การพิสูจน์ตัวจริงอิงบทบาทสำหรับเว็บเซอร์วิสองค์กร

นายภูวนาถ กอบคำ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

Role-based Authentication for Organization Web Services

Mr. Poowanart Korbkum

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2015

หัวข้อวิทยานิพนธ์	การพิสูจน์ตัวจริงอิงบทบาทสำหรับเว็บเซอร์วิสองค์กร
โดย	นายภูวนาถ กอบคำ
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร. ญาใจ ลิ่มปิยะกรณ์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร. สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ศาสตราจารย์ ดร. บุญเสริม กิจศิริกุล)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร. ญาใจ ลิ่มปิยะกรณ์)

.....กรรมการภายนอกมหาวิทยาลัย
(อาจารย์ ดร. ภาสกร อภิรักษ์วรพินิต)

ภูวนาถ กอบคำ : การพิสูจน์ตัวจริงอิงบทบาทสำหรับเว็บเซอร์วิสองค์กร (Role-based Authentication for Organization Web Services) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร. ญาใจ ลิ่มปิยะกรณ์, 53 หน้า.

โดยปกติทั่วไป การพิสูจน์ตัวจริงจำเป็นต้องมีเพื่อป้องกันผู้ใช้ที่ไม่มีสิทธิ์เข้าถึงการใช้งาน นอกเหนือจากมิติการรักษาความปลอดภัยสำหรับการเข้าถึงเว็บเซอร์วิส การจำกัดสิทธิ์ผู้ใช้งานก็เป็นอีกสิ่งหนึ่งที่องค์กรต้องคำนึงถึง บริการพิสูจน์ตัวจริงดั้งเดิมแบบหนึ่งต่อหนึ่งไม่เพียงพอสำหรับการให้บริการผู้ใช้งานที่มีความหลากหลายและสามารถเข้าถึงบริการต่างๆ อย่างไม่จำกัดโดเมนได้อย่างมีประสิทธิผล งานวิจัยนี้จึงได้นำเสนอแนวทางการพัฒนาการบริการพิสูจน์ตัวจริงด้วยหลักคิดการควบคุมการเข้าถึงอิงบทบาท ส่วนของเอพีไอและเว็บเซอร์วิสการจัดการข้อมูลถูกพัฒนาขึ้นเพื่อสาธิตการใช้งานที่ยืดหยุ่นของเว็บเซอร์วิสบนโดเมนที่แตกต่างกัน

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2558

5770953621 : MAJOR COMPUTER SCIENCE
KEYWORDS: ROLE-BASED ACCESS CONTROL / PERMISSION / AUTHENTICATION / WEB SERVICES

POOWANART KORBKUM: Role- based Authentication for Organization Web Services. ADVISOR: ASSOC. PROF. DR. YACHAI LIMPIYAKORN, 53 pp.

Authentication is typically required to prevent unauthorized users. In addition to satisfy the security dimension, restricted permission grants are also in organization concerns for web services access. In order to effectively serve a wide range of users and enable accesses to various services by non-specified domains, the traditional one-to-one authentication service is not adequate. This research thus presents an approach to implementing the authentication service with the notion of role- based access control. The development includes the parts of API and Administration web service to demonstrate the flexible usage of web services on different domains.

Department: Computer Engineering Student's Signature .....
Field of Study: Computer Science Advisor's Signature .....
Academic Year: 2015

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณ รองศาสตราจารย์ ดร. ญาใจ ลิ่มปิยะกรณ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่เสียสละเวลาและช่วยเหลือในการให้คำปรึกษา คำแนะนำและข้อคิดเห็นที่มีเป็นประโยชน์ ทำให้การจัดทำวิทยานิพนธ์ให้สำเร็จลุล่วงไปด้วยดี ขอขอบพระคุณคณาจารย์ทุกท่านที่แนะนำสั่งสอน และให้ความรู้แก่ข้าพเจ้าตลอดระยะเวลาการศึกษา

ขอขอบพระคุณ ศาสตราจารย์ ดร. บุญเสริม กิจศิริกุล ประธานกรรมการสอบวิทยานิพนธ์ อาจารย์ ดร. ภาสกร อภิรักษ์วรพินิต กรรมการสอบวิทยานิพนธ์ ที่กรุณาให้คำแนะนำตรวจสอบ และแก้ไขวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณบิดา มารดา และญาติพี่น้องที่ให้การสนับสนุนและเป็นกาลังใจที่ดีให้เสมอมาและสนับสนุนด้านทุนทรัพย์ในการศึกษารวมไปถึงทุกท่านที่มีส่วนช่วยเหลือในการทำวิทยานิพนธ์ครั้งนี้ ซึ่งมิได้กล่าวนามในที่นี้

ท้ายที่สุด ผู้วิจัยขอขอบพระคุณเพื่อนๆ ทุกคน ที่คอยติดตามและให้กาลังใจ รวมถึงท่านอื่น ๆ ที่มิได้กล่าวลงนามไว้ ณ ที่นี้ที่มีส่วนทำให้วิทยานิพนธ์สำเร็จลุล่วงไปได้ด้วยดี ผู้วิจัยหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์บ้างไม่มากก็น้อยสำหรับผู้ที่สนใจจะศึกษารายละเอียดต่อไป

สารบัญ

หน้า

หน้า

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การเข้าใช้เว็บเซอร์วิส (Web Services) จำเป็นต้องมีการพิสูจน์ตัวจริง (Authentication) ของผู้ใช้ นอกจากเป็นการรักษาความปลอดภัยของระบบ ยังเป็นการจำกัดสิทธิ์การใช้งานของผู้ใช้ด้วย เว็บเซอร์วิสในปัจจุบันมีการพิสูจน์ตัวจริงของผู้ใช้งานอยู่หลายรูปแบบ ที่เห็นได้ทั่วไปคืองานบริการพิสูจน์ตัวจริงที่เว็บเซอร์วิสสร้างขึ้นมาใช้เองโดยการให้ผู้ใช้งานลงทะเบียน (Register) ก่อนเข้าใช้งานครั้งแรกเพื่อแลกกับสิทธิ์การเข้าใช้งานของผู้ใช้ การพิสูจน์ตัวจริงรูปแบบนี้เป็นการใช้งานแบบหนึ่งต่อหนึ่ง (One-to-One) โดยที่มีงานบริการพิสูจน์ตัวจริงหนึ่งบริการต่อเว็บเซอร์วิสหนึ่งเว็บเซอร์วิส อีกรูปแบบที่ได้รับความนิยมเป็นอย่างมากในตอนนี้คือ การใช้งานผ่านงานบริการการพิสูจน์ตัวจริง (Authentication Services) ที่เป็นบริการของผู้ให้บริการจากภายนอกเว็บเซอร์วิส หรือ SSO (Single Sign-on) ซึ่งรูปแบบการใช้งานคือ ผู้ใช้งานลงทะเบียนกับบริการพิสูจน์ตัวจริงเพียงครั้งเดียว สามารถใช้ได้กับทุกเว็บเซอร์วิสที่มีการรองรับบริการพิสูจน์ตัวจริงนี้ได้

ตัวอย่างงานบริการพิสูจน์ตัวจริงที่รู้จักกันโดยทั่วไปเช่น OpenID, Facebook และ Twitter เป็นต้น ผู้ใช้ที่ลงทะเบียนกับบริการเหล่านี้สามารถใช้เข้าใช้เว็บเซอร์วิสที่รองรับได้ในทันที งานบริการการพิสูจน์ตัวจริงรูปแบบนี้ เป็นการเพียงการพิสูจน์ตัวจริงในระดับต้น คือการทำให้ทราบว่าผู้ใช้งานสามารถเข้าใช้เว็บเซอร์วิสได้ แต่ไม่สามารถระบุได้ว่าผู้ใช้งานมีสิทธิ์เข้าในบริการตัวใดบ้าง หรือมีสิทธิ์ในเข้าถึงข้อมูลอะไรในบริการบ้าง ทำให้เว็บเซอร์วิสต้องเป็นผู้คอยกำหนดการอนุญาต (Permission) เข้าถึงสิทธิ์ต่าง ๆ ให้กับผู้เข้าใช้งานหลังจากผ่านการพิสูจน์ตัวจริงเสร็จสิ้น

องค์กรที่มีการบริการบนอินเทอร์เน็ตไว้ใช้ภายในองค์กร จำเป็นต้องมีการพิสูจน์ตัวจริงแบบครั้งเดียวแล้วสามารถเข้าถึงบริการต่าง ๆ ได้ โดยไม่จำกัดโดเมน การใช้เว็บเซอร์วิสที่มีอยู่อาจยังไม่เพียงพอสำหรับองค์กรที่มีผู้ใช้หลากหลายประเภทและต้องการความยืดหยุ่นในการกำหนดขอบเขตการเข้าถึงของกลุ่มผู้ใช้ต่าง ๆ ได้อย่างมีประสิทธิภาพ ด้วยความต้องการดังกล่าว การนำ RBAC model (Role-based Access Control model) [1, 2] เข้ามาพัฒนาการพิสูจน์ตัวจริงเพื่อทำให้สามารถจัดการผู้ใช้งานที่มีความหลากหลายได้ RBAC model เป็นแบบจำลองการควบคุมการเข้าถึงโดยอ้างอิงบทบาท โดยบทบาทเป็นการกำหนดหน้าที่ให้กับผู้ใช้ และ กำหนดการอนุญาต (Permission) ที่สัมพันธ์กับบทบาทนั้น ๆ ผู้ใช้คนหนึ่งสามารถมีหลายบทบาทได้ และ ผู้ใช้สามารถมีบทบาทแตกต่างกันได้ตามแต่ว่าผู้ใช้อยู่ในกลุ่มของผู้ใช้ประเภทใด และกลุ่มของผู้ใช้นั้นได้กำหนดให้มีบทบาทอะไรบ้าง ดังนั้น องค์กรที่มีผู้ใช้จำนวนมาก หากเป็นการใช้การพิสูจน์ตัวจริงแบบทั่วไป

จำเป็นต้องกำหนดการอนุญาตให้กับผู้ใช้ทุกคนเมื่อมีการสร้างเว็บเซอร์วิสบนอินเทอร์เน็ตใหม่ในองค์กร หากนำแบบจำลอง RBAC เข้ามาช่วยพัฒนาบริการพิสูจน์ตัวจริงจะสามารถลดภาระในส่วนนี้และควบคุมการเข้าถึงการใช้งานของผู้ใช้ได้อย่างมีประสิทธิภาพ

งานวิจัยนี้นำเสนอแนวคิดการพัฒนาระบบการพิสูจน์ตัวจริง สำหรับเว็บเซอร์วิสที่ใช้งานภายในองค์กร และสามารถกำหนดการอนุญาตเข้าถึงสิทธิ์การใช้งานให้กับผู้ใช้โดยใช้แบบจำลอง RBAC เป็นแนวทางในการพัฒนา

1.2 วัตถุประสงค์ของการวิจัย

นำเสนอวิธีการและพัฒนางานบริการพิสูจน์ตัวจริง สำหรับใช้กับเว็บเซอร์วิสองค์กร เพื่อกำหนดสิทธิ์การเข้าถึงบริการตามประเภทของผู้ใช้งานได้สะดวกขึ้น และลดภาระในการสร้างงานบริการพิสูจน์ตัวจริงของเว็บเซอร์วิส

1.3 ขอบเขตงานวิจัย

1) การให้งานการพิสูจน์ตัวจริงสำหรับเว็บเซอร์วิสจะถูกใช้งานผ่าน API ของงานบริการพิสูจน์ตัวจริง และส่งข้อมูลกลับเป็น JSON
2) พัฒนางานบริการพิสูจน์ตัวจริงโดยใช้ Role-based Access Control Model
3) สามารถใช้งานกับเว็บเซอร์วิสได้โดยไม่จำกัดโดเมน
4) เว็บเซอร์วิสสามารถกำหนดกลุ่มผู้ใช้และบทบาทพิเศษของตัวเองได้โดยไม่อิงกับบทบาททั่วไปที่บริการพิสูจน์ตัวจริงกำหนดให้

1.4 ขั้นตอนและวิธีการดำเนินการวิจัย

1) ศึกษาและทำความเข้าใจทฤษฎีและงานวิจัยที่เกี่ยวข้อง
2) ศึกษาการใช้เครื่องมือ
3) วิเคราะห์และกำหนดระเบียบวิธีวิจัย
4) ออกแบบ ตั้งสมมติฐาน ที่เกี่ยวข้องกับงานวิจัย
5) พัฒนาระบบ
6) ทดสอบและประเมินผลงานวิจัย
7) สรุปผลงานวิจัย และนำผลที่ได้ไปปรับปรุงระบบเพื่อให้ได้ตามวัตถุประสงค์ที่กำหนด
8) ตีพิมพ์ผลงานทางวิชาการ
9) จัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ได้วิธีการและรูปแบบการสร้างงานบริการพิสูจน์ตัวจริงสำหรับใช้กับเว็บเซอร์วิสองค์กร ซึ่งช่วยลดภาระในการจัดการผู้ใช้ที่มีความหลากหลายในแต่ละองค์กร สามารถกำหนดสิทธิ์การเข้าใช้งานให้กับผู้ใช้ได้ตามบทบาทของผู้ใช้งานในแต่ล่ะเว็บเซอร์วิสได้อย่างเหมาะสม และเพื่อความยืดหยุ่นในการสร้างเว็บเซอร์วิสองค์กร

1.6 โครงสร้างของเนื้อหาในวิทยานิพนธ์

เนื้อหาของวิทยานิพนธ์ฉบับนี้แบ่งออกเป็น 6 บทด้วยกันคือ บทที่ 1 อธิบายถึงที่มาและความสำคัญของปัญหา รวมถึงขอบเขตและประโยชน์ของงานวิจัย บทที่ 2 อธิบายถึงทฤษฎีที่เกี่ยวข้องและงานวิจัยที่เกี่ยวข้อง บทที่ 3 อธิบายถึงแนวคิดและวิธีการดำเนินการวิจัยในการสร้างงานบริการพิสูจน์ตัวจริงสำหรับใช้กับเว็บเซอร์วิสองค์กร บทที่ 4 อธิบายถึงวิธีการพัฒนาเครื่องมือสนับสนุนแนวคิดของงานวิจัย บทที่ 5 อธิบายวิธีการทดสอบและการวิเคราะห์ผลและในบทสุดท้ายจะสรุปงานวิจัยทั้งหมด รวมถึงงานวิจัยในอนาคต

1.7 ผลงานตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์ในรายงานสืบเนื่องจากการประชุมวิชาการระดับนานาชาติเรื่อง “Approach to Implementing Authentication Service with Role-based Access Control”, Poowanart Korbkum and Yachai Limpiyakorn, Proceedings of 2016 International Conference on Information Technology and Science (ICITS 2016), June 17-19, 2016, Tokyo

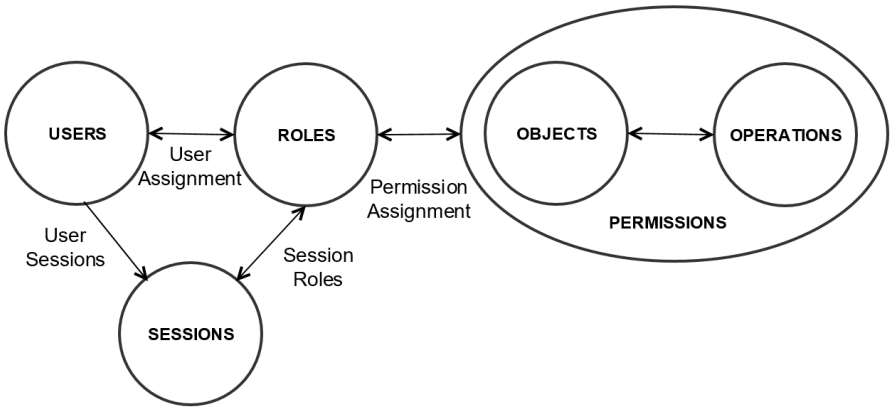
บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1. ทฤษฎีที่เกี่ยวข้อง

2.1.1. RBAC Model (Role-based Access Control Model) [3]

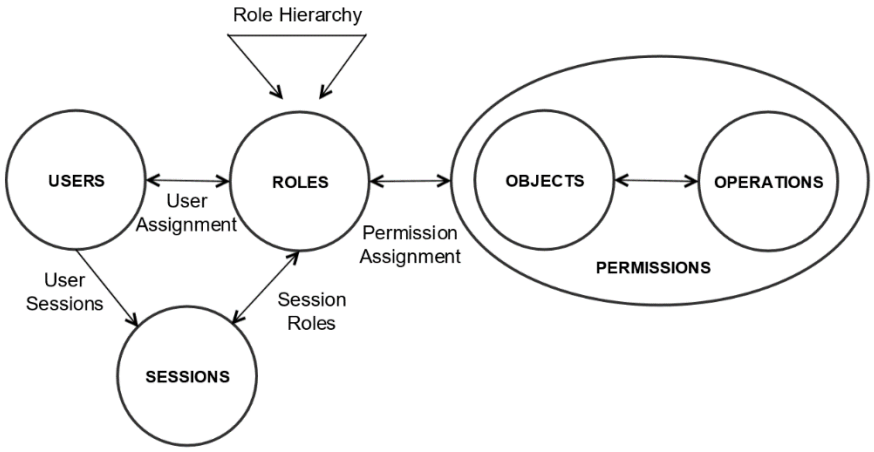
RBAC Model เป็นแบบจำลองการควบคุมการเข้าถึงที่แตกต่างจากการควบคุมการเข้าถึงแบบทั่วไปโดยใช้การอ้างอิงบทบาท (Role-Based) ของผู้ใช้งานในการกำหนดการอนุญาตเข้าถึงสิทธิ์ต่าง ๆ เพื่อใช้ในระบบ หรือกระบวนการนั้น ๆ หลักการของ RBAC คือการกำหนดบทบาท (Roles) ของผู้ใช้งานที่สัมพันธ์กับการอนุญาต (Permissions) นั้น ๆ และกำหนดบทบาทที่เหมาะสมให้กับผู้ใช้ โดยที่ผู้ใช้และการอนุญาตจะถูกนำมาใช้รวมกันผ่านบทบาท และถูกรวมเข้าไว้ในกลุ่มผู้ใช้ (User Group) ซึ่ง RBAC นั้นสามรถแบ่งได้ดังนี้

Core RBAC model เป็นแบบจำลองที่ชุดข้อมูลพื้นฐานซึ่งประกอบไปด้วย ผู้ใช้ (USERS), บทบาท (ROLES), วัตถุ (OBJECTS), การปฏิบัติการ (OPERATIONS) และ การอนุญาต (PERMISSIONS) ดังรูปที่ 1 แบบจำลองนี้นิยามให้ผู้ใช้ และ การอนุญาตถูกกำหนดโดยบทบาท ซึ่งมีการนำชุดของเซสชั่น (SESSIONS) มาช่วยจับคู่ระหว่างผู้ใช้ และ ชุดย่อยของบทบาทที่ถูกกำหนดให้กับผู้ใช้ในขณะนั้น



รูปที่ 1 Core RBAC model

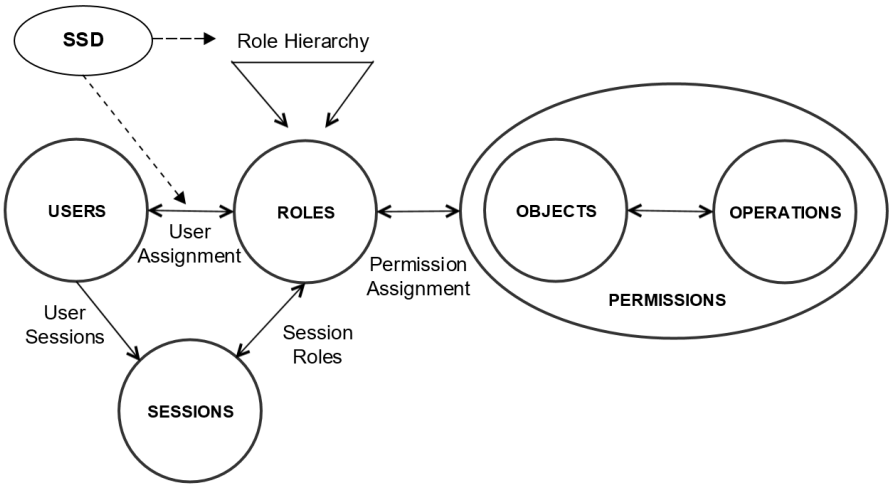
Hierarchal RBAC model เป็นแบบจำลองที่เพิ่มการจัดลำดับชั้นของบทบาท (Role Hierarchies) ดังรูปที่ 2 การจัดลำดับชั้นของบทบาทจะทำให้บทบาทในลำดับสูงกว่าได้รับคุณสมบัติของบทบาทที่อยู่ลำดับล่างกว่า เป็นต้น



รูปที่ 2 Hierarchal RBAC model

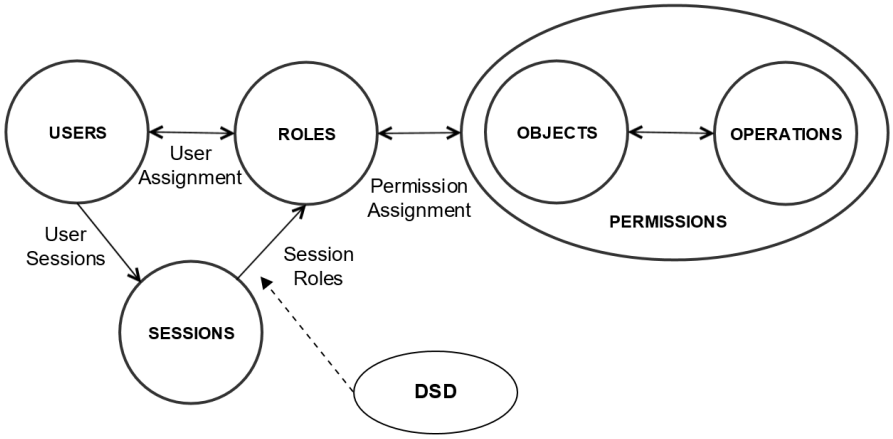
Constrained RBAC model แบบจำลองนี้แบ่งออกเป็นสองประเภทตามความสัมพันธ์ของความรับผิดชอบ (Duty) ได้แก่

1. SSD (Static Separation of Duty Relations) ตามรูปที่ 3 เป็นแบบจำลองที่ถูกปรับปรุงให้สามารถป้องกันข้อขัดแย้งที่เกิดจากผลของการพิสูจน์การอนุญาตของของผู้ใช้กับบทบาทที่มีความขัดแย้งอยู่



รูปที่ 3 SSD (Static Separation of Duty Relations)

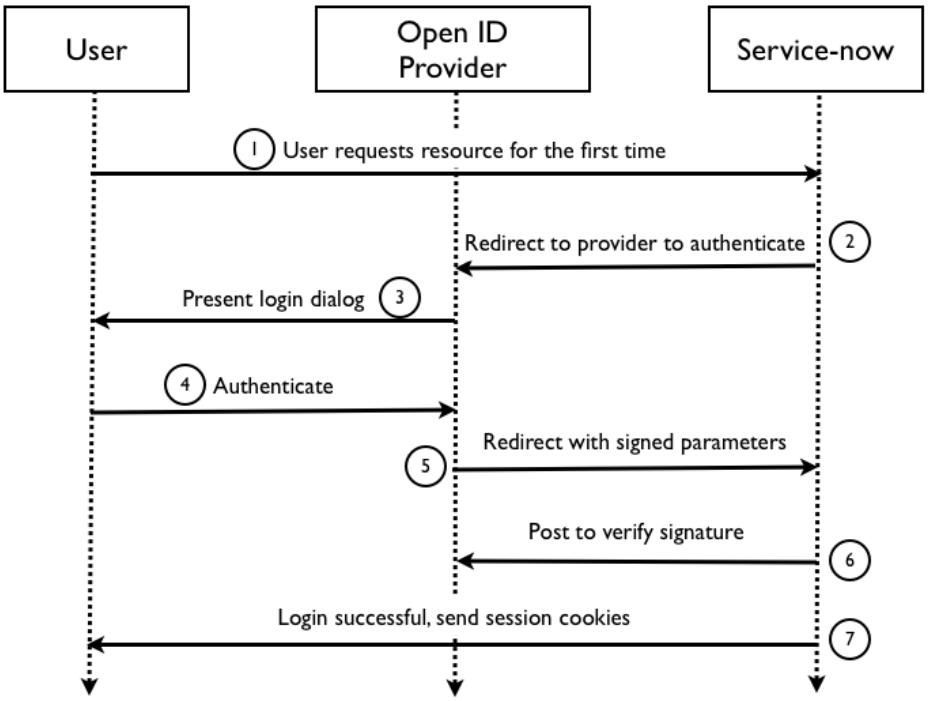
2. DSD (Dynamic Separation of Duty Relations) ตามรูปที่ 4 เป็นแบบจำลองที่คล้ายกับ SSD แต่ต่างที่สามารถกำหนดการอนุญาตให้ใช้งานได้ระหว่างที่ผู้ใช้เข้าใช้งานอยู่



รูปที่ 4 DSD (Dynamic Separation of Duty Relations)

2.1.2. OpenID

OpenID คือ งานบริการพิสูจน์ตัวจริงแบบ SSO (Single Sign-on) ที่มีหลักการคือลงทะเบียนครั้งเดียว สามารถใช้สำหรับการพิสูจน์ตัวจริงเข้าในเว็บเซอร์วิสได้ทุกทีที่รองรับ OpenID โดยกระบวนการทำงานแสดงดังรูปที่ 5

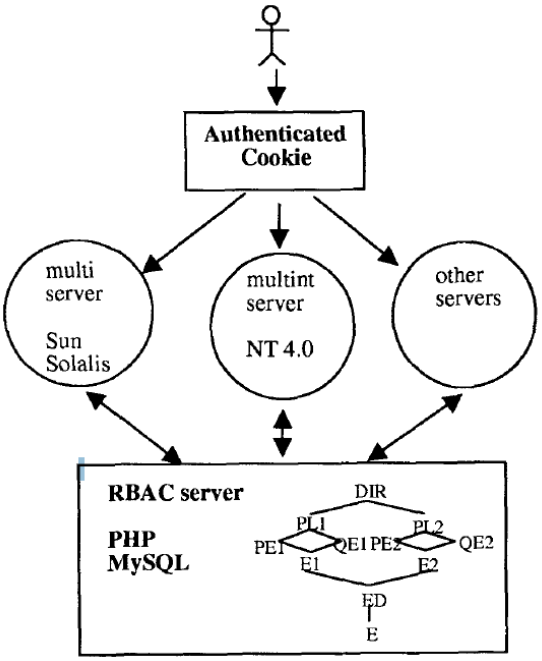


รูปที่ 5 กระบวนการทำงานของ OpenID

2.2. งานวิจัยที่เกี่ยวข้อง

2.2.1 Implementing Web Access Control System for the Multiple Web Servers in the Same Domain Using RBAC [4]

งานวิจัยนี้ได้อธิบายแนวคิดของการพัฒนาระบบการควบคุมการเข้าถึงเว็บไซต์สำหรับเว็บเซิร์ฟเวอร์ในโดเมนเดียวกัน โดยการนำ Role-based Access Control เข้ามาประยุกต์ใช้ในการควบคุมการเข้าถึงหลายๆ เว็บเซอร์วิสในเว็บเซิร์ฟเวอร์และความคุมการเข้าชมเอกสารต่างๆ โดยขึ้นอยู่กับบทบาทของผู้ใช้งาน โดยมีการเก็บการอนุญาตการเข้าถึงไว้ในหน่วยความจำแบบคุกกี้ (Cookie) ของเว็บเบราวเซอร์ ดังรูปที่ 6



รูปที่ 6 แนวทางรูปแบบการทำงานของงานวิจัยนี้

2.2.2 Design and Implementation of Authorization System Based on RBAC [5]

งานวิจัยนี้ได้อธิบายแนวคิดของการพัฒนาระบบการพิสูจน์ตัวจริงอิง Role-based Access Control โดยนำเสนอแนวทางการออกแบบแบบเรียบง่ายสำหรับการควบคุมการเข้าถึง หรือ ระบบการขออนุมัติการเข้าใช้งาน ซึ่งได้ออกแบบฐานข้อมูลสำหรับระบบการอนุมัติการเข้าใช้งานโดยตารางข้อมูล 3 ตาราง ได้แก่ ตาราง user สำหรับเก็บข้อมูลผู้ใช้ ตาราง department สำหรับเก็บขอบเขตของการให้บริการทั้งหมดที่ผู้ใช้สามารถเข้าถึงได้ และตารางสิทธิ์การเข้าถึงของผู้ใช้ (user's right table) ที่จะการอนุญาตของแต่ล่ะผู้ใช้ที่จะสามารถเข้าใช้งานโดยขึ้นอยู่กับประเภทของผู้ใช้งาน ดังตารางที่ 1ตารางที่ 2ตารางที่ 3

ตารางที่ 1 ตาราง user

NO.	Field name	DataType	Identity	Primary
1	ID	bigint	yes	yes
2	DepartmentID	int		
3	UserType	int		
3	UserName	nvarchar		
4	PassWord	nvarchar		
5	RealName	nvarchar		
6	UserSex	nvarchar		
7	Birthday	datetime		
8	Nation	nvarchar		
9	Party	nvarchar		

ตารางที่ 2 ตาราง department

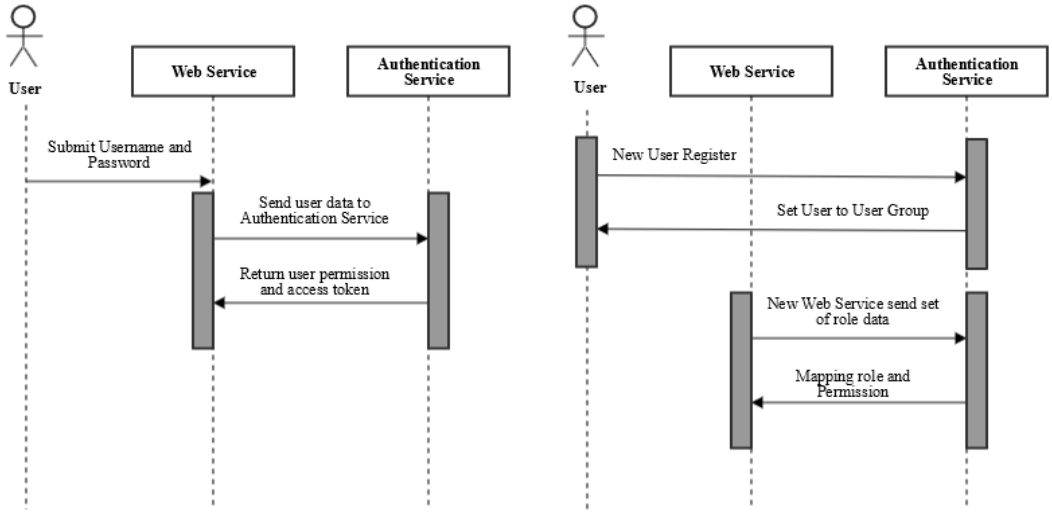
NO.	Field name	DataType	Identity	Primary
1	ID	int	yes	yes
2	DepartmentName	nvarchar		
3	ManagerName	nvarchar		
4	ParentID	int		
5	DepartmentType	int		
6	DepartmentDate	datetime		
7	UserName	nvarchar		
8	PassWord	nvarchar		
9	Status	nvarchar		
10	AddTime	datetime		

ตารางที่ 3 ตารางสิทธิ์การเข้าถึงของผู้ใช้

NO.	Field name	DataType	Identity	Primary
1	ID	int	yes	yes
2	UserType	int		
3	UserPower	ntext		

บทที่ 3
แนวคิดและวิธีดำเนินการวิจัย

ในบทนี้จะกล่าวถึงแนวคิดและวิธีการดำเนินการวิจัย โดยแนวคิดและดำเนินการวิจัยในการสร้างระบบการพิสูจน์ตัวจริงอิงบทบาท โดยแผนภาพซีเควนซ์ ที่แสดงลำดับการทำงานของระบบพิสูจน์ตัวจริง ดังรูปที่ 7 เมื่อผู้ใช้งานเข้ามาใช้งานเข้าสู้ระบบเว็บเซอร์วิสและทำการเข้าสู่ระบบ ชื่อผู้ใช้งานและรหัสผ่านที่ผู้ใช้งานได้ใช้ในการเข้าสู่ระบบจะถูกส่งไปยังระบบพิสูจน์ตัวจริงเพื่อยืนยันตัวผู้ใช้ งานและรับสิทธิ์ที่ได้ที่ถูกอนุญาตให้เข้าใช้งานผ่าน API (Application Programming Interface) ของระบบพิสูจน์ตัวจริง สำหรับผู้ใช้งานใหม่ที่มีการลงทะเบียนเข้าเพิ่มเข้ามาในระบบพิสูจน์ตัวจริง ผู้ใช้งานใหม่จะถูกกำหนดบทบาทบทบาทเพื่อระบุการอนุญาตเข้าในงานต่างๆ ที่สำพันธ์กับบทบาทของผู้ใช้งาน



รูปที่ 7 แผนภาพซีเควนซ์ของบริการพิสูจน์ตัวอิงบทบาท

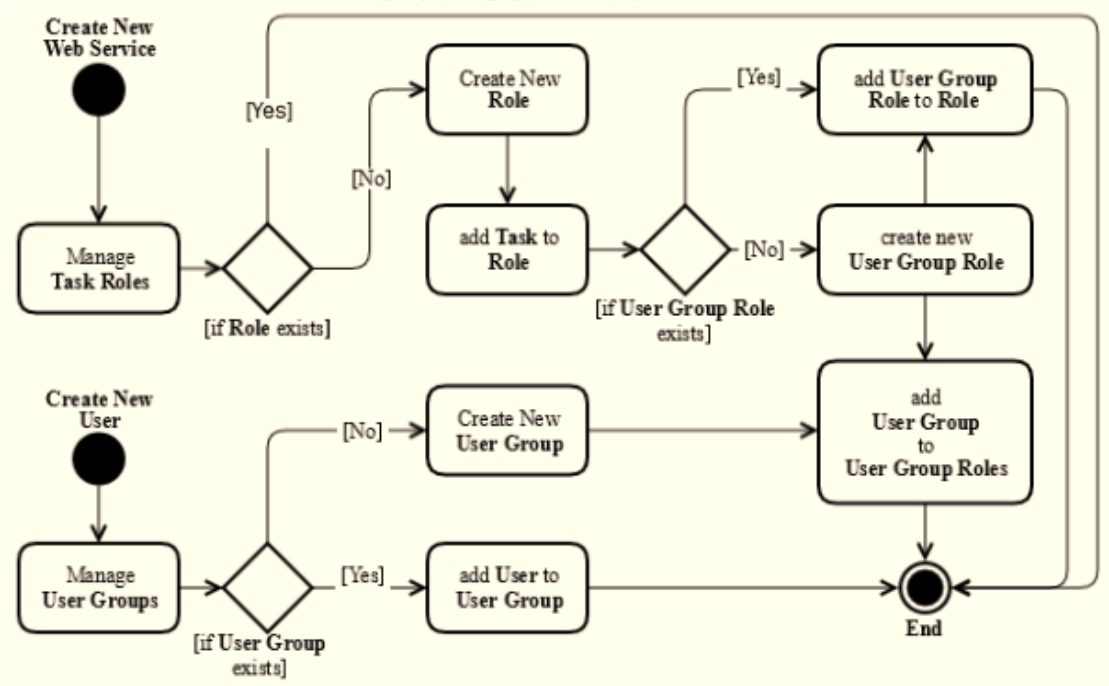
3.1. แนวทางการออกแบบบริการพิสูจน์ตัวจริง

องค์ประกอบหลักของระบบพิสูจน์ตัวจริงอิงบทบาทที่ผู้วิจัยได้พัฒนาขึ้นมาจะประกอบไปด้วย 2 ส่วนคือ API และ เว็บไซต์ที่เป็นส่วนบริหาร (Web Administration) โดยที่ API จะมีการปฏิสัมพันธ์โดยตรงกับเว็บเซอร์วิสเพื่อโต้ตอบคำร้องขอการพิสูจน์ตัวจริงของผู้ใช้งานและการกำหนดการอนุญาตเข้าใช้งานในส่วนต่างๆ ที่ขึ้นอยู่กับบทบาทของผู้ใช้งานที่ถูกกำหนดไว้ก่อน ในส่วนของเว็บไซต์ที่เป็นส่วนบริหารเป็นส่วนรับผิดชอบของผู้ดูแลระบบ ในส่วนของผู้พัฒนาเว็บเซอร์วิสจำเป็นต้องมีบริการลงทะเบียนเว็บเซอร์วิสด้วยตนเองโดยไม่ต้องอาศัยผู้ดูแลระบบคอยอำนวยความ

สะดวกให้และสามารถเข้าใช้งานเว็บส่วนบริหารเพื่อจัดการข้อมูลการอนุญาต บทบาทผู้ใช้ และข้อมูลอื่นๆ ที่เกี่ยวข้องกับเว็บเซอร์วิสที่ลงทะเบียนไว้ โดยที่จะมีรูปแบบการใช้งานหลักๆ ดังนี้

1) การจัดการผู้ใช้งาน
2) การจัดการบทบาท
3) การจัดการการอนุญาตต่างๆ
4) การจัดการกลุ่มของผู้ใช้งาน
5) การจัดการความสัมพันธ์ของบทบาทและกลุ่มผู้ใช้งาน
6) การลงทะเบียนเว็บเซอร์วิสด้วยผู้พัฒนาจากภายนอก

จากแผนภาพกิจกรรมของเว็บไซต์ที่เป็นส่วนบริหาร ดังรูปที่ 8 จะแสดงถึงความสัมพันธ์ระหว่างกลุ่มผู้ใช้งานกับบทบาทที่ถูกเชื่อมเข้าด้วยกันโดยบทบาทกลุ่มผู้ใช้งาน (User Group Role) ซึ่งกลุ่มผู้ใช้งาน (User Group) เป็นการจัดกลุ่มของผู้ใช้งานที่มีลักษณะการใช้งานในแบบเดียวกัน โดยที่ผู้ใช้งานสามารถถูกกำหนดให้อยู่ได้หลากหลายกลุ่ม กลุ่มของผู้ใช้งานหลายๆ กลุ่มสามรถมีบทบาทเดียวกันได้ โดยจะถูกเรียกว่า บทบาทกลุ่มผู้ใช้งาน และกลุ่มผู้ใช้งานสามารถมีบทบาทได้มากกว่าหนึ่งบทบาท



รูปที่ 8 แผนภาพกิจกรรมกระบวนการทำงานของเว็บไซต์ส่วนบริหาร

ส่วนของการจัดการบทบาทจะเป็นตัวทำหน้าที่ในการกำหนดบทบาทให้กับเว็บเซอร์วิสที่ถูกสร้างขึ้นมาใหม่ ส่วนบทบาทที่ถูกกำหนดขึ้นมาใหม่ก็จะถูกกำหนดการอนุญาตการใช้งานให้กับกลุ่มผู้ใช้ที่มีความสัมพันธ์เกี่ยวข้องกับบทบาทนั้น

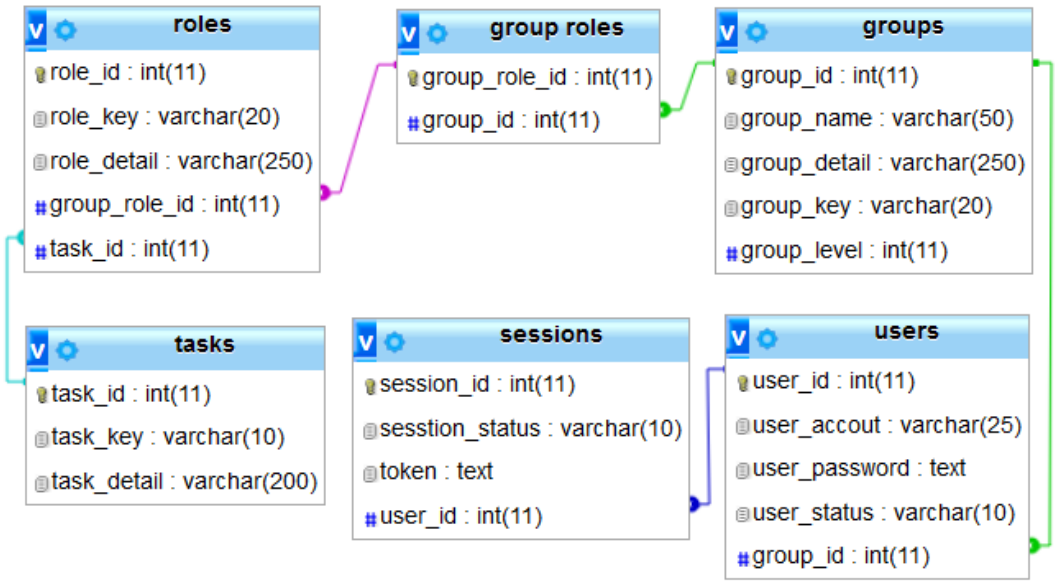
เมื่อมีผู้ใช้งานใหม่ถูกสร้างขึ้น ผู้ใช้งานจะถูกจัดประเภทของกลุ่มผู้ใช้งานที่เหมาะสม ซึ่งผู้ใช้งานจะถูกกำหนดการอนุญาตการใช้งานตามบทบาทที่มีความสัมพันธ์กับกลุ่มนั้น ในกรณีที่ไม่มีกลุ่มที่เหมาะสมสำหรับผู้ใช้งานใหม่ กลุ่มผู้ใช้งานใหม่จะถูกสร้างขึ้นและมีการกำหนดความสัมพันธ์ของบทบาทโดยบทบาทกลุ่มผู้ใช้ หลังจากนั้นถึงจะเพิ่มผู้ใช้งานใหม่เข้าไปยังกลุ่มที่เพิ่งถูกสร้างขึ้น

บทบาทของผู้ใช้งานเป็นชุดของการอนุญาตที่ผู้ใช้สามารถเข้าสู่การใช้งานต่างๆ ที่ถูกกำหนดไว้ล่วงหน้า โดยการจัดการการอนุญาตเป็นตัวกลางในการกำหนดตามเงื่อนไขของแต่ล่ะงานที่ผู้ใช้งานสามารถเข้าถึงได้และกำหนดบทบาทที่เกี่ยวข้องของแต่ล่ะงาน

3.2. แนวทางการออกแบบฐานข้อมูลสำหรับบริการพิสูจน์ตัวจริง

การออกแบบโครงร่างฐานข้อมูลสำหรับระบบพิสูจน์ตัวจริงในงานวิจัยนี้ได้ถูกแสดงในรูปที่ 9 โดยจะประกอบไปด้วย 6 ตารางได้แก่

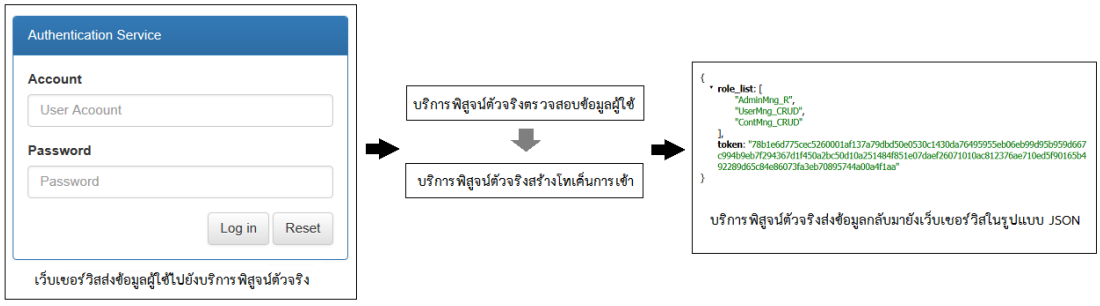
1) ตาราง tasks มีหน้าที่จัดเก็บการอนุญาตของแต่ล่ะงานที่มีอยู่
2) ตาราง roles สำหรับจัดเก็บบทบาททั้งหมดและมีความสัมพันธ์กับงานต่างๆ โดยใช้การอ้างอิงจาก task_id ในตาราง tasks และ ชุดของบทบาทกลุ่มผู้ใช้งาน โดยอ้างอิงจาก group_role_id จาก ตาราง group roles
3) ตาราง group roles จะจัดเก็บชุดของกลุ่มผู้ใช้งานที่มีความสัมพันธ์ในบทบาทเดียวกัน
4) ตาราง groups เป็นตารางสำหรับจัดเก็บชุดของผู้ใช้งานที่ถูกจัดให้อยู่ในประเภทเดียวกัน โดยมีความสัมพันธ์กันระหว่างผู้ใช้งานและบทบาทของผู้ใช้งาน โดยมีคุณลักษณะ group_level เป็นตัวกำหนดลำดับความสำคัญของกลุ่มผู้ใช้งาน โดยที่กลุ่มผู้ใช้งานที่มีระดับสูงกว่าสามารถเข้าถึงการอนุญาตการใช้งานของกลุ่มผู้ใช่ที่มีระดับต่ำกว่าได้ ในกรณีที่ผู้ใช้งานถูกจัดอยู่ในหลายกลุ่ม
5) ตาราง users มีหน้าที่สำหรับจัดเก็บข้อมูลของผู้ใช้งาน ตัวอย่างเช่น ชื่อผู้ในงาน และรหัสผ่านที่ได้ถูกเข้ารหัสไว้ เป็นต้น
6) ตาราง sessions จัดเก็บสถานะการพิสูจน์ตัวจริงเพื่อผู้ใช้ได้ทำการเข้าสู่ระบบแล้ว ระบบจะสร้างโทเค็นการเข้าถึง (Access Token) โดยอ้างอิงกับคุณลักษณะ user_id ของผู้ใช้งานและจะส่งโทเค็นนี้ไปยังเว็บเซอร์วิสที่ผู้ใช้ได้ทำการร้องขอการพิสูจน์ตัวจริง



รูปที่ 9 โครงร่างฐานข้อมูลของบริการพิสูจน์ตัวจริง

3.3. แนวทางการติดต่อสื่อสารรหว่างระหว่างเว็บเซอร์วิสกับบริการพิสูจน์ตัวจริง

การติดต่อสื่อสารกันระหว่างเว็บเซอร์วิสที่ผู้ใช้ใช้งานอยู่กับบริการพิสูจน์ตัวจริงได้แสดงดังรูปที่ 10 เมื่อผู้ใช้งานทำการเข้าสู่ระบบเว็บเซอร์วิสจะส่งข้อมูลผู้ใช้ไปยังบริการยืนยันตัวตนเพื่อทำการตรวจสอบความถูกต้องผ่านสคริปต์ด้านเซิร์ฟเวอร์ (Server-side scripting) เพื่อรักษาความปลอดภัยของข้อมูลผู้ใช้เบื้องต้น ถ้าหากข้อมูลผู้ใช้งานถูกต้องบริการยืนยันตัวจริงจะสร้างโทเค็นการเข้าถึงหรือปรับปรุงโทเค็นเดิมที่มีอยู่แล้วให้สามารถใช้งานได้ จากนั้นดูว่าผู้ใช้งานมีการอนุญาตการใช้งานอะไรบ้างจากบทบาทของผู้ใช้ในฐานข้อมูล สุดท้ายจึงส่งโทเค็นการเข้าถึงและการอนุญาตการใช้งานต่างๆ กลับไปยังเว็บเซอร์วิสในรูปแบบของ JSON (JavaScript Object Notation)



รูปที่ 10 ทางการติดต่อสื่อสารรหว่างระหว่างเว็บเซอร์วิสกับบริการพิสูจน์ตัวจริง

บทที่ 4
การพัฒนาเครื่องมือ

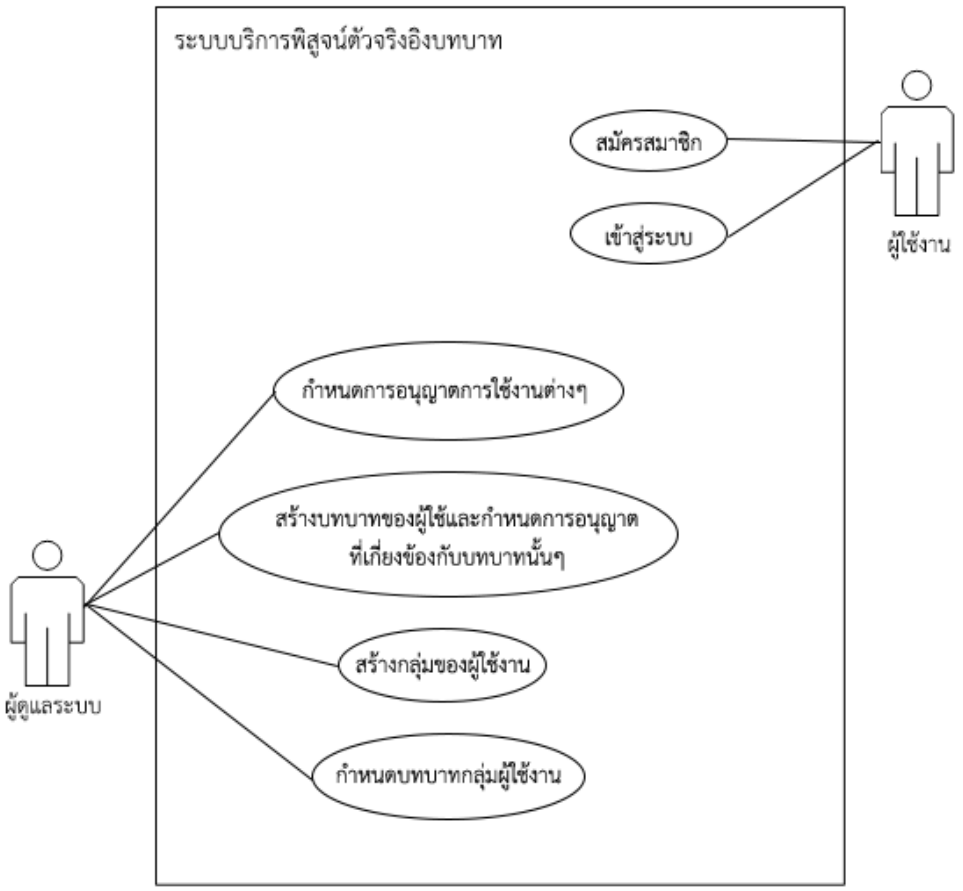
รายละเอียดในบทนี้จะกล่าวถึงวิธีการออกแบบและพัฒนาเครื่องมือต้นแบบสนับสนุนแนวทางในการทดสอบคุณลักษณะของระบบการพิสูจน์ตัวจริงจากความต้องการที่ได้นำเสนอในบทที่ 3 โดยจะกล่าวถึงโครงสร้างของซอฟต์แวร์และสภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือ ซึ่งมีรายละเอียดดังต่อไปนี้

4.1. ความต้องการเชิงฟังก์ชัน

1) ระบบสามารถเพิ่มเว็บเซอร์วิสที่สามารถเข้าใช้งานระบบได้
2) ระบบสามารถเพิ่มผู้ใช้ที่สามารถใช้งานระบบได้
3) ระบบสามารถจัดการบทบาทของผู้ใช้และกลุ่มของผู้ใช้งานระบบได้
4) ระบบสามารถจัดการความสัมพันธ์ระหว่างผู้ใช้งานกับกลุ่มผู้ใช้งานและบทบาทของผู้ใช้งานได้
5) ระบบสามารถใช้งานได้กับเว็บเซอร์วิสที่มีโดเมนแตกต่างกันได้
6) ผู้ใช้สามารถสมัครสมาชิกได้จากเว็บเซอร์วิส
7) ผู้ใช้สามารถเข้าสู่ระบบของเว็บเซอร์วิสและใช้งานในส่วนที่อนุญาตได้
8) ผู้พัฒนาเว็บเซอร์วิสสามารถสมัครการใช้งานบริการพิสูจน์ตัวจริงได้เอง
9) ผู้พัฒนาเว็บเซอร์วิสสามารถสร้างกลุ่มผู้ใช้ขึ้นเองเพื่อใช้เฉพาะภายในเว็บเซอร์วิสเองและสามารถสร้างบทบาทและการอนุญาตสำหรับกลุ่มผู้ใช้ที่สร้างขึ้นมาได้
10) ผู้พัฒนาเว็บเซอร์วิสสามารถเข้าใช้งานเว็บส่วนบริหารของบริการพิสูจน์ตัวจริงหลังจากสมัครการใช้งานได้

4.2. การวิเคราะห์ความต้องการและแผนภาพฟังก์ชันงานของระบบ

จากความต้องการเชิงฟังก์ชัน สามารถวิเคราะห์การออกแบบการพัฒนาบริการพิสูจน์ตัวจริง ผู้วิจัยจึงออกมาเป็นแบบจำลองเชิงฟังก์ชันที่สามารถแสดงเป็นแผนภาพยูสเคส (Use case diagram) ดังรูปที่ 11



รูปที่ 11 แผนภาพยูสเคสของระบบบริการพิสูจน์ตัวจริง

จากแผนภาพยูสเคสเชิงฟังก์ชันแสดงให้เห็นถึงกิจกรรมของผู้ใช้งานและผู้ดูแลระบบ โดยจะอธิบายรายละเอียดของแต่ละฟังก์ชันงานดังต่อไปนี้

1) สมัครสมาชิก

ผู้ใช้สมัครสมาชิกเพื่อเข้าใช้บริการเว็บเซอร์วิสผ่านหน้าสมัครสมาชิกของเว็บเซอร์วิสที่ได้เตรียมไว้ โดยผู้ใช้จะต้องกรอกข้อมูลที่จำเป็นในการสมัครสมาชิกเช่น ชื่อผู้ใช้งาน รหัสผ่าน อีเมล เป็นต้น โดยจำเป็นต้องมีการระบุว่าผู้ใช้ที่ทำการสมัครสมาชิกมานั้น เป็นผู้ใช้ประเภทใด อาจจะมีการให้เลือกในขั้นตอนการกรอกข้อมูลที่จำเป็นในการสมัครสมาชิก หรือเว็บเซอร์วิสจะกำหนดค่าตายตัวก็ได้ จากนั้นเว็บเซอร์วิสจะส่งข้อมูลการสมัครสมาชิกมายังบริการพิสูจน์ตัวจริงผ่านการเรียกใช้ API จากนั้นบริการพิสูจน์ตัวจริงจะเอาข้อมูลผู้ใช้จัดเก็บลงฐานข้อมูลแล้วทำการจัดกลุ่มของผู้ใช้ตามประเภทของผู้ใช้ที่ส่งมาเพื่อผู้ใช้จะได้รับสิทธิ์การเข้าถึงและการอนุญาตการใช้งานตามประเภทของผู้ใช้ที่ถูกต้อง

2) เข้าสู่ระบบ

ผู้ใช้เข้าสู่ระบบเพื่อเข้าใช้งานเว็บเซอร์วิสโดยการกรอกชื่อผู้ใช้งานและรหัสผ่านที่หน้าเว็บเซอร์วิส จากนั้นเว็บเซอร์วิสจึงส่งข้อมูลไปยังบริการพิสูจน์ตัวจริงเพื่อทำการพิสูจน์ว่ามีชื่อ

ผู้ใช้และรหัสผ่านดังกล่าวอยู่ในฐานข้อมูลหรือไม่และมีตรงกับข้อมูลที่จัดเก็บไว้หรือไม่ซึ่งหากข้อมูลถูกต้องระบบจะส่งโทเค็นการเข้าถึงและการอนุญาตการใช้งานต่างๆ ตามกลุ่มของผู้ใช้ที่ได้ถูกเลือกไว้

3) กำหนดการอนุญาตการใช้งานต่างๆ

ผู้ดูแลระบบต้องสร้างการอนุญาตต่างๆ สำหรับใช้กับบทบาทของผู้ใช้ โดยการกรอกชื่อการอนุญาตที่สื่อความหมายถึงสิ่งที่ผู้ใช้สามารถทำได้รวมถึงรายละเอียดของสิ่งที่ผู้ใช้งานสามารถทำได้ในช่องรายละเอียดการใช้งาน และกำหนดตัวย่อเพื่อใช้แทนชื่อเต็มในการสื่อสารระหว่างเว็บเซอร์วิสเป็นการลดขนาดข้อมูลเพื่อจะได้ส่งไปยังเว็บเซอร์วิสได้เร็วขึ้น หลังจากสร้างการอนุญาตครบถ้วน

4) สร้างบทบาทของผู้ใช้และกำหนดการอนุญาตที่เกี่ยวข้องกับบทบาทผู้ใช้

ผู้ดูและระบบสามารถสร้างบทบาทผู้ใช้ขึ้นมาโดยกำหนดชื่อบทบาทและชื่อย่อ (Standardization) จากนั้นจึงกำหนดว่าบทบาทนนี้ต้องมีการอนุญาตอะไรบ้าง ซึ่งสามารถเลือกได้มากกว่าหนึ่งการอนุญาตต่อหนึ่งบทบาท

5) สร้างกลุ่มของผู้ใช้งาน

ผู้ดูแลระบบสร้างกลุ่มผู้ใช้งานโดยการกำหนดชื่อกลุ่มและชื่อย่อ ระบุรายละเอียดประเภทของกลุ่มเพื่อให้ผู้ใช้งานได้เลือกว่าตัวเองอยู่กลุ่มไหน หรือให้ผู้พัฒนาเว็บเซอร์วิสสามารถกำหนดช่องทางในการสมัครสมาชิกให้กับกลุ่มผู้ใช้เฉพาะกลุ่มได้

6) กำหนดบทบาทของผู้ใช้งาน

หลังจากสร้างกลุ่มและบทบาทผู้ใช้ ผู้ดูแลระบบสามารถสร้างบทบาทกลุ่มผู้ใช้โดยการกำหนดชื่อบทบาทกลุ่มผู้ใช้จากนั้นเลือกบทบาทผู้ใช้มาหนึ่งบทบาทแล้วกลุ่มผู้ใช้ที่มีความเกี่ยวข้องกับบทบาทดังกล่าวเข้ามาได้มากกว่าหนึ่งกลุ่ม การสร้างบทบาทกลุ่มผู้ใช้งานเป็นการกำหนดบทบาทให้กับกลุ่มผู้ใช้ว่ากลุ่มผู้ใช้แต่ล่ะกลุ่มมีบทบาทอะไร โดยที่แต่ล่ะกลุ่มสามารถมีบทบาทได้มากกว่าหนึ่งบทบาท

4.3. สภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือสนับสนุน

สภาพแวดล้อมที่ใช้ในการพัฒนาระบบจะอ้างอิงมาจากคอมพิวเตอร์ที่ใช้ในการพัฒนา โดยประกอบไปด้วยฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่ใช้ในการพัฒนาระบบ ซึ่งมีรายละเอียดดังนี้

1) ระบบฮาร์ดแวร์

เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบควรมีฮาร์ดแวร์ขั้นต่ำดังต่อไปนี้

- หน่วยการประมวลผล (CPU) ซีพียูอินเทลคอร์ไอ 7 ความเร็ว 2.5 กิกะเฮิรตซ์ (Intel(R) Core(TM) i7-4710HQ 2.5GHz)
- หน่วยความจำ (Memory) ขนาด 8 กิกะไบต์ (Ram 8 GB)
- จานบันทึกแบบแข็ง (Hard disk) ความจุ 1 เทระไบต์ (Hard disk 1 TB)

2) ซอฟต์แวร์

เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบมีซอฟต์แวร์ดังต่อไปนี้

- ระบบปฏิบัติการไมโครซอฟท์วินโดวส์ 10 โปร 64 บิต (Microsoft Windows 10 Pro 64x bit)
- พีเอชพี เซิร์ฟเวอร์-ไซด์ สคริปต์ (PHP Server side script) เวอชั่น 5.6.5
- อะแพชี เอชทีทีพี เว็บเซิร์ฟเวอร์ (Apache HTTP Server)
- โปรแกรมพีเอชพีสตอร์ม (PhpStorm) เวอร์ชัน 2016.1.2
- มอซิลลา ไฟร์ฟอกซ์ เว็บบราวเซอร์ (Mozilla Firefox web browser) เวอร์ชั่น 47.0.1
- โค้ดอิกไนเตอร์ พีเอชพีเฟรมเวิร์ก (Codeigniter PHP Framework) เวอร์ชั่น 3.0.6

3) การติดตั้งซอฟต์แวร์

ทำการติดตั้งเครื่องมือในการพัฒนาระบบทั้งหมดลงในเครื่องคอมพิวเตอร์ที่ใช้พัฒนาระบบโดยเริ่มลำดับการติดตั้งตามขั้นตอนดังต่อไปนี้

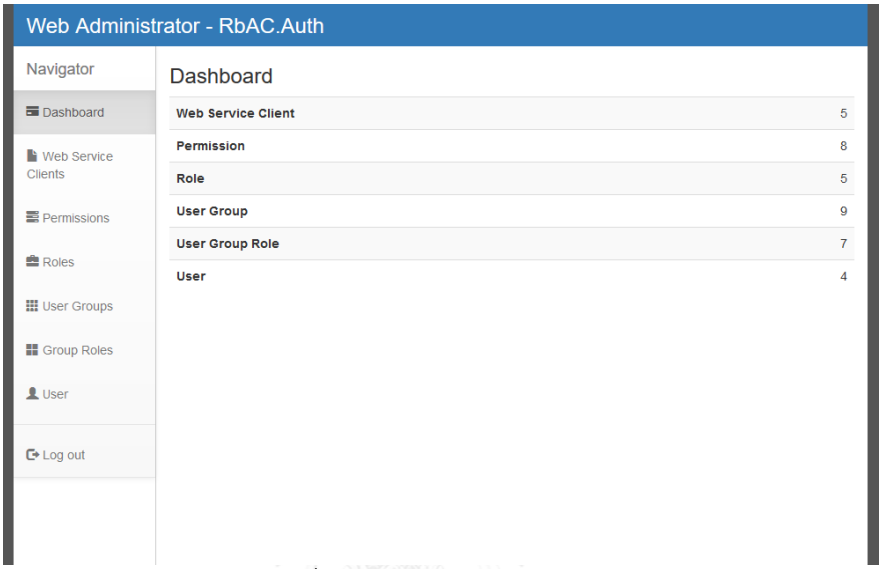
1) ติดตั้งระบบปฏิบัติการไมโครซอฟท์วินโดวส์ 10 โปร 64
2) ติดตั้งอะแพชี เอชทีทีพี เว็บเซิร์ฟเวอร์
3) ติดตั้งพีเอชพี เซิร์ฟเวอร์-ไซด์ สคริปต์
4) ติดตั้งโปรแกรมพีเอชพีสตอร์ม
5) ติดตั้งโปรแกรมมอซิลลา ไฟร์ฟอกซ์ เว็บบราวเซอร์
6) ติดตั้งโค้ดอิกไนเตอร์

4.4. ขั้นตอนการทำงานของเครื่องมือ

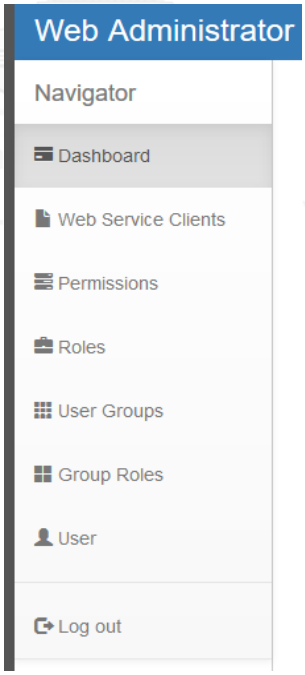
เครื่องมือมีขั้นตอนการทำงานและภาพส่วนต่อประสานดังต่อไปนี้

1) เว็บส่วนบริกหารประกอบด้วยรายการดังนี้ 1) Dashboard หน้าหลักที่แสดงรายละเอียดโดยรวมข้อมูลต่างๆ ที่มีผู้ดูแลระบบได้ทำการสร้างไว้ เช่น จำนวนเว็บเซอร์วิสที่ได้ลงทะเบียนขอใช้งานบริการพิสูจน์จริง จำนวนการอนุญาตทั้งหมด จำนวนบทบาททั้งหมด ดังรูปที่ 12 เป็นต้น 2) Web Service Clients รายการจัดการเว็บเซอร์วิสที่

ลงทะเบียนขอใช้งานบริการพิสูจน์ตัวจริง 3) Permissions รายการสำหรับจัดการการอนุญาตการใช้งานเว็บเซอร์วิสของผู้ใช้ 4) Roles รายการจัดการบทบาทผู้ใช้โดยสามารถกำหนดการอนุญาตการใช้งานกับบทบาทต่างๆ 5) User Groups รายการจัดการกลุ่มผู้ใช้ 6) Group Roles รายการจัดการกลุ่มผู้ใช้ 7) User รายการจัดการผู้ใช้ 8) ออกจากระบบเว็บส่วนบริหาร ดังรูปที่ 13



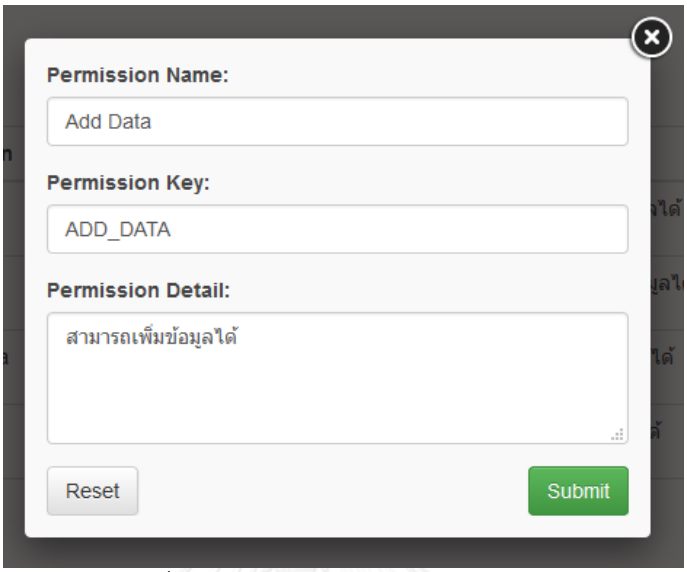
รูปที่ 12 Dashboard หน้าหลัก



รูปที่ 13 รายการของเว็บส่วนบริหาร

2) ผู้ดูแลระบบทำการสร้างการอนุญาตการใช้งานจากเว็บส่วนบริหารในส่วนรายการ Permissions โดยกำหนดชื่อการอนุญาตและชื่อย่อในแบบฟอร์ม กรอกรายละเอียด

เกี่ยวกับการอนุญาตการใช้งาน ดังรูปที่ 14 หลังจากสร้างการอนุญาตจะได้รายการการอนุญาต ดังรูปที่ 15 การสร้างการอนุญาตในส่วนนี้เพื่อให้ผู้ดูแลระบบสามารถนำไปกำหนดการอนุญาตให้กับบทบาทที่เกี่ยวข้องได้

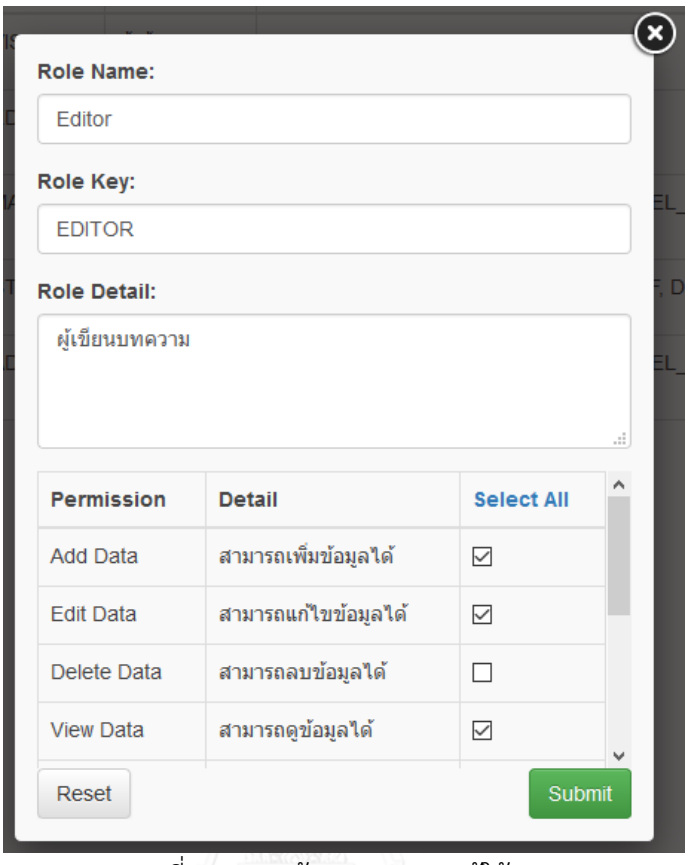


รูปที่ 14 การสร้างการอนุญาตการใช้งาน

#	Permission	Key	Detail	Tools
1	Add Data	ADD_DATA	สามารถเพิ่มข้อมูลได้	Edit Delete
2	Edit Data	EDIT_DATA	สามารถแก้ไขข้อมูลได้	Edit Delete
3	Delete Data	DEL_DATA	สามารถลบข้อมูลได้	Edit Delete
4	View Data	VIEW_DATA	สามารถดูข้อมูลได้	Edit Delete
5	Add Staff	ADD_STAFF	เพิ่มเจ้าหน้าที่	Edit Delete
6	View Staff	VIEW_DATA	ดูข้อมูลเจ้าหน้าที่	Edit Delete
7	Edit Staff	EDIT_DATA	แก้ไขข้อมูลเจ้าหน้าที่	Edit Delete
8	Delete Staff	DEL_DATA	ลบข้อมูลเจ้าหน้าที่	Edit Delete

รูปที่ 15 รายการการอนุญาต

3) ผู้ดูแลระบบทำการสร้างบทบาทของผู้ใช้งานจากเว็บส่วนบริหารในส่วนรายการ Roles โดยกำหนดชื่อบทบาทและชื่อย่อในแบบฟอร์มต่างๆ รวมทั้งเลือกการอนุญาตที่เกี่ยวข้องกับบทบาทจากรายการที่มีอยู่ ดังรูปที่ 16 หลังจากสร้างบทบาทจะได้รายการบทบาทดังรูปที่ 17 ซึ่งการอนุญาตได้มาจากการสร้างในข้อที่ 2



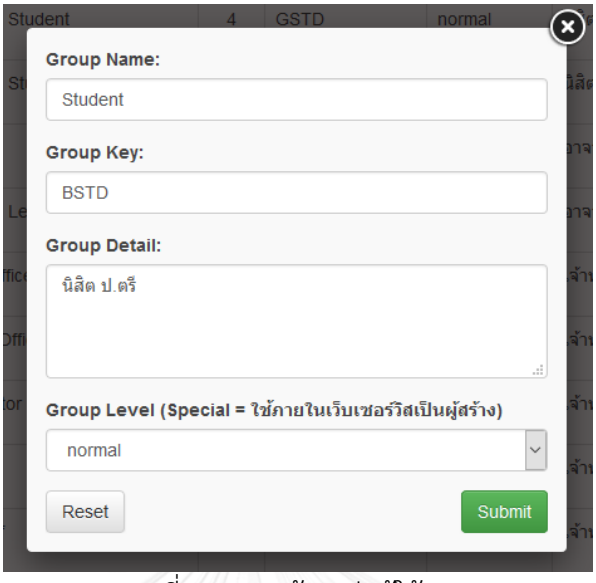
รูปที่ 16 การสร้างบทบาทของผู้ใช้งาน

#	Role	Key	Detail	Permission	Tools
1	Visitor	VISITOR	ผู้เข้าชม	VIEW_DATA	Edit Delete
2	Editor	EDITOR	ผู้เขียนบทความ	VIEW_DATA, ADD_DATA, EDIT_DATA	Edit Delete
3	Manger	MANAGER	ผู้จัดการบทความ	VIEW_DATA, ADD_DATA, EDIT_DATA, DEL_DATA	Edit Delete
4	Staff	STAFF	เจ้าหน้าที่	VIEW_STAFF, ADD_STAFF ,EDIT_STAFF, DEL_STAFF	Edit Delete
5	Administrator	ADMIN	เจ้าหน้าที่ดูแลระบบ	VIEW_DATA, ADD_DATA, EDIT_DATA, DEL_DATA, VIEW_STAFF, ADD_STAFF, EDIT_STAFF,D EL_STAFF	Edit Delete

รูปที่ 17 รายการบทบาท

4) ผู้ดูแลระบบทำการสร้างกลุ่มผู้ใช้งานจากเว็บส่วนบริหารในส่วนรายการ Groups โดยต้องชื่อกลุ่มของผู้ใช้งานและรายละเอียดต่างๆ ตามแบบฟอร์ม ดังรูปที่ 18 หลังจากสร้างกลุ่มผู้ใช้งานจะได้รายการกลุ่มผู้ใช้งาน ดังรูปที่ 19 การสร้างกลุ่มของผู้ใช้เพื่อให้ผู้ใช้งานสามารถเลือกกลุ่มของตนเองในขั้นตอนการสมัครสมาชิกได้ นอกจากนั้นผู้พัฒนาเว็บเซอร์วิสยังสามารถแยกการสมัครสมาชิกของผู้ใช้งานตามกลุ่มของผู้ใช้ได้อย่างอิสระ ในการสร้ากลุ่มผู้ใช้งานสามารถกำหนดว่าเป็นกลุ่มทั่วไปหรือกลุ่มที่สามารถใช้ได้เฉพาะเว็บ

เซอร์วิสที่เป็นผู้สร้างขึ้นเท่านั้น โดยการเลือก normal สำหรับกลุ่มทั่วไป และ special สำหรับกลุ่มภายในของเว็บเซอร์วิส



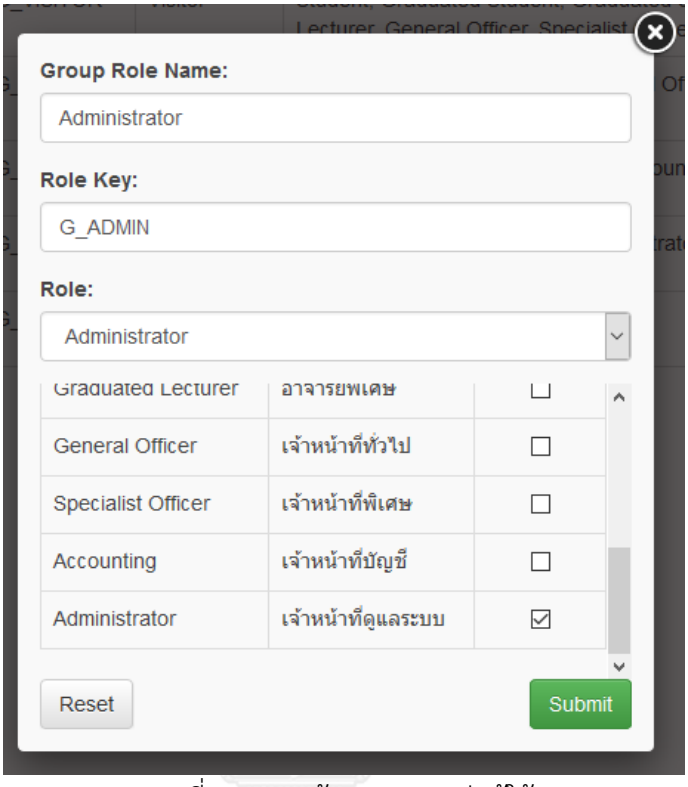
รูปที่ 18 การสร้างกลุ่มผู้ใช้งาน

#	Group	ID	Key	Level	Detail	Tools
1	Student	3	BSTD	normal	นิสิต ป.ตรี	Edit Delete
2	Graduated Student	4	GSTD	normal	นิสิต ป.โท	Edit Delete
3	Graduated Student	5	PSTD	normal	นิสิต ป.เอก	Edit Delete
4	Lecturer	6	BLCT	normal	อาจารย์	Edit Delete
5	Graduated Lecturer	7	GLCT	normal	อาจารย์บัณฑิตศึกษา	Edit Delete
6	General Officer	8	GOFC	normal	เจ้าหน้าที่ทั่วไป	Edit Delete
7	Specialist Officer	9	SOFC	normal	เจ้าหน้าที่พิเศษ	Edit Delete
8	Administrator	10	ADMN	special	เจ้าหน้าที่ดูแลระบบ	Edit Delete
9	Staff	11	STAFF	special	เจ้าหน้าที่	Edit Delete
10	Client Staff	12	C_STAFF	special	เจ้าหน้าที่เว็บเซอร์วิส	Edit Delete

รูปที่ 19 รายการกลุ่มผู้ใช้งาน

5) ผู้ดูแลระบบทำการสร้างบทบาทกลุ่มผู้ใช้จากเว็บส่วนบริหารในส่วนรายการ Group Roles โดยการตั้งชื่อบบทบาทกลุ่มผู้ใช้ ชื่อย่อ เลือกบทบาทแลกลุ่มผู้ใช้งานที่มีอยู่ในรายการ ดังรูปที่ 20 หลังจากนั้นจะได้รายการบทบาทกลุ่มผู้ใช้งาน ดังรูปที่ 21 การสร้างบทบาทกลุ่มผู้ใช้งานเป็นการกำหนดบทบาทให้กับกลุ่มผู้ใช้ต่างๆ โดยแต่ละบทบาท

สามารถกำหนดให้กับกลุ่มผู้ใช้ได้มากกว่าหนึ่งกลุ่ม และกลุ่มผู้ใช้ก็สามารถถูกกำหนดให้อยู่กับบทบาทใดก็ได้



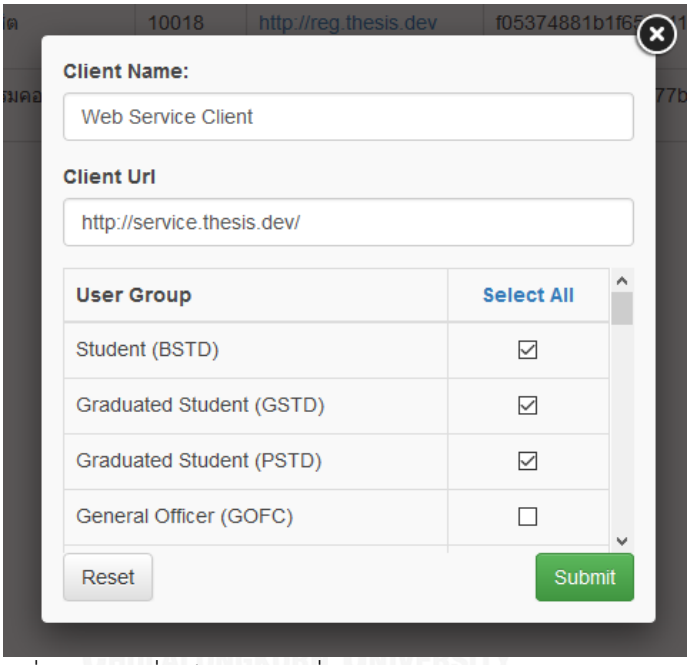
รูปที่ 20 การสร้างบทบาทกลุ่มผู้ใช้

#	Group Role	Key	Role	User Group	Tools
1	Administrator	G_ADMIN	Administrator	ADMN,	Edit Delete
2	All Student	ALL_STD	Visitor	BSTD, GSTD, PSTD,	Edit Delete
3	All Lecturer - Editor	ALL_LECTURER_E	Editor	BLCT, GLCT,	Edit Delete
4	All Lecturer - Manager	ALL_LECTURER_M	Manager	GLCT,	Edit Delete
5	Manager	G_MANAGER	Manager	GLCT, GOFC, SOFC,	Edit Delete
6	All Staff	G_STAFF	Staff	SOFC, ADMN,	Edit Delete
7	CMS Staff	CMS_STAFF	Staff	ADMN, STAFF, C_STAFF,	Edit Delete

รูปที่ 21 รายการบทบาทกลุ่มผู้ใช้งาน

6) ผู้ดูแลระบบทำการเพิ่มเว็บเซอร์วิสที่ต้องการใช้งานบริการพิสูจน์ตัวจริงจากเว็บส่วนบริหารในส่วนรายการ Web Service Client โดยกรอกรายละเอียดต่างๆ ตามแบบฟอร์ม และเลือกกลุ่มผู้ใช้งานที่เกี่ยวข้องกับเว็บเซอร์วิสดังกล่าว ดังรูปที่ 22 จากนั้นจะได้รายการของเว็บเซอร์วิสที่สามารถใช้งานบริการพิสูจน์ตัวจริง โดยจะได้ Client ID และ Secret Key สำหรับให้เว็บเซอร์วิสใช้ในการเรียกใช้งาน API ของบริการพิสูจน์ตัว

จริง ดังรูปที่ 23 การเลือกกลุ่มผู้ใช้ในขั้นตอนการเพิ่มเว็บเซอร์วิสเป็นการกำหนดขอบเขตของผู้ใช้งานที่สามารถเข้าสู่ระบบเพื่อใช้งานเว็บเซอร์วิส ผู้ใช้งานที่ไม่ได้อยู่ภายในกลุ่มที่ถูกเลือกไว้จะไม่สามารถเข้าสู่ระบบจากเว็บเซอร์วิสดังกล่าวได้ การใช้งานบริการพิสูจน์ตัวจริงโดยเว็บเซอร์วิสจำเป็นต้องใช้ Client ID และ Secret Key ในการติดต่อสื่อสาร โดยอ้างอิง URL ของเว็บเซอร์วิสที่ทำการติดต่อสื่อสารว่าตรงกับที่ได้กรอกไว้ในขั้นตอนการเพิ่มเว็บเซอร์วิสหรือไม่ และ Client ID กับ Secret Key ถูกต้องหรือไม่ ถึงจะสามารถเรียกใช้งานบริการพิสูจน์ตัวจริงได้ เพื่อเป็นการป้องกันการแอบอ้างใช้งานและเป็นยืนยันความถูกต้องอของเว็บเซอร์วิส



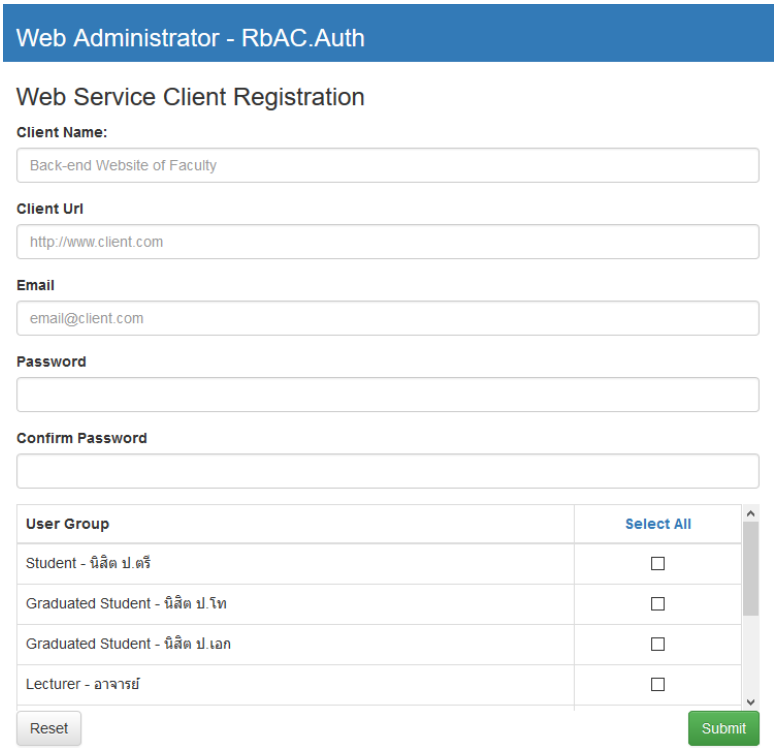
รูปที่ 22 การเพิ่มเว็บเซอร์วิสที่ต้องการใช้งานบริการพิสูจน์ตัวจริง

#	Client name	Client ID	Client Url	Secret Key	Tools
1	cms.thesis.dev	10004	http://cms.thesis.dev	c28714ab025f764cd814093ad01f42a97bb4d74a	Edit Delete
2	ส่วนทะเบียนนิสิต	10018	http://reg.thesis.dev	f05374881b1f650011853de99bd8fa0bb75ea011	Edit Delete
3	ภาควิชาวิศวกรรมคอมพิวเตอร์	10022	http://cs.eng.thesis.dev	8095ec6bf6ef42277b453d684beeb2d9cace39e4	Edit Delete

รูปที่ 23 รายการของเว็บเซอร์วิสที่สามารถใช้งานบริการพิสูจน์ตัวจริง

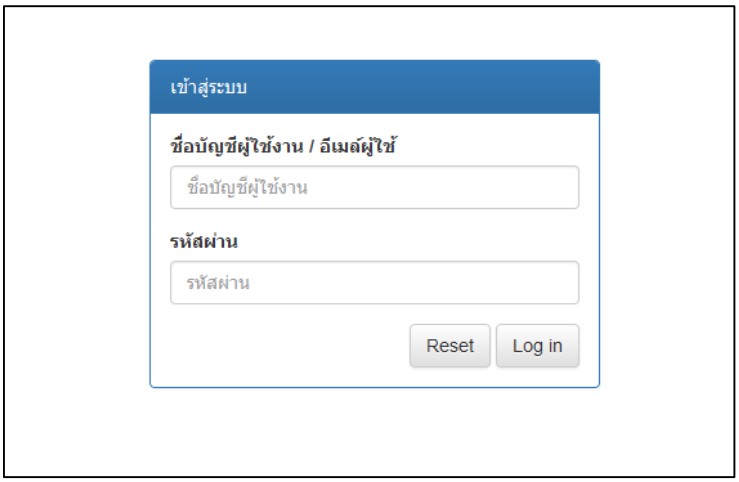
7) ผู้พัฒนาเว็บเซอร์วิสสามารถลงทะเบียนเว็บเซอร์วิสได้ด้วยตนเอง เพื่อขอใช้งานบริการพิสูจน์ตัวจริงได้จากหน้าลงทะเบียน ดังรูปที่ 24 โดยการกรอกข้อมูลของเว็บเซอร์วิสที่ต้องการขอใช้บริการ เลือกกลุ่มของผู้ใช้งาน ซึ่งกลุ่มที่มีให้เลือกเป็นกลุ่มที่ถูกสร้างขึ้นโดยเจ้าหน้าที่ดูแลระบบของบริการพิสูจน์ตัวจริงเพื่อใช้เป็นกลุ่มของผู้ใช้ทั่วไปที่ทุกเว็บเซอร์วิสที่ใช้บริการอยู่นำไปใช้เป็นกลุ่มผู้ใช้พื้นฐาน นอกจากนั้นผู้พัฒนาเว็บเซอร์วิสต้อง

กรอกอีเมล์ของผู้พัฒนาเว็บเซอร์วิสและรหัสผ่านเพื่อใช้ในการเข้าสู่เว็บส่วนบริหารของบริการพิสูจน์ตัวจริงหลังจากลงทะเบียนเสร็จเรียบร้อย



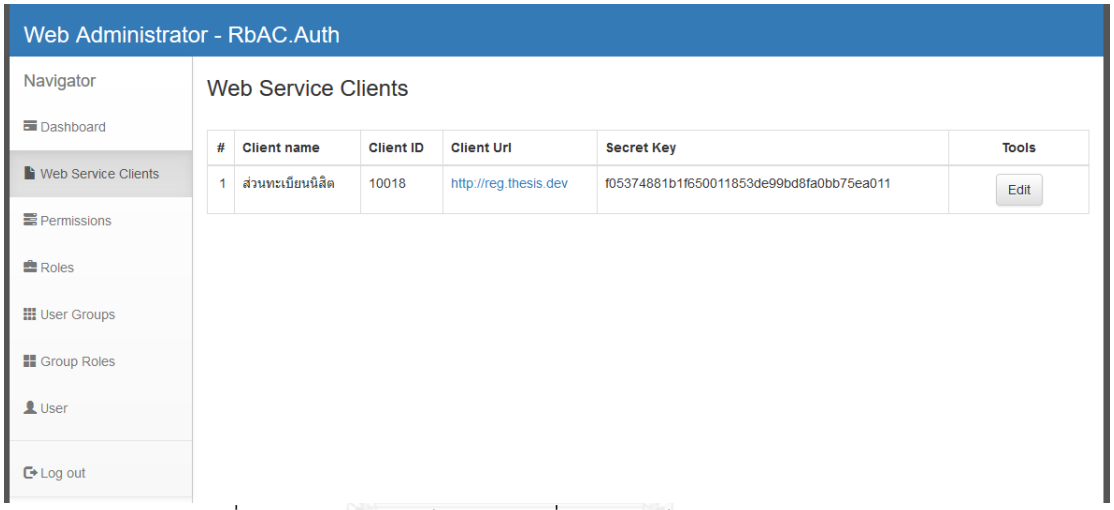
รูปที่ 24 หน้าลงทะเบียนเว็บเซอร์วิสด้วยตนเอง

8) หลังจากผู้พัฒนาเว็บเซอร์วิสทำการลงทะเบียนขอใช้บริการพิสูจน์ตัวจริงสามารถเข้าใช้งานเว็บบริหารของบริการพิสูจน์ตัวจริงได้ โดยใช้อีเมล์และรหัสผ่านที่ผู้พัฒนาเว็บเซอร์วิสได้กรอกในขั้นตอนการลงทะเบียนจากหน้าเข้าสู่ระบบของเว็บบริหาร ดังรูปที่ 25



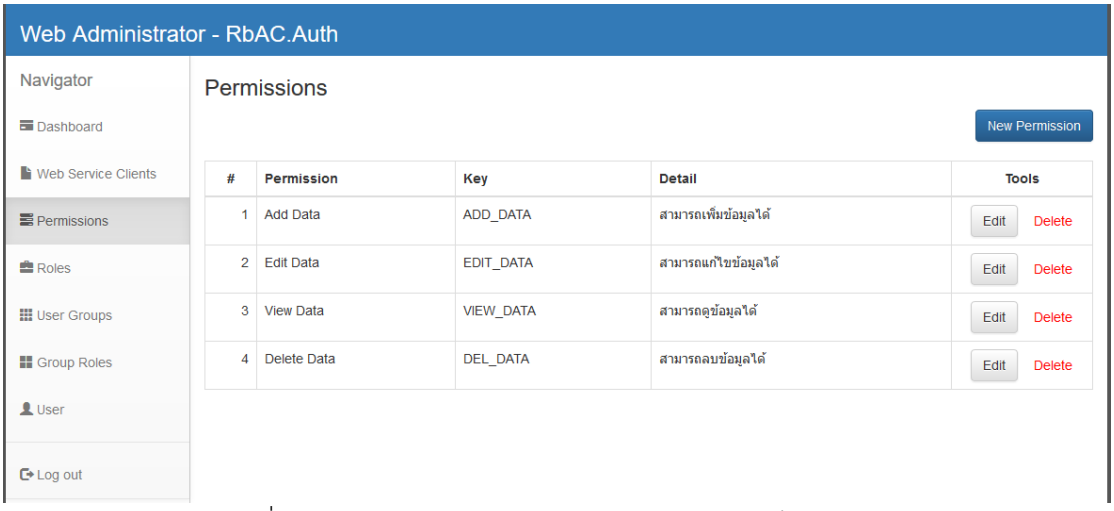
รูปที่ 25 หน้าเข้าสู่ระบบของเว็บบริหาร

9) เมื่อเข้าสู่ระบบเว็บบริหารในหน้าจัดการเว็บเซอร์วิสที่เลือกจากรายการ Web Service Clients จะแสดงข้อมูลของเว็บเซอร์วิสที่ผู้พัฒนาเว็บเซอร์วิสได้ลงทะเบียนไว้ พร้อมทั้งข้อมูลของ Client ID และ Secret Key สำหรับนำไปใช้ในการติดต่อสื่อสารระหว่างเว็บเซอร์วิสและบริการพิสูจน์ตัวจริง ดังรูปที่ 26 นอกจากนั้นผู้พัฒนาเว็บเซอร์วิส ยังสามารถแก้ไขข้อมูลของเว็บเซอร์วิสที่ลงทะเบียนไว้ได้ เช่น ชื่อของเว็บเซอร์วิส URL ของเว็บเซอร์วิส กลุ่มพื้นฐานที่เลือกไว้ เป็นต้น ข้อแตกต่างระหว่างผู้ดูละรับบเว็บส่วนบริหารกับผู้พัฒนาเว็บเซอร์วิสในหน้าจัดการเว็บเซอร์วิสคือ ผู้พัฒนาเว็บเซอร์วิสไม่สามารถเพิ่มเว็บเซอร์วิสใหม่ได้



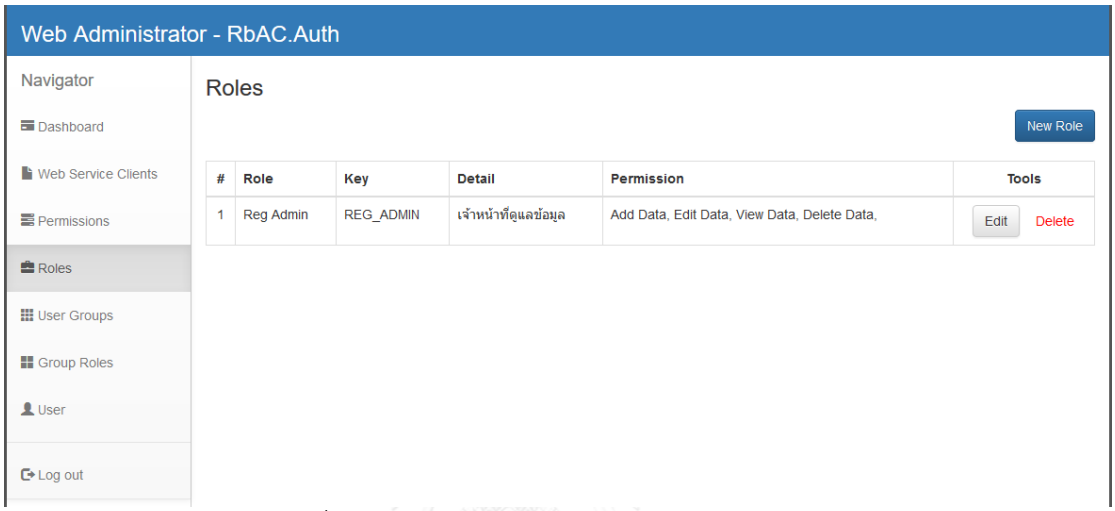
รูปที่ 26 หน้าจัดการเว็บเซอร์วิสที่ผู้พัฒนาเว็บเซอร์วิสลงทะเบียนไว้

10) ผู้พัฒนาเว็บเซอร์วิสสามารถสร้างการอนุญาตใช้งานของผู้ใช้สำหรับใช้กับเว็บเซอร์วิสของตนเองได้ในหน้าจัดการการอนุญาตจากรายการ Permissions โดยการอนุญาตที่สร้างขึ้นไม่สามารถใช้งานร่วมกับเว็บเซอร์วิสอื่นได้ ดังรูปที่ 27



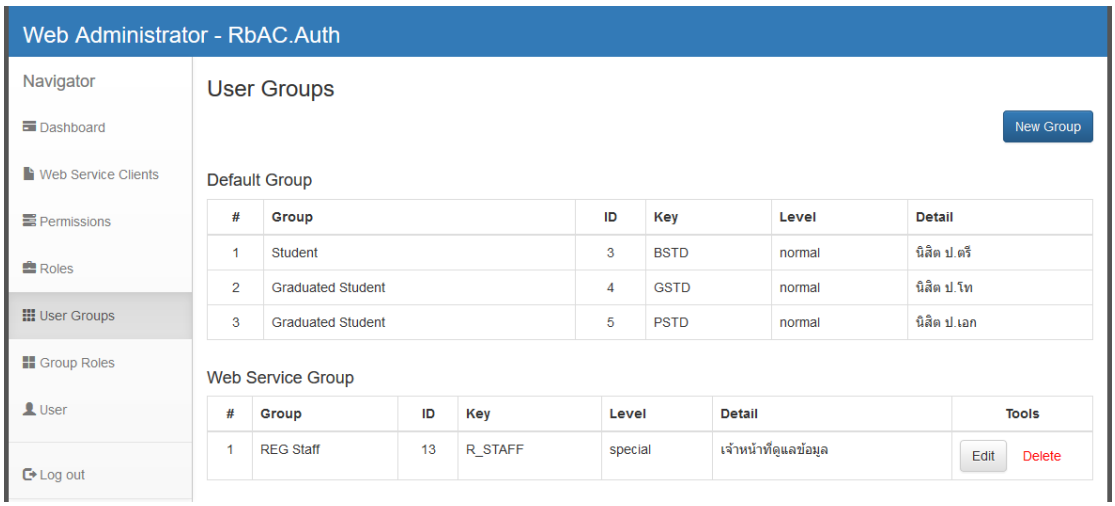
รูปที่ 27 หน้าจัดการการอนุญาตสำหรับใช้ภายในเว็บเซอร์วิส

11) ผู้พัฒนาเว็บเซอร์วิสสามารถสร้างบทบาทผู้ใช้เฉพาะสำหรับใช้ภายในเว็บเซอร์วิสเองได้เช่นเดียวกับการอนุญาตในหน้าจัดการบทบาทผู้ใช้ ดังรูปที่ 28 การสร้างบทบาทเฉพาะเพื่อใช้ภายในเว็บเซอร์วิสเป็นการเพิ่มบทบาทพิเศษที่ไม่มีในกลุ่มพื้นฐานที่บริหารพิสูจน์ตัวจริงมีให้ หรือเพื่อกำหนดบทบาทพิเศษให้กับผู้ใช้บางกลุ่มเพื่อให้ได้สิทธิ์พิเศษสำหรับใช้งานเว็บเซอร์วิส การสร้างบทบาทเฉพาะสามารถเลือกการอนุญาตที่สร้างขึ้นมาในข้อที่ 10 เพื่อกำหนดสิทธิ์ในการเข้าถึงของบทบาทเฉพาะนั้น



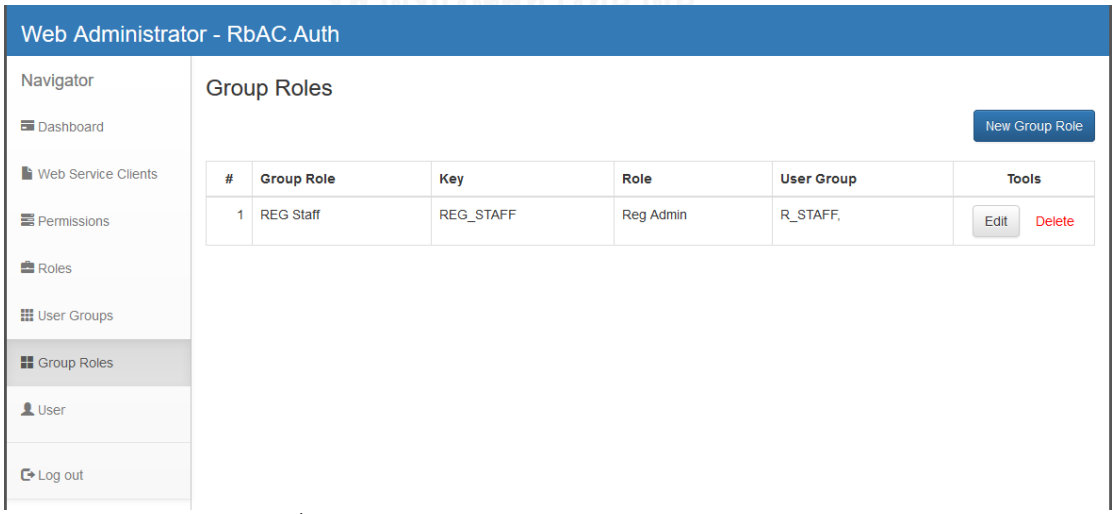
รูปที่ 28 หน้าจัดการบทบาทผู้ใช้ภายในเว็บเซอร์วิส

12) ผู้พัฒนาเว็บเซอร์วิสสามารถสร้างกลุ่มผู้ใช้พิเศษเพื่อใช้ภายในเว็บเซอร์วิสได้ในหน้าจัดการกลุ่มผู้ใช้จากรายการ User Groups อยู่ด้านซ้ายมือ ดังรูปที่ 29 การสร้างกลุ่มผู้ใช้พิเศษสำหรับใช้ภายในเว็บเซอร์วิสเป็นการสร้างกลุ่มผู้ใช้ที่มีสิทธิ์พิเศษนอกเหนือจากกลุ่มผู้ใช้พื้นฐานที่ผู้ดูแลระบบบริการพิสูจน์ตัวจริงได้เตรียมไว้เพื่อสร้างความแตกต่างระหว่างเว็บเซอร์วิสอื่นๆ โดยผู้ใช้กลุ่มที่อยู่ในกลุ่มพื้นฐานเดียวกันในแต่ละเว็บเซอร์วิสเมื่อผู้ใช้อยู่ในกลุ่มพิเศษที่ผู้พัฒนาเว็บเซอร์วิสสร้างขึ้น ก็สามารถได้รับการอนุญาตเข้าใช้งานแตกต่างกันได้



รูปที่ 29 หน้าจัดการกลุ่มผู้ใช้ภายในเว็บเซอร์วิส

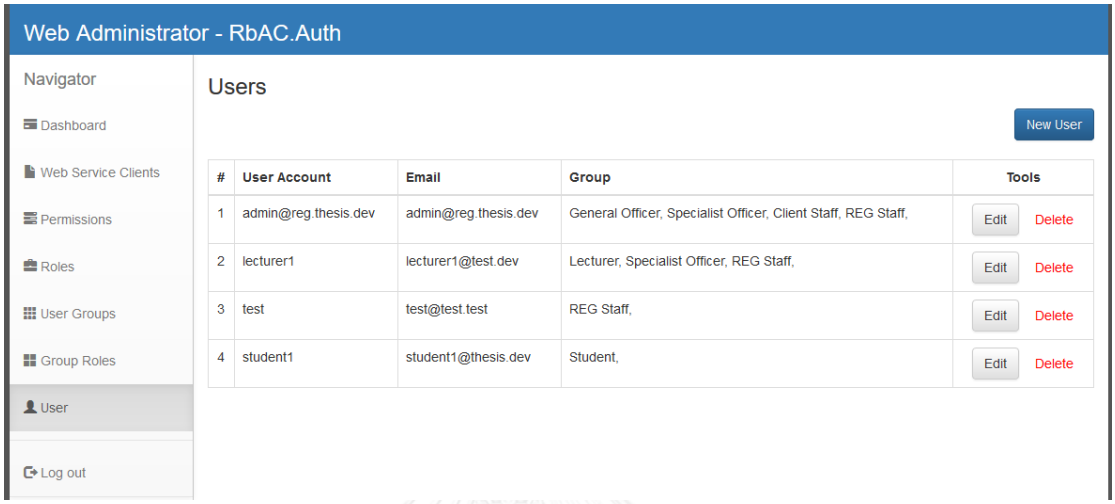
13) ผู้ใช้สามารถกำหนดบทบาทกลุ่มผู้ใช้งานเฉพาะเพื่อใช้งานภายในเว็บเซอร์วิสได้ในหน้าจัดการบทบาทกลุ่มผู้ใช้งานจากรายการ Group Roles ดังรูปที่ 30 การกำหนดบทบาทกลุ่มผู้ใช้งานเฉพาะเป็นการกำหนดบทบาทให้กับกลุ่มผู้ใช้ที่ถูกสร้างขึ้นมาเพื่อใช้เฉพาะภายในเว็บเซอร์วิส ซึ่งบทบาทก็เป็นบทบาทเฉพาะที่สร้างขึ้นในข้อที่ 11 เพื่อให้ผู้ใช้กลุ่มดังกล่าวได้รับการอนุญาตใช้งานพิเศษเฉพาะภายในเว็บเซอร์วิสนั้นๆ ยกตัวอย่างเช่น ผู้ใช้งานคนหนึ่งที่อยู่ในกลุ่มอาจารย์ทั่วไป เมื่อเข้าใช้เว็บเซอร์วิสการอนุญาตเข้าใช้งานก็จะเหมือนกันทุกเว็บเซอร์วิส ยกเว็บเว็บเซอร์วิสที่ผู้ใช้งานคนดังกล่าวถูกจัดอยู่ในกลุ่มผู้ดูแลเว็บเซอร์วิส ผู้ใช้งานสามารถได้รับการอนุญาตใช้งานในส่วนของผู้ดูแลเว็บเซอร์วิสเพิ่มเติมจากปกติ เป็นต้น



รูปที่ 30 หน้าจัดการบทบาทกลุ่มผู้ใช้ภายในเว็บเซอร์วิส

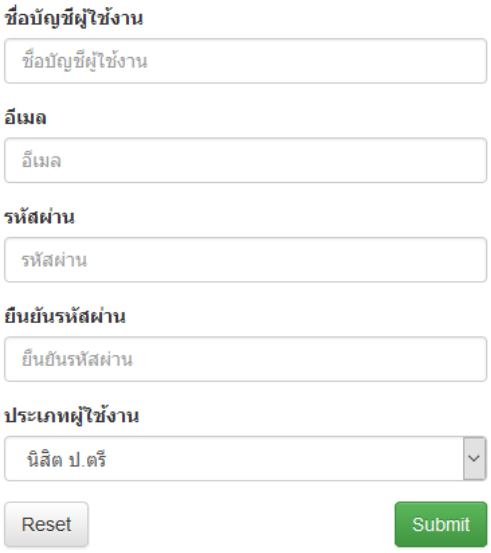
14) หน้าจัดการผู้ใช้งานจากรายการ User ผู้พัฒนาเว็บเซอร์วิสสามารถดูผู้ใช้งานที่มีสิทธิ์เข้าในเว็บเซอร์วิสของตนเอง ดังรูปที่ 31โดยที่รายการผู้ใช้ที่แสดงให้เห็น เป็นรายการของ

ผู้ใช้งานที่อยู่ในกลุ่มผู้ใช้พื้นฐานผู้พัฒนาเว็บเซอร์วิสได้เลือกไว้ และ ผู้ใช้ที่อยู่ในกลุ่มเฉพาะที่ผู้พัฒนาเว็บเซอร์วิสได้สร้างขึ้น นอกจากนั้นผู้พัฒนาเว็บเซอร์วิสสามารถเพิ่มผู้ใช้งานใหม่โดยสามารถเลือกกลุ่มให้กับผู้ใช้งานใหม่ได้ทั้งกลุ่มพื้นฐานที่เลือกแล้วและกลุ่มเฉพาะที่สร้างไว้ได้



รูปที่ 31 หน้าจัดการผู้ใช้งานภายในเว็บเซอร์วิส

15) ผู้พัฒนาเว็บเซอร์วิสสามารถแบบฟอร์มสำหรับให้ผู้ใช้งานทำการสมัครสมาชิกในหน้าเว็บเซอร์วิส โดยทำการเลือกประเภทกลุ่มของผู้ใช้งาน ดังรูปที่ 32 หรือผู้พัฒนาเว็บเซอร์วิสสามารถกำหนดกลุ่มให้กับผู้สมัครใหม่ได้เช่นกัน



รูปที่ 32 การสมัครสมาชิกในหน้าเว็บเซอร์วิส

16) เมื่อมีการสมัครสมาชิกจากผู้ใช้งานใหม่ เว็บเซอร์วิสส่งข้อมูลผู้ใช้งานที่ทำการสมัครสมาชิกไปยังบริการพิสูจน์ตัวจริงผ่าน API โดยใช้การส่งข้อมูลแบบ Server-side Script

เพื่อรักษาความปลอดภัยของข้อมูลเบื้องต้น โดยจำเป็นต้องใช้ Client ID และ Secret Key ที่จากการเพิ่มเว็บเซอร์วิสในข้อที่ 6 โดยโค้ดในการใช้งาน ดังรูปที่ 33

```php
$url = 'http://auth.thesis.dev/register';
$data = array(
    'username' => $username,
    'password' => $password,
    'group' => $group,
    'client_id' => 10001,
    'secret_key' => "6c447a8fe7677ddc4c4cd2efddcfe650e4e6c706"
);
$respond = $this->curl->simple_post($url,$data);
```

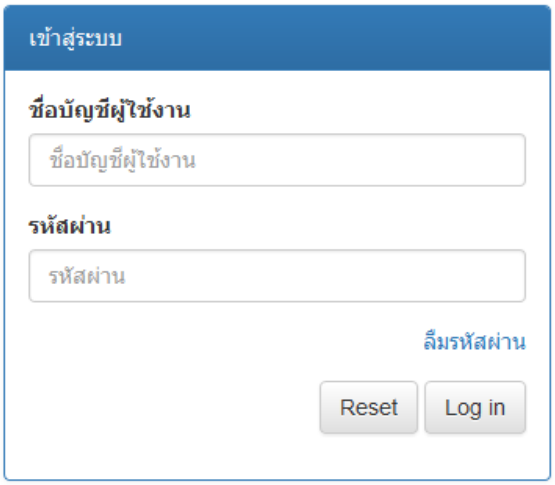
รูปที่ 33 ส่งข้อมูลผู้ใช้ที่ทำการสมัครสมาชิกแบบ Servier-side Script ยังบริการพิสูจน์ตัวจริง

17) หลังจากได้รับข้อมูลจากเว็บเซอร์วิสบริการพิสูจน์ตัวจริงนำข้อมูลที่ได้มาทำการตรวจสอบความสมบูรณ์ของข้อมูลว่าครบถ้วนหรือไม่ หากข้อมูลผู้ใช้ที่ส่งมาสมบูรณ์ครบถ้วนบริการพิสูจน์ตัวจริงจึงทำการบันทึกข้อมูลผู้ใช้ลงฐานข้อมูล และเพิ่มผู้ใช้งานเข้ากับกลุ่มผู้ใช้งานที่ได้เลือกไว้ จากนั้นส่งผลลัพธ์การดำเนินการกลับไปยังเว็บเซอร์วิสในรูปแบบข้อมูล JSON ดังรูปที่ 34

```
{
    status: "OK",
    code: "200",
    message: "การสมัครสมาชิกเรียบร้อย"
}
```

รูปที่ 34 ผลลัพธ์การดำเนินการในรูปแบบข้อมูล JSON

18) ผู้ใช้ที่ทำการสมัครสมาชิกสำเร็จ สามารถทำการเข้าสู่ระบบในหน้าเว็บเซอร์วิส จากนั้นเว็บเซอร์วิสส่งข้อมูลผู้ใช้ที่ทำการเข้าสู่ระบบไปยังบริการพิสูจน์ตัวจริงผ่านทาง API โดยใช้การส่งข้อมูลแบบ Server-side Script เพื่อทำการพิสูจน์ตัวจริงและขอการอนุญาตการใช้งานตามกลุ่มของผู้ใช้ ดังรูปที่ 35-รูปที่ 36



รูปที่ 35 การเข้าสู่ระบบในหน้าเว็บเซอร์วิส

```
43          $url = 'http://auth.thesis.dev/authentication';
44          $data = array(
45              'username' => $username,
46              'password' => $password,
47              'client_id' => 10001,
48              'secret_key' => "6c447a8fe7677ddc4c4cd2efddcfe650e4e6c706"
49          );
50          $respond = $this->curl->simple_post($url,$data);
```

รูปที่ 36 การส่งข้อมูลผู้ใช้ที่ทำการเข้าสู่ระบบแบบ Servier-side Script ยังบริการพิสูจน์ตัวจริง

19) บริการพิสูจน์ตัวจริงทำการตรวจสอบความถูกต้องของข้อมูลผู้ใช้ โดยตรวจสอบการมีอยู่ของชื่อผู้ใช้งานในฐานข้อมูล สถานะการใช้งานของชื่อผู้ใช้งาน และความเข้ากันได้ของชื่อผู้ใช้งานและรหัสผ่าน จากนั้นบริการพิสูจน์ตัวจริงทำการสร้างโทเค็นการใช้งานหรือปรับปรุงโทเค็นเดิมที่มีอยู่แล้ว และสร้างรายการอนุญาตการใช้งานต่างๆ โดยอ้างอิงจากบทบาทกลุ่มผู้ใช้ที่ผู้ใช้งาน และเว็บเซอร์วิสที่เป็นตัวเรียกใช้งานบริการพิสูจน์ตัวจริง ซึ่งแต่ล่ะเว็บเซอร์วิสผู้ใช้สามารถได้การอนุญาตที่แตกต่างกัน ขึ้นอยู่กับกลุ่มผู้ใช้งานที่เว็บเซอร์วิสเลือกไว้และกลุ่มผู้ใช้พิเศษที่เว็บเซอร์วิสสร้างขึ้น แล้วส่งข้อมูลโทเค็นและรายการการอนุญาตเข้าใช้งานกลับไปยังเว็บเซอร์วิสในรูปแบบข้อมูล JSON ดังรูปที่ 37

```
{
    status: "OK",
    code: "200",
    message: "การเข้าสู่ระบบเรียบร้อย",
    access_token: "17c395b0bed0d2947cee2ed001cb747317de18d4",
  ▾ group: {
        name: "Student",
        key: "BSTD"
    },
  ▾ role: {
        name: "Visitor",
        key: "VISITOR"
    },
  ▾ permission: [
        "VIEW_DATA"
    ]
}
```


รูปที่ 37 ข้อมูลโทเค็นและรายการการอนุญาตเข้าใช้งานกลับไปยังเว็บเซอร์วิส

20) การเข้าสู่ระบบของแต่ล่ะเว็บเซอร์วิส ผู้ใช้สามารถได้รับการอนุญาตการใช้งานที่แตกต่างกัน ขึ้นอยู่กับกลุ่มผู้ใช้พื้นฐานที่ผู้พัฒนาเว็บเซอร์วิสเลือกในขั้นตอนการลงทะเบียนเว็บเซอร์วิส รวมทั้งกลุ่มผู้ใช้พิเศษที่ผู้พัฒนาเว็บเซอร์วิสสร้างขึ้นเพื่อใช้ภายในเว็บเซอร์วิส ตัวอย่างของการได้รับการอนุญาตที่แตกต่างกันของผู้ใช้คนเดียวกัน แสดงในรูปที่ 38-รูปที่ 39 ซึ่งจะเห็นว่าผู้ใช้งานคนเดียวกันสามารถได้รับการอนุญาตการใช้งานที่ต่างกัน ได้รับกลุ่มผู้ใช้ที่ต่างกัน มีบทบาทที่ต่างกันกลุ่มของผู้ใช้ในแต่ล่ะเว็บเซอร์วิส


```
{
  "status": "OK",
  "code": "200",
  "message": "การเข้าสู่ระบบเรียบร้อย",
  "access_token": "0cd3ac65ccae0cc769eadc653d8b710260c1cc04X$dd139bc1543309f340b8d5364dc2bd8beadc62c6",
  "group": {
    "name": "Lecturer",
    "key": "BLCT"
  },
  "role": [
    {
      "name": "Editor",
      "key": "EDITOR"
    },
    {
      "name": "Manager",
      "key": "MANAGER"
    },
    {
      "name": "Staff ",
      "key": "STAFF"
    }
  ],
  "permission": [
    "ADD_DATA",
    "EDIT_DATA",
    "VIEW_DATA",
    "DEL_DATA",
    "ADD_STAFF",
    "VIEW_STAFF",
    "DEL_STAFF",
    "EDIT_STAFF"
  ],
  "user_id": "20",
  "user_email": "lecturer1@test.dev"
}
```


รูปที่ 38 ตัวอย่างการอนุญาตที่แตกต่างกันของผู้ใช้คนในเว็บเซอร์วิส A

```
{
  "status": "OK",
  "code": "200",
  "message": "การเข้าสู่ระบบเรียบร้อย",
  "access_token": "7db0b440f28e21c838e4fb78885528f434d73a17X$1e583b3d635ac5d66e371fe9604a44d8c7cb7a48",
  "group": {
    "name": "REG Staff",
    "key": "R_STAFF"
  },
  "role": [
    {
      "name": "Reg Admin",
      "key": "REG_ADMIN"
    }
  ],
  "permission": [
    "ADD_DATA",
    "EDIT_DATA",
    "VIEW_DATA",
    "DEL_DATA"
  ],
  "user_id": "20",
  "user_email": "lecturer1@test.dev"
}
```


รูปที่ 39 ตัวอย่างการอนุญาตที่แตกต่างกันของผู้ใช้คนในเว็บเซอร์วิส B

21) ตัวอย่างการนำข้อมูลจากบริการพิสูจน์ตัวจริงไปใช้งานกับเว็บเซอร์วิสโดยประยุกต์ในกับส่วนรายการนำทางของเว็บเซอร์วิสที่ผู้ใช้งานสามรถใช้งานได้ โดยใช้ข้อมูลบทบาทผู้ใช้และการใช้ข้อมูลการอนุญาตการใช้งาน ดังรูปที่ 40-รูปที่ 41

```
<?php if(in_array('STAFF',$role)){?>
    <li role="presentation" class="<?php echo ($pageName=="user")?'active':'';?>">
        <a href="<?php echo site_url('user')?>">User</a>
    </li>
<?php }?>
```

รูปที่ 40 การประยุกต์ใช้ข้อมูลบทบาทผู้ใช้ในส่วนรายการนำทางของเว็บเซอร์วิส

```
<?php if(in_array('EDITOR',$role)&&in_array('ADD_DATA',$permission)){?>
    <button class="btn btn-primary">New Article</button>
<?php }?>
```

รูปที่ 41 การประยุกต์ใช้ข้อมูลบทบาทผู้ใช้และการอนุญาตกับเว็บเซอร์วิส

บทที่ 5
การทดสอบและการวิเคราะห์ผล

5.1. วัตถุประสงค์ของการทดสอบ

จุดประสงค์ของการทดสอบ เพื่อสนับสนุนแนวทางในการพัฒนาบริการพิสูจน์ตัวจริงที่ได้ออกแบบและพัฒนาเครื่องมือที่สนับสนุนแนวทางในบทที่ 4 โดยเนื้อหาจะประกอบไปด้วยการทดสอบระบบ ตั้งแต่การสร้างบทบาทและการอนุญาตใช้งาน การจัดกลุ่มผู้ใช้และบทบาทกลุ่มผู้ใช้ การเพิ่มผู้ใช้งานใหม่ การเพิ่มเว็บเซอร์วิสใหม่ ตลอดจนการเรียกใช้บริการพิสูจน์ตัวจริงผ่านเว็บเซอร์วิส

5.2. การทดสอบระบบ

การทดสอบบริการพิสูจน์ตัวจริงทั้งในส่วนของ API และ เว็บส่วนบริหารจะถูกแบ่งการทดสอบออกตามฟังก์ชันการใช้งานหลักๆ ของระบบที่ได้ออกแบบไว้ ซึ่งจะมุ่งเน้นทดสอบฟังก์ชันการทำงาน และความถูกต้องของการจัดการข้อมูลของเว็บส่วนบริหาร รวมถึงผลลัพธ์ที่ได้จากการเรียกใช้บริการพิสูจน์ตัวจริงโดยเว็บเซอร์วิสผ่าน API ดังต่อไปนี้

1) ทดสอบจัดการบทบาทของผู้ใช้และการจัดการการอนุญาตการใช้งาน

   การทดสอบการจัดการบทบาทของผู้ใช้งานทั้งการสร้างบทบาทใหม่ การแก้ไขบทบาทเดิมที่มีอยู่การลบบทบาทที่มีอยู่ และการจัดการการอนุญาตการใช้งาน ทั้งการสร้างการอนุญาตใหม่ การแก้ไขและการลบการอนุญาตที่มีอยู่

2) ทดสอบการจัดการความสัมพันธ์ระหว่างบทบาทและการอนุญาต

   วัตถุประสงค์ในการทดสอบคือการทดสอบความสัมพันธ์ของบทบาทและการอนุญาตใช้งานที่ได้มีการอ้างอิงซึ่งกันและกันหลังจากมีการแก้ไขเปลี่ยนแปลง หรือการสร้างความสัมพันธ์ขึ้นมาใหม่

3) ทดสอบการจัดการกลุ่มผู้ใช้และการจัดการบทบาทกลุ่มผู้ใช้

   การทดสอบการจัดการกลุ่มผู้ใช้งานทั้งการสร้างกลุ่มผู้ใช้งานใหม่ การแก้ไขกลุ่มผู้ใช้งานเดิมที่มีอยู่การลบกลุ่มผู้ใช้งานที่มีอยู่ และการจัดบทบาทการกลุ่มผู้ใช้งาน ทั้งการสร้างบทบาทการกลุ่มผู้ใช้งาน การแก้ไขและการลบบทบาทการกลุ่มผู้ใช้งานที่มีอยู่

4) ทดสอบความสัมพันธ์ระหว่างกลุ่มผู้ใช้และบทบาทกลุ่มผู้ใช้

วัตถุประสงค์ในการทดสอบคือการทดสอบความสัมพันธ์ของบทบาทการกลุ่มผู้ใช้งานและกลุ่มผู้ใช้งานที่ได้มีการอ้างอิงซึ่งกันและกันหลังจากมีการแก้ไขเปลี่ยนแปลง หรือการสร้างขความสัมพันธ์ขึ้นมาใหม่

5) ทดสอบการจัดผู้ใช้งานและการเพิ่มผู้ใช้งานใหม่

การทดสอบการจัดการผู้ใช้งาน การเพิ่มผู้ใช้งานใหม่ การเลือกกลุ่มของผู้ใช้งาน และดูความถูกต้องของบทบาทที่ได้หลังจากการเลือกกลุ่ม

6) ทดสอบการจัดการเว็บเซอร์วิสจะสามารถใช้งานบริการพิสูจน์ตัวจริงได้

ทดสอบการจัดการข้อมูลของเว็บเซอร์วิสที่มีการเรียกใช้งานบริการ พิสูจน์ตัวจริง และการเพิ่มเว็บเซอร์วิสใหม่ให้สามารถใช้งานบริการพิสูจน์ตัวจริงได้

7) ทดสอบทดสอบเรียกใช้งานบริการพิสูจน์ตัวจริงโดยเว็บเซอร์วิสผ่าน API

ทดสอบความถูกต้องของการใช้งานบริการพิสูจน์ตัวจริงผ่าน API โดยดูว่าได้โทเค็นและการอนุญาตส่งไปให้กับเว็บเซอร์วิสอย่างถูกต้อง

8) ทดสอบความถูกต้องของการแสดงข้อมูลภายในเว็บส่วนบริหาร

ทดสอบความถูกต้องของการแสดงข้อมูลในแต่ล่ะหน้าของเว็บส่วนบริหารของบริการพิสูจน์ตัวจริง

9) ทดสอบการใช้งานของผู้พัฒนาเว็บเซอร์วิส

ทดสอบความถูกต้องของการใช้งานในส่วนของผู้พัฒนาเว็บเซอร์วิสที่ต้องการใช้งานบริการพิสูจน์ตัวจริง การลงทะเบียนเว็บเซอร์วิส และ การใช้งานเว็บบริหารของบริการพิสูจน์ตัวจริง

ตารางที่ 4 ทดสอบจัดการบทบาทของผู้ใช้และการจัดการการอนุญาตการใช้งาน

รหัส	**คำอธิบาย**	**ผลการทดสอบที่คาดหวัง**	**ผลลัพธ์**
TC01	จัดการการอนุญาตการใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถสร้างข้อมูลการอนุญาตการใช้งาน	ถูกต้อง
TC02	จัดการการอนุญาตการใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถแก้ไขข้อมูลการอนุญาตการใช้งาน	ถูกต้อง

TC03	จัดการการอนุญาตการใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถลบข้อมูลการอนุญาตการใช้งาน	ถูกต้อง
TC04	จัดการบทบาทผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลบทบาทผู้ใช้งาน	สามารถสร้างข้อมูลบทบาทผู้ใช้งาน	ถูกต้อง
TC05	จัดการบทบาทผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลบทบาทผู้ใช้งาน	สามารถแก้ไขข้อมูลบทบาทผู้ใช้งาน	ถูกต้อง
TC06	จัดการบทบาทผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลบทบาทผู้ใช้งาน	สามารถลบข้อมูลบทบาทผู้ใช้งาน	ถูกต้อง

ตารางที่ 5 ทดสอบการจัดการความสัมพันธ์ระหว่างบทบาทและการอนุญาต

รหัส	**คำอธิบาย**	**ผลการทดสอบที่คาดหวัง**	**ผลลัพธ์**
TC07	แก้ไขข้อมูลการอนุญาตการใช้งานข้อมูลที่ปรากฏในบทบาทที่มีความสัมพันธ์กันจะมีการเปลี่ยนแปลง	สามารถแก้ไขความสัมพันธ์การอนุญาตในข้อมูลบทบาทได้	ถูกต้อง
TC08	แก้ไขข้อมูลการอนุญาตการใช้งานข้อมูลที่ปรากฏในบทบาทที่มีความสัมพันธ์กันจะมีการเปลี่ยนแปลง	ข้อมูลการอนุญาตในแต่ละบทบาทมีการเปลี่ยนแปลงตามที่ได้แก้ไขการอนุญาต	ถูกต้อง
TC09	แก้ไขข้อมูลบทบาทที่มีความสัมพันธ์อยู่กับการอนุญาตจะจ้องไม่มีผลกระทบกับการอนุญาตนั้น	ข้อมูลการอนุญาตไม่มีการเปลี่ยนแปลง	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC10	การลบข้อมูลการอนุญาตโดยที่ยังมีความสัมพันธ์กับทบาทอยู่จะต้องไม่เกิดข้อผิดพลาด	การลบการอนุญาตแล้วความสัมพันธ์ที่มีต่อบทบาทจะต้องถูกลบด้วย	ถูกต้อง

ตารางที่ 6 ทดสอบการจัดการกลุ่มผู้ใช้และการจัดการบทบาทกลุ่มผู้ใช้

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC11	จัดการกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถสร้างกลุ่มผู้ใช้งานได้	ถูกต้อง
TC12	จัดการกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถแก้ไขกลุ่มผู้ใช้งานได้	ถูกต้อง
TC13	จัดการกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถลบกลุ่มผู้ใช้งานได้	ถูกต้อง
TC14	จัดการบทบาทกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถสร้างบทบาทกลุ่มผู้ใช้งานได้	ถูกต้อง
TC15	จัดการบทบาทกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถแก้ไขบทบาทกลุ่มผู้ใช้งานได้	ถูกต้อง
TC16	จัดการบทบาทกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถลบบทบาทกลุ่มผู้ใช้งานได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC17	จัดการบทบาทกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถเลือกบทาทจากรายการบทบาทที่มีอยู่ได้	ถูกต้อง
TC18	จัดการบทบาทกลุ่มผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลการอนุญาตการใช้งาน	สามารถเลือกกลุ่มผู้ใช้งานจากรายการกลุ่มผู้ใช้งานได้มากกว่า 1 กลุ่ม	ถูกต้อง

ตารางที่ 7 ทดสอบความสัมพันธ์ระหว่างกลุ่มผู้ใช้ บทบาทผู้ใช้และบทบาทกลุ่มผู้ใช้

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC19	การแก้ไขข้อมูลของกลุ่มผู้ใช้งานข้อมูลกลุ่มผู้ใช้งานที่อยู่ในกลุ่มบทบาทจะต้องมีการเปลี่ยนแปลงตาม	ข้อมูลกลุ่มผู้ใช้ในบทบาทกลุ่มผู้ใช้มีการเปลี่ยนแปลงถูกต้อง	ถูกต้อง
TC20	การแก้ไขข้อมูลของบทบาทผู้ใช้งานข้อมูลกลุ่มผู้ใช้งานที่อยู่ในกลุ่มบทบาทจะต้องมีการเปลี่ยนแปลงตาม	ข้อมูลบทบาทผู้ใช้ในบทบาทกลุ่มผู้ใช้มีการเปลี่ยนแปลงถูกต้อง	ถูกต้อง
TC21	การยกเลิกความสัมพันธ์ของกลุ่มผู้ใช้งานในข้อมูลบทบาทผู้ใช้งาน	ข้อมูลกลุ่มผู้ใช้งานที่ถูกยกเลิกถูกลบออกจากข้อมูลบทบาทกลุ่มผู้ใช้งาน	ถูกต้อง
TC22	การลบบทบาทที่มีความสัมพันธ์กับข้อมูลบทบาทผู้ใช้งาน	ข้อมูลบทบาทในบทบาทกลุ่มผู้ใช้ถูกลบออก	ถูกต้อง

ตารางที่ 8 ทดสอบการจัดผู้ใช้งานและการเพิ่มผู้ใช้งานใหม่

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC23	จัดการผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลผู้ใช้งาน	สามารถเพิ่มผู้ใช้งานใหม่ได้	ถูกต้อง
TC24	จัดการผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลผู้ใช้งาน	สามารถแก้ไขข้อมูลผู้ใช้งานได้	ถูกต้อง
TC25	จัดการผู้ใช้งานโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลผู้ใช้งาน	สามารถลบข้อมูลผู้ใช้งานได้	ถูกต้อง

ตารางที่ 9 ทดสอบการจัดการเว็บเซอร์วิสที่จะสามารถใช้งานบริการพิสูจน์ตัวจริงได้

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC26	จัดการเว็บเซอร์วิสที่จะสามารถใช้งานบริการพิสูจน์ตัวจริงโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลได้	สามารถเพิ่มเว็บเซอร์วิสที่สามารถใช้งานบริการพิสูจน์ตัวจริงได้	ถูกต้อง
TC27	จัดการเว็บเซอร์วิสที่จะสามารถใช้งานบริการพิสูจน์ตัวจริงโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลได้	สามารถแก้ไขเว็บเซอร์วิสที่สามารถใช้งานบริการพิสูจน์ตัวจริงได้	ถูกต้อง
TC28	จัดการเว็บเซอร์วิสที่จะสามารถใช้งานบริการพิสูจน์ตัวจริงโดยสามารถสร้าง แก้ไข และ ลบ ข้อมูลได้	สามารถลบเว็บเซอร์วิสที่สามารถใช้งานบริการพิสูจน์ตัวจริงได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC29	จัดการเว็บเซอร์วิสที่จะสามารถใช้งานบริการพิสูจน์ตัวจริงโดยได้รับ Client ID	ได้รับ Client ID	ถูกต้อง
TC30	จัดการเว็บเซอร์วิสที่จะสามารถใช้งานบริการพิสูจน์ตัวจริงโดยได้รับ Secret Key	ได้รับ Secret Key	ถูกต้อง

ตารางที่ 10 ทดสอบทดสอบเรียกใช้งานบริการพิสูจน์ตัวจริงโดยเว็บเซอร์วิสผ่าน API

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC31	ผู้ใช้งานสมัครสมาชิกผ่านเว็บเซอร์วิส	สามารถสมัครสมาชิกได้	ถูกต้อง
TC32	ผู้ใช้งานสมัครสมาชิกผ่านเว็บเซอร์วิส	บริการพิสูจน์ตัวจริงจัดเก็บข้อมูลผู้ใช้ลงฐานข้อมูลถูกต้อง	ถูกต้อง
TC33	ผู้ใช้งานเข้าสู่ระบบผ่านเว็บเซอร์วิส	บริการพิสูจน์ตัวจริงสร้างโทเค็นได้	ถูกต้อง
TC34	ผู้ใช้งานเข้าสู่ระบบผ่านเว็บเซอร์วิส	บริการพิสูจน์ตัวจริงปรับปรุงโคเค็นที่มีอยู่แล้วได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC35	ผู้ใช้งานเข้าสู่ระบบผ่านเว็บเซอร์วิส	บริการพิสูจน์ตัวจริงสามารถสร้างรายการการอนุญาตได้	ถูกต้อง
TC36	ผู้ใช้งานเข้าสู่ระบบผ่านเว็บเซอร์วิส	บริการพิสูจน์ตัวจริงสามารถสร้างรายการบทบาทผู้ใช้ได้	ถูกต้อง
TC37	ผู้ใช้งานเข้าสู่ระบบผ่านเว็บเซอร์วิส	บริการพิสูจน์ตัวจริงสามารถส่งข้อมูลกลับไปยังเว็บเซอร์วิสได้ถูกต้อง	ถูกต้อง
TC38	เว็บเซอร์วิสใช้งานข้อมูลที่ได้จากบริการพิสูจน์ตัวจริง	สามารถใช้งานข้อมูลที่ส่งมาจากบริการพิสูจน์ตัวจริงได้	ถูกต้อง
TC39	ป้องกันการใส่ชื่อผู้ใช้งานซ้ำกับที่มีอยู่ในระบบในการลงทะเบียน	สามารถป้องกันการใส่ชื่อผู้ใช้งานซ้ำกับที่มีอยู่ในระบบในการลงทะเบียนได้	ถูกต้อง
TC40	ป้องกันการไม่ใส่ชื่อผู้ใช้งานในการลงทะเบียน	สามารถป้องกันการไม่ใส่ชื่อผู้ใช้งานในการลงทะเบียนได้	ถูกต้อง
TC41	ป้องกันการใส่รหัสผ่านและยืนยันรหัสผ่านไม่ตรงกันในการลงทะเบียน	สามารถป้องกันการใส่รหัสผ่านและยืนยันรหัสผ่านไม่ตรงกันในการลงทะเบียนได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC42	ป้องกันการไม่ใส่รหัสผ่านในการลงทะเบียน	สามารถป้องกันการไม่ใส่รหัสผ่านในการลงทะเบียนได้	ถูกต้อง
TC43	ป้องกันการใส่อีเมล์ซ้ำกับที่มีอยู่ในระบบในการลงทะเบียน	สามารถป้องกันการใส่อีเมล์ซ้ำกับที่มีอยู่ในระบบในการลงทะเบียนได้	ถูกต้อง
TC44	ป้องกันการไม่ใส่อีเมล์ในการลงทะเบียน	สามารถป้องกันการไม่ใส่อีเมล์ในการลงทะเบียนได้	ถูกต้อง
TC45	ป้องกันการไม่เลือกกลุ่มผู้ใช้ในการลงทะเบียน	สามารถป้องกันการไม่เลือกกลุ่มผู้ใช้ในการลงทะเบียนได้	ถูกต้อง
TC46	ได้รับบทบาทที่แตกต่างกันจากเว็บเซอร์วิสต่างเว็บกัน	สามารถได้รับบทบาทที่แตกต่างกันจากเว็บเซอร์วิสต่างเว็บกันได้	ถูกต้อง
TC47	ได้รับการอนุญาตที่แตกต่างกันจากเว็บเซอร์วิสต่างเว็บกัน	สามารถได้รับการอนุญาตที่แตกต่างกันจากเว็บเซอร์วิสต่างเว็บกันได้	ถูกต้อง
TC48	ระบุกลุ่มผู้ใช้ถูกต้องในการเข้าสู่ระบบของแต่ล่ะเว็บเซอร์วิส	สามารถระบุกลุ่มผู้ใช้ถูกต้องในการเข้าสู่ระบบของแต่ล่ะเว็บเซอร์วิสได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC49	ผู้ใช้ที่ไม่ได้อยู่ในกลุ่มที่เว็บเซอร์วิสเลือกไม่สามารถเข้าสู่ระบบของเว็บเซอร์วิส	ผู้ใช้ที่ไม่ได้อยู่ในกลุ่มที่เว็บเซอร์วิสเลือกไม่สามารถเข้าสู่ระบบของเว็บเซอร์วิสได้	ถูกต้อง
TC50	เพิ่มผู้ใช้ให้อยู่ในกลุ่มพิเศษที่ผู้พัฒนาเว็บเซอร์วิสสร้างขึ้น	สามารถเพิ่มผู้ใช้ให้อยู่ในกลุ่มพิเศษที่ผู้พัฒนาเว็บเซอร์วิสสร้างขึ้นได้	ถูกต้อง

ตารางที่ 11 ทดสอบความถูกต้องของการแสดงข้อมูลภายในเว็บส่วนบริหาร

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC51	การแสดงข้อมูลภาพรวมในหน้า Dash Board ของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลภาพรวมของบริการพิสูจน์ตัวจริงได้ถูกต้อง	ถูกต้อง
TC52	การแสดงผลหน้าจัดการการอนุญาตของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลหน้าจัดการอนุญาตได้ถูกต้อง	ถูกต้อง
TC53	การแสดงผลหน้าจัดการบทบาทผู้ใช้ของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลบทบาทผู้ใช้ได้ถูกต้อง	ถูกต้อง
TC54	การแสดงผลหน้าจัดการกลุ่มผู้ใช้ ของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลกลุ่มผู้ใช้ได้ถูกต้อง	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC55	การแสดงผลหน้าจัดการบทบาทกลุ่มผู้ใช้ ของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลบทบาทกลุ่มผู้ใช้ได้ถูกต้อง	ถูกต้อง
TC56	การแสดงผลหน้าจัดการผู้ใช้ ของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลผู้ใช้ได้ถูกต้อง	ถูกต้อง
TC57	การแสดงผลหน้าจัดการเว็บเซอร์วิสของเจ้าหน้าที่ดูแลระบบเว็บส่วนบริหาร	แสดงข้อมูลเว็บเซอร์วิสได้ถูกต้อง	ถูกต้อง
TC58	การแสดงข้อมูลภาพรวมในหน้า Dash Board ของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลภาพรวมของบริการพิสูจน์ตัวจริงได้ถูกต้อง	ถูกต้อง
TC59	การแสดงผลหน้าจัดการการอนุญาตของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลหน้าจัดการอนุญาตได้ถูกต้อง	ถูกต้อง
TC60	การแสดงผลหน้าจัดการบทบาทผู้ใช้ของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลบทบาทผู้ใช้ได้ถูกต้อง	ถูกต้อง
TC61	การแสดงผลหน้าจัดการกลุ่มผู้ใช้ ของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลกลุ่มผู้ใช้ได้ถูกต้อง	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC62	การแสดงผลหน้าจัดการบทบาทกลุ่มผู้ใช้ ของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลบทบาทกลุ่มผู้ใช้ได้ถูกต้อง	ถูกต้อง
TC63	การแสดงผลหน้าจัดการผู้ใช้ ของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลผู้ใช้ได้ถูกต้อง	ถูกต้อง
TC64	การแสดงผลหน้าจัดการเว็บเซอร์วิสของผู้พัฒนาเว็บเซอร์วิส	แสดงข้อมูลเว็บเซอร์วิสได้ถูกต้อง	ถูกต้อง

ตารางที่ 12 ทดสอบการใช้งานของผู้พัฒนาเว็บเซอร์วิส

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC65	ผู้พัฒนาสามารถลงทะเบียนเว็บเซอร์วิสด้วยตนเองผ่านหน้าลงทะเบียน	สามารถลงทะเบียนเว็บเซอร์วิสได้	ถูกต้อง
TC66	ไม่สามารถลงทะเบียนเว็บเซอร์วิสโดยใช้อีเมล์ที่ซ้ำกับที่มีอยู่ในระบบผ่านหน้าลงทะเบียน	ไม่สามารถลงทะเบียนเว็บเซอร์วิสโดยใช้อีเมล์ที่ซ้ำได้	ถูกต้อง
TC67	ไม่สามารถลงทะเบียนโดยไม่เลือกกลุ่มผู้ใช้งานเว็บเซอร์วิสผ่านหน้าลงทะเบียน	ไม่สามารถลงทะเบียนโดยไม่เลือกกลุ่มผู้ใช้งานได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC68	ไม่สามารถลงทะเบียนโดยใส่รหัสผ่านและยืนยันรหัสผ่านไม่ตรงกันในหน้าลงทะเบียน	ไม่สามารถลงทะเบียนโดยใส่รหัสผ่านและยืนยันรหัสผ่านไม่ตรงกันได้	ถูกต้อง
TC69	ผู้พัฒนาเว็บเซอร์วิสสามารถเข้าสู่เว็บบริหารของบริการพิสูจน์ตัวจริงหลังจากลงทะเบียนสำเร็จ	สามารถเข้าสู่เว็บบริหารของบริการพิสูจน์ตัวจริงได้	ถูกต้อง
TC70	ผู้พัฒนาเว็บเซอร์วิสแก้ไขข้อมูลเว็บเซอร์วิสที่ลงทะเบียนไว้	สามารถแก้ไขข้อมูลเว็บเซอร์วิสที่ลงทะเบียนไว้ได้	ถูกต้อง
TC71	ผู้พัฒนาเว็บเซอร์วิสจัดการการอนุญาตเฉพาะใช้ภายในเว็บเซอร์วิส	สามารถจัดการการอนุญาตเฉพาะใช้ภายในเว็บเซอร์วิสได้	ถูกต้อง
TC72	ผู้พัฒนาเว็บเซอร์วิสจัดการบทบาทผู้ใช้เฉพาะใช้ภายในเว็บเซอร์วิส	สามารถจัดการบทบาทผู้ใช้เฉพาะใช้ภายในเว็บเซอร์วิสได้	ถูกต้อง
TC73	ผู้พัฒนาเว็บเซอร์วิสจัดการกลุ่มผู้ใช้เฉพาะใช้ภายในเว็บเซอร์วิส	สามารถจัดการกลุ่มผู้ใช้เฉพาะใช้ภายในเว็บเซอร์วิสได้	ถูกต้อง
TC74	ผู้พัฒนาเว็บเซอร์วิสจัดการบทบาทกลุ่มผู้ใช้เฉพาะใช้ภายในเว็บเซอร์วิส	สามารถจัดการบทบาทกลุ่มผู้ใช้เฉพาะใช้ภายในเว็บเซอร์วิสได้	ถูกต้อง

รหัส	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลลัพธ์
TC75	ผู้พัฒนาเว็บเซอร์วิสจัดการผู้ใช้งานของเว็บเซอร์วิส	สามารถจัดการผู้ใช้งานของเว็บเซอร์วิสได้	ถูกต้อง
TC76	ผู้พัฒนาเว็บเซอร์วิสเพิ่มผู้ใช้งานใหม่	สามารถเพิ่มผู้ใช้งานใหม่ได้	ถูกต้อง
TC77	ผู้พัฒนาเว็บเซอร์วิสเพิ่มผู้ใช้งานเข้ากลุ่มเฉพาะใช้ภายในเว็บเซอร์วิส	สามารถเพิ่มผู้ใช้งานเข้ากลุ่มเฉพาะใช้ภายในเว็บเซอร์วิสได้	ถูกต้อง

5.3. สรุปผลการทดสอบ

ผู้วิจัยสามารถสรุปผลการทดสอบตามวัตถุประสงค์ของการทดสอบได้ดังต่อไปนี้

1) การจัดการบทบาทของผู้ใช้ในส่วนของการสร้างบทบาท การแก้ไขบทบาท และการลบบทบาทผู้ใช้สามารถทำงานได้อย่างถูกต้อง ข้อมูลมีการเปลี่ยนแปลงถูกต้อง
2) การจัดการการอนุญาตการใช้งานในส่วนของการสร้างการอนุญาตการใช้งาน การแก้ไขการอนุญาตการใช้งาน และการลบการอนุญาตการใช้งานสามารถทำงานได้อย่างถูกต้อง
3) การจัดการความสัมพันธ์ระหว่างบทบาทผู้ใช้งานและการอนุญาตการใช้งานมีการปรับปรุงข้อมูลระหว่างกันอย่างถูกต้อง
4) การจัดการกลุ่มผู้ใช้ในส่วนของการสร้างกลุ่มผู้ใช้ การแก้ไขกลุ่มผู้ใช้ และการลบกลุ่มผู้ใช้สามารถทำงานได้อย่างถูกต้อง
5) การจัดการบทบาทกลุ่มผู้ใช้ในส่วนของการสร้างบทบาทกลุ่มผู้ใช้ การแก้ไขบทบาทกลุ่มผู้ใช้ และการลบบทบาทกลุ่มผู้ใช้สามารถทำงานได้อย่างถูกต้อง
6) การจัดการความสัมพันธ์ระหว่างกลุ่มผู้ใช้และบทบาทกลุ่มผู้ใช้มีการปรับปรุงข้อมูลระหว่างกันอย่างถูกต้อง
7) การจัดการผู้ใช้งานในส่วนของการสร้างผู้ใช้งาน การแก้ไขผู้ใช้งาน และการลบผู้ใช้งานสามารถทำงานได้อย่างถูกต้อง

8) การจัดการเว็บเซอร์วิสที่สามารถใช้งานบริการพิสูจน์ตัวจริงในส่วนของการเพิ่มเว็บเซอร์วิส การแก้ไข และการลบเว็บเซอร์วิสสามารถทำงานได้อย่างถูกต้อง
9) การทดสอบการใช้งานบริการพิสูจน์ตัวจริงผ่านเว็บเซอร์วิสโดยการสมัครสมาชิกของผู้ใช้งาน สามารถสมัครสมาชิกได้และข้อมูลของผู้สมัครสมาชิกถูกจัดเก็บลงฐานข้อมูลโดยบริการพิสูจน์ตัวจริง การเข้าสู่ระบบของผู้ใช้งานผ่านเว็บเซอร์วิสสามาระเข้าสู่ระบบได้ โดยบริการพิสูจน์ตัวจริงสามารถสร้างโทเค็นเข้าใช้งานได้ และสามารถปรับปรุงโทเค็นเดิมในกรณีที่มีอยู่แล้วให้สามารถใช้งานได้ โดยมีการสร้างรายการการอนุญาต บทบาทผู้ใช้ และกลุ่มผู้ใช้งานได้อย่างถูกต้อง
10) การทดสอบการแสดงผลข้อมูลต่างๆ ในเว็บส่วนบริหารของงานบริการพิสูจน์ตัวจริงสามารถแสดงได้ถูกต้องตามหน้าที่ของแต่ล่ะหน้าเว็บเพจ
11) การทดสอบการใช้งานในส่วนของผู้พัฒนาเว็บเซอร์วิสสามารถใช้งานได้อย่างที่ควรจะเป็น สามารถลงทะเบียนเว็บเซอร์วิสได้ สามารถเข้าสู่ระบบและจัดการข้อมูลต่างๆ ในเว็บบริหารของงานบริการพิสูจน์ตัวจริงได้ถูกต้อง

บทที่ 6
สรุปผลการวิจัย

ในบทนี้จะกล่าวถึงสรุปผลการวิจัย ข้อจำกัดของงานวิจัย งานวิจัยในอนาคตและผลงานตีพิมพ์จากวิทยานิพนธ์ โดยแต่ละส่วนที่กล่าวมานั้นมีรายละเอียดดังต่อไปนี้

6.1. สรุปผลการวิจัย

บริการพิสูจน์ตัวจริงเป็นสิ่งจำเป็นสำหรับการใช้งานกับบริการต่างๆ ที่มีการให้บริการผ่านอินเทอร์เน็ต ไม่ว่าจะเป็นเว็บไซต์ทั่วไป เว็บเซอร์วิส เว็บแอปพลิเคชัน หรือแม้แต่แอปพลิเคชันบนโทรศัพท์มือถือในปัจจุบัน เพื่อใช้เป็นเครื่องมือในการเข้าสู่ระบบสำหรับให้ผู้ใช้งานเข้าถึงบริการที่มีไว้ให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงเท่านั้น อีกส่วนหนึ่งเป็นการรักษาความปลอดภัยของข้อมูลหรือเอกสารต่างๆ ที่ไม่อนุญาตให้บุคคลเท่าไปเข้าถึงได้ แต่สำหรับเว็บเซอร์วิสที่ต้องรองรับผู้ใช้ที่มีความหลากหลาย ทำให้ผู้ดูแลระบบประสบปัญหาในการจัดการข้อมูลผู้ใช้และการจัดการการอนุญาตเข้าใช้งานในส่วนที่สงวนไว้ให้ผู้ใช้ที่มีประเภทแตกต่างกัน นอกจากนั้น ในกรณีที่ต้องการสร้างเว็บเซอร์วิสจำนวนมาก จึงจำเป็นต้องสร้างบริการพิสูจน์ตัวจริงแยกเป็นบริการส่วนกลางที่เว็บเซอร์วิสต่างๆ สามารถเข้ามาใช้บริการได้ งานวิจัยนี้จึงนำเสนอแนวคิดการพัฒนาบริการพิสูจน์ตัวจริงอิงบทบาท โดยการนำแบบจำลอง Role-based Access Control เข้ามาเป็นแนวทางในการจัดการการอนุญาตการใช้งานต่างๆ ของเว็บเซอร์วิสที่เข้ามาใช้บริการ ซึ่งแบบจำลองดังกล่าวมีแนวคิดว่าด้วยบทบาทของผู้ใช้งานที่แยกตามกลุ่มของผู้ใช้งาน เพื่อการกำหนดการอนุญาตการใช้งานต่างๆ ได้ละเอียดมากขึ้น สำหรับงานวิจัยนี้ได้พัฒนาขึ้นในรูปแบบบริการส่วนกลางโดยไม่จำกัดโดเมนของเว็บเซอร์วิส สามารถให้บริการกับเว็บเซอร์วิสที่มีโดเมนใดก็ได้ โดยมีเว็บส่วนบริหาร (Web Administrator) เป็นเครื่องมือในการจัดการข้อมูลเว็บเซอร์วิสที่สามารถใช้บริการพิสูจน์ตัวจริงได้ การอนุญาตการใช้งาน บทบาทผู้ใช้ กลุ่มผู้ใช้งาน และ บทบาทผู้ใช้งาน ในส่วนการติดต่อสื่อสารกันระหว่างบริการพิสูจน์ตัวจริงจะติดต่อสื่อสารผ่าน API ของบริการพิสูจน์ตัวจริงผ่าน Server-side Script โดยจำเป็นต้องใช้ Client ID และ Secret Key ของเว็บเซอร์วิสที่ได้เพิ่มไว้ในเว็บส่วนบริหารโดยมีการตรวจสอบว่า Client ID และ Secret Key นั้นตรงกับโดเมนของเว็บเซอร์วิสที่เรียกใช้งาน จึงจะสามารถให้บริการได้ ในส่วนของผู้พัฒนาเว็บเซอร์วิส สามารถลงทะเบียนเว็บเซอร์วิสได้ด้วยตนเองและเข้าใช้งานเว็บส่วนบริหารของงานบริการพิสูจน์ตัวจริงเพื่อจัดการข้อมูลต่างๆ ที่ใช้งานกับเว็บเซอร์วิส ยกตัวอย่างเช่น การอนุญาตบทบาทผู้ใช้ กลุ่มผู้ใช้ เป็นต้น นอกจากนี้เพื่อความยืดยุ่นในการใช้งานของเว็บเซอร์วิส ผู้พัฒนาเว็บเซอร์วิสสามารถสร้างกลุ่มผู้ใช้ขึ้นมาใช้เฉพาะในเว็บเซอร์วิสที่ตนลงทะเบียนไว้ โดยผู้ใช้ที่อยู่ในกลุ่มนี้สามารถได้รับการอนุญาตการใช้งานพิเศษกว่าผู้ใช้งานทั่วไปที่ผู้พัฒนาเว็บเซอร์วิสกำหนดไว้

จากการทดลองการใช้งาน ผู้พัฒนาเว็บเซอร์วิสจะต้องเข้าใจและทราบถึงบทบาทและการอนุญาตต่างๆ ที่มีอยู่ในบริการพิสูจน์ตัวจริงว่ามีการอนุญาตให้ทำอะไรบ้าง มีบทบาทแต่ล่ะบทบาทแต่ล่ะบทบาทมีหน้าที่อะไร กลุ่มผู้ใช้งานแต่ล่ะกลุ่มอ้างอิงบทบาทกลุ่มผู้ใช้อะไรบ้าง จึงจำเป็นต้องให้ผู้พัฒนาเว็บเซอร์วิสเข้าถึงเว็บบริหารของบริการพิสูจน์ตัวจริงเพื่อศึกษาข้อมูลต่างๆ เพื่อนำไปประยุกต์ใช้ในการจำกัดการเข้าถึงหรือการอนุญาตเข้าถึงส่วนต่างๆ ภายในเว็บเซอร์วิส หรือออกเอกสารประกอบการใช้งานบริการพิสูจน์ตัวจริงแบบออนไลน์เพื่อให้ผู้พัฒนาเว็บเซอร์วิสสามารถเข้าถึงข้อมูลได้อย่างสะดวก

6.2. ข้อจำกัดของงานวิจัย

1) ผู้ดูแลระบบต้องกำหนดตัวย่อ (Standardization) ของบทบาทและการอนุญาตด้วยตัวเอง
2) ผู้ดูแลระบบต้องกำหนดการอนุญาตการใช้งานต่างๆด้วยตัวเอง
3) ผู้ดูแลระบบต้องกำหนดความสัมพันธ์ระหว่างบทบาทและและกลุ่มผู้ใช้ในบทบาทกลุ่มผู้ใช้ด้วยตัวเอง
4) ขาดการทดสอบกับเว็บเซอร์วิสที่มีกลุ่มผู้ใช้ทีความซับซ้อนในความหลากหลาย ยกตัวอย่างเช่น ผู้ใช้ประเภทอาจารย์ที่มีแค่บทบาทผู้สอนในเว็บเซอร์วิสหนึ่ง แต่อีกเว็บเซอร์วิสหนึ่งมีบทบาทเจ้าหน้าที่ดูแลระบบ

6.3. งานวิจัยในอนาคต

1) นำแนวทางในการพัฒนาบริการยืนยันตัวจริงอ้างอิงบทบาทมาประยุกต์ใช้กับการพัฒนาระบบควบคุมการเข้าถึงของทรัพยากรในเครื่องแม่ข่ายและฐานข้อมูลที่ใช้ผ่านในองค์กร
2) นำแนวทางในการพัฒนาบริการยืนยันตัวจริงอ้างอิงบทบาทไปประยุกต์ใช้กับอุตสาหกรรมซอฟต์แวร์สื่อสังคมออนไลน์ภายในองค์กรเพื่อสร้างเป็นศูนย์กลางการติดต่อสื่อสารผ่านในองค์กร
3) สร้างออกเอกสารออนไลน์ของบริการพิสูจน์ตัวจริงสำหรับให้ผู้พัฒนาเว็บเซอร์วิสเข้าถึงข้อมูลต่างๆ และวิธีการใช้งานต่างๆ ได้อย่างสะดวก

รายการอ้างอิง

1. B. S. Won, a.P.S., *Implementing Web Access Control System for the Multiple Web Servers in the Same Domain Using RBAC Concept*, in *Eighth International Conference on Parallel and Distributed Systems*. 2001. p. 768-773.
2. D. F. Ferraiolo, a.D.R.K., *Role-Based Access Controls*, in *15th National Computer Security Conference*. 1992. p. 554-563.
3. F. Li, a.H.W., *Design and Implementation of Authorization System Based on RBAC*, in *7th International Conference on Intelligent Human-Machine Systems and Cybernetics*. 2015. p. 502-504.
4. R. S. Sandhu, E.J.C., H. L. Feistein, and C. E. Youman, *Role-Based Access Control Models.* IEEE Computer, 1996. **29**: p. 38-47.
5. Technology, A.N.S.f.I., *International Committee for Information Technology Standards. Role Based Access Control.* 2004: p. 11-19.

ภาคผนวก

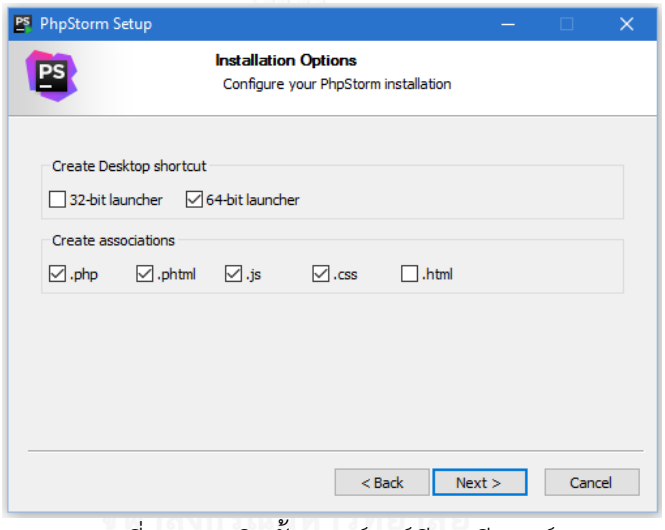
ภาคผนวก

การติดตั้งซอฟต์แวร์พีเอชพีสตอร์ม (PhpStorm)

งานวิจัยนี้ใช้ซอฟต์แวร์พีเอชพีสตอร์มสำหรับใช้ในการพัฒนาบริการพิสูจน์ตัวจริงและเว็บส่วนบริหาร โดยขั้นตอนการติดตั้งซอฟต์แวร์พีเอชพีสตอร์ม มีดังต่อไปนี้

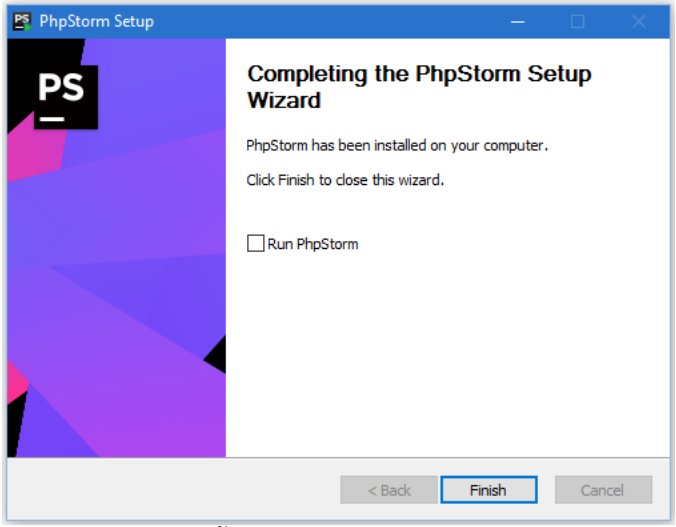
ดาวน์โหลดตัวติดตั้งซอฟต์แวร์ต่อไปนี้

1) ดาวน์โหลดตัวติดตั้งซอฟต์แวร์พีเอชพีสตอร์มจากลิงค์ https://www.jetbrains.com/phpstorm/download/
2) เมื่อคลิ๊กเปิดตัวติดตั้งขึ้นมาแล้วให้กำหนดค่าต่างๆ ตามที่ซอฟต์แวร์นั้นได้กำหนดค่าเริ่มต้นจากนั้นให้กดติดตั้ง ดังรูปที่ 42



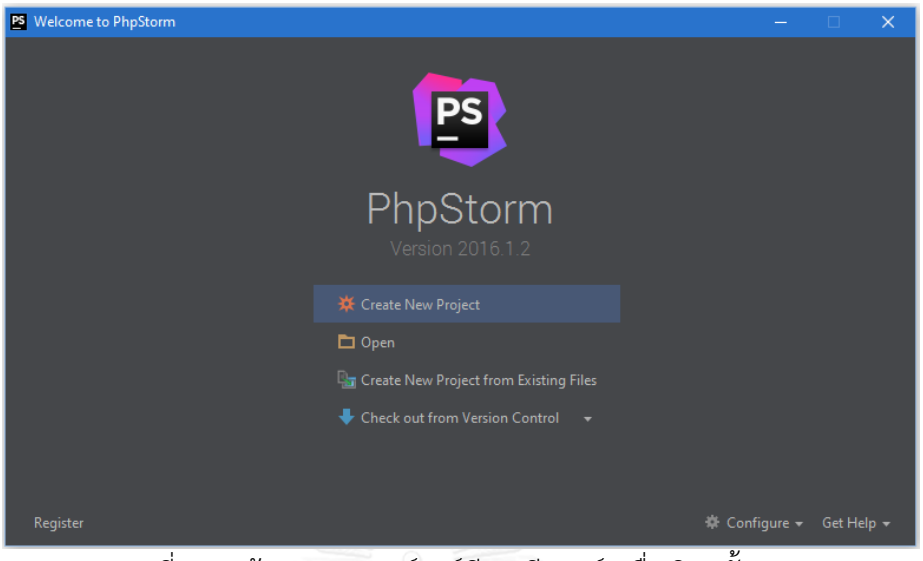
รูปที่ 42 การติดตั้งซอฟต์แวร์พีเอชพีสตอร์ม

3) เมื่อติดตั้งซอฟต์แวร์พีเอชพีสตอร์มสมบูรณ์ ตัวติดตั้งจะแจ้งให้ทราบ ดังรูปที่ 43



รูปที่ 43 ติดตั้งซอฟต์แวร์พีเอชพีสตอร์มสมบูรณ์

4) ทดลองเปิดซอฟต์แวร์พีเอชพีสตอร์มขึ้นมาลองใช้งาน จะได้หน้าตาของซอฟต์แวร์ดังรูปที่ 44



รูปที่ 44 หน้าตาของซอฟต์แวร์พีเอชพีสตอร์มเมื่อเปิดครั้งแรก

ประวัติผู้เขียนวิทยานิพนธ์

นายภูวนาถ กอบคำ เกิดเมื่อวันที่ 19 มีนาคม พ.ศ. 2530 ที่จังหวัดเชียงราย สำเร็จการศึกษาปริญญาตรีหลักสูตรวิทยาศาสตรบัณฑิต (วท.บ.) สาขาวิชาวิทยาการคอมพิวเตอร์ สำนักวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่ฟ้าหลวง ในปีการศึกษา 2553 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2557