**การพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ**

**Development of Authentication Gateway Service using REST API**

**ศิวพล บุญปั๋น**

**540510828**

**การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิทยาศาสตรบัณฑิต**

**สาขาวิชาวิทยาการคอมพิวเตอร์**

**คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่**

**ปีการศึกษา 2557**

**การพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ**

ก

**Development of Authentication Gateway Service using REST API**

**ศิวพล บุญปั๋น**

**540510828**

การค้นคว้าอิสระนี้ได้รับการพิจารณาอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษา

ตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

คณะกรรมการสอบการค้นคว้าอิสระ

………………………………………………………. ประธานกรรมการ

( อาจารย์ ดร รัศมีทิพย์ วิตา )

………………………………………………………. กรรมการ

( อาจารย์ กิตติพิชญ์ คุปตะวาณิช )

วันที่ ........... เดือน ................................... พ.ศ. ........................

# กิตติกรรมประกาศ

การค้นคว้าอิสระนี้ จบลงได้ด้วยความกรุณาจากบุคคลหลายท่าน กราบขอบพระคุณ อาจารย์ ดร.รัศมีทิพย์ วิตา ที่ให้ความกรุณาเป็นอาจารย์ที่ปรึกษาการค้นคว้าอิสระ ผู้ซึ่งกรุณาให้ความรู้ คำแนะนำ คำปรึกษา รวมทั้งสละเวลาตรวจทาน และแก้ไขจนการค้นคว้าอิสระนี้สมบูรณ์ ขอกราบขอบพระคุณ อาจารย์กิตติพิชญ์ คุปตะวาณิช ที่กรุณารับเป็นกรรมการสอบการค้นคว้าอิสระนี้ รวมทั้งกรุณาให้คำแนะนำที่เป็นประโยชน์เป็นอย่างดีตลอดมา ขอกราบขอบพระคุณอาจารย์ประจำภาควิชาวิทยาการคอมพิวเตอร์ทุกท่าน ที่ได้ประสิทธิ์ประสาทความรู้ และทักษะ ทางคอมพิวเตอร์อันเป็นพื้นฐานที่ดีอันส่งผลทำให้การค้นคว้าอิสระครั้งนี้สำเร็จ ขอบพระคุณเจ้าหน้าที่ประจำภาควิชาวิทยาการคอมพิวเตอร์ทุกท่าน โดยเฉพาะ คุณถนอม กองใจ ที่ให้ข้อมูลที่เป็นประโยชน์ในการพัฒนา ขอบคุณเพื่อน ๆ ในภาควิชาวิทยาการคอมพิวเตอร์ที่ให้ความช่วยเหลือ คำแนะนำ และช่วยสนับสนุนการพัฒนางานค้นคว้าอิสระนี้ หวังเป็นอย่างยิ่งว่า การค้นคว้าอิสระนี้จะเป็นประโยชน์สำหรับภาควิชาวิทยาการคอมพิวเตอร์ และผู้ที่สนใจ เพื่อเป็นแนวทางในการพัฒนาระบบต่อไป

ศิวพล บุญปั๋น

**ชื่อหัวข้อการค้นคว้าอิสระ** การพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ

**ชื่อเจ้าของโครงงาน** นายศิวพล บุญปั๋น

**รหัสนักศึกษา** 540510828

**วิทยาศาสตรบัณฑิต** สาขาวิชาวิทยาการคอมพิวเตอร์

**อาจารย์ที่ปรึกษาการค้นคว้าอิสระ** อาจารย์ ดร.รัศมีทิพย์ วิตา

# บทคัดย่อ

งานค้นคว้าอิสระ เรื่องการพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ มีวัตถุประสงค์เพื่อพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนที่มีความปลอดภัย ที่ทำให้ผู้ใช้ ประกอบด้วย นักศึกษา อาจารย์ และผู้ดูแลระบบสามารถยืนยันตัวตนโดยใช้บัญชีผู้ใช้ไอทีของมหาวิทยาลัยเชียงใหม่ โดยปัญหาจากการยืนยันตัวตนแบบเดิม คือ นักศึกษาใช้รหัสแบบสุ่มสี่ตัวเพื่อเข้าระบบจัดการการส่งการบ้านปฏิบัติการ เกิดการสูญหายของรหัส และถูกจดจำได้ง่าย ก่อให้เกิดความเสียหายต่อข้อมูลภายในระบบจัดการการส่งการบ้านปฏิบัติการของนักศึกษาเอง

โดยโมดูลที่พัฒนาขึ้นนั้นมีการยืนยันตัวตนโดยใช้บัญชีผู้ใช้ไอที และรหัสผ่านของมหาวิทยาลัยเชียงใหม่ ยืนยันตัวตนนักศึกษาผ่านส่วนบริการเรสต์เอพีไอของสำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ ถูกพัฒนาโดยใช้ภาษาพีเอชพี การเชื่อมต่อระหว่างผู้ขอยืนยันตัวตนกับส่วนบริการเกตเวย์ยืนยันตัวตนส่งผ่านเรสต์เอพีไอ สำหรับการจัดเก็บข้อมูลนั้นใช้มายเอสคิวแอลเป็นฐานข้อมูล หลังจากการพัฒนาเสร็จสิ้นส่วนบริการเกตเวย์ยืนยันตัวตนจะถูกใช้กับระบบภายในภาควิชาวิทยาการคอมพิวเตอร์อีกต่อไป

**Title** Development of Authentication Gateway Service using REST API

**Author** Siwaphol Boonpan

**Student ID** 540510828

**Major** Computer Science

**Supervisor Advisor** Ph. D. Ratsameetip Wita

# Abstract

This independent study is about Development of Authentication Gateway Service using REST API. The objective is to create a secure authentication gateway service helping users (student, teacher and administrator) authenticate using Chiang Mai University IT accounts. This module helps with problems from old authentication method for laboratory homework management system that student has to log in with a new 4 random digit password causing password loss and easy to remember for other student, which their information in the laboratory homework management system could be edited.

The authentication module requires Chiang Mai University’s IT username and password for log in and verifies user identities with Information Technology Service Center, Chiang Mai University’s REST API service. The developed module is written using PHP. The connection between requestor and the authentication gateway service uses REST. For data storage uses MySQL as database. After completion of development, this authentication gateway service will be integrated with Computer Sciences' systems.

# สารบัญ

**เรื่อง หน้า**

[กิตติกรรมประกาศ ก](#_Toc420063004)

[บทคัดย่อ ข](#_Toc420063005)

[Abstract ค](#_Toc420063006)

[สารบัญ ง](#_Toc420063007)

[สารบัญตาราง ฉ](#_Toc420063008)

[สารบัญรูป ช](#_Toc420063009)

[บทที่ 1 บทนำ 1](#_Toc420063010)

[1.1 หลักการและเหตุผล 1](#_Toc420063011)

[1.2 วัตถุประสงค์ของโครงงาน 2](#_Toc420063012)

[1.3 ประโยชน์ที่จะได้รับจากการศึกษาเชิงประยุกต์และ/หรือ เชิงทฤษฏี 2](#_Toc420063013)

[1.4 ขอบเขตของโครงงาน/วิธีการวิจัย 2](#_Toc420063014)

[บทที่ 2 หลักการและทฤษฏีที่เกี่ยวข้อง 3](#_Toc420063015)

[2.1 ทีแอลเอส (TLS) หรือชื่อเดิม เอสเอสแอล 3](#_Toc420063016)

[2.2 เรเดียส (RADIUS) 4](#_Toc420063017)

[2.3 คำสั่งบนเทอร์มินอลที่จำเป็นสำหรับลินุกซ์ 5](#_Toc420063018)

[2.4 ซิงเกิลไซน์ออน (Single Sign-on) 8](#_Toc420063019)

[2.5 เทคโนโลยีการยืนยันตัวตนนักศึกษา ที่มีใช้งานในมหาวิทยาลัยเชียงใหม่ 11](#_Toc420063020)

[บทที่ 3 การวิเคราะห์ และออกแบบระบบ 15](#_Toc420063021)

[3.1 การศึกษาระบบงานเดิม 15](#_Toc420063022)

[3.2 การวิเคราะห์ความต้องการของระบบ (System Requirement) 16](#_Toc420063023)

[3.3 แผนภาพยูเอ็มแอล (UML) 17](#_Toc420063024)

[บทที่ 4 การออกแบบฐานข้อมูล 32](#_Toc420063025)

# สารบัญ (ต่อ)

**เรื่อง หน้า**

[4.1 การออกแบบฐานข้อมูล 32](#_Toc420063026)

[4.2 การออกแบบฐานข้อมูลในระดับตรรกะและกายภาพ 35](#_Toc420063027)

[4.3 รายละเอียดของข้อมูลแต่ละตาราง 36](#_Toc420063028)

[บทที่ 5 การออกแบบหน้าจอ 39](#_Toc420063029)

[5.1 หน้าจอหลักยืนยันตัวตน 39](#_Toc420063030)

[5.2 หน้าจอจัดการข้อมูลผู้ใช้งาน 40](#_Toc420063031)

[5.3 หน้าจอกู้คืนรหัสผ่านทางอีเมล 41](#_Toc420063032)

[บทที่ 6 ผลการดำเนินงาน 42](#_Toc420063033)

[6.1 การยืนยันตัวตน 42](#_Toc420063034)

[6.2 การจัดการข้อมูลนักศึกษา 43](#_Toc420063035)

[บทที่ 7 บทสรุป 44](#_Toc420063036)

[7.1 สรุปผลการศึกษาและพัฒนาระบบ 44](#_Toc420063037)

[ภาคผนวก ก การติดตั้งระบบปฏิบัติการอูบุนตู และซอฟต์แวร์อื่นพร้อมการตั้งค่าที่จำเป็น 46](#_Toc420063038)

[ก.1 การติดตั้งอูบุนตู 46](#_Toc420063039)

[ก.2 การตั้งค่าอาปาเช่เตรียมสำหรับโมดูลยืนยันตัวตน 52](#_Toc420063040)

[ภาคผนวก ข การติดตั้ง และตั้งค่า SimpleSAMLphp 54](#_Toc420063041)

[ข.1 การติดตั้ง SimpleSAMLphp 54](#_Toc420063042)

[ข.2 กำหนด SimpleSAMLphp ให้เป็นผู้พิสูจน์เอกลักษณ์ 56](#_Toc420063043)

[ข.3 กำหนด SimpleSAMLphp ให้เป็นผู้ให้การบริการ 58](#_Toc420063044)

[เอกสารอ้างอิง 60](#_Toc420063045)

# สารบัญตาราง

**ตาราง หน้า**

[ตารางที่ 2.1 ตารางแสดงคำสั่งบนโปรแกรม Vi 6](#_Toc419678401)

[ตารางที่ 3.1 ตารางแสดงรูปแบบการยืนยันตัวตนของผู้ใช้ และหน้าที่การทำงานกับโมดูลยืนยันตัวตน 16](#_Toc419678402)

[ตารางที่ 3.2 ตารางเปรียบเทียบคุณสมบัติของเรเดียสยืนยันตัวตน และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี 17](#_Toc419678403)

[ตารางที่ 3.3 ตารางสัญลักษณ์แผนภาพยูสเคส 18](#_Toc419678404)

[ตารางที่ 3.4 ตารางสัญลักษณ์แผนภาพกิจกรรม 21](#_Toc419678405)

[ตารางที่ 3.5 ตารางอธิบายคำศัพท์เฉพาะภายในแผนภาพยูเอ็มแอล 22](#_Toc419678406)

[ตารางที่ 3.6 ตารางสัญลักษณ์แผนภาพขั้นลำดับ 25](#_Toc419678407)

[ตารางที่ 4.1 แสดงสัญลักษณ์ที่ใช้ในการสร้างแผนภาพความสัมพันธ์ของเอนทิตี 32](#_Toc419678409)

[ตารางที่ 4.3 ข้อมูลรายละเอียดของตารางทั้งหมดของโมดูล 35](#_Toc419678411)

[ตารางที่ 4.4 รายละเอียดข้อมูลในตารางกระบวนวิชา 36](#_Toc419678413)

[ตารางที่ 4.5 รายละเอียดข้อมูลในตารางโปรแกรม 37](#_Toc419678414)

[ตารางที่ 4.6 รายละเอียดข้อมูลในตารางบทบาท 37](#_Toc419678415)

[ตารางที่ 4.7 รายละเอียดข้อมูลในตารางโปรแกรมบทบาท 38](#_Toc419678416)

[ตารางที่ 6.1 ผลการทดสอบการยืนยันตัวของนักศึกษา 42](#_Toc419678417)

[ตารางที่ 6.2 ตารางทดสอบการจัดการข้อมูลนักศึกษา 43](#_Toc419678418)

# สารบัญรูป

**รูป**  **หน้า**

[รูปที่ 2.1 แสดงการส่งข้อมูลบนทีแอลเอสระหว่างลูกข่ายและแม่ข่าย 4](#_Toc420063363)

[รูปที่ 2.2 การส่ง-ผ่านข้อมูลของเครื่องแม่ข่ายโปรแกรม ผู้ใช้ และศูนย์กลางกระจายกุญแจ 9](#_Toc420063364)

[รูปที่ 2.3 การส่งผ่านข้อมูลของ ผู้ใช้ ผู้ให้การบริการ และผู้พิสูจน์เอกลักษณ์ 9](#_Toc420063365)

[รูปที่ 2.4 การส่งข้อมูลของซิงเกิลไซน์ออนบนพื้นฐานรวมของแซมแอล และเคอร์เบอร์รอส 10](#_Toc420063366)

[รูปที่ 2.5 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการ และบริการเรเดียสของสำนักบริการเทคโนโลยี 11](#_Toc420063367)

[รูปที่ 2.6 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและเอพีไอของสำนักบริการเทคโนโลยี 14](#_Toc420063368)

[รูปที่ 3.1 แผนภาพยูสเคสของโมดูลยืนยันตัวตน 19](#_Toc420063369)

[รูปที่ 3.2 แผนภาพกิจกรรมแสดงการยืนยันตัวตนของผู้ใช้ และการส่งข้อมูลระหว่างระบบ 24](#_Toc420063370)

[รูปที่ 3.3 แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของนักศึกษา 26](#_Toc420063371)

[รูปที่ 3.4 แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของอาจารย์ และผู้ดูแล 27](#_Toc420063372)

[รูปที่ 3.5 แผนภาพขั้นลำดับการกู้คืนรหัสผ่านของอาจารย์ และผู้ดูแลระบบ 28](#_Toc420063373)

[รูปที่ 3.6 แผนภาพขั้นลำดับแสดงการจัดการฐานข้อมูลของโมดูลยืนยันตัวตนของผู้ดูแล 29](#_Toc420063374)

[รูปที่ 3.7 แผนภาพขั้นลำดับแสดงระบบส่งการบ้านร้องขอการยืนยันตัวตนแก่ผู้ใช้ 30](#_Toc420063375)

[รูปที่ 3.8 แผนภาพขั้นลำดับแสดงระบบจัดการการส่งการบ้านปฏิบัติการร้องขอข้อมูลนักศึกษา 31](#_Toc420063376)

[รูปที่ 4.1 แผนภาพความสัมพันธ์ระหว่างเอนทิตีต่างภายในโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ 33](#_Toc420063377)

[รูปที่ 4.2 แผนภาพความสัมพันธ์ระหว่างเอนทิตีผู้ใช้ และเอนทิตีบทบาท 34](#_Toc420063378)

[รูปที่ 4.3 แผนภาพความสัมพันธ์ระหว่างเอนทิตีโปรแกรม และเอนทิตีบทบาท 34](#_Toc420063379)

[รูปที่ 5.1 หน้าจอหลักยืนยันตัวตน 39](#_Toc420063380)

[รูปที่ 5.2 หน้าจอจัดการข้อมูลผู้ใช้งาน 40](#_Toc420063381)

[รูปที่ 5.3 หน้าจอกู้คืนรหัสผ่านทางอีเมล 41](#_Toc420063382)

[รูปที่ ก.1 แสดงหน้าจอเลือกแผงแป้นอักขระ 46](#_Toc420063383)

[รูปที่ ก.2 แสดงหน้าจอเลือกรูปแบบแป้นพิมพ์ 47](#_Toc420063384)

[รูปที่ ก.3 แสดงส่วนค้นหาข้อมูลฮาร์ดแวร์ของระบบ 47](#_Toc420063385)

**สารบัญรูป (ต่อ)**

**รูป**  **หน้า**

[รูปที่ ก.4 แสดงหน้าจอส่วนกรอกชื่อเครื่อง 47](#_Toc420063386)

[รูปที่ ก.5 แสดงหน้าจอส่วนกรอกชื่อผู้ใช้ 48](#_Toc420063387)

[รูปที่ ก.6 แสดงหน้าจอส่วนกรอกรหัสผู้ใช้ 48](#_Toc420063388)

[รูปที่ ก.7 แสดงหน้าจอส่วนตัวเลือกเข้ารหัสสารบบ 48](#_Toc420063389)

[รูปที่ ก.8 แสดงหน้าจอส่วนตัวเลือกเขตเวลา 49](#_Toc420063390)

[รูปที่ ก.9 แสดงหน้าจอส่วนตัวเลือกการใช้พื้นที่ของอูบุนตู 49](#_Toc420063391)

[รูปที่ ก.10 แสดงหน้าจอส่วนตัวเลือกพื้นที่ส่วนแบ่ง 49](#_Toc420063392)

[รูปที่ ก.11 แสดงหน้าจอส่วนกรอกที่อยู่เครื่องบริการแทน 50](#_Toc420063393)

[รูปที่ ก.12 แสดงหน้าจอส่วนเลือกรูปแบบการอัพเดต 50](#_Toc420063394)

[รูปที่ ก.13 แสดงหน้าจอส่วนเลือกซอฟต์แวร์เสริม 51](#_Toc420063395)

[รูปที่ ก.14 แสดงหน้าจอส่วนตัวเลือกใช้งาน GRUB 51](#_Toc420063396)

[รูปที่ ก.15 แสดงหน้าจอส่วนเลือกจบการติดตั้งอูบุนตู 51](#_Toc420063397)

[รูปที่ ข.1 แสดงหน้าจอเริ่มต้นของ SimpleSAMLphp 55](#_Toc420063398)

[รูปที่ ข.2 ภาพแสดงตัวเลือกสำหรับเมทาดาทาของผู้ให้การบริการ 56](#_Toc420063399)

# บทที่ 1 บทนำ

ส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ ช่วยในการยืนยันตัวตนของนักศึกษา อาจารย์ และผู้ดูแลระบบ ผู้ใช้แต่ละคนมีชื่อผู้ใช้ที่ไม่เหมือนกัน คือ ผู้ใช้ทุกคน มีชื่อผู้ใช้งานสารสนเทศของมหาวิทยาลัยเชียงใหม่เฉพาะตัว ใช้ยืนยันตัวตนผู้ใช้เพื่อเข้าใช้งานระบบได้ ซึ่งในบทนี้จะกล่าวถึงภาพรวมของการจัดทำโครงงานดังนี้ ได้แก่ หลักการและเหตุผล วัตถุประสงค์ของโครงงาน ขอบเขต ประโยชน์ของการทำโครงงานนี้ และแผนการดำเนินงานและระยะเวลาดำเนินงานในการจัดทำระบบ

## หลักการและเหตุผล

ระบบสารสนเทศสำหรับส่งการบ้านปฏิบัติการของภาควิชาวิทยาการคอมพิวเตอร์ เป็นระบบช่วยการเรียนการสอนปฏิบัติการเพื่อ เพิ่มความสะดวกแก่การทำงานกับเอกสารอิเล็กทรอนิกส์ ในแต่ละวิชาผู้สอนสามารถให้ นักศึกษาทำงานแต่ละปฏิบัติการ ส่งภายในระหว่างการเรียน หรือนอกเวลา ช่วยจัดเก็บเพิ่มความสะดวกต่อการตรวจงานของอาจารย์ และการจัดการเอกสารภายในระบบ

แต่เดิมระบบส่งการบ้านสำหรับปฏิบัติการ ของภาควิชาวิทยาการคอมพิวเตอร์ ใช้การแจกรหัสตัวเลขเฉพาะให้นักศึกษา และอาจารย์แต่ละคนเพื่อเข้าใช้งานระบบ ปัญหาที่เกิดคือ นักศึกษาบางคนลืมรหัส หรือการขโมยรหัสเข้าใช้งานเพื่อเปลี่ยนแปลงข้อมูลบนระบบในนามของเจ้าของบัญชี

ด้วยเหตุนี้โครงงานจึงได้มุ่งเน้นที่จะปรับปรุงระบบให้นักศึกษา อาจารย์ และผู้ดูแลระบบ เข้าใช้ระบบโดยใช้ บัญชีผู้ใช้ไอที (IT Account) ของมหาวิทยาลัยเชียงใหม่ และรหัสผ่านของผู้ใช้ไอที เพื่อลดภาระการจดจำให้กับผู้ใช้ระบบที่ต้องจดจำชื่อบัญชีกับรหัสผ่านเพิ่ม ซึ่งการที่จะเชื่อมต่อยืนยันตัวตนกับระบบ แบบใช้บัญชีผู้ใช้ไอทีนั้นมีความจำเป็นที่จะต้องแลกเปลี่ยนข้อมูลระหว่าง เรเดียสเซิร์ฟเวอร์ (RADIUS Server) หรือเรสต์เอพีไอ ของสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ โดยทางระบบจะต้องส่งข้อมูลเข้าที่จำเป็น เช่น บัญชีผู้ใช้ไอที และรหัสผ่าน ส่วนของข้อมูลที่คาดหวังกลับมา เช่น การยืนยันว่านักศึกษา อาจารย์ และผู้ดูแลระบบมีอยู่จริง จากนั้นจึงร้องขอข้อมูลผู้ใช้งานที่จำเป็น เช่น ชื่อ-นามสกุล ไทย อังกฤษ รหัสนักศึกษา สถานะ และข้อมูลอื่นที่จำเป็น นอกจากนั้น ยังต้องเพิ่มเพิ่มความปลอดภัยต่อการเข้าสู่ระบบและส่งผ่านข้อมูล โดยใช้โครงสร้างพื้นฐานในการส่งข้อมูลที่มีความปลอดภัย เอสเอสแอล (SSL)

## วัตถุประสงค์ของโครงงาน

จัดทำส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอเพื่อให้ผู้ใช้เข้าใช้งานระบบจัดการการส่งการบ้านปฏิบัติการ โดยยืนยันตัวตนผู้ใช้งานจาก บัญชีผู้ใช้ไอทีของมหาวิทยาลัยเชียงใหม่ และรหัสผ่านของบัญชีผู้ใช้ไอที

## ประโยชน์ที่จะได้รับจากการศึกษาเชิงประยุกต์และ/หรือ เชิงทฤษฏี

- การติดตั้ง ตั้งค่าปรับแต่งเครื่องแม่ข่ายบนระบบลินุกซ์โครงสร้างพื้นฐานด้านการส่งข้อมูลที่มีความปลอดภัยของระบบจัดการสารสนเทศสำหรับส่งการบ้านปฏิบัติการที่ใช้อยู่

- ความรู้การเชื่อมต่อเพื่อยืนยันตัวตนโดยใช้ เรเดียสเซอร์วิส (RADIUS service) และเรสต์เอพีไอ

- การส่งผ่านข้อมูลแบบปลอดภัยผ่านเครือข่ายอินเทอร์เน็ตประสานระหว่างผู้ใช้งาน

## ขอบเขตของโครงงาน/วิธีการวิจัย

### ขอบเขตของสถาปัตยกรรม

ระบบที่ทำการทดลองใช้งานก่อนติดตั้งจริงทำงานบนระบบอินเทอร์เน็ต

1. ฮาร์ดแวร์ (Hardware) ที่ใช้ในการพัฒนาระบบประกอบด้วย

- เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เฮชพี (HP) ใช้เป็นเครื่องแม่ข่าย

- หน่วยประมวลผล (CPU) อินเทลคอร์ 2 ควอด 2.00 กิกะเฮิร์ตซ์ (Intel Core 2 Quad 2.00 GHz)

- ฮาร์ดดิสก์ (Harddisk) ขนาดความจุ 250 กิกะไบต์

1. ซอฟต์แวร์ (Software) ที่ใช้ในการพัฒนาระบบประกอบด้วย

- เครื่องแม่ข่ายติดตั้ง ระบบปฏิบัติการลินุกซ์ อุบุนตุ ระบบทำงานผ่านอินเทอร์เน็ต

- การเข้าสู่ระบบและส่งผ่านข้อมูลเพื่อความปลอดภัยโดยใช้เอสเอสแอล

- อาปาเช่ (Apache) เป็นเครื่องเม่ข่ายจัดการเว็บ

### ขอบเขตของระบบงาน

- ติดตั้งปรับแต่งระบบความปลอดภัยสำหรับเครื่องแม่ข่ายระบบจัดการสารสนเทศสำหรับปฏิบัติการ

- ติดตั้งโครงสร้างพื้นฐานความปลอดภัยในการส่งข้อมูลสำหรับส่วนบริการ

- ทำการเชื่อมต่อส่วนบริการกับระบบจัดการการส่งการบ้านปฏิบัติการเพื่อพิสูจน์ตัวตน และดึงข้อมูลผู้ใช้งานผ่านระบบ บัญชีผู้ใช้ไอทีเดียวกันกับของมหาวิทยาลัยเชียงใหม่

### ขอบเขตของข้อมูล

- บัญชีผู้ใช้ไอทีมหาวิทยาลัยเชียงใหม่ และรหัสผ่าน ของนักศึกษา อาจารย์ และผู้ดูแลระบบ

- ข้อมูลทั่วไปของผู้ใช้งาน เช่น ชื่อ นามสกุล รหัสนักศึกษา

- รายละเอียดของผู้ใช้งาน ข้อมูลนักศึกษาได้มาจาก สำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่ ผ่านทางเรเดียสเซอร์วิส หรือเรสต์เอพีไอ

# บทที่ 2 หลักการและทฤษฏีที่เกี่ยวข้อง

การพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ โดยการปรับปรุงใหม่นั้นจำเป็นต้องใช้บัญชีผู้ใช้ไอทีของทางมหาวิทยาลัยเชียงใหม่ ทำให้ต้องปรับปรุงทางด้านความปลอดภัยต่อการใช้งานของนักศึกษา อาจารย์ และผู้ดูแลระบบ โดยการใช้โพรโทคอลรักษาความปลอดภัยเอสเอสแอลในการแลกเปลี่ยนข้อมูล ตรวจความถูกต้องของบัญชีผู้ใช้ไอที และรับข้อมูลรายละเอียดนักศึกษาได้รับจากเอพีไอ ของทางสำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่

## ทีแอลเอส (TLS) หรือชื่อเดิม เอสเอสแอล

เอสเอสแอล [1] โพรโทคอลรักษาความปลอดภัย เพื่อให้โปรแกรมบนเครื่องแม่ข่ายและเครื่องลูกข่ายเชื่อมต่อส่งผ่านข้อมูลระหว่างเครือข่ายอย่างปลอดภัย โดยถูกออกแบบมาเพื่อป้องกันการถูกดักจับข้อมูล  
การใช้งานจริงทีแอลเอส หรือ เอสเอสแอล ถูกนำมาประยุกต์กับโพรโทคอลในชั้นสื่อสารทรานสปอร์ต (Transport Layer Protocols) ห่อหุ้มโพรโทคอลที่ใช้งาน เช่น เฮสทีทีพี (HTTP) เอฟทีพี (FTP) เอสเอมทีพี (SMTP) โดยปกติมักถูกใช้บนเว็บที่ต้องการความปลอดภัยเข้าใช้งานของผู้ใช้งาน และเว็บซื้อขายบนอินเทอร์เน็ต เครื่องแม่ข่ายและลูกข่ายจะสามารถใช้เอสเอสแอล ได้เมื่อมีการตกลงที่จะใช้เหมือนกัน คือ วิธีการจับมือกัน (Handshake) โดยระหว่างการจับมือทั้งเครื่องแม่ข่ายและแลูกข่ายต้องตกลงกันในแต่ละเงื่อนไขเพื่อความปลอดภัยของการเชื่อมต่อโดยมีขั้นตอนดังนี้

1. เครื่องลูกข่ายส่ง หมายเลขรุ่นของเอสเอสแอล รายละเอียดการตั้งค่าเข้ารหัส (Cipher Settings) ข้อมูลของช่องสื่อสาร (Session) ที่ได้รับ และข้อมูลจำเป็นอื่นที่แม่ข่ายต้องใช้ติดต่อกับเครื่องลูกข่ายผ่านเอสเอสแอล
2. เครื่องแม่ข่ายส่ง หมายเลขรุ่นของเอสเอสแอล รายละเอียดการตั้งค่าเข้ารหัส ข้อมูลของช่องสื่อสาร ที่ส่งไป ข้อมูลอื่นที่ลูกข่ายต้องใช้ติดต่อกับเครื่องแม่ข่ายผ่านเอสเอสแอล ทั้งส่งหนังสือรับรอง (Certificate) ของแม่ข่าย และถ้าหากเครื่องลูกข่ายร้องขอทรัพยากรของแม่ข่ายเพื่อการยืนยันตัวตนบนระบบ เครื่องแม่ข่ายจะร้องขอหนังสือรับรอง จากเครื่องลูกข่ายด้วย
3. เครื่องลูกข่ายใช้ข้อมูลที่ได้มาจากแม่ข่ายเพื่อยืนยันตัวตนเครื่องแม่ข่าย ยกตัวอย่างเช่น เว็บเบราว์เซอร์(Web Browser) เชื่อมต่อกับเครื่องแม่ข่าย ตรวจสอบหนังสือรับรองที่ได้รับว่าชื่อแม่ข่ายตรงกับที่ได้รับเชื่อถือหนังสือรับรองได้หรือไม่ หนังสือรับรองหมดอายุแล้วหรือไม่ ถ้าไม่สามารถยืนยันเครื่องแม่ข่ายได้จึงเตือนผู้ใช้ว่าเชื่อมต่อไม่ได้ หรือ สามารถยืนยันแม่ข่ายได้ถูกต้องก็ดำเนินการขั้นต่อไป
4. จากข้อมูลทั้งหมดในกระบวนการจับมือ เครื่องลูกข่ายต้องสร้างรหัสลับพื้นฐาน (Pre-master secret) สำหรับช่องสื่อสารปัจจุบัน เข้ารหัสด้วยกุญแจสาธารณะ (Public Key) ที่ได้จากเครื่องแม่ข่ายในขั้นตอนที่ 2 จากนั้นจึงส่งรหัสลับพื้นฐานที่ถูกเข้ารหัสให้กับแม่ข่าย
5. (กรณีเครื่องแม่ข่ายร้องขอการยืนยันตัวตนจากลูกข่าย) เครื่องลูกค่ายต้องสร้างข้อมูลอื่นซึ่งจะเป็นที่เด่นชัดว่าเป็นเครื่องที่ควรส่งข้อมูลหากันอยู่จริง ซึ่งกรณีนี้เครื่องลูกข่ายต้องส่งเอกสารใหม่ พร้อมใบรับรองเครื่อง และส่งรหัสลับพื้นฐานที่ถูกเข้ารหัสให้กับแม่ข่าย
6. (กรณีเครื่องแม่ข่ายร้องขอการยืนยันตัวตนจากลูกข่าย) เครื่องแม่ข่ายยืนยันลูกข่ายว่าเข้าใช้งานได้

* ถ้าไม่สามารถยืนยันตัวตนของลูกข่ายให้ทำการปิดช่องสื่อสารกับลูกข่าย
* ถ้ายืนยันลูกข่ายได้สำเร็จ เครื่องแม่ข่ายทำการถอดรหัสลับพื้นฐานโดยใช้กุญแจลับ(Private Key) ที่มีเฉพาะเครื่องแม่ข่าย และทำงานพร้อมเครื่องลูกข่ายเพื่อสร้าง รหัสลับหลัก(Master Secret)

1. ทั้งเครื่องแม่ข่ายและลูกข่ายใช้รหัสลับหลักเพื่อสร้าง กุญแจสื่อสาร (Session Key) ซึ่งเป็นกุญแจใช้ร่วมกันของแม่ข่ายและลูกข่าย เพื่อการเข้ารหัสและถอดรหัสข้อมูลสื่อสารแลกเปลี่ยนระหว่างช่วงเปิดเอสเอสแอล และเพื่อยืนยันความเป็นบูรณภาพของข้อมูล
2. เครื่องลูกข่ายส่งข้อความให้แก่เครื่องแม่ข่ายเพื่อบอกว่าในอนาคตข้อมูลจะถูกส่งโดยถูกเข้ารหัสด้วยกุญแจสื่อสาร จากนั้นจึงบอกว่าการจับมือด้านเครื่องลูกข่ายได้เสร็จสิ้น
3. เครื่องแม่ข่ายส่งข้อความให้แก่เครื่องลูกข่ายเพื่อบอกว่าในอนาคตข้อมูลจะถูกส่งโดยถูกเข้ารหัสด้วยกุญแจสื่อสาร จากนั้นจึงบอกว่าการจับมือด้านเครื่องแม่ข่ายได้เสร็จสิ้น



รูปที่ 2.1 แสดงการส่งข้อมูลบนทีแอลเอสระหว่างลูกข่ายและแม่ข่าย

หมายเหตุ

- ถึงขั้นตอนสุดท้ายถือเป็นการเสร็จสิ้นของการจับมือของเอสเอสแอล และเริ่มการเปิดช่องการสื่อสาร ทั้งสองด้านใช้กุญแจสื่อสารเข้ารหัสและแกะรหัสข้อมูล

- ถ้ามีขั้นตอนด้านบนขั้นตอนใดล้มเหลว จะไม่มีการเชื่อมต่อระหว่างสองฝั่ง

## เรเดียส

เรเดียส [2] ย่อมาจาก Remote Access Dial In User Service เป็นโพรโทคอลเครือข่ายที่ให้การตรวจสอบ, อนุมัติ และการจัดการการบัญชี (AAA) จากส่วนกลาง สำหรับคอมพิวเตอร์ที่เชื่อมต่อและใช้บริการเครือข่าย   
 เรเดียสเป็นโพรโทคอลแบบไคลเอ็นต์/เซิร์ฟเวอร์ที่วิ่งในชั้นแอพพลิเคชัน ใช้ยูดีพีเป็นช่องทางขนส่ง  
หลักการของเอเอเอ

เอเอเอ ย่อมาจาก การตรวจสอบ (Authentication), การอนุมัติ (Authorization) และการจัดการการบัญชี (Accounting) เป็นโครงสร้างความปลอดภัยสำหรับระบบที่กระจายการบริการใช้งานเพื่อควบคุมผู้ใช้ที่จะเข้าใช้งาน  
 การตรวจสอบ คือ การที่ผู้ใช้ที่เข้าใช้ระบบนั้นเป็นผู้ใช้จริงหรือไม่

การอนุมัติ คือ การอนุญาตว่าผู้ใช้แต่ละคนสามารถใช้ทรัพยากรได้อย่างไร ใช้ระบบได้นานเท่าไหร่ ฯลฯ

การจัดการการบัญชี คือ การเก็บข้อมูลการใช้งานของผู้ใช้ เวลาเริ่มใช้งาน เวลาที่เลิกใช้งาน จำนวนทรัพยากร ระยะเวลา ระหว่างที่ใช้งานระบบ

## คำสั่งบนเทอร์มินอลที่จำเป็นสำหรับลินุกซ์

[ ] = ไม่จำเป็นต้องมีก็ได้ เป็นส่วนเสริมเพิ่มกับคำสั่ง

### คำสั่งจัดการกับไฟล์ [3]

1. เปลี่ยนที่อยู่โฟลเดอร์กำลังทำงาน

**cd**[*options(s)*] [*directory*]

เช่น cd /etc เข้าไปยังโฟลเดอร์หลักชื่อ etc

1. แสดงไฟล์ในไดเรคทอรี่ (Directory) ปัจจุบัน

**ls**[*option(s)*] [*file(s)*]

เช่น ls –a แสดงไฟล์ทั้งหมดในไดเรคทอรี่ปัจจุบันรวมทั้งไฟล์ที่ซ่อนไว้

1. ทำการลบไฟล์ในระบบ

**rm**[*option(s)*] *file(s)*

เช่น rm text.txt ทำการลบไฟล์ที่ชื่อว่า text.txt

1. คัดลอกไฟล์บนระบบ

**cp**[*option(s)*] *sourcefile targetfile*

เช่น cp ./myfolder/thisfile /etc/ คัดลอกไฟล์จาก myfolder ชื่อไฟล์ thisfile ไปยังโฟลเดอร์ etc

1. ย้ายไฟล์บนระบบ

**mv**[*option(s)*] *sourcefile targetfile*

1. สร้างโฟลเดอร์บนระบบ

**mkdir**[*option(s)*] *directoryname*

เช่น mkdir newfolder สร้างโฟลเดอร์ใหม่ชื่อ newfolder

1. ลบโฟลเดอร์บนระบบ

**rmdir**[*option(s)*] *directoryname*

เช่น rmdir newfolder ลบโฟลเดอร์ชื่อ newfolder

1. โอนย้ายความเป็นเจ้าของไฟล์ให้ผู้ใช้

**chown**[*option(s)*] *username\_group file(s)*

เช่น chown wwwdata config.conf โอนย้ายให้ผู้ใช้ wwwdata สามารถใช้ไฟล์ config.conf ได้

1. เปลี่ยนการอนุญาตเข้าใช้งานไฟล์

**chmod**[*options*] *mode file(s)*เช่น chmod u=rw,g=r,o= internalPlan.txt ผู้ใช้เจ้าของไฟล์แก้ไขและอ่านไฟล์ได้ กลุ่มสามารถอ่านได้นอกเหนือจากนั้นไม่สามารถเข้าถึงไฟล์ได้

### คำสั่งทำงานกับข้อมูลอักขระภายในไฟล์

1. แสดงรายละเอียดภายในไฟล์

**cat**[*option(s)*] *file(s)*

1. โปรแกรมเพื่อใช้เปิดดูไฟล์

**less**[*option(s)*] *file(s)*

PgUp - PgDown เลื่อนดูข้อความที่ละครึ่งจอ ขึ้น-ลง

Space เพื่อเลื่อนลงเต็มจอ

Home – End เลื่อนไปที่บนสุด – ท้ายสุดของไฟล์

Q เพื่อออกโปรแกรม

1. การค้นหาคำเฉพาะในไฟล์

**grep**[*option(s)*] *searchstring filenames*

ผลลัพธ์ที่ได้คือข้อความทั้งบรรทัดที่มีคำเฉพาะนั้นอยู่ สามารถค้นหาโดยใช้นิพจน์ปกติ (Regular Expression) สามารถใช้ค้นหาหลังจากได้ผลลัพธ์จากคำสั่งอื่น เช่น cat studentname.txt | grep suchat โดยระบบจะใช้ข้อความนำเข้าแทนไฟล์นำเข้า

1. เปรียบเทียบข้อมูลอักขระภายในไฟล์

**diff**[*option(s)*] *file1 file2*

ผลลัพธ์ที่ได้คือการแสดงอักขระในบรรทัดที่ไม่เหมือนกัน

1. โปรแกรมสำหรับแก้ไขไฟล์

**vi** *filename*

โปรแกรม Vi ทุกชื่อโหมดการทำงานไม่สามารถใช้พิมพ์ใหญ่แทนพิมพ์เล็ก หรือเล็กแทนใหญ่ก็ไม่ได้ โดยแสดงที่กำลังทำงานอยู่ในโหมดทางด้านล่างซ้าย การบันทึกและออกจากไฟล์ให้ใช้: (Semi-colon) นำหน้าคำสั่งนั้น

|  |  |
| --- | --- |
| ESC | ออกจากทุกโหมดที่กำลังทำงาน |
| i | เข้าสู่โหมดแก้ไขข้อความในไฟล์ |
| u | ย้อนกลับการแก้ไขล่าสุด |
| dd | ลบทั้งบรรทัดที่ตำแหน่งตัวชี้อยู่ |
| :q! | ออกจากไฟล์โดยไม่สนใจการเปลี่ยนแปลงใดๆ |
| :w [*filename*] | บันทึกไฟล์ |
| :x | บันทึกการแก้ไขล่าสุดและออกจากโปรแกรม |

ตารางที่ 2.1 ตารางแสดงคำสั่งบนโปรแกรม Vi

### คำสั่งทำงานกับระบบปฏิบัติการ

1. แสดงข้อมูล รายละเอียดของหน่วยความจำสำรอง

**df**[*option(s)*] [*directory*]

เมื่อใช้โดยไม่เติม พารามิเตอร์จะเป็นการแสดงพื้นที่ทั้งหมด ส่วนที่ถูกใช้ และส่วนที่ว่างต่อการใช้งาน

1. แสดงข้อมูลโปรแกรมที่กำลังทำงาน หน่วยประมวลผลทำงานที่อยู่

**top**[*options(s)*]

1. แสดงข้อมูลโปรแกรมที่กำลังทำงาน หน่วยประมวลผลทำงานที่อยู่ อย่างละเอียด

**ps**[*option(s)*] [*process\_ID*]

1. การปิดโปรแกรมที่ไม่สามารถปิดด้วยวิธีธรรมดา

**kill**[*option(s*)] *process\_ID*

**killall**[*option(s)*] *processname*

โดย process\_ID หาได้จากการเรียก ps ส่วนการเรียกโดย killall จะใช้ชื่อโปรแกรมที่ต้องการหยุดโดยทุกหน่วยที่มีชื่อตาม processname จะถูกหยุดทำงานทั้งหมด

1. การทดสอบการเชื่อมต่อของเครือข่าย

**ping**[*option(s)*] *host\_name* หรือ *IP\_address*

โดยใช้ชื่อเครื่องเป้าหมาย หรือหมายเลขไอพี เพื่อทดสอบการเชื่อมต่อ ถ้าไม่ใส่ค่าจำนวนครั้งจะไม่หยุดการทำงานจนกว่าจะกด Ctrl+C

### คำสั่งเสริมที่จำเป็น

1. การเปลี่ยนรหัสเข้าใช้งาน

**passwd**[*option(s)*] [*username*]

ผู้ใช้งานที่เรียกคำสั่งสามารถเปลี่ยนรหัสเฉพาะของตัวเองเท่านั้น แต่สิทธิผู้ดูแลระบบ root สามารถเปลี่ยนรหัสให้กับผู้ใช้ทุกคน

1. การเปลี่ยนการใช้งานเป็นผู้ใช้งานอื่น

**su**[*option(s)*] [*username*]

โดยสามารถเรียกได้จากผู้ใช้ทุกคน ถ้าไม่มีการใส่ username จะเป็นการเรียกใช้ผู้ดูแลระบบ root โดยจะต้องมีรหัสเข้าใช้งาน root เท่านั้น

1. คำสั่งหยุดการใช้งานระบบ

**halt**[*option(s)*]

เพื่อป้องกันความเสียหายต่อข้อมูล halt จะช่วยปิดโปรแกรมและหยุดระบบเพื่อปิดใช้งานเครื่องด้วยให้เติม –p เพื่อให้ปิดกระแสไฟในเครื่องอัตโนมัติ

1. คำสั่งให้เครื่องเริ่มต้นทำงานใหม่

**reboot**[*option(s)*]

1. การลบทุกอักขระบนหน้าจอผู้ใช้

**clear**

1. การเรียกคำสั่งโดยผู้ใช้ที่ไม่ใช่ผู้ดูแลระบบ แต่ต้องใช้สิทธิผู้ดูแลระบบ

**sudo** [*commands*]

ผู้ใช้ที่สามารถเรียก sudo ต้องมีการบันทึกชื่อไว้ภายในไฟล์ /usr/local/etc/sudoers (บางครั้ง /etc/sudoers) โดยปกติจะใช้รหัสของผู้ใช้ที่เรียก แต่สามารถเปลี่ยนให้ใช้รหัสผู้ดูแลระบบเท่านั้นได้โดยเติมคำสั่ง Defaults rootpw

1. แสดงตำแหน่งที่อยู่เต็มของโปรแกรม

**which** [*options*] *programname*

โดย programname เป็นชื่อโปรแกรมที่ได้ติดตั้งในระบบแล้ว

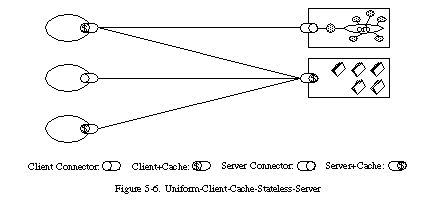
## เรสต์ (REST)

REST [8] ย่อมาจาก Representational State Transfer เป็นต้นแบบสถาปัตยกรรมสำหรับการออกแบบโปรแกรมประยุกต์บนเครือข่าย โดยสร้างการเชื่อมต่ออย่างง่ายบนเอชทีทีพีระหว่างอุปกรณ์ โปรแกรมประยุกต์แบบเรสต์ฟุล (RESTful) ใช้การร้องขอแบบเอชทีทีพีในการส่งข้อมูลแบบ POST เพื่อจัดการกับข้อมูล ซึ่งมีทั้ง สร้าง อ่าน ปรับแก้ และลบ โดยเรสต์มีข้อกำหนด 6 อย่างถ้ามีครบเรียก เรสต์ฟุล

### ข้อกำหนด 6 อย่างของเรสต์

#### ส่วนต่อประสานแบบเดียวกัน (Uniform Interface)

กำหนดส่วนต่อประสานระหว่างลูกข่าย และแม่ข่าย ซึ่งทำให้แต่ละส่วนแยกจากกันอย่างชัดเจน หลักการมีอยู่ 4 ข้อ



รูปที่ . แสดงแผนภาพส่วนต่อประสานแบบเดียวกัน

#### การขึ้นกับทรัพยากร (Resource-Based)

ตัวแปรทรัพยากรที่ร้องขอกำหนดไว้ในยูอาร์ไอ โดยแม่ข่ายจะส่งข้อมูลที่ได้จากฐานข้อมูลในรูปแบบ เอกซ์เอ็มแอล หรือเจสัน กลับคืน

#### การจัดการทรัพยากรผ่านการแทน (Manipulation of Resources through Representations)

ถ้าลูกข่ายมีตัวแทนข้อมูลในมือและการอนุญาต ถือว่าลูกข่ายสามารถแก้ไขข้อมูลบนเครื่องแม่ข่ายได้

#### ข้อความอธิบายในตัว (Self-descriptive Messages)

ข้อความที่ใช้ในการส่งข้อมูล มีข้อมูลเพียงพอที่จะบอกถึงแนวทางการประมวลผลข้อมูล

* + - * 1. **สื่อหลายมิติเป็นตัวขับเคลื่อนสถานะของโปรแกรมประยุกต์ (Hypermedia as the Engine of Application State, HATEOAS)**

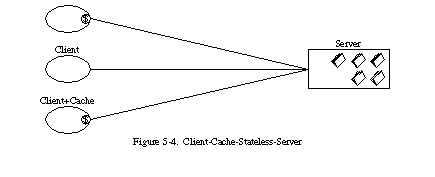
เครื่องลูกข่ายส่งสถานะผ่านเนื้อหาส่วนหลัก (Body Contents) ตัวแปรข้อความสอบถาม (Query-string Parameters) หัวเรื่องร้องขอ (Request Headers) และยูอาร์ไอร้องขอ (Requested URI) ส่วนบริการส่งสถานะให้กับลูกข่ายผ่านเนื้อหาส่วนหลัก เลขรหัสตอบกลับ และส่วนหัวข้อความตอบกลับ

#### การไม่จดจำสถานะ (Stateless)

การไม่จดจำสถานะเป็นหัวใจสำคัญของเรสต์ โดยสถานะที่จำเป็นในการจัดการคำร้องอยู่ภายในคำร้องแล้ว โดยอยู่ในรูปแบบ ยูอาร์ไอ ตัวแปรข้อความสอบถาม ส่วนหลัก หรือส่วนหัวของคำร้อง หลังจากเครื่องแม่ข่ายประมวลผลเสร็จ สถานะที่จำเป็นถูกส่งกลับผ่านส่วนหัว สถานะ และส่วนหลักของข้อความตอบกลับ การไม่จดจำสถานะโดยเครื่องแม่ข่ายมีข้อดี คือ ไม่ต้องมีการดูแลเซสชั่น ทำให้รองรับกับการขยายได้อย่างดี

#### สามารถแคชได้ (Cacheable)

เมื่อข้อความตอบกลับระบุว่าสามารถแคชได้ เครื่องลูกข่ายสามารถใช้ข้อมูลในข้อความตอบกลับเพื่อการร้องขอครั้งต่อไปได้ ช่วยลดเวลาแฝงในการส่งข้อมูลได้



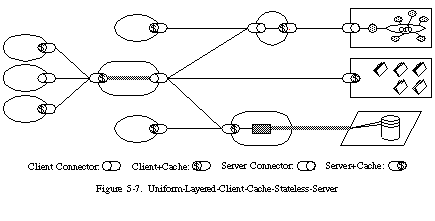
รูปที่ . แผนภาพแสดงการเชื่อมต่อทั้งแบบมี และไม่มีแคช

#### เครื่องลูกข่าย และเครื่องแม่ข่าย (Client-Server)

ส่วนต่อประสานแบบเดียวกันทำให้เครื่องลูกข่าย และเครื่องแม่ข่ายแยกจากกันชัดเจน ส่งผลให้เครื่องลูกข่ายไม่ยุ่งกับส่วนจัดเก็บข้อมูล การเคลื่อนย้ายทำได้ง่าย เครื่องแม่ข่ายไม่ยุ่งเกี่ยวกับส่วนต่อประสานผู้ใช้ หรือสถานะของผู้ใช้ ทำให้ง่ายต่อการสร้าง และขยายได้ดี ทำให้ทั้งสองส่วนถูกพัฒนาโดยไม่ขึ้นต่อกัน

#### ระบบมีลำดับชั้น (Layered System)

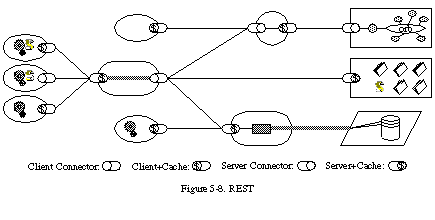
เครื่องลูกข่ายไม่ทราบว่ากำลังเชื่อมต่อกับแม่ข่ายโดยตรง หรือผ่านตัวกลาง ทำให้ตัวกลางสามารถเพิ่มความสามารถในการจัดเก็บแคช และสมดุลภาระคำร้องได้



รูปที่ . แสดงแผนภาพระบบแบบมีลำดับขั้น

#### เขียนตามต้องการ (Code on Demand)

ข้อกำหนดสุดท้ายเป็นทางเลือกสำหรับเครื่องแม่ข่าย ที่สามารถเปลี่ยนแปลง หรือขยายการทำงานของเครื่องลูกข่ายโดยส่งผ่านตรรกะให้เครื่องลูกข่ายประมวลผล



รูปที่ . แสดงแผนภาพข้อกำหนดเรสต์แบบเขียนตามต้องการ

### เทคนิคของเรสต์

#### ใช้กริยาเอชทีทีพีที่ตรงตามการทำงาน

#### ผู้ใช้เอพีไอมีความสามารถในการส่งกริยาแบบ GET POST PUT และ DELETE ได้ซึ่งช่วยอธิบายว่าแต่ละคำร้องมีความต้องการอะไร ข้อควรระวัง เช่น ไม่ควรร้องขอแบบ GET เมื่อต้องการเปลี่ยนแปลงข้อมูล

#### ชื่อทรัพยากรสื่อความหมาย

#### ใช้ชื่อสื่อความหมายช่วยในการทำความเข้าใจว่าแต่ละคำร้องต้องกาอะไร เช่น ใช้ /posts/23 แทนการใช้ /api?type=posts&id=23 เพื่อทำงาน posts โดยมีไอดีเท่ากับ 23

#### ชื่อตัวทรัพยากรที่ใช้ควรเป็นคำนาม หลีกเลี่ยงการใช้คำกริยา ใช้เมท็อดเอชทีทีพีสำหรับกำหนดกริยาของคำร้อง

#### เอกซ์เอ็มแอล และเจสัน

#### เจสัน ควรเป็นตัวเลือกแรกสำหรับข้อมูลส่งกลับ แต่สามารถให้ผู้ใช้บริการเลือกได้ว่าต้องการอย่างใดมากกว่า โดยการเปลี่ยนนามสกุลจาก .xml เป็น .json หรือจาก .json เป็น .xml

#### เจสัน ตามมาตรฐานแล้วมีข้อกำหนดที่ต้องการน้อยมาก โดยข้อกำหนดที่ต้องการคือการสร้างข้อความให้ถูกต้อง ไม่เกี่ยวกับการวางรูปแบบ และการวางผัง

#### ในขณะที่เอกซ์เอ็มแอล ถูกใช้เพื่อต้องการใช้งานป้ายระบุ และข้อความที่ถูกต้องเท่านั้น

#### คำนึงถึงการเชื่อมต่อ

#### เอพีไอ สามารถลิงก์ไว้กับข้อความตอบกลับ เพื่อบอกกับเครื่องลูกข่ายถึงข้อมูลก่อนหน้า หรือข้อมูลต่อไปได้ซึ่งง่ายต่อการเรียกใช้กรณีข้อความตอบกลับมีความเชื่อมโยงต่อกัน

#### การสร้างทรัพยากรแบบละเอียด

#### เมื่อเริ่มต้นสร้างเอพีไอ ควรจะสร้างส่วนบริการขนาดย่อยที่ทำหน้าที่เฉพาะก่อน จากนั้นเมื่อต้องการรวมส่วนบริการให้ใหญ่ขึ้นจึงทำได้ง่าย แทนการสร้างส่วนบริการขนาดใหญ่แล้วแตกออกเป็นส่วนย่อยจำนวนมาก

## เทคโนโลยีการยืนยันตัวตนนักศึกษา ที่มีใช้งานในมหาวิทยาลัยเชียงใหม่

### เรเดียส (RADIUS)

#### การเชื่อมต่อกับการบริการเรเดียส

การเชื่อมต่อกับส่วนบริการเรเดียส ของมหาวิทยาลัยเชียงใหม่มีความต้องการ คือ เครื่องแม่ข่ายใช้ไอพีสาธารณะ การส่งข้อมูลยืนยันใช้อีเมล รหัสผ่าน ที่อยู่ของผู้ให้บริการเรเดียส และรหัสลับเข้าใช้งาน โดยสามารถเชื่อมต่อผ่านพีเฮชพี โดยการใช้คลังโปรแกรมของ พีอีซีแอลเรเดียส (PECL Radius)

โดย 2 ค่าที่ได้กลับมาคือ Access-Accept ระบบยืนยันว่ามีผู้ใช้ และ Access-Reject คือการยืนยันตัวตนไม่สำเร็จ



รูปที่ 2.6 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการ และบริการเรเดียสของสำนักบริการเทคโนโลยี

### เรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

#### คำสั่งเพื่อทำงานกับเรสต์เอพีไอ

* **การยืนยันตัวตนนักศึกษา**

https://account.cmu.ac.th/v3/api/validateUser

ร้องขอแบบ GET ตามยูอาร์แอล (URL) มีตัวแปรส่วนหัว (Header) คำร้องขอ ดังนี้

1. appId คือ หมายเลขของเรสต์เอพีไอที่กำลังเรียกฟังก์ชัน validateUser
2. appSecret คือ รหัสลับเพื่อเข้าใช้งานเรสต์เอพีไอ
3. user คือ ชื่อบัญชีผู้ใช้ไอทีมหาวิทยาลัยเชียงใหม่ ไม่ใส่ @cmu.ac.th
4. pw คือ รหัสผ่านของบัญชีผู้ใช้ไอทีมหาวิทยาลัยเชียงใหม่

* **การร้องขอข้อมูลนักศึกษา**

https://account.cmu.ac.th/v3/api/students

การขอข้อมูลนักศึกษาแบบ GET ส่งค่าตัวแปรผ่านส่วนหัว ดังนี้

1. appId คือ หมายเลขของเรสต์เอพีไอที่กำลังเรียกฟังก์ชัน students
2. appSecret คือ รหัสลับเพื่อเข้าใช้งานเรสต์เอพีไอ
3. userName คือ ชื่อบัญชีผู้ใช้ไอที
4. access\_token คือ โทเค็นผ่าน เป็นสายอักขระที่ได้รับหลังยืนยันตัวตนผู้ใช้สำเร็จ

* **การร้องขอข้อมูลอาจารย์ และผู้ดูแลระบบ**

https://account.cmu.ac.th/v3/api/employees

การขอข้อมูลนักศึกษาแบบ GET ส่งค่าตัวแปรผ่านส่วนหัว ดังนี้

1. appId คือ หมายเลขของเรสต์เอพีไอที่กำลังเรียกฟังก์ชัน students
2. appSecret คือ รหัสลับเพื่อเข้าใช้งานเรสต์เอพีไอ
3. userName คือ ชื่อบัญชีผู้ใช้ไอที
4. access\_token คือ โทเค็นผ่าน เป็นสายอักขระที่ได้รับหลังยืนยันตัวตนผู้ใช้สำเร็จ

* **การลงบันทึกออก**

https://account.cmu.ac.th/v3/api/logout

การขอข้อมูลนักศึกษาแบบ GET ส่งค่าตัวแปรผ่านส่วนหัว ดังนี้

1. appId คือ หมายเลขของเรสต์เอพีไอที่กำลังเรียกฟังก์ชัน students
2. appSecret คือ รหัสลับเพื่อเข้าใช้งานเรสต์เอพีไอ
3. userName คือ ชื่อบัญชีผู้ใช้ไอที
4. access\_token คือ โทเค็นผ่าน เป็นสายอักขระที่ได้รับหลังยืนยันตัวตนผู้ใช้สำเร็จ

หมายเหตุ การร้องขอข้อมูลทุกครั้งจะทำให้ access\_token เปลี่ยนไปทุกครั้ง

#### ตัวอย่างรูปแบบข้อมูล เจสัน (JSON) ที่ได้จากเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

* **ข้อมูลเจสันที่ได้มาจากการยืนยันตัวนักศึกษาสำเร็จ**

{

"success": true,

"ticket": {

"access\_token": "zMbjvFfRCD",

"expires\_in": 1800,

"userName": "siwaphol\_boonpan",

"issued": "19/11/2557 16:18:12",

"expires": "19/11/2557 16:48:12"

}

}

* **ข้อมูลเจสันที่ได้มาจากการร้องขอข้อมูลนักศึกษา**

{

"success": true,

"ticket": {

"success": true,

"ticket": {

"access\_token": "26ggzJGG1f",

"expires\_in": 1800,

"userName": "siwaphol\_boonpan",

"issued": "19/11/2557 16:20:41",

"expires": "19/11/2557 16:50:41"

}

},

"student": {

"id": "540510828",

"personType": {

"th\_TH": "นักศึกษาปัจจุบัน",

"en\_US": "Present Student"

},

"prefix": {

"th\_TH": "ศิวพล",

"en\_US": "siwaphol"

},

"firstName": {

"th\_TH": "ศิวพล",

"en\_US": "SIWAPHOL"

},

"lastName": {

"th\_TH": "บุญปั๋น",

"en\_US": "BOONPAN"

},

"level": null,

"citizen\_id": "1579900428149",

"faculty": {

"code": "05",

"th\_TH": "คณะวิทยาศาสตร์",

"en\_US": "Faculty of Science"

},

"image": null

}

}

โดยค่าของตัวแปร ticket จะถูกสร้างก็ต่อเมื่อการร้องขอสำเร็จ คือ ค่าของ success เป็นจริง



รูปที่ 2.7 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและเอพีไอของสำนักบริการเทคโนโลยี

# บทที่ 3 การวิเคราะห์ และออกแบบระบบ

บทนี้กล่าวถึงการวิเคราะห์ และออกแบบระบบงาน โดยจะทำการศึกษาลักษณะการทำงานของระบบเดิม โดยจะทำการศึกษาลักษณะของระบบใช้งานเดิมว่ามีคุณสมบัติการทำงานเป็นอย่างไร มีปัญหาอะไร และทำการสำรวจความต้องการในการพัฒนาระบบเดิมจากคุณ ถนอม กองใจ ผู้ดูแลระบบส่งงานของภาควิชาวิทยาการคอมพิวเตอร์ เพื่อศึกษารายละเอียดงานของระบบเดิมเพื่อทำการออกแบบ และปรับปรุงระบบบริการผ่านเว็บใหม่ให้เกิดการเข้าใช้งานที่สะดวกขึ้น โดยมุ่งเน้นรายละเอียดในการยืนยันตัวตนของผู้ใช้งานผ่านบัญชีผู้ใช้ไอทีมหาวิทยาลัยเชียงใหม่

## การศึกษาระบบงานเดิม

การศึกษาระบบงานเดิมทั่วไป เป็นการศึกษารายละเอียดของขั้นตอนการยืนยันตัวตนของระบบส่งการบ้านเดิมที่ใช้งานอยู่ ซึ่งมีการยืนยันตัวตนกับระบบผ่านเว็บเพจหน้าพีเอชพี โดยมีการยืนยันตัวตนนักศึกษาใช้เลขรหัสประจำตัวนักศึกษา และรหัสผ่านเป็นลักษณะเลขสุ่มจำนวน 4 หลักเพื่อยืนยันตัวตนกับฐานข้อมูลในระบบ ส่วนอาจารย์ และผู้ดูแลระบบใช้ชื่อ และรหัสเลขสุ่มสี่ตัวเพื่อเข้าระบบ เพื่อเข้าสู่ระบบสารสนเทศส่งการบ้านแต่ละตอนของกระบวนวิชาต่างๆ ส่วนอาจารย์ และผู้ดูแลระบบเข้าเรียกดูการส่งการบ้านของนักศึกษาโดยตรงจากไดเรกทอรี (Directory) ของกระบวนวิชานั้น เพื่อการตรวจ และให้คะแนนฐานข้อมูลมีการจัดเก็บข้อมูลนักศึกษาประกอบไปด้วย รหัสนักศึกษาเป็นกุญแจหลัก ชื่อ-นามสกุลรหัสเลขสุ่มจำนวน 4 หลักในฐานข้อมูลของอาจารย์ และผู้ดูแลระบบประกอบไปด้วย ไอดี ชื่อ-นามสกุล และเลขสุ่ม 4 หลักจึงนำข้อมูลมาวิเคราะห์หาปัญหา เพื่อที่จะนำมาพัฒนาโมดูล

### ลักษณะระบบงานเดิม

ลักษณะการทำงานของระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ในส่วนของการยืนยันตัวตนของนักศึกษา มีการกรอกเลขรหัสนักศึกษาเก้าตัว และรหัสคือเลขสุ่ม 4 หลักที่จัดเก็บไว้ในฐานข้อมูลเพื่อเข้าใช้งานภายในระบบ ส่วนของอาจารย์เป็นใช้ชื่อจริง และ รหัสผ่านเลขสุ่ม 4 หลัก

### ปัญหาของระบบงานเดิม

จากการวิเคราะห์ระบบงานเดิม พบว่ามีปัญหาในการกำหนดให้ใช้รหัสผ่านเลขสุ่มสี่ตัวในการยืนยันตัวตนกับระบบของนักศึกษา เกิดการจำรหัสผ่านเพิ่มเติม ทำให้นักศึกษาลืมรหัสผ่านที่ตัวเองได้รับไป และรหัสผ่านที่ถูกแอบมอง ดักจับ ซึ่งปัญหาของระบบงานเดิมมีดังนี้

1. การกำหนดรหัสผ่านให้แก่นักศึกษา เนื่องจากเป็นตัวเลขสุ่มสี่ตัว เพิ่มภาระการจำให้แก่นักศึกษา ทำให้เกิดการลืม และความผิดพลาดในการจำตัวเลขได้
2. ความปลอดภัยของรหัสเข้าใช้งาน ที่อาจถูกแอบมอง และดักจับ
3. ขั้นตอนของการสร้าง และแจกรหัสผ่านแก่นักศึกษายังมีความยุ่งยาก

## การวิเคราะห์ความต้องการของระบบ

### ความต้องการของผู้ใช้

จากการวิเคราะห์ส่วนยืนยันตัวตนของระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ และข้อมูลความต้องการจากคุณถนอม กองใจ ผู้ดูแลระบบ และคำแนะนำจาก อาจารย์ ดร.รัศมีทิพย์ วิตา จึงนำความต้องการที่ได้มาพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ ซึ่งแยกผู้ใช้งานดังตารางที่ 3.1

ตารางที่ 3.1 ตารางแสดงรูปแบบการยืนยันตัวตนของผู้ใช้

|  |  |  |
| --- | --- | --- |
| **กลุ่มผู้ใช้งาน** | **ข้อมูลที่ส่วนบริการต้องการ** | **ผลลัพธ์ที่คาดหวัง** |
| อาจารย์ และผู้ดูแลระบบ | ชื่อบัญชีผู้ใช้ไอที (ไม่มี @cmu.ac.th) และรหัสผ่าน ของมหาวิทยาลัย เชียงใหม่ | ได้รับการยืนยันตัวในระดับอาจารย์ หรือผู้ดูแลระบบ เพื่อเข้าใช้งานระบบอื่น |
| นักศึกษา | ชื่อบัญชีผู้ใช้ไอที (ไม่มี @cmu.ac.th) และรหัสผ่าน ของมหาวิทยาลัย เชียงใหม่ | ได้รับการยืนยันตัวในระดับนักศึกษาเพื่อเข้าใช้งานระบบอื่น |

### การเปรียบเทียบบริการยืนยันตัวตนจากสำนักบริการเทคโนโลยีที่มีอยู่

ส่วนบริการยืนยันตัวตนของสำนักบริการเทคโนโลยีที่ให้มีดังนี้ โดยการเปรียบเทียบดูจากตารางที่ 3.2

1. บริการเรเดียสยืนยันตัวตนของสำนักบริการเทคโนโลยี มีข้อจำกัด คือ ระบบที่เรียกใช้ต้องมี ไอพีภายนอก การยืนยันตัวตนใช้ชื่อบัญชีผู้ใช้ไอทีกับรหัสผ่าน ผู้ใช้ยูอาร์แอลผู้ให้การบริการเรเดียส และรหัสลับ ในการร้องขอแต่ละครั้ง
2. เรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี ความต้องการ การเรียกแบบ GET ผ่านยูอาร์แอล ของสำนักบริการเทคโนโลยี พร้อมพารามิเตอร์ส่วนหัวที่ส่งไปพร้อมกัน เช่น ชื่อบัญชีผู้ใช้ไอที รหัสผ่าน เลขที่โปรแกรม และรหัสของโปรแกรม โทเค็นที่ได้หลังยืนยันตัวตนสำเร็จ

ตารางที่ 3.2 ตารางเปรียบเทียบคุณสมบัติของเรเดียสยืนยันตัวตน และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

|  |  |  |
| --- | --- | --- |
| **คุณสมบัติ** | **เรเดียสยืนยันตัวตนของสำนักบริการเทคโนโลยี** | **เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี** |
| ให้ข้อมูลผู้ใช้ | ไม่ได้ | ได้ ผลลัพธ์เป็นข้อมูลผู้ใช้แบบเจสัน  นักศึกษาใช้ฟังก์ชันชื่อ students  อาจารย์ และผู้ดูแลระบบใช้ฟังก์ชันชื่อ employees |
| ทำงานบนเอสเอสแอล | ได้ | ได้ |
| ทำงานได้กับพีเฮชพี | ได้ แต่ต้องเพิ่มส่วนขยายเรเดียสให้กับตัวบริการเว็บ เพื่อส่งข้อมูลไปยังเครื่องแม่ข่ายเรเดียสจากพีเอชพี | ได้ |

จากการวิเคราะห์แล้ว พบว่าการใช้เรสต์เอพีไอสำหรับยืนยันตัวตนมีความเหมาะสมที่สุดเพราะฟังก์ชันที่มีให้ตรงความต้องการ สามารถยืนยันตัวตน และให้ข้อมูลผู้ใช้ต่อคน ง่ายต่อการใช้งานเพราะเป็นการส่งข้อมูลแบบเรสต์ ไม่จำกัดเครื่องที่ร้องขอจะต้องมีไอพีภายนอก ทำให้ส่วนบริการเกตเวย์ยืนยันตัวตนที่สร้างขึ้นง่ายต่อการนำไปใช้ และรองรับการปรับเพิ่มในอนาคต

## แผนภาพยูเอ็มแอล (UML)

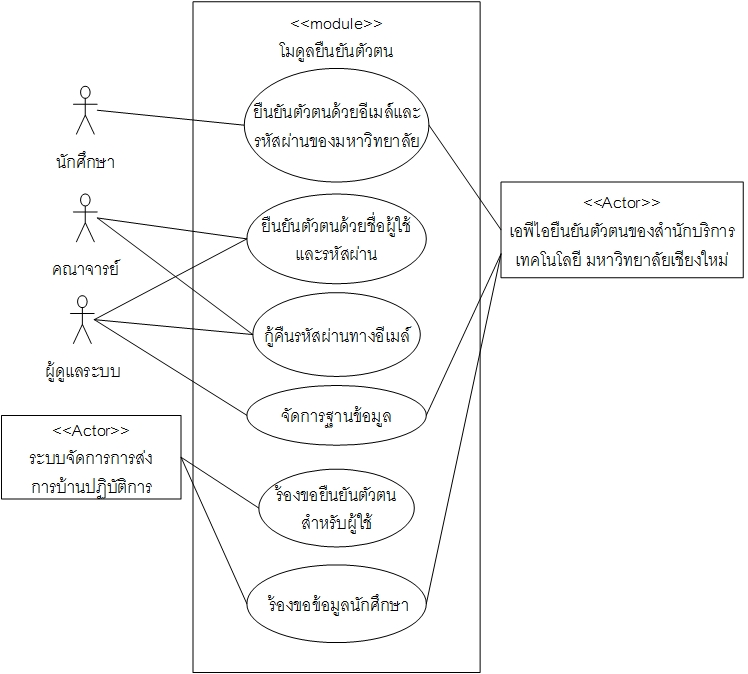
แผนภาพยูเอ็มแอล [7] ของการวิเคราะห์เพื่อการออกแบบส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอนั้น ทางผู้ออกแบบได้ใช้แผนภาพแบบยูเอ็มแอลเพื่อแสดงการทำงานในภาพรวมระดับสูง เช่น แผนภาพยูสเคส (Use Case Diagram) ที่แสดงให้เห็นว่าผู้ใช้งานกับระบบภายนอกมีส่วนทำงานประสานกับโมดูล ทำงานอะไรบ้างเพื่อง่ายต่อการแสดงความต้องการของโมดูลแผนภาพกิจกรรม (Activity Diagram) แสดงการทำงานแบบกว้าง และแผนภาพขั้นลำดับ (Sequence Diagram) แสดงการทำงานและการส่งข้อมูลแบบละเอียด

### แผนภาพยูสเคส

แผนภาพยูสเคส [7] ที่แสดงการทำงานของผู้ใช้ระบบ (User) และความสัมพันธ์กับระบบย่อย (Sub Systems) ภายในระบบใหญ่ ในการเขียนแผนภาพการใช้งาน ผู้ใช้ระบบ จะถูกกำหนดว่าให้เป็นผู้ใช้งาน (Actor) และ ระบบย่อย คือ แผนภาพยูสเคส ซึ่งใช้สัญญาลักษณ์ดังตารางที่ 3.3

ตารางที่ 3.3 ตารางสัญลักษณ์แผนภาพยูสเคส

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Actor | สัญลักษณ์ แทนสิ่งที่อยู่นอกระบบ เช่น คน สิ่งของ หน่วยงาน |
|  | Use Case | สัญลักษณ์ แทนกระบวนการ หรือการประมวลผล |
|  | Association | สัญลักษณ์เชื่อมความสัมพันธ์ |
|  | System | สัญลักษณ์ กรอบการทำงานของระบบ |



รูปที่ 3.1 แผนภาพยูสเคสของโมดูลยืนยันตัวตน

**ชื่อการใช้งาน:** ยืนยันตัวตนด้วยอีเมล และรหัสผ่านของมหาวิทยาลัย

**คำอธิบาย:** นักศึกษาในฐานะนักแสดงทำการยืนยันตัวตนกับโมดูลโดยใช้อีเมล และรหัสผ่าน เดียวกันกับที่ใช้ของมหาวิทยาลัยเชียงใหม่ โดยโมดูลนำอีเมล และรหัสผ่านที่ได้ตรวจสอบกับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี เพื่อนักศึกษาสามารถเข้าใช้ระบบที่ต้องการ เช่น ระบบจัดการการส่งการบ้านปฏิบัติการ

**จุดสำคัญของเหตุการณ์:** อีเมล และรหัสผ่านนักศึกษามีความถูกต้อง

**เงื่อนไขก่อน:** นักศึกษาเข้าสู่หน้าเว็บกรอกข้อมูลยืนยันตัวตนเพื่อเข้าใช้ระบบที่ต้องการ

**ผลลัพธ์เมื่อสำเร็จ:** นักศึกษายืนยันตัวตนสำเร็จ

**ชื่อการใช้งาน:** ยืนยันตัวตนด้วยชื่อผู้ใช้ และรหัสผ่าน

**คำอธิบาย:** ผู้ดูแลระบบ/อาจารย์ ยืนยันตัวตนกับโมดูลโดยใช้ ชื่อผู้ใช้ และรหัสผ่านที่ถูกกำหนดไว้ก่อนภายในฐานข้อมูลของโมดูลแล้ว เพื่อให้ได้สิทธิ์แบบผู้ดูแลระบบ/อาจารย์ เข้าใช้ระบบที่ต้องการ เช่น สิทธิ์การจัดการข้อมูลภายในระบบนั้น

**จุดสำคัญของเหตุการณ์:** ชื่อผู้ใช้ และรหัสผ่านมีความถูกต้อง

**เงื่อนไขก่อน:** ผู้ดูแลระบบ/อาจารย์ เข้าสู่หน้าเว็บกรอก ชื่อผู้ใช้ และรหัสผ่าน เพื่อยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบ/อาจารย์สามารถยืนยันตัวตนกับโมดูลได้สำเร็จ

**ชื่อการใช้งาน:** กู้คืนรหัสผ่านทางอีเมล

**คำอธิบาย:** ผู้ดูแลระบบ/อาจารย์ร้องขอรหัสผ่านจากฐานข้อมูลในระบบ โดยระบบจะส่งผ่านทางอีเมลของผู้ใช้ จากฐานข้อมูลในโมดูล โดยโมดูลรับเข้าชื่อผู้ใช้เพื่อกำหนดอีเมลเป้าหมายที่ต้องส่งข้อความ

**จุดสำคัญของเหตุการณ์:** ชื่อผู้ใช้ที่กรอกถูกต้อง

**เงื่อนไขก่อน:** ผู้ดูแลระบบ/อาจารย์เข้าสู่เมนู กู้คืนรหัสผ่านทางอีเมลแล้วกรอกชื่อผู้ใช้ของตัวเอง

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบ/อาจารย์ ได้รับข้อความอีเมลแสดงรหัสผ่าน ที่โมดูลยืนยันตัวตนส่งให้

**ชื่อการใช้งาน:** จัดการฐานข้อมูล

**คำอธิบาย:** ผู้ดูแลระบบ จัดการข้อมูลในฐานข้อมูลของโมดูลได้ ทั้งจากหน้าเว็บที่โมดูลมีให้ และจากคำสั่งเอสคิวแอลโดยตรง ผู้ดูแลระบบสามารถจัดการข้อมูลทุกอย่างภายในฐานข้อมูล เช่น การเปลี่ยนชื่อ และอีเมลของผู้ใช้

**จุดสำคัญของเหตุการณ์:** คำสั่งจัดการ และข้อมูลมีความถูกต้อง

**เงื่อนไขก่อน:** ถ้าจัดการผ่านหน้าเว็บผู้ดูแลระบบเข้าสู่ยูอาร์แอลจากเบราเซอร์ สำหรับการจัดการเอสคิวแอลโดยตรงให้เข้าระบบปฏิบัติการโดยตรงหรือผ่านการควบคุมระยะไกล โดยใช้บัญชีผู้ใช้ของระบบปฏิบัติการ

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบสามารถเพิ่ม แก้ไข หรือลบข้อมูลผู้ใช้ในฐานข้อมูลของโมดูลได้

**ชื่อการใช้งาน:** ร้องขอยืนยันตัวตนสำหรับผู้ใช้

**คำอธิบาย:** ระบบนอกในที่นี้คือ ระบบจัดการการส่งการบ้านปฏิบัติการ ทำการสร้างคำร้องยืนยันตัวตนแบบแซมแอล (SAML Request Assertion) เพื่อให้เบราเซอร์ส่งต่อมายังโมดูลยืนยันตัวตน เมื่อการยืนยันตัวตนสำเร็จระบบนอกจึงรับผลลัพธ์การยืนยันตัวตนแซมแอล (SAML Response Assertion) จากโมดูลยืนยันตัวตน เพื่อใช้ในการยืนยันว่าผู้ใช้งานสามารถเข้าใช้งานระบบได้

**จุดสำคัญของเหตุการณ์:** ผลลัพธ์การยืนยันตัวตนแซมแอลที่ได้รับแสดงถึงการยืนยันตัวตนของผู้ใช้สำเร็จ

**เงื่อนไขก่อน:** ระบบนอกสร้างคำร้องยืนยันตัวตนแบบแซมแอล เพื่อเบราเซอร์ใช้ยืนยันตัวตนกับโมดูลยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ใช้ยืนยันตัวตนสำเร็จเข้าใช้งานระบบได้

**ชื่อการใช้งาน:** ร้องขอข้อมูลนักศึกษา

**คำอธิบาย:** ระบบนอกส่งคำร้องเพื่อขอข้อมูลผู้ใช้ภายในฐานข้อมูลของโมดูลยืนยันตัวตน โดยส่งข้อมูลระหว่างกันผ่านทางโพรโทคอลเอชทีทีพี (HTTP Protocol)

**จุดสำคัญของเหตุการณ์:** คำร้องขอของระบบนอกมีความถูกต้อง

**เงื่อนไขก่อน:** ระบบนอกสร้างคำสั่งร้องขอข้อมูลนักศึกษาแบบ GET โดยกำหนดตัวแปร และข้อมูลที่ต้องการจากโมดูลยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ระบบนอกได้รับข้อมูลผู้ใช้ตรงตามความต้องการ

### แผนภาพกิจกรรม

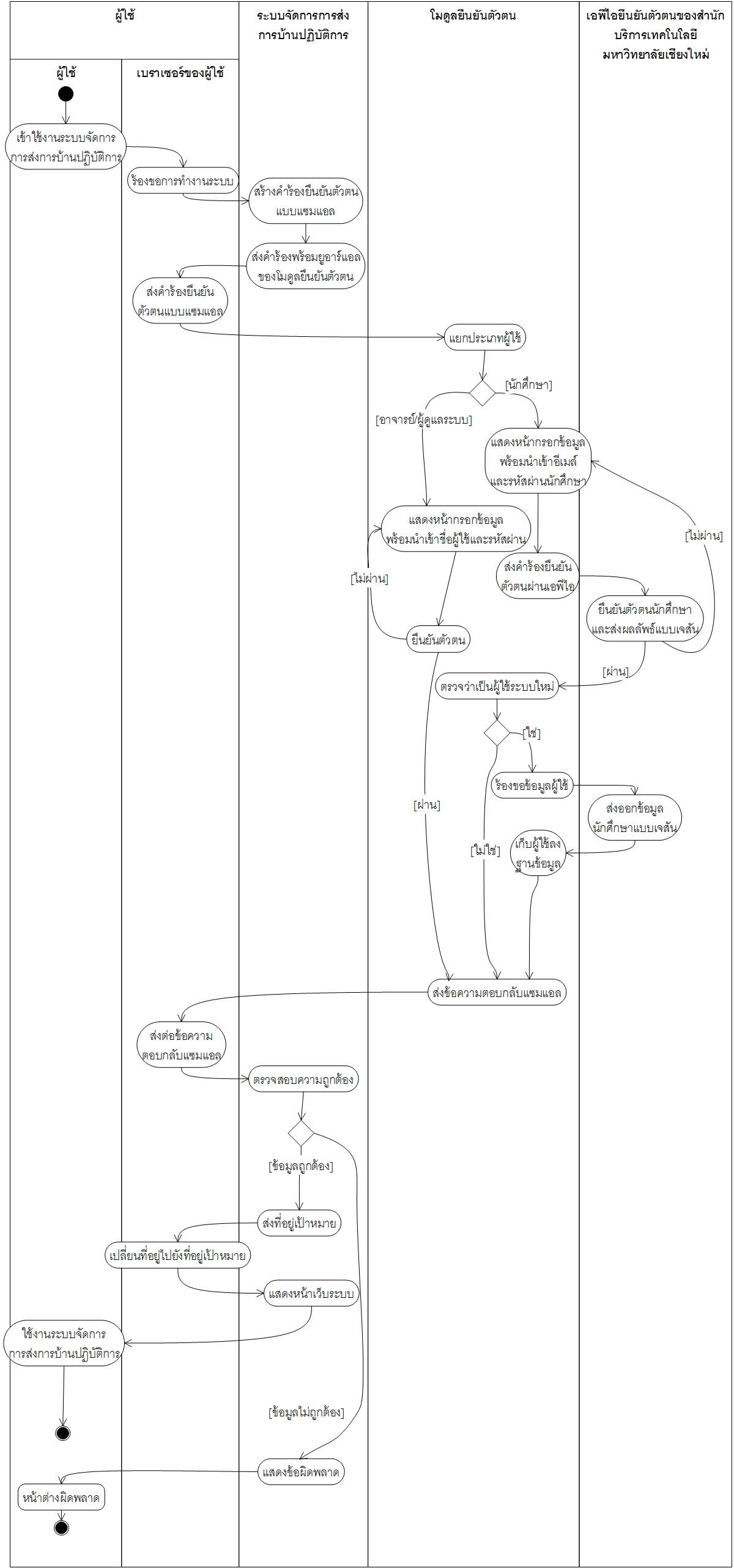
การใช้แผนภาพกิจกรรม [7] เป็นไปเพื่อแสดงขั้นตอนการส่งข้อมูล การทำงานแสดงความสัมพันธ์ระหว่างผู้ใช้ระบบนอก เช่น ระบบจัดการการส่งการบ้านปฏิบัติการ และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี ที่มีต่อโมดูลยืนยันตัวตน โดยมีการรวมการใช้งานในบางแผนภาพเพื่อให้เห็นการทำงานร่วมกันของผู้ใช้และระบบ ซึ่งแผนภาพนี้ใช้สัญญาลักษณ์ดังตาราง 3.4

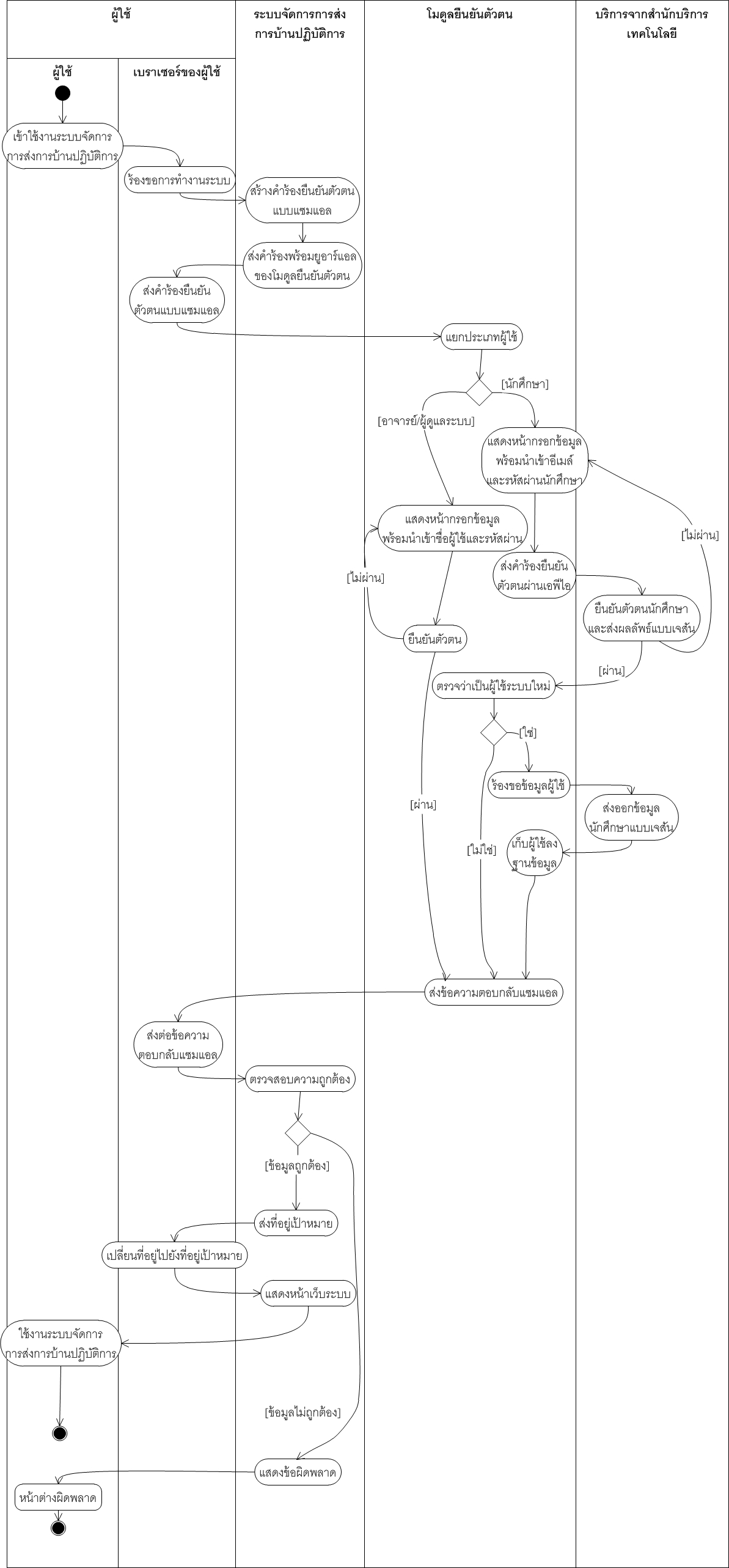
ตารางที่ 3.4 ตารางสัญลักษณ์แผนภาพกิจกรรม

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Start State | สัญญาลักษณ์สถานะเริ่มต้นในระบบ |
|  | Final State | สัญญาลักษณ์สถานะสุดท้ายในระบบ แสดงถึงการจบการทำงาน |
|  | State | สัญญาลักษณ์แสดงสถานะของระบบ |
|  | Decision | สัญญาลักษณ์การตัดสินใจเลือกสถานะของระบบ |
|  | Flow | สัญญาลักษณ์ให้เห็นลำดับถานะการทำงานในระบบ |
|  | System | สัญลักษณ์กรอบการทำงานของระบบ |

ตารางที่ 3.5 ตารางอธิบายคำศัพท์เฉพาะภายในแผนภาพยูเอ็มแอล

|  |  |
| --- | --- |
| **คำศัพท์** | **คำอธิบาย** |
| คำร้องยืนยันตัวตนแบบแซมแอล | เป็นข้อความคำร้องยืนยันตัวตนแบบแซมแอล ซึ่งถูกสร้างด้วยระบบนอก โดยโมดูลยืนยันตัวตนใช้เพื่อตรวจสอบก่อนให้บริการยืนยันตัวตนแก่ผู้ใช้ |
| ข้อความตอบกลับแบบแซมแอล | เป็นข้อความตอบกลับแสดงผลลัพธ์ยืนยันตัวตนแบบแซมแอล หลังจากผู้ใช้ยืนยันตัวตนกับโมดูลยืนยันตัวตนได้สำเร็จเพื่อให้เบราเซอร์ใช้ในการขอบริการกับระบบส่งการบ้าน โดยภายในข้อความประกอบไปด้วยค่าตัวแปรที่จำเป็นสำหรับการทำงานของระบบอื่น |
| ระบบจัดการการส่งการบ้านปฏิบัติการ | เปรียบเสมือนผู้ให้การบริการ ให้บริการนักศึกษาที่ลงทะเบียนกระบวนวิชาของภาควิชาวิทยาการคอมพิวเตอร์ อาจารย์ประจำภาควิชา และผู้ดูแลระบบซึ่งมีการใช้บริการยืนยันตัวผู้ใช้งานผ่านโมดูลยืนยันตัวตน |
| เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ | ส่วนให้บริการทำงานผ่าน เอชทีทีพี แบบ GET   1. ยืนยันตัวตนนักศึกษา 2. บริการส่งผ่านข้อมูลนักศึกษา |
| เงื่อนไข | เป็นแบบรูปแบบเงื่อนไขที่รวมทั้งข้อมูล ซึ่งถูกนำไปใช้เพื่อดึงข้อมูลบางส่วนจากฐานข้อมูลของโมดูลยืนยันตัวตน |
| ข้อมูลนักศึกษา | ข้อมูลนักศึกษา ประกอบไปด้วย ชื่อ นามสกุล เลขที่ประจำตัวนักศึกษาเป็นต้น |





รูปที่ 3.2 แผนภาพกิจกรรมแสดงการยืนยันตัวตนของผู้ใช้ และการส่งข้อมูลระหว่างระบบ

จากแผนภาพกิจกรรมจะเห็นว่า โมดูลแบ่งผู้ใช้เป็น 2 กลุ่ม คือ 1.นักศึกษา 2.อาจารย์ และผู้ดูแลระบบ

สำหรับข้อมูลที่ใช้ยืนยันตัวตนของนักศึกษา คือ อีเมล และรหัสผ่านของมหาวิทยาลัยเชียงใหม่ โดยโมดูลยืนยันตัวตนตรวจสอบตัวตนนักศึกษากับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีโดยค่าตอบกลับที่ได้เป็นแบบเจสัน เมื่อยืนยันตัวตนนักศึกษากับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีได้สำเร็จ จากนั้นจึงตรวจสอบว่ามีข้อมูลนักศึกษาที่ยืนยันตัวตนสำเร็จในระบบหรือไม่ ถ้าไม่มีให้ทำการเพิ่มข้อมูลนักศึกษาโดยร้องขอข้อมูลจากเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีเพื่อจัดเก็บไว้ในฐานข้อมูลของโมดูลยืนยันตัวตน

สำหรับอาจารย์ และผู้ดูแลระบบยืนยันตัวตนกับโมดูลโดยใช้ชื่อผู้ใช้ และรหัสผ่านที่มีอยู่ในฐานข้อมูลของโมดูลยืนยันตัวตน

การติดต่อระหว่างโมดูลยืนยันตัวตน และระบบนอกที่ร้องขอการยืนยันตัวตน (ระบบจัดการการส่งการบ้านปฏิบัติการ) ใช้การส่งข้อความแซมแอลเป็นสื่อแลกเปลี่ยนข้อมูลระหว่างกันในการยืนยันตัวตนของผู้ใช้ โดยที่ระบบจัดการการส่งการบ้านปฏิบัติการทำการสร้างคำร้องยืนยันตัวตนแบบแซมแอลสำหรับแต่ละผู้ใช้ และส่งให้เบราเซอร์ของผู้ใช้เพื่อส่งต่อให้กับโมดูลยืนยันตัวตน เมื่อโมดูลยืนยันตัวตนได้รับคำร้องจึงจะให้บริการแก่ผู้ใช้ เมื่อการยืนยันตัวสำเร็จ โมดูลยืนยันตัวตนสร้างข้อความตอบกลับแบบแซมแอลโดยข้อความตอบกลับจะประกอบไปด้วยประเภทของผู้ใช้และข้อมูลผู้ใช้ที่จำเป็น จากนั้นจึงส่งให้เบราเซอร์เพื่อใช้ในการขอบริการกับระบบจัดการการส่งการบ้านปฏิบัติการ

### แผนภาพขั้นลำดับ

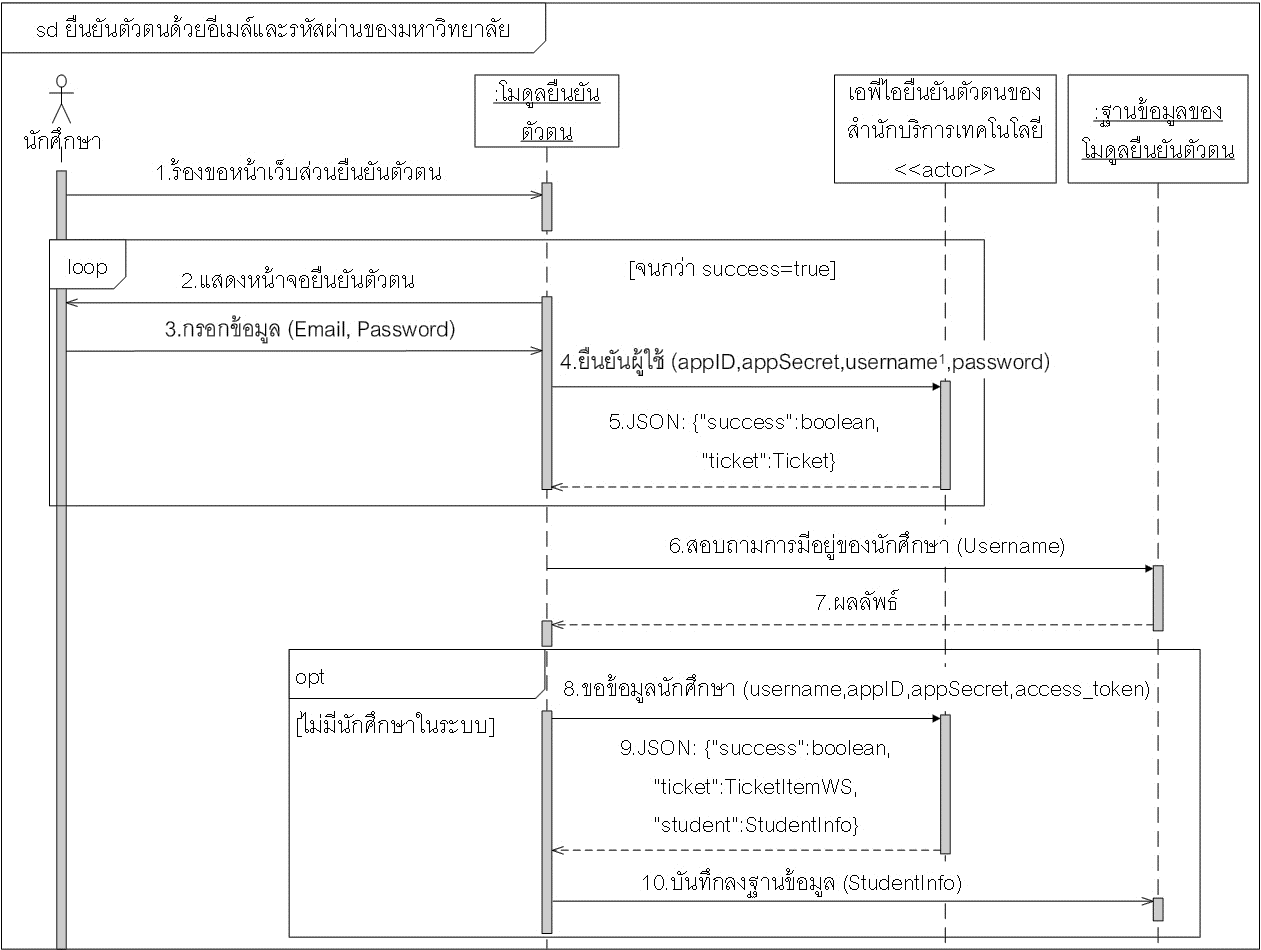
แผนภาพแสดงลำดับการทำงานของระบบ [7] โดยมีวัตถุและเวลาเป็นตัวกำหนดลำดับของงาน และเน้นไปที่ การแสดงปฏิสัมพันธ์ ระหว่างวัตถุ ตามลำดับของเหตุการณ์ที่เกิดขึ้น ณ เวลาที่กำหนด ข้อความที่เกิดขึ้นระหว่างวัตถุ ซึ่งแผนภาพนี้ใช้สัญญาลักษณ์ดังตาราง 3.6

ตารางที่ 3.6 ตารางสัญลักษณ์แผนภาพขั้นลำดับs

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Actor | สัญลักษณ์แสดงผู้ใช้งานที่เกี่ยวข้องกับระบบ |
|  | Instance | สัญลักษณ์แสดงสิ่งที่ระบบตอบสนองต่อผู้ใช้งาน |
|  | Lifeline | สัญลักษณ์เส้นแสดงถึงขอบเขตของแต่ละส่วนเกี่ยวข้อง |

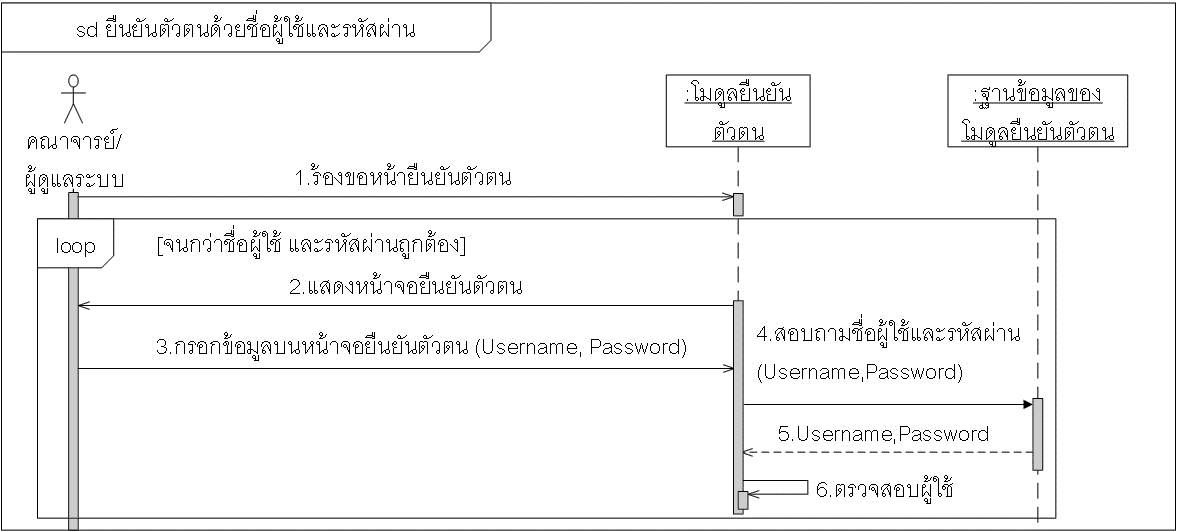
ตารางที่ 3.7 ตารางสัญลักษณ์แผนภาพขั้นลำดับ (ต่อ)

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Message | สัญลักษณ์แสดงคำสั่งหรือการสั่งการ |
|  | Message Return | สัญลักษณ์แสดงถึงค่าส่งกลับจากระบบด้านขวาไปหาด้านซ้ายของแผนภาพ |
|  | Focus of Control/Activation | สัญลักษณ์จุดเริ่มต้นและจุดสิ้นสุดของแต่ละกิจกรรมในระหว่างการทำงาน |



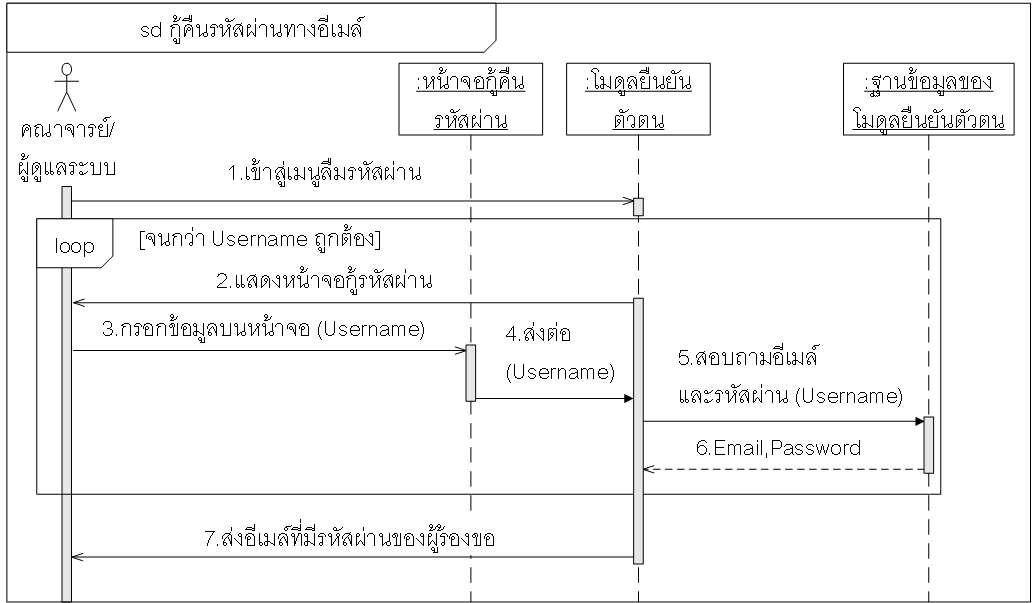
รูปที่ 3.3 แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของนักศึกษา

จากแผนภาพขั้นลำดับแสดงการยืนยันตัวตนกับระบบของนักศึกษา โดยโมดูลจะแสดงหน้าจอเพื่อรอรับข้อมูลเมื่อรับข้อมูลได้แล้วจึงจะส่งอีเมล และรหัสผ่านให้กับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี โดยส่งข้อความในรูปแบบ การร้องขอเอชทีทีพีแบบ GET โดยที่ appID และ appSecret เป็นตัวแปรสำคัญในการร้องขอการบริการจากระบบที่ถูกต้อง ต่อด้วยชื่อผู้ใช้ (มาจากอีเมลโดยจะไม่ใส่ @cmu.ac.th ) และรหัสผ่านของนักศึกษาเป็นรายบุคคล การตอบกลับสำหรับส่วนบริการยืนยันตัวตน จะเป็นข้อมูลแบบเจสัน ตัวแปรที่สำคัญ คือ success ที่จะบอกว่านักศึกษายืนยันตัวตนกับเอพีไอยืนยันตัวตนได้สำเร็จ และ ticket ที่มีสมาชิกคือ access\_token ซึ่งจะถูกใช้ในการร้องขอข้อมูลนักศึกษาต่อไป เมื่อได้ผลลัพธ์ว่าเป็นนักศึกษาถูกต้องจึงตรวจสอบว่ามีข้อมูลนักศึกษาในฐานข้อมูลของโมดูล ถ้าไม่ให้ร้องขอแบบ GET โดยขอข้อมูลตามชื่อผู้ใช้ และได้ข้อมูลกลับมาแบบเจสันเช่นกัน โดยที่ในครั้งนี้ success จะบอกว่าขอข้อมูลนักศึกษาได้สำเร็จ ตัวแปร ticket จะเปลี่ยนแปลงค่าทุกครั้งเมื่อมีการร้องขอข้อมูลนักศึกษา และที่สำคัญคือ student ซึ่งเก็บข้อมูลกลุ่มของตัวแปรที่ระบุข้อมูลประจำตัวนักศึกษา เช่น ชื่อ นามสกุล (ไทย-อังกฤษ) รหัสนักศึกษา เป็นต้น ซึ่งค่าในตัวแปร student จะถูกจัดเก็บต่อไป



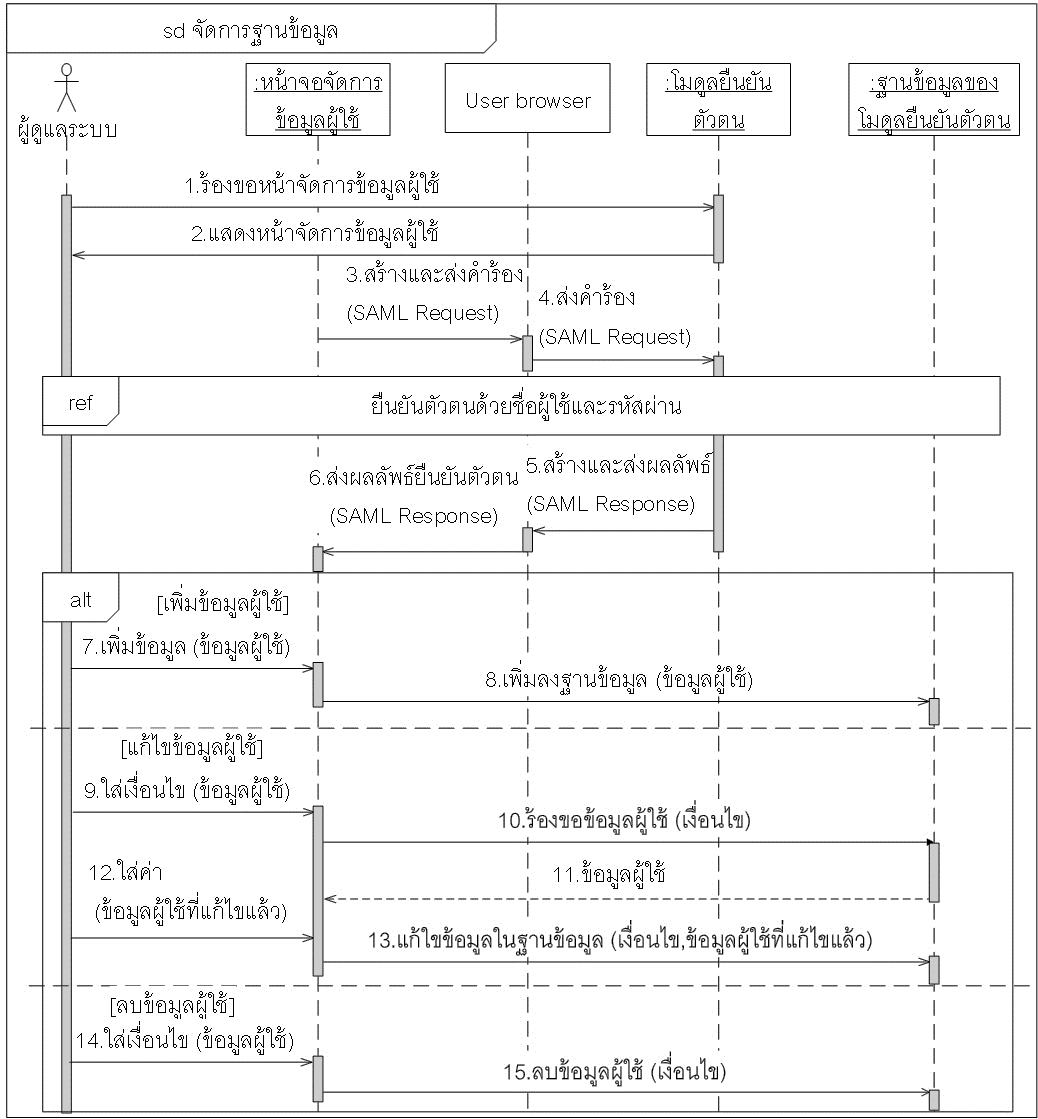
รูปที่ 3.4 แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของอาจารย์ และผู้ดูแล

เมื่อผู้ใช้เป็นอาจารย์หรือผู้ดูแลระบบ สิ่งที่ใช้ยืนยันตัวตน คือ ชื่อผู้ใช้ และรหัสผ่าน ที่จัดเก็บอยู่ภายในฐานข้อมูลของโมดูลยืนยันตัวตน การตรวจสอบยืนยันตัวตนจึงทำภายในโมดูลยืนยันตัวตน ไม่มีการร้องขอจากระบบภายนอก



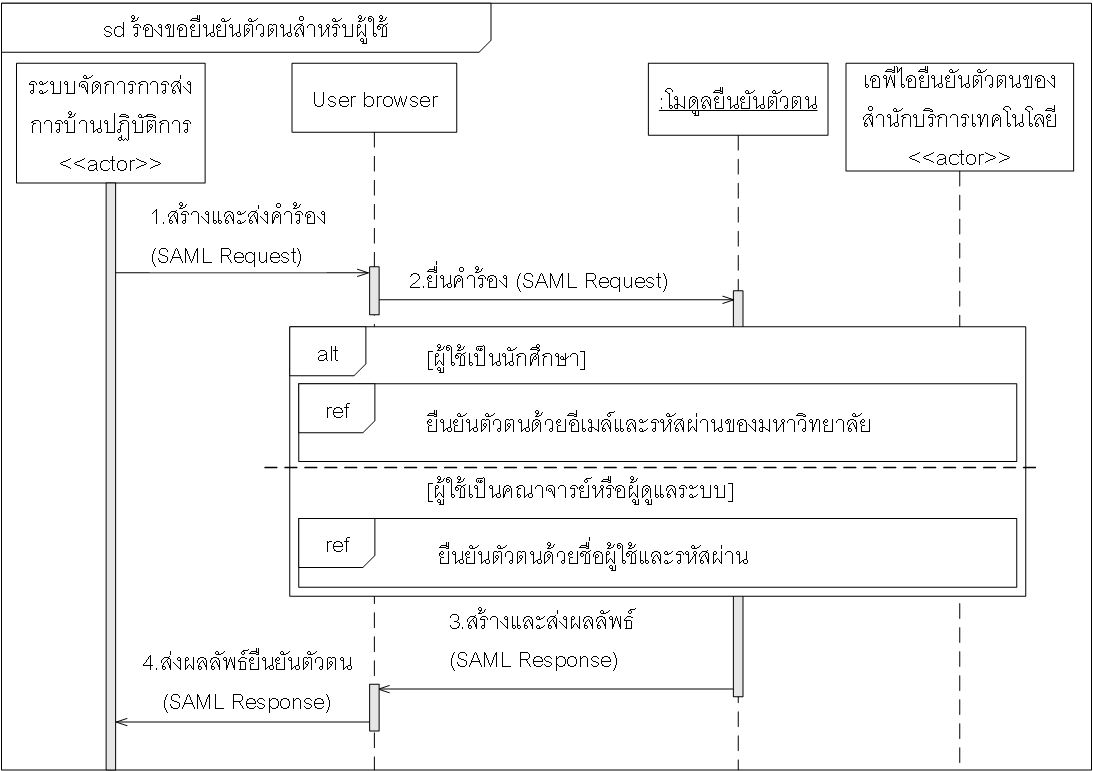
รูปที่ 3.5 แผนภาพขั้นลำดับการกู้คืนรหัสผ่านของอาจารย์ และผู้ดูแลระบบ

การกู้คืนรหัสผ่านเป็นส่วนสำหรับอาจารย์หรือผู้ดูแลระบบ ที่จะสามารถสอบถามรหัสผ่านเมื่อทำรหัสผ่านหาย หรือลืมรหัสผ่าน โดยจะให้ผู้ใช้กรอกชื่อผู้ใช้บนหน้าจอ แล้วโมดูลจะตรวจสอบที่อยู่อีเมล โมดูลยืนยันตัวตนจะใช้สำหรับส่งรหัสผ่านในฐานข้อมูลให้กับผู้ใช้ต่อไป



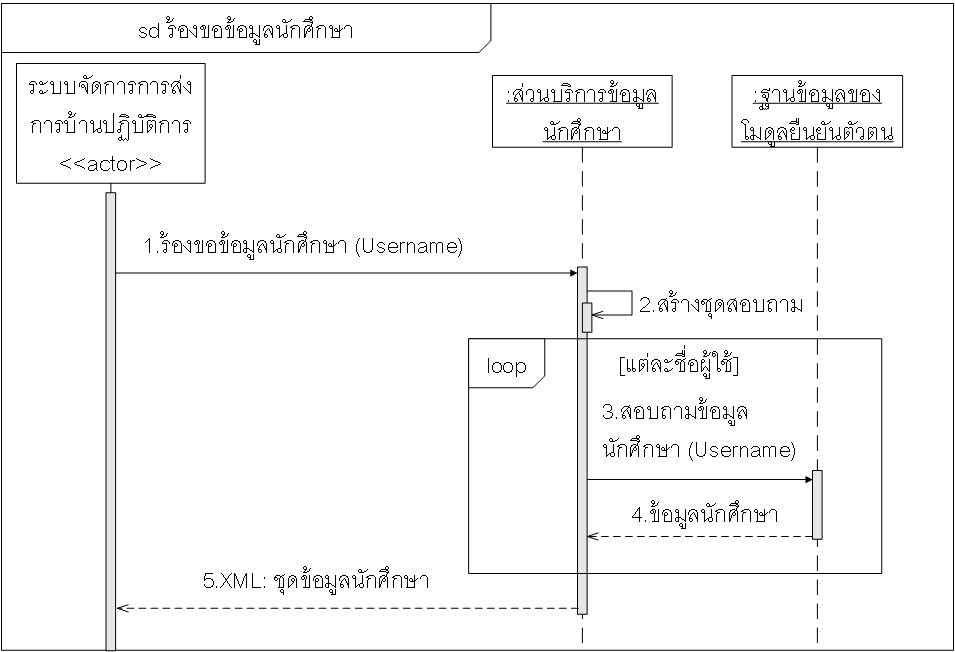
รูปที่ 3.6 แผนภาพขั้นลำดับแสดงการจัดการฐานข้อมูลของโมดูลยืนยันตัวตนของผู้ดูแล

จากแผนภาพเป็นการจัดการข้อมูลผู้ใช้ภายในฐานข้อมูลของโมดูลยืนยันตัวตน โดยผู้ใช้ที่มีสิทธ์มีเพียงผู้ดูแลระบบโดยการทำงานผ่านหน้าจอจัดการข้อมูลผู้ใช้ โดยหน้าจอจัดการข้อมูลผู้ใช้ทำงานเสมือนระบบนอกที่ต้องสร้างคำขอยืนยันตัวตนให้กับผู้ดูแลระบบ และรับข้อความยืนยันจากโมดูลยืนยันตัวตน เมื่อการเข้าระบบสำเร็จผู้ใช้สามารถเพิ่ม แก้ไข และลบข้อมูลผู้ใช้ภายในฐานข้อมูล ทั้งของนักศึกษา อาจารย์ และผู้ดูแลระบบ



รูปที่ 3.7 แผนภาพขั้นลำดับแสดงระบบส่งการบ้านร้องขอการยืนยันตัวตนแก่ผู้ใช้

การร้องขอการยืนยันตัวให้กับผู้ใช้ของระบบจัดการการส่งการบ้านปฏิบัติการ ใช้ข้อความร้องขอแบบ  
แซมแอลซึ่งทำงานบนโพรโทคอลที่อยู่บนพื้นฐานข้อมูลแบบเอ็กซ์เอ็มแอล ทำให้การง่ายต่อการใช้เป็นบัตรผ่านเพื่อให้เบราเซอร์ของผู้ใช้ร้องขอยืนยันตัวตนแก่ผู้ใช้ โดยโมดูลยืนยันตัวตนจะเป็นส่วนคัดแยกว่าผู้ใช้เป็นนักศึกษา อาจารย์ หรือผู้ดูแลระบบ ข้อความตอบกลับแซมแอลจะประกอบด้วยข้อมูลของผู้ใช้ เช่น ชนิดของผู้ใช้ที่ยืนยันตัวตนสำเร็จ ชื่อ นามสกุล เป็นต้น ทำให้ระบบจัดการการส่งการบ้านปฏิบัติการสามารถนำไปใช้ได้ทันที โดยไม่ต้องร้องขอข้อมูลจากโมดูลยืนยันตัวตนหลายครั้ง เพิ่มประสิทธิภาพในการทำงาน



รูปที่ 3.8 แผนภาพขั้นลำดับแสดงระบบจัดการการส่งการบ้านปฏิบัติการร้องขอข้อมูลนักศึกษา

เมื่อระบบภายนอกต้องการปรับปรุงข้อมูลให้มีความเป็นปัจจุบัน จึงต้องมีการร้องขอข้อมูลกับโมดูลยืนยันตัวตน โดยที่สามารถร้องขอได้ทีละผู้ใช้ หรือร้องขอแบบเป็นกลุ่มผู้ใช้จำแนกตามชื่อผู้ใช้ ซึ่งการร้องขอแบบกลุ่มมีข้อดีในการลดการส่งข้อมูลจำนวนหลายรอบ ช่วยเพิ่มประสิทธิภาพของเครื่องแม่ข่าย โมดูลยืนยันตัวตนจึงมีส่วนบริการข้อมูลนักศึกษาที่จะคอยรับคำร้องจากระบบภายนอก และคืนค่าข้อมูลนักศึกษาตามจำนวนที่ถูกร้องขอ

# บทที่ 4 การออกแบบฐานข้อมูล

ในการพัฒนาการพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอสำหรับการเตรียมข้อมูลเพื่อจัดทำฐานข้อมูล จำเป็นต้องศึกษาลักษณะเฉพาะของข้อมูล และรายละเอียดข้อมูลของผู้ใช้งานโมดูลยืนยันตัวตน เพื่อออกแบบความสัมพันธ์ของข้อมูลที่รองรับการทำงานของระบบด้วยความเหมาะสมสามารถแบ่งขั้นตอนการออกแบบฐานข้อมูลออกเป็น 3 ขั้นตอน คือ การออกแบบฐานข้อมูลในระดับความคิด (Conceptual Database Design) การออกแบบฐานข้อมูลในระดับตรรกะ (Logical Database Design) การออกแบบฐานข้อมูลระดับในกายภาพ (Data Dictionary) แต่ละขั้นตอนมีรายละเอียดดังนี้

## การออกแบบฐานข้อมูล

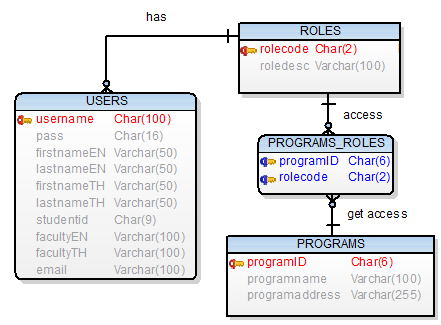
การออกแบบฐานข้อมูลของโมดูลยืนยันตัวตน อ้างอิงจากข้อมูลของผู้ใช้งานเป็นหลัก ประกอบด้วย นักศึกษา อาจารย์ และผู้ดูแลระบบ จากการศึกษาข้อมูลสามารถสร้างความสัมพันธ์ของข้อมูล โดยใช้แผนภาพแสดงความสัมพันธ์ของเอนทิตี (Entity Relationship Diagram: ER - Diagram) แสดงความสัมพันธ์ระหว่างเอนทิตี โดยมีการแทนความสัมพันธ์ของข้อมูลโดยใช้สัญลักษณ์ดังตารางที่ 4.1 และรูปที่ 4.1 แสดงภาพความสัมพันธ์ของเอนทิตี้

ตารางที่ 4.1 แสดงสัญลักษณ์ที่ใช้ในการสร้างแผนภาพความสัมพันธ์ของเอนทิตี

|  |  |
| --- | --- |
| **สัญลักษณ์** | **คำอธิบาย** |
|  | เอนทิตี (Entity) สิ่งที่สามารถระบุได้อย่างแจ้งชัด เป็นรูปธรรมหรือนามธรรม |
|  | คุณสมบัติ (Attribute) รายละเอียดที่เกี่ยวข้องกับลักษณะของเอนทิตี โดยคุณสมบัติมีอยู่ในทุกเอนทิตี |
|  | คุณสมบัติคีย์หลัก (Primary Key Attribute) ทำหน้าที่เป็นคีย์ที่มีคุณสมบัติของค่าข้อมูลไม่ซ้ำกัน |
|  | คุณสมบัติคีย์นอก (Foreign Key Attribute) ทำหน้าที่เป็นคีย์ที่มีคุณสมบัติ ได้มาจากคีย์หลักของเอนทิตีนอก |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ 1 : 1 (One to One Relationship) |

ตารางที่ 4.2 แสดงสัญลักษณ์ที่ใช้ในการสร้างแผนภาพความสัมพันธ์ของเอนทิตี (ต่อ)

|  |  |
| --- | --- |
| **สัญลักษณ์** | **คำอธิบาย** |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ 1 : N (One to Many Relationship) |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ M : N (Many to Many Relationship) |

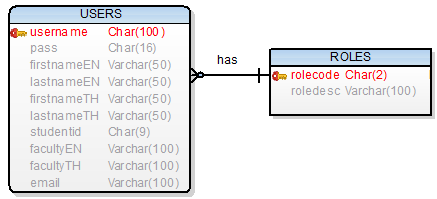


รูปที่ 4.1 แผนภาพความสัมพันธ์ระหว่างเอนทิตีต่างภายในโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่

### แผนภาพความสัมพันธ์ระหว่างเอนทิตี

จากแผนภาพแสดงความสัมพันธ์ดังรูปที่ 4.1 สามารถอธิบายความสัมพันธ์ระหว่างเอนทิตีได้ดังนี้

1. เอนทิตีผู้ใช้งานใช้อ้างถึงผู้ใช้งานทุกระดับการใช้งาน โดยผู้ใช้งานแต่ละคนมีบทบาทประจำตัวผู้ใช้งาน ซึ่งผู้ใช้งานมีได้แค่บทบาทเดียว แต่หนึ่งบทบาทมีได้หลายผู้ใช้ ดังนั้น ความสัมพันธ์ระหว่างสองเอนทิตีนี้มีความสัมพันธ์แบบกลุ่มต่อหนึ่ง ดังรูปที่ 4.2



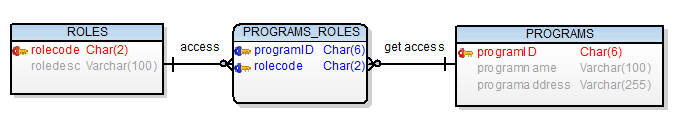
รูปที่ 4.2 แผนภาพความสัมพันธ์ระหว่างเอนทิตีผู้ใช้ และเอนทิตีบทบาท

จากผังความสัมพันธ์ของเอนทิตี สามารถแปลงแผนภาพเป็นความสัมพันธ์ ได้ดังนี้

USERS (username, firstnameEN, lastnameEN, firstnameTH, lastnameTH, studentid, facultyEN,   
 facultyTH, email, role)

ROLES (rolecode, roledesc)

1. เอนทิตีโปรแกรมใช้อ้างถึงโปรแกรมประยุกต์ที่ใช้งานโมดูลยืนยันตัวตน โดยผู้ใช้งานที่สามารถเข้าสู่การใช้งานโปรแกรมประยุกต์ขึ้นอยู่กับบทบาทของผู้ใช้งาน โดยหลายโปรแกรมสามารถถูกใช้งานโดยหลายบทบาทของผู้ใช้งาน ดังนั้น ความสัมพันธ์ระหว่างสองเอนทิตีนี้มีความสัมพันธ์แบบกลุ่มต่อกลุ่ม   
   ดังรูปที่ 4.3 และจากลักษณะความสัมพันธ์ดังกล่าว ก่อให้เกิดเอนทิตีใหม่ คือ เอนทิตีแฝงความสัมพันธ์แบบกลุ่มต่อกลุ่ม ชื่อว่า โปรแกรม\_บทบาท (PROGRAMS\_ROLES)



รูปที่ 4.3 แผนภาพความสัมพันธ์ระหว่างเอนทิตีโปรแกรม และเอนทิตีบทบาท

จากผังความสัมพันธ์ของเอนทิตี สามารถแปลงแผนภาพเป็นความสัมพันธ์ ได้ดังนี้

ROLES (rolecode, roledesc)

PROGRAMS (programID, programname, programaddress)

PROGRAMS\_ROLES (programID, rolecode)

## การออกแบบฐานข้อมูลในระดับตรรกะและกายภาพ

การออกแบบฐานข้อมูลในระดับตรรกะและระดับกายภาพ เป็นขั้นตอนที่แปลงจากตัวแบบข้อมูลในระดับแนวคิด ซึ่งเป็นตัวแบบที่จะนำไปปฏิบัติใช้งานจริง โดยในขั้นตอนนี้จะได้ตารางที่ใช้สำหรับจัดเก็บข้อมูลของส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอจำนวน 4 ตาราง เพื่อให้ได้โครงสร้างของตารางที่ถูกต้อง และลดความซ้ำซ้อนของข้อมูลภายในฐานข้อมูล ซึ่งแสดงรายละเอียดของตารางทั้งหมด ดังตาราง 4.2

ตารางที่ 4.3 ข้อมูลรายละเอียดของตารางทั้งหมดของโมดูล

|  |  |  |
| --- | --- | --- |
| **ลำดับที่** | **ชื่อตาราง** | **คำอธิบาย** |
| 1 | USERS | ตารางเก็บข้อมูลผู้ใช้งาน ประกอบด้วยลักษณะประจำดังนี้   * ชื่อผู้ใช้ (username) * รหัส (pass) * ชื่อภาษาอังกฤษ (firstnameEN) * นามสกุลภาษาอังกฤษ (lastnameEN) * ชื่อภาษาไทย (firstnameTH) * นามสกุลภาษาไทย (lastnameTH) * รหัสนักศึกษา (studentid) * ชื่อคณะภาษาอังกฤษ (facultyEN) * ชื่อคณะภาษาไทย (facultyTH) * อีเมล (email) * บทบาท (role) |
| 2 | PROGRAMS | ตารางเก็บข้อมูลโปรแกรมที่เชื่อมต่อกับโมดูล ประกอบด้วยลักษณะประจำดังนี้   * เลขโปรแกรม (programID) * ชื่อโปรแกรม (programname) * ที่อยู่โปรแกรม (programaddress) |
| 3 | ROLES | ตารางเก็บข้อมูลบทบาท ประกอบด้วยลักษณะประจำดังนี้   * รหัสบทบาท (rolecode) * คำอธิบายบทบาท (roledesc) |

ตารางที่ 4.4 ข้อมูลรายละเอียดของตารางทั้งหมดของโมดูล (ต่อ)

|  |  |  |
| --- | --- | --- |
| **ลำดับที่** | **ชื่อตาราง** | **คำอธิบาย** |
| 4 | PROGRAMS\_ROLES | ตารางเก็บข้อมูลการใช้โปรแกรมของแต่ละบทบาท ประกอบด้วยลักษณะประจำดังนี้   * เลขโปรแกรม (programID) * รหัสบทบาท (rolecode) |

## รายละเอียดของข้อมูลแต่ละตาราง

จากการออกแบบฐานข้อมูลในระดับกายภาพ จะได้ตารางที่เกี่ยวข้องกับระบบทั้งหมด 4 ตาราง ได้แก่ตารางนักศึกษา ตารางอาจารย์ผู้สอน ตารางผู้ใช้งาน ตารางโปรแกรม ตารางบทบาท และตารางโปรแกรมบทบาท ซึ่งรายละเอียดภายในตารางแต่ละตารางมีดังต่อไปนี้

### รายละเอียดข้อมูลในตารางผู้ใช้งาน

ตารางที่ 4.5 รายละเอียดข้อมูลในตารางกระบวนวิชา

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ตาราง : USERS  คำอธิบาย : เก็บข้อมูลผู้ใช้งาน  คีย์หลัก : username  ตารางอ้างอิง : rolecode จาก ROLES | | | | |
| ลำดับ | ชื่อฟิลด์ | ชนิด | ความหมาย | ค่าตัวอย่าง |
| 1 | username | Char(100) | ชื่อผู้ใช้งาน รูปแบบ ชื่อ\_นามสกุล | “siwaphol\_boonpan” |
| 2 | pass | Char(16) | รหัสเข้าใช้งาน | “ASFWsCS” |
| 3 | firstnameEN | Varchar(50) | ชื่อจริงภาษาอังกฤษ | “Siwaphol” |
| 4 | lastnameEN | Varchar(50) | นามสกุลภาษาอังกฤษ | “ศิวพล” |
| 5 | firstnameTH | Varchar(50) | ชื่อจริงภาษาไทย | “Boonpan” |
| 6 | lastnameTH | Varchar(50) | นามสกุลภาษาไทย | “บุญปั๋น” |
| 7 | studentid | Char(9) | รหัสนักศึกษา | “540510828” |
| 8 | facultyEN | Varchar(100) | ชื่อคณะภาษาอังกฤษ | “Faculty of Science” |
| 9 | facultyTH | Varchar(100) | ชื่อคณะภาษาไทย | “คณะวิทยาศาสตร์” |
| 10 | email | Varchar(100) | อีเมล | siwaphol.test@gmail.com |
| 11 | role | Char(2) | บทบาทของผู้ใช้ | “ST” |

### รายละเอียดข้อมูลในตารางโปรแกรม

ตารางที่ 4.6 รายละเอียดข้อมูลในตารางโปรแกรม

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ตาราง : PROGRAMS  คำอธิบาย : เก็บข้อมูลโปรแกรมที่เชื่อมต่อกับโมดูลยืนยันตัวตน  คีย์หลัก : programID  ตารางอ้างอิง : ไม่มี | | | | |
| ลำดับ | ชื่อฟิลด์ | ชนิด | ความหมาย | ค่าตัวอย่าง |
| 1 | programID | Char(6) | รหัสของโปรแกรม | “STDWEB” |
| 2 | programname | Varchar(100) | ชื่อโปรแกรม | “ระบบจัดการการส่งการบ้าน” |
| 3 | programaddress | Varchar(255) | ที่อยู่ยูอาร์แอลของโปรแกรม | “http://localhost/StudentWeb” |

### รายละเอียดข้อมูลในตารางบทบาท

ตารางที่ 4.7 รายละเอียดข้อมูลในตารางบทบาท

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ตาราง : ROLES  คำอธิบาย : เก็บข้อมูลบทบาทผู้ใช้งาน  คีย์หลัก : rolecode  ตารางอ้างอิง : ไม่มี | | | | |
| ลำดับ | ชื่อฟิลด์ | ชนิด | ความหมาย | ค่าตัวอย่าง |
| 1 | rolecode | Char(2) | รหัสของบทบาทโดยเป็นตัวย่อ | ถ้าเป็นนักศึกษา “ST”  ถ้าเป็นอาจารย์ “TE”  ถ้าเป็นนักศึกษาช่วยสอน “TA”  ถ้าเป็นผู้ดูแลระบบ “AD” |
| 2 | roledesc | Varchar(100) | คำอธิบายบทบาทนั้น | “Student” |

### รายละเอียดข้อมูลในตารางโปรแกรมบทบาท

ตารางที่ 4.8 รายละเอียดข้อมูลในตารางโปรแกรมบทบาท

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ตาราง : PROGRAMS\_ROLES  คำอธิบาย : เก็บข้อมูลการให้สิทธิแต่ละบทบาท เข้าใช้งานโปรแกรม  คีย์หลัก : programID, rolecode  ตารางอ้างอิง : programID จาก PROGRAMS และ rolecode จาก ROLES | | | | |
| ลำดับ | ชื่อฟิลด์ | ชนิด | ความหมาย | ค่าตัวอย่าง |
| 1 | programID | Char(6) | รหัสของโปรแกรม | “STDWEB” |
| 2 | rolecode | Char(2) | รหัสของบทบาทโดยเป็นตัวย่อ | “ST” |

# บทที่ 5 การออกแบบหน้าจอ

การออกแบบส่วนต่อประสานเพื่อให้ตรงกับความต้องการของผู้ใช้ ได้ทำตามขอบเขตของการวิเคราะห์ความต้องการและออกแบบระบบที่ได้ทำไว้ เพื่อให้ส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอมีการทำงานตรงตามความต้องการของผู้ใช้ เกิดการใช้งานที่ง่ายและสะดวก ดังนั้นจึงนำเสนอจอภาพการทำงานในแต่ละส่วน ของระบบ ดังแสดงส่วนของการทำงานภายใต้ระบบ ซึ่งประกอบด้วยหลายส่วน ซึ่งจะอธิบายการออกแบบและพัฒนาระบบ ดังนี้

## หน้าจอหลักยืนยันตัวตน

ส่วนของหน้าจอหลักยืนยันตัวตน กระบวนการทำงานจากไฟล์ loginuserpass.php ในโฟลเดอร์ modules/core/www ซึ่งสามารถอธิบายรายละเอียดดังรูปที่ 5.1

รูปที่ 5.1 หน้าจอหลักยืนยันตัวตน

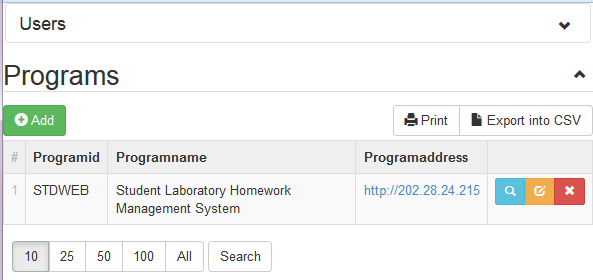
จากรูปที่ 5.1 อธิบายรายละเอียดหน้าจอได้ดังนี้

ส่วนที่ 1 คือ ส่วนแสดงภาษา สำหรับเปลี่ยนภาษาแสดงแก่ผู้ใช้งาน

ส่วนที่ 2 คือ ส่วนสำหรับผู้ใช้กรอกข้อมูลยืนยันตัวตน

## หน้าจอจัดการข้อมูลผู้ใช้งาน

ส่วนของหน้าจอจัดการข้อมูลผู้ใช้งาน เป็นส่วนสำหรับผู้ดูแลระบบ เพิ่ม แก้ไข และลบข้อมูล ภายในฐานข้อมูล โดยกระบวนการทำงานจากไฟล์ index.php ในโฟลเดอร์ admin888 ซึ่งสามารถอธิบายรายละเอียดดังรูปที่ 5.2



**5**

**4**

**3**

**2**

**1**

รูปที่ 5.2 หน้าจอจัดการข้อมูลผู้ใช้งาน

จากรูปที่ 5.2 อธิบายรายละเอียดหน้าจอได้ดังนี้

ส่วนที่ 1 คือ ส่วนแท็บด์ของแต่ละฐานข้อมูลใช้สำหรับซ่อน และแสดงข้อมูล

ส่วนที่ 2 คือ ส่วนเพิ่มข้อมูล

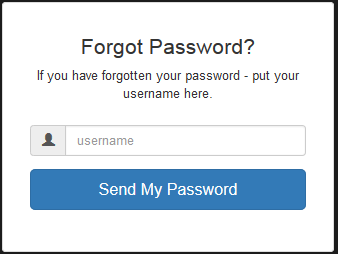
ส่วนที่ 3 คือ ส่วนการแสดงผลออกของข้อมูล ทั้งการพิมพ์ และส่งออกเป็นรูปแบบซีเอสวี (CSV)

ส่วนที่ 4 คือ ส่วนแสดงข้อมูลในตาราง โดยปุ่มด้านขวาเป็นคำสั่งดูข้อมูล แก้ไขข้อมูล และลบข้อมูล

ส่วนที่ 5 คือ ส่วนค้นหาข้อมูล โดยสามารถระบุจำนวนที่แสดงผล และค้นหาข้อมูลที่ต้องการ

## หน้าจอกู้คืนรหัสผ่านทางอีเมล

ส่วนของหน้าจอกู้คืนรหัสผ่านทางอีเมล เป็นส่วนสำหรับผู้ใช้ที่ไม่ใช่นักศึกษา ทำการขอรหัสผ่าน โดยกรอกชื่อผู้ใช้ที่มีในระบบ จากนั้นระบบจะทำการแจ้งผ่านอีเมลของผู้ใช้งานในฐานข้อมูล โดยกระบวนการทำงานจากไฟล์ index.php ในโฟลเดอร์ forgotpassword ซึ่งสามารถอธิบายรายละเอียดดังรูปที่ 5.3



**2**

**1**

รูปที่ . หน้าจอกู้คืนรหัสผ่านทางอีเมล

จากรูปที่ 5.3 อธิบายรายละเอียดหน้าจอได้ดังนี้

ส่วนที่ 1 คือ ส่วนช่องสำหรับกรอกชื่อผู้ใช้ที่ร้องขอรหัสผ่าน

ส่วนที่ 2 คือ ส่วนของปุ่มกดเพื่อให้ระบบทำงานส่งรหัสผ่านมายังอีเมลของผู้ใช้

# บทที่ 6 ผลการดำเนินงาน

ในบทนี้จะอธิบายในส่วนของผลการดำเนินงาน และสรุปผลการดำเนินงาน เพื่อเป็นการตรวจสอบการทำงานของระบบที่ได้จัดทำขึ้นนั้นทำงานได้อย่างถูกต้อง และตรงตามความต้องการ โดยการทดสอบระบบเพื่อหาจุดบกพร่อง และแก้ไขจุดเหล่านั้นให้ระบบใช้งานได้อย่างมีประสิทธิภาพ

## การยืนยันตัวตน

การทดสอบโมดูลยืนยันตัวตนที่ดีทีสุด คือ การกรอกข้อมูลผู้ใช้แล้วทำการยืนยันตัวตนกับระบบ โดยในการยืนยันตัวตนของนักศึกษา จะมีการกรอกชื่อผู้ใช้ คือ ชื่อจริง\_นามสกุล และรหัสผ่าน โดยมีการดำเนินการทดสอบระบบดังตารางที่ 6.1

ตารางที่ . ผลการทดสอบการยืนยันตัวของนักศึกษา

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test Case Name | | ทดสอบการยืนยันตัวตนของนักศึกษา | | | | |
| Test Description | | เพื่อทดสอบการยืนยันตัวตนของนักศึกษาและเข้าสู่ระบบส่งการบ้าน | | | | |
| Pre Condition | | นักศึกษามีอีเมล และรหัสจากสำนักบริการเทคโนโลยี พร้อมทั้งมีชื่ออยู่ในระบบส่งการบ้าน | | | | |
| No. | Test Case & Test Description | | Expected Result | Test Result | | Remark |
| Pass | Fail |
| 1 | Case : ผู้ใช้งานยืนยันตัวตน โดยใส่ชื่อผู้ใช้ และรหัสผ่านถูกต้อง | | ผู้ใช้สามารถเข้าสู่ระบบจัดการการส่งการบ้านปฏิบัติการ | 🗸 |  |  |
| 2 | Case : นักศึกษายืนยันตัวตน โดยใส่ชื่อผู้ใช้ และรหัสผ่านผิด | | ระบบแจ้งเตือนว่าไม่มีผู้ใช้งานในระบบ | 🗸 |  |  |
| 3 | Case : ผู้ใช้งานอื่นนอกจากนักศึกษายืนยันตัวตน โดยชื่อผู้ใช้ถูกต้อง แต่รหัสผ่านไม่ถูกต้อง | | ระบบแจ้งเตือนว่าไม่มีผู้ใช้งานในระบบ โดยระบบจะส่งที่อยู่สำหรับหน้าจอกู้คืนรหัสผ่านทางอีเมลให้ | 🗸 |  |  |
| 4 | Case : ผู้ใช้งานอื่นนอกจากนักศึกษายืนยันตัวตน โดยชื่อผู้ใช้และรหัสผ่านผิด | | ระบบแจ้งเตือนว่าไม่มีผู้ใช้งานในระบบ | 🗸 |  |  |

## การจัดการข้อมูลนักศึกษา

การทดสอบการจัดการข้อมูลนักศึกษา เป็นส่วนที่ผู้ดูแลระบบจะต้องใช้งาน โดยในการจัดการข้อมูล ผู้ดูแลระบบทำงานผ่านหน้าจอที่โมดูลเตรียมให้ การจัดการมีการเพิ่ม แก้ไข และลบข้อมูลนักศึกษา โดยมีการดำเนินการทดสอบระบบดังตารางที่ 6.2

ตารางที่ . ตารางทดสอบการจัดการข้อมูลนักศึกษา

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test Case Name | | ทดสอบการจัดการข้อมูลนักศึกษา | | | | |
| Test Description | | เพื่อทดสอบการจัดการข้อมูลนักศึกษาของผู้ดูแลระบบ | | | | |
| Pre Condition | | ผู้ใช้มีบทบาทของผู้ดูแลระบบ | | | | |
| No. | Test Case & Test Description | | Expected Result | Test Result | | Remark |
| Pass | Fail |
| 1 | Case : เพิ่มข้อมูลนักศึกษา | | ผู้ใช้สามารถเพิ่มข้อมูลนักศึกษาได้ | 🗸 |  |  |
| 2 | Case : แก้ไขข้อมูลนักศึกษา | | ผู้ใช้สามารถแก้ไขข้อมูลนักศึกษาได้ | 🗸 |  |  |
| 3 | Case : ลบข้อมูลนักศึกษา | | ผู้ใช้สามารถลบข้อมูลนักศึกษาได้ | 🗸 |  |  |

# บทที่ 7 บทสรุป

การค้นคว้าอิสระนี้ มีวัตถุประสงค์เพื่อพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอเพื่อใช้งานในรูปแบบเว็บเพจ ให้นักศึกษาได้ส่งงานผ่านทางระบบเครือข่าย ทางอินเทอร์เน็ต โดยสรุปเป็นประเด็นต่าง ๆ ดังนี้

7.1 สรุปผลการศึกษาและพัฒนาระบบ

7.2 ปัญหาและอุปสรรค

7.3 ข้อจำกัดของระบบงาน

7.4 ข้อเสนอแนะ

## สรุปผลการศึกษาและพัฒนาระบบ

การค้นคว้าอิสระนี้ เป็นการพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอโดยใช้มายเอสคิวแอลในการจัดการฐานข้อมูล เป็นการพัฒนาระบบโดยใช้ภาษาพีเอชพี และจาวาสคริปต์ในการทำงานติดต่อกับผู้ใช้ มีส่วนจัดการการยืนยันตัวตนของผู้ใช้งานเป็นหลัก และส่วนจัดการข้อมูลภายในระบบ โดยการทำงานจะแบ่งผู้ใช้ออกเป็น 3 กลุ่มคือ นักศึกษา อาจารย์ผู้สอน และผู้ดูแลระบบ ทำหน้าที่ดังนี้

1. นักศึกษา ยืนยันตัวตนกับระบบ เพื่อเข้าใช้งานระบบจัดการการส่งการบ้านปฏิบัติการ
2. อาจารย์ผู้สอน ยืนยันตัวตนเพื่อรับสิทธิแบบอาจารย์กับระบบจัดการการส่งการบ้านปฏิบัติการ
3. ผู้ดูแลระบบ ทำการจัดการข้อมูลผู้ใช้งาน ข้อมูลบทบาทผู้ใช้ และข้อมูลโปรแกรมที่เชื่อมต่อกับโมดูล

**7.2 ปัญหา และอุปสรรค**

ปัญหาและอุปสรรคที่เกิดขึ้นในการพัฒนาระบบ มีดังนี้

1. การพัฒนาระบบที่มีการเชื่อมต่อแบบแซมแอลค่อนข้างมีความซับซ้อน ทำให้ผู้ที่ศึกษาใหม่เกิดปัญหาในการติดตั้ง และการตั้งค่าระบบได้
2. เมทาดาทา เป็นส่วนสำคัญในการทำงานประสานระหว่างผู้ให้การบริการ และผู้พิสูจน์เอกลักษณ์ ความผิดพลาดเพียงเล็กน้อยทำให้ระบบไม่สามารถทำงานได้

**7.3 ข้อจำกัดของระบบงาน**

ส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอมีข้อจำกัดของระบบดังนี้

1. หน้าจอยืนยันตัวตนไม่สามารถใช้งานเอแจ็กซ์ช่วยได้ เพราะการทำงานตามหลักการของการยืนยันตัวตนแบบแซมแอล ผู้ใช้งานจะต้องถูกเปลี่ยนที่อยู่ไปยังผู้พิสูจน์เอกลักษณ์ และหลังจากยืนยันตัวตนเสร็จสิ้นผู้ใช้งานจะถูกเปลี่ยนที่อยู่กลับไปยังหน้าเว็บที่ร้องขอ
2. ส่วนของการกำหนดเมทาดาทา ระหว่างผู้ให้การบริการกับผู้พิสูจน์เอกลักษณ์ยังคงต้องเป็นหน้าที่ของผู้ดูแลระบบ กำหนดค่าในระบบโดยตรง โดยจะต้องใส่เมทาดาทาของผู้ให้การบริการ ให้กับส่วนผู้พิสูจน์เอกลักษณ์ เพื่อเป็นการบอกว่ามีผู้ให้การบริการร้องขอใช้งาน และใส่เมทาดาทาของผู้พิสูจน์เอกลักษณ์ ในส่วนฝั่งผู้ให้การบริการ
3. เมื่อผู้ใช้งานเข้ามาสู่หน้าจอยืนยันตัวตน ผู้ใช้ไม่สามารถคั่นหน้าได้ เพราะระบบมีการสร้างรหัสสุ่มสำหรับแต่ละการเข้าใช้งาน ดังนั้นผู้ใช้งานต้องทำการคั่นหน้าเว็บที่ร้องขอโมดูลยืนยันตัวตน

**7.4 ข้อเสนอแนะ**

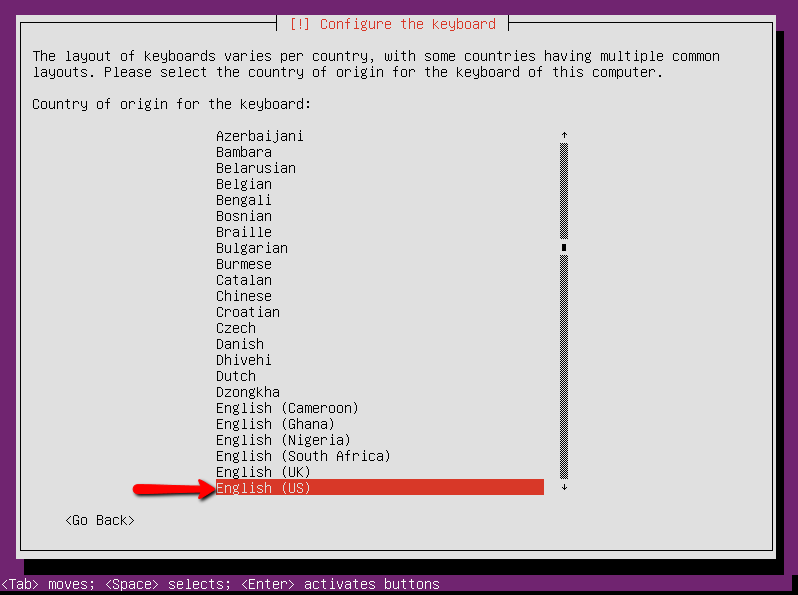
การนำระบบไปพัฒนานั้นมีข้อเสนอแนะ ข้อบกพร่องของระบบ ดังนี้

1. การยืนยันตัวตนสามารถ ยืนยันตัวตนผ่านเฟซบุ๊ก (Facebook) เป็นอีกทางเลือกหนึ่งผ่านโมดูล authfacebook ของ SimpleSAMLphp
2. การออกแบบหน้าจอการใช้งานให้มีความน่าสนใจ หรือดึงดูดผู้ใช้งาน

# ภาคผนวก ก การติดตั้งระบบปฏิบัติการอูบุนตู และซอฟต์แวร์อื่นพร้อมการตั้งค่าที่จำเป็น

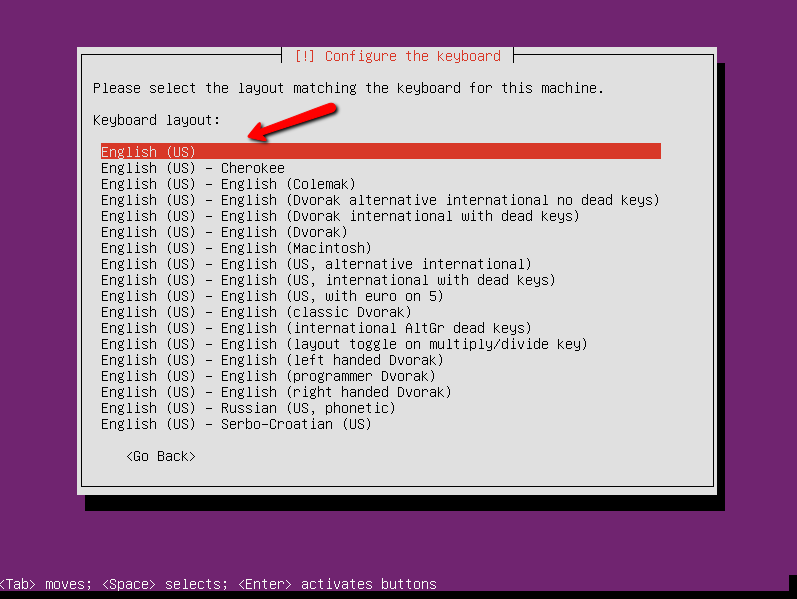
## การติดตั้งอูบุนตู

1. เลือกภาษาสำหรับการติดตั้ง
2. เลือกเมนู Install Ubuntu Server.
3. เลือกประเทศที่อยู่
4. เลือก No ในขั้นตอน Detect Keyboard Layout
5. เลือก English (US) ส่วน Country Origin



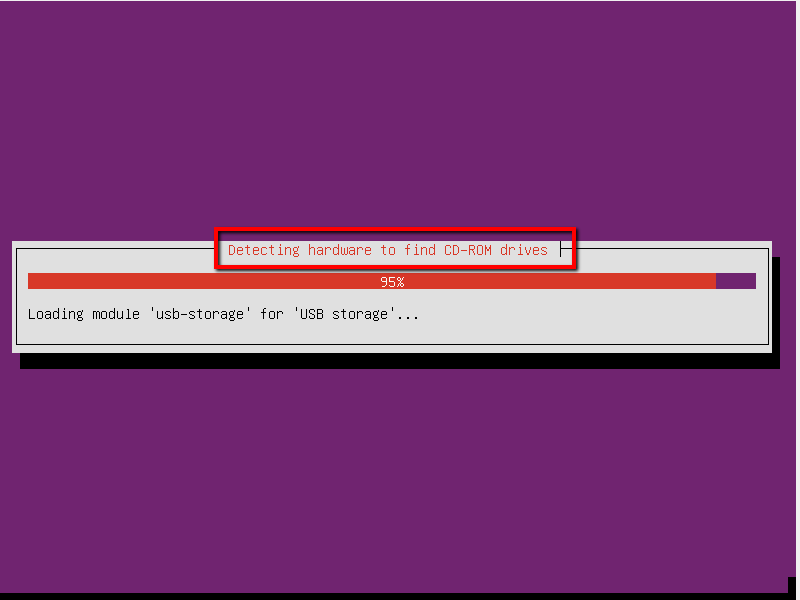
รูปที่ . แสดงหน้าจอเลือกแผงแป้นอักขระ

1. เลือก English (US) keyboard layout.



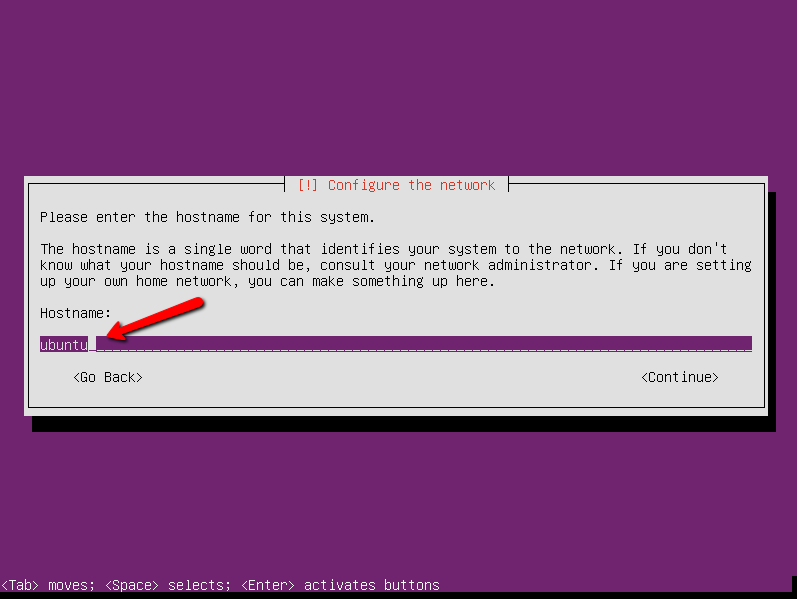
รูปที่ . แสดงหน้าจอเลือกรูปแบบแป้นพิมพ์

1. หลังจากนั้นโปรแกรมจะค้นหาข้อมูลฮาร์ดแวร์ของระบบ



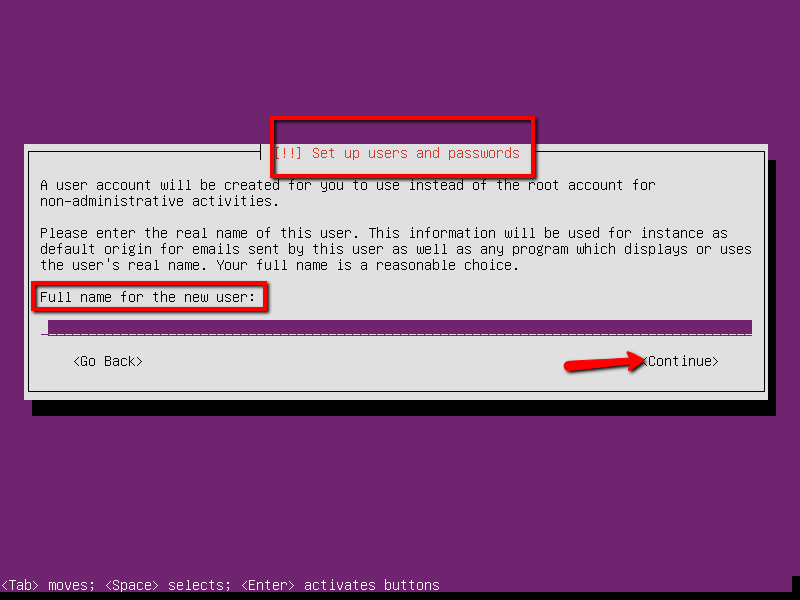
รูปที่ . แสดงส่วนค้นหาข้อมูลฮาร์ดแวร์ของระบบ

1. กรอกชื่อเครื่อง



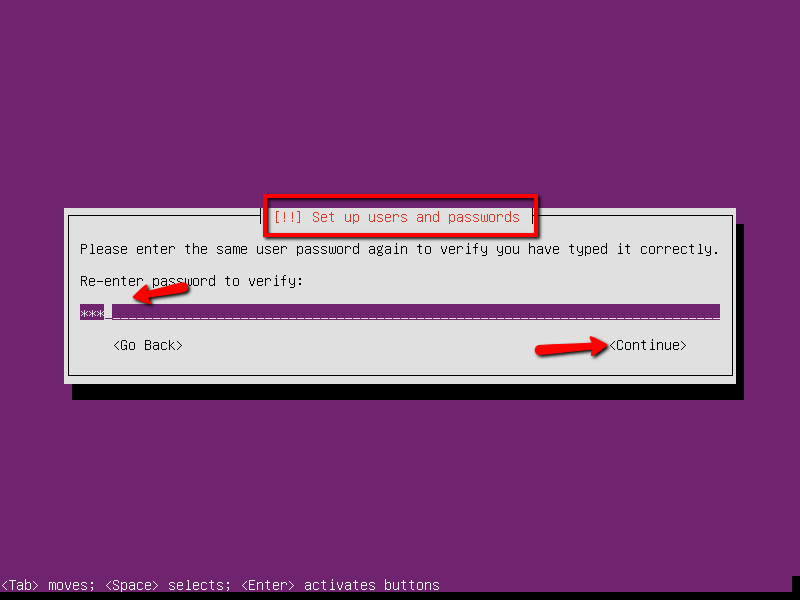
รูปที่ . แสดงหน้าจอส่วนกรอกชื่อเครื่อง

1. กรอกชื่อผู้ใช้ที่จะเป็นผู้ใช้คนแรก



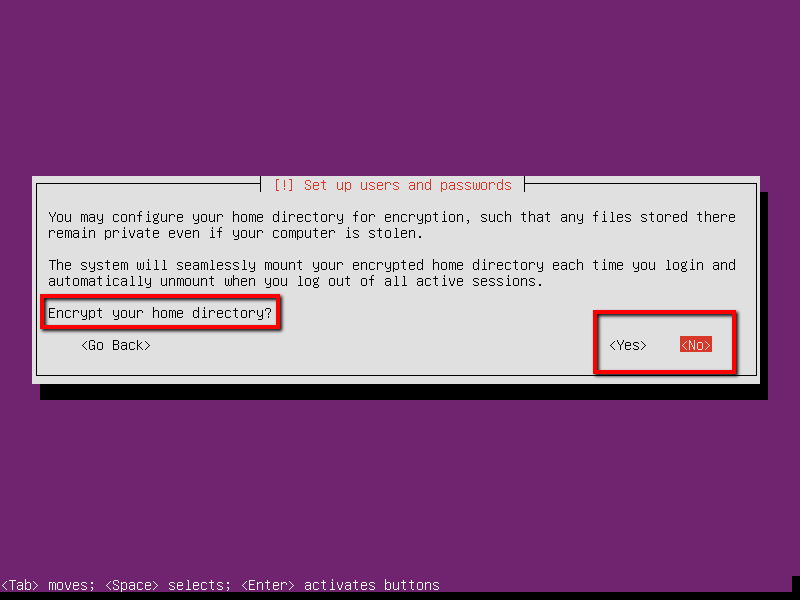
รูปที่ . แสดงหน้าจอส่วนกรอกชื่อผู้ใช้

1. กรอกรหัสสำหรับผู้ใช้งาน



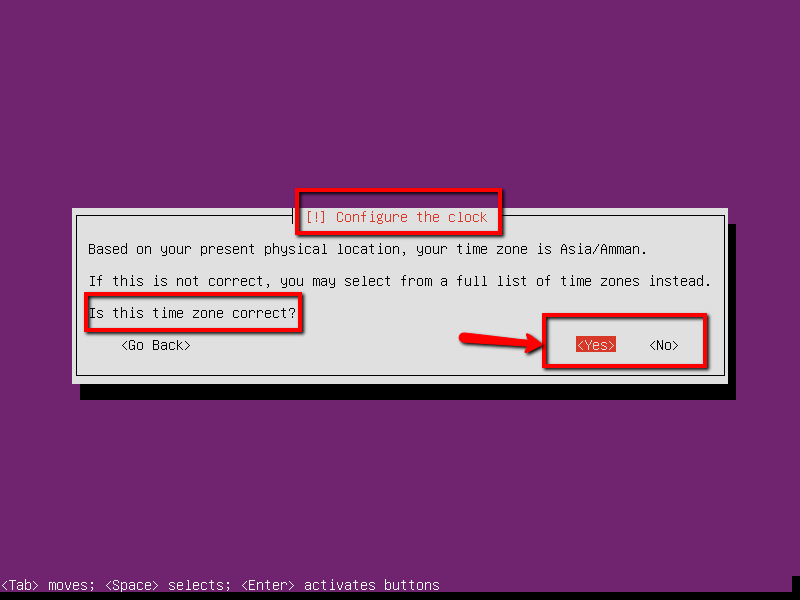
รูปที่ . แสดงหน้าจอส่วนกรอกรหัสผู้ใช้

1. เลือกการเข้ารหัสของ home directory แนะนำให้เลือก No เพราะ การทำ recovery ง่ายกว่าระบบที่เข้ารหัส



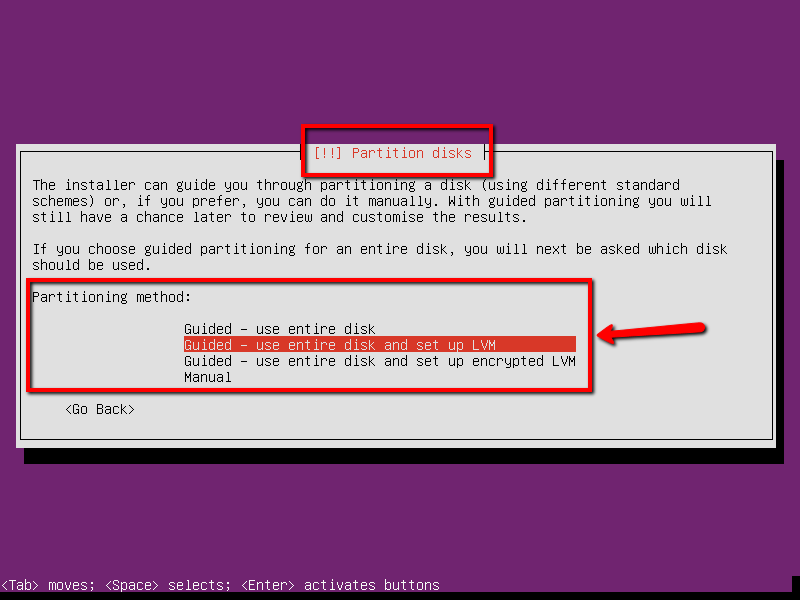
รูปที่ . แสดงหน้าจอส่วนตัวเลือกเข้ารหัสสารบบ

1. เลือก Time Zone



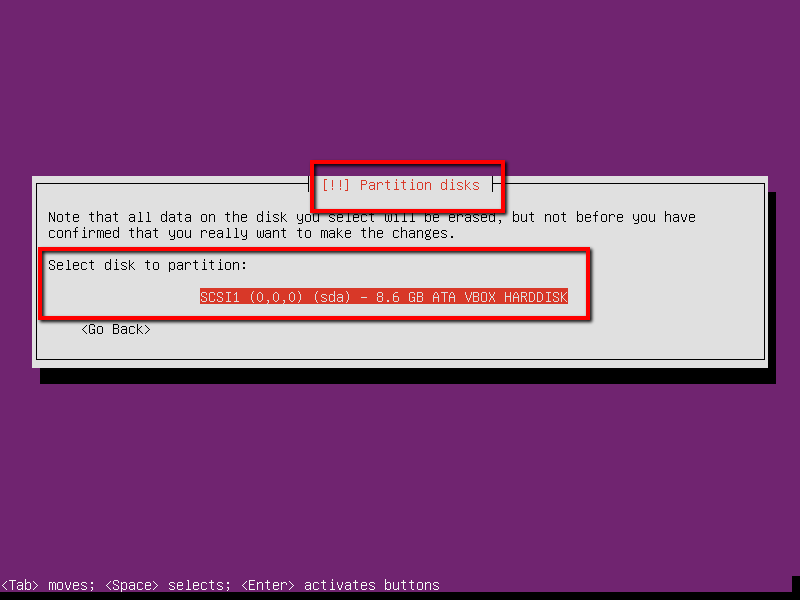
รูปที่ . แสดงหน้าจอส่วนตัวเลือกเขตเวลา

1. เลือก Guided – use entire disk เพื่อให้อูบุนตูใช้งานพื้นที่ทั้งหมด



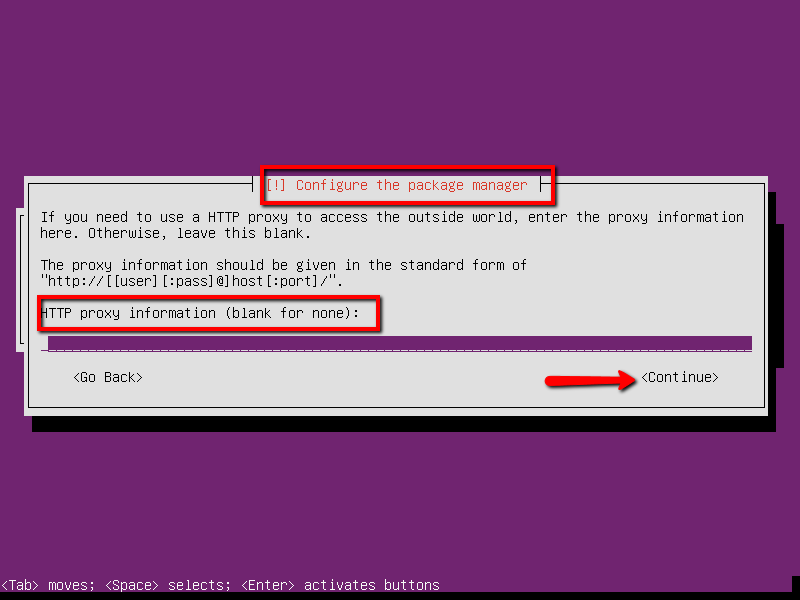
รูปที่ . แสดงหน้าจอส่วนตัวเลือกการใช้พื้นที่ของอูบุนตู

1. เลือก Partition



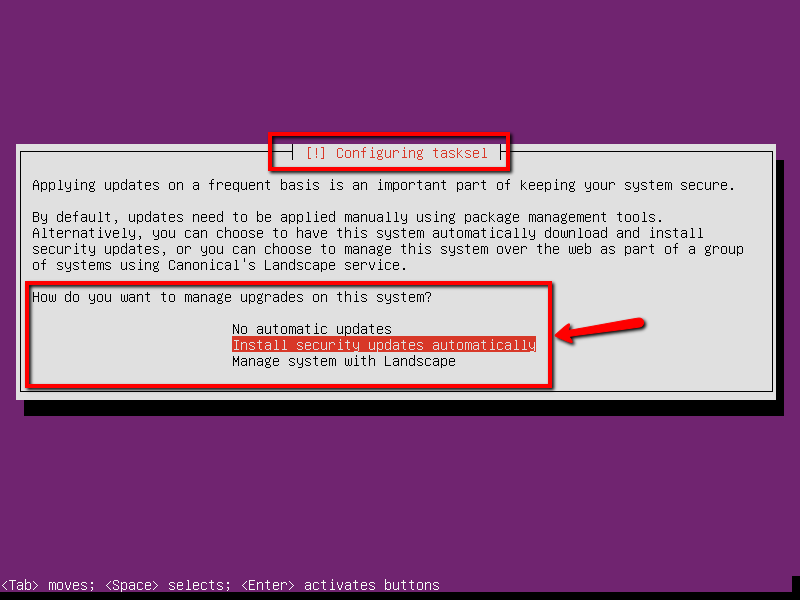
รูปที่ . แสดงหน้าจอส่วนตัวเลือกพื้นที่ส่วนแบ่ง

1. ส่วน Partition disks เลือก Yes เพื่อทำการยืนยันการติดตั้ง
2. หลังจากนั้นปล่อยให้อูบุนตูทำการติดตั้ง
3. กรณีใช้เครื่องบริการแทนให้กรอกข้อมูล



รูปที่ . แสดงหน้าจอส่วนกรอกที่อยู่เครื่องบริการแทน

1. สำหรับการติดตั้งอัพเดตเลือก Install security updates automatically



รูปที่ . แสดงหน้าจอส่วนเลือกรูปแบบการอัพเดต

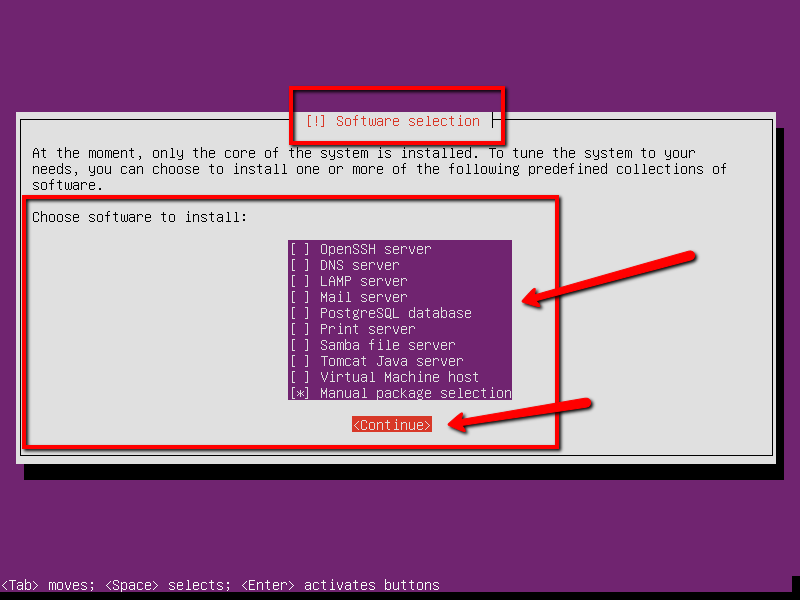
1. เลือกซอฟต์แวร์ที่ต้องการติดตั้ง

โดยที่จำเป็นหลัก คือ

OpenSSH server สำหรับการเชื่อมต่อทางไกล

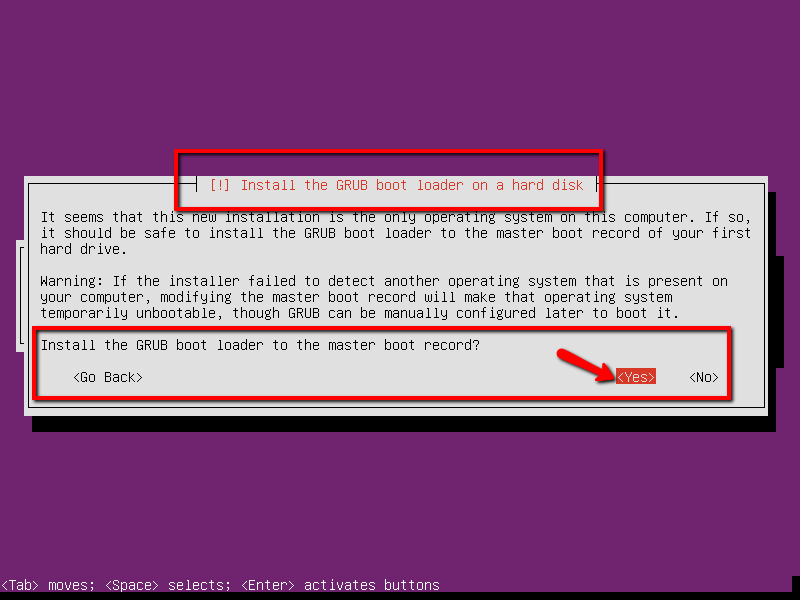
DNS server สำหรับการใช้งานบนไอพีสาธารณะ

LAMP server สำหรับการทำงานของเว็บ



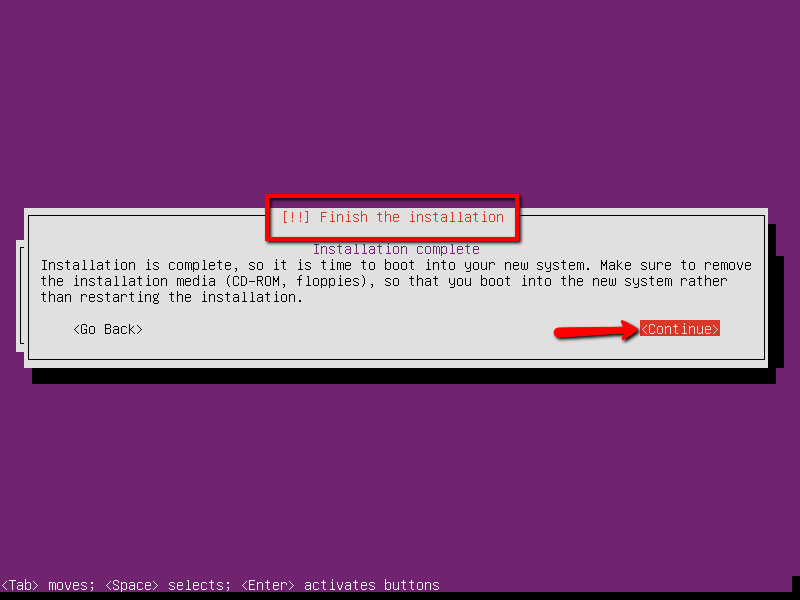
รูปที่ . แสดงหน้าจอส่วนเลือกซอฟต์แวร์เสริม

1. เลือก Yes ในส่วนติดตั้ง GRUB ลงสู่ Master Boot Record



รูปที่ . แสดงหน้าจอส่วนตัวเลือกใช้งาน GRUB

1. เลือก Continue เพื่อ จบการติดตั้งอูบุนตู



รูปที่ . แสดงหน้าจอส่วนเลือกจบการติดตั้งอูบุนตู

## การตั้งค่าอาปาเช่เตรียมสำหรับส่วนบริการเกตเวย์ยืนยันตัวตนยืนยันตัวตน

แก้ไขค่าใน 000-default.conf เพื่อกำหนดที่อยู่ของไฟล์แสดงผล โดยใช้คำสั่ง

sudo vim /etc/apache2/sites-available/000-default.conf

โดยปกติจะมี 2 ป้ายระบุ คือ <VirtualHost \*:80> สำหรับการทำงานผ่านพอร์ต 80 (HTTP)   
และ<VirtualHost \*:443> สำหรับการทำงานผ่านพอร์ต 443 (HTTPS) โดยค่าที่ต้องกำหนดในแต่ละป้ายระบุมีดังนี้

* กำหนดที่อยู่เริ่มต้นสำหรับ Apache เช่น DocumentRoot /home/siwaphol/www
* กำหนดสมนาม (Alias) ให้เพิ่มตัวแปร Alias เช่น

Alias /simplesaml /home/siwaphol/simplesamlphp/www

กรณีที่มีการใช้งานของ HTTPS ให้ทำตามขั้นตอนดังนี้

ขั้นตอนแรกสร้างใบรับรองเอสเอสแอล

1. สร้าง RSA Private Key ขนาด 1024 บิต เข้ารหัสโดยใช้ Triple-DES และบันทึกในรูปแบบ PEM

openssl genrsa –des3 –out mykey.key 1024

Generating RSA private key, 1024 bit long modulus  
โดยใส่รหัสพีอีเอ็มตามข้อความข้างล่าง  
Enter PEM pass phrase: (ใส่รหัสปลดล็อกที่ต้องการ)  
Verifying password - Enter PEM pass phrase: (ใส่รหัสปลดล็อกที่ต้องการ)

1. สร้าง CSR (Certificate Signing Request) โดย [] คือปล่อยเป็นค่าว่างได้

openssl req -new -key mykey.key -out mykey.csr

จากนั้นให้กรอกค่า

Country Name (2 letter code) [GB]: TH(กรอกตัวย่อประเทศสองอักขระ)  
State or Province Name (full name) [Berkshire]: Muang (ชื่ออำเภอ)  
Locality Name (eg, city) [Newbury]: Oberdiessbach(ชื่อเมือง)  
Organization Name (eg, company) [My Company Ltd]: CMU (ชื่อบริษัท)  
Organizational Unit Name (eg, section) []: Computer Science (ชื่อแผนก)  
Common Name (eg, your name or your server's hostname) []: example.com (ชื่อเครื่อง)  
Email Address []: siwaphol.boonpan@gmail(อีเมล)  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []: (กรณีต้องการให้ผู้ใช้กรอกรหัส โดยปกติเป็นค่าว่าง)  
An optional company name []: (ชื่อบริษัท ถ้ามี)

1. ทำการลบ passphrase ออกจาก key

cp mykey.key mykey.key.org  
openssl rsa -in mykey.key.org -out mykey.key

1. สร้าง Self-Signed Certificate โดยมีอายุ 365 วัน

openssl x509 -req -days 365 -in mykey.csr -signkey mykey.key -out mykey.crt

1. จากนั้นทำการตั้งค่าในป้ายระบุ <VirtualHost \*:443> ของไฟล์ 000-default.conf ดังนี้

SSLEngine on  
SSLCertificateFile /ที่อยู่ของไฟล์/mykey.crt  
SSLCertificateKeyFile /ที่อยู่ของไฟล์/mykey.key  
SetEnvIf User-Agent ".\*MSIE.\*" nokeepalive ssl-unclean-shutdown  
CustomLog logs/ssl\_request\_log \  
   "%t %h %{SSL\_PROTOCOL}x %{SSL\_CIPHER}x \"%r\" %b"

1. ทำการเริ่มอาปาเช่ใหม่

sudo service apache2 restart

แก้ไขการตั้งค่าสำหรับอาปาเช่ที่ไฟล์ apache2.conf โดยใช้คำสั่ง

sudo vim /etc/apache2/apache2.conf

โดยค่าหลักที่ต้องเพิ่ม คือ

* เพิ่มป้ายระบุ Directory เพื่อกำหนดรูปแบบการเข้าถึงของที่อยู่ เช่น

<Directory /home/siwaphol/simplesamlphp>

Options FollowSymLinks Includes ExecCGI

AllowOverride All

Require all granted

</Directory>

ให้การอนุญาตใช้งานแบบ 755 คือ เจ้าของไฟล์ และผู้ใช้งานที่อยู่กลุ่มเดียวกันกับเจ้าของไฟล์ สามารถอ่าน เขียนได้ โดยปกติแล้วชื่อผู้ใช้โดยปริยายของอาปาเช่สำหรับอูบุนตู คือ www-data

* ให้ความเป็นเจ้าของแก่ชื่อผู้ใช้ www-data ดังนี้

Chown –R www-data /home/siwaphol/simplesamlphp

* เพิ่มสิทธิอนุญาตให้แก่กลุ่มของเจ้าของไฟล์

Chmod –R 755 /home/siwaphol/simplesamlphp

# เอกสารอ้างอิง

[1] Microsoft. TLS/SSL Technical Reference [ระบบออนไลน์] แหล่งที่มา  
 https://technet.microsoft.com/en-us/library/cc784149%28v=ws.10%29.aspx (01 ตุลาคม 2557)

[2] Cisco. How Does RADIUS Work? [ระบบออนไลน์] แหล่งที่มา http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html (01 ตุลาคม 2557)

[3] Tom Adelstein และ Bill Lubanovic. Linux System Administration. March 2007. O'Reilly Media, 2007.

[4] OASIS. SAML V2.0 Kerberos Web Browser SSO Profile Version 1.0 [ระบบออนไลน์] แหล่งที่มา http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-browser-sso-cd-01.pdf   
(01 ตุลาคม 2557)

[5] Kelly D. LEWIS, James E. LEWIS. "Web Single Sign-On Authentication using SAML", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009. 2009.

[6] Uninet. SimpleSAMLphp Documentation [ระบบออนไลน์] แหล่งที่มา https://simplesamlphp.org/docs/stable/ (01 ธันวาคม 2557)

[7] ผศ.ดร. อัษฎาพร ทรัพย์สมบูรณ์. ธันวามคม 2552. " การวิเคราะห์และออกแบบเชิงวัตถุ (Object-Oriented Analysis And Design)" : เคทีพี 2552

[8] Todd Fredrich. RESTful Service Best Practices ,Recommendations for Creating Web Services [ระบบออนไลน์] แหล่งที่มา http://www.restapitutorial.com/media/RESTful\_Best\_Practices-v1\_1.pdf