ Access Token จากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) แล้วระบบผู้ใช้บริการ (Consumer System) สามารถนำ Access Token มาประกอบเป็นส่วนหนึ่งของ HTTP Authorization Request Header เพื่อเรียกใช้บริการ REST API จากระบบผู้ให้บริการ (Provider System) ดังตัวอย่างต่อไปนี้

```
GET /resource HTTP/1.1
    Host: server.example.com
    Authorization: Bearer
eyJhbGciOiJIUzIINiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiodHRwOi8vbXktZG9tYWluLmF1dGgwLmNvSlsI
nN1Yil6ImF1dGgwfDEyMzQ1NilsimF1ZCI6IjEyMzRhYmNKZWYiLCJleHAiOjEZMTEyODESNzAsImlh
dCIGMTMxMTI4MDk3MCwibmFtZS|6lkphbmUgRGOlliwiZ2|2ZW5fomFtZS|6lkphbmUiLCJmYWpb
HfomFtZSI6IkRvZSJ9.bqljxtG9B_bielkqOnjTY9DI9FilFb6IMQINXoYs
```

ขั้นตอนที่ ก.2.4: การตรวจสอบความถูกต้องของ Access Token (Validate Access Token)

ในขั้นตอนนี้ ระบบผู้ให้บริการ (Provider System) ต้องดำเนินการตรวจสอบความถูกต้องของ Access Token ว่าเป็น Access Token ที่ออกจากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) และเป็น Access Token ที่ไม่หมดอายุ แล้วดำเนินการให้บริการ API ตามที่ถูกร้องขอเมื่อ Access Token ถูกต้อง ดังรูปที่ 4 ซึ่งการตรวจสอบ Access Token มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

ขั้นตอนที่ ก.2.5: การตอบกลับผลการให้บริการ API (Return Data)

เมื่อระบบผู้ให้บริการ (Provider System) ตรวจสอบความถูกต้องของ Access Token แล้วดำเนินการให้บริการ API ตามข้อมูลที่ถูกร้องขอสำเร็จควรตอบกลับด้วย HTTP Code 200 ตามตัวอย่างนี้ หรือ HTTP Code อื่นๆ ตามความเหมาะสม ดังรูปที่ 4

```
        “messageStatus": {
         “status": “200",
         “description": " REST API successfully carried out the client requested"
}
```

แต่หากระบบผู้ให้บริการ (Provider System) ต้องการปฏิเสธการให้บริการกรณี Access Token ไม่ถูกต้องควรตอบกลับด้วย HTTP Code 401 ตามตัวอย่างต่อไปนี้

```
“messageStatus": {
         “status": “401",
         “description": " Unauthorized - Access Token invalid or Access Token not found"
}
```

บรรณานุกรม

[1] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[2] M. Jones. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework: Bearer Token Usage. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6750. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[3] Microsoft. (2021). Microsoft identity platform ID tokens. [ออนไลน์]. เข้าถึงได้จาก: https://docs.microsoft.com/en-us/azure/active-directory/develop/id-tokens. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[4] Information Technology Industry Council. (2017). Information technology - Role Based Access Control. [ออนไลน์]. เข้าถึงได้จาก: https://standards.incits.org/apps/group_public/project/details.php?project_id=1906. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[5] OWASP Foundation, Inc. (2019). OWASP API Security. [ออนไลน์]. เข้าถึงได้จาก: https://owasp.org/www-project-api-security/. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[6] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.1. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.1. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[7] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.2. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.2. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[8] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.3. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.3. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[9] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.4. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.4. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)