**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**

รายงานนี้เป็นส่วนหนึ่งของกระบวนวิชา 204499

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 ขอบคุณเจ้าหน้าที่ดูแลส่วนระบบยืนยันตัวตนของสำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ คุณปรเมศวร์ พูลประสาธน์พร ที่ให้ข้อมูลเกี่ยวกับการใช้งานเรสต์เอพีไอยืนยันตัวตน และให้ความช่วยเหลือเมื่อเกิดปัญหา 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 โดยรหัสผ่านจะถูกสร้างใหม่สำหรับทุกรายวิชา ทำให้เกิดปัญหากับนักศึกษาในการจัดการ อีกทั้งยังเกิดปัญหาในการเดารหัสผ่านของเพื่อน และทำให้เกิดความเสียหายต่อข้อมูล เกิดการสูญหายของรหัส และถูกจดจำได้ง่าย ก่อให้เกิดความเสียหายต่อข้อมูลภายในระบบจัดการการส่งการบ้านปฏิบัติการของนักศึกษาเอง

โดยส่วนบริการเกตเวย์ที่พัฒนาขึ้นนั้นมีการยืนยันตัวตนโดยใช้บัญชีผู้ใช้ไอที และรหัสผ่านของมหาวิทยาลัยเชียงใหม่ ยืนยันตัวตนนักศึกษาผ่านส่วนบริการเรสต์เอพีไอของสำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ ถูกพัฒนาเป็นลักษณะของส่วนบริการเว็บโดยใช้ภาษาพีเอชพี 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 solving problems from current authentication method for laboratory homework management system. In current authentication system, student has to log in with a randomly generated 4-digit password. The students has different password for different course, which is difficult to manage and easily shared among students.

The authentication module requires Chiang Mai University’s IT account consist of username and password for login and verifies user identities with Information Technology Service Center, Chiang Mai University’s REST API service. The developed module is developed as a web service 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](#_Toc425341946)

[บทคัดย่อ ข](#_Toc425341947)

[Abstract ค](#_Toc425341948)

[สารบัญ ง](#_Toc425341949)

[สารบัญตาราง ฉ](#_Toc425341950)

[สารบัญรูป ช](#_Toc425341951)

[บทที่ 1 บทนำ 1](#_Toc425341952)

[1.1 หลักการและเหตุผล 1](#_Toc425341953)

[1.2 วัตถุประสงค์ของโครงงาน 2](#_Toc425341954)

[1.3 ประโยชน์ที่จะได้รับจากการศึกษาเชิงประยุกต์และ/หรือ เชิงทฤษฏี 2](#_Toc425341955)

[1.4 ขอบเขตของโครงงาน/วิธีการวิจัย 2](#_Toc425341956)

[บทที่ 2 หลักการและทฤษฏีที่เกี่ยวข้อง 3](#_Toc425341957)

[2.1 ทีแอลเอส (TLS) หรือชื่อเดิม เอสเอสแอล 3](#_Toc425341958)

[2.2 เรเดียส 5](#_Toc425341959)

[2.3 คำสั่งบนเทอร์มินอลที่จำเป็นสำหรับลินุกซ์ 5](#_Toc425341960)

[2.4 เรสต์ (REST) 8](#_Toc425341961)

[2.5 เทคโนโลยีการยืนยันตัวตนนักศึกษา ที่มีใช้งานในมหาวิทยาลัยเชียงใหม่ 12](#_Toc425341962)

[บทที่ 3 การวิเคราะห์ และออกแบบระบบ 16](#_Toc425341963)

[3.1 การศึกษาระบบงานเดิม 16](#_Toc425341964)

[3.2 การวิเคราะห์ความต้องการของระบบ 17](#_Toc425341965)

[3.3 แผนภาพยูเอ็มแอล (UML) 18](#_Toc425341966)

# สารบัญตาราง

**ตาราง หน้า**

[ตารางที่ 2.1 ตารางแสดงคำสั่งบนโปรแกรม Vi 7](#_Toc429562308)

[ตารางที่ 3.1 ตารางเปรียบเทียบคุณสมบัติของเรเดียสยืนยันตัวตน และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี 20](#_Toc429562309)

[ตารางที่ 3.3 ตารางสัญลักษณ์แผนภาพยูสเคส 21](#_Toc429562310)

[ตารางที่ 3.4 ตารางสัญลักษณ์แผนภาพกิจกรรม 24](#_Toc429562311)

[ตารางที่ 3.5 ตารางอธิบายคำศัพท์เฉพาะภายในแผนภาพยูเอ็มแอล 24](#_Toc429562312)

[ตารางที่ 3.6 ตารางสัญลักษณ์แผนภาพขั้นลำดับ 28](#_Toc429562313)

[ตารางที่ 4.1 แสดงรายละเอียดของตารางชื่อว่า Applications 32](#_Toc429562314)

[ตารางที่ 4.2 แสดงรายละเอียดของตาราง Monitor 33](#_Toc429562315)

[ตารางที่ 4.3 แสดงสัญลักษณ์ที่ใช้ในการสร้างแผนภาพความสัมพันธ์ของเอนทิตี 35](#_Toc429562316)

[ตารางที่ 4.4 แสดงสัญลักษณ์ที่ใช้ในการสร้างแผนภาพความสัมพันธ์ของเอนทิตี (ต่อ) 35](#_Toc429562317)

[ตารางที่ 5.1 ตารางแสดงเลขสถานะเอชทีทีพีที่ใช้ในส่วนบริการเกตเวย์ยืนยันตัวตน 39](#_Toc429562318)

[ตารางที่ 5.2 แสดงชื่อตัวแปรในข้อความเจสันกรณีเกิดข้อผิดพลาด 40](#_Toc429562319)

[ตารางที่ 5.3 ตารางแสดงยูอาร์ไอของแต่ละบริการของส่วนบริการเกตเวย์ยืนยันตัวตน 42](#_Toc429562320)

[ตารางที่ 5.4 ตารางแสดงสายอักขระสอบถามของบริการยืนยันตัวตน 43](#_Toc429562321)

[ตารางที่ 5.5 ตารางแสดงสายอักขระสอบถามของบริการให้ข้อมูลนักศึกษา 43](#_Toc429562322)

[ตารางที่ 5.6 ตารางแสดงการใช้งานรหัสสถานะเอชทีทีพีภายในส่วนบริการเกตเวย์ยืนยันตัวตน 43](#_Toc429562323)

[ตารางที่ 6.1 ผลการทดสอบการยืนยันตัวของนักศึกษา 45](#_Toc429562324)

[ตารางที่ 6.2 ตารางทดสอบการการร้องขอยืนยันตัวตน 46](#_Toc429562325)

[ตารางที่ 6.3 ตารางทดสอบการการร้องขอข้อมูลผู้ใช้งาน 47](#_Toc429562326)

# สารบัญรูป

**รูป**  **หน้า**

[รูปที่ 2.1 แสดงการส่งข้อมูลบนทีแอลเอสระหว่างลูกข่ายและแม่ข่าย 4](#_Toc425342094)

[รูปที่ 2.2 แสดงแผนภาพส่วนต่อประสานแบบเดียวกัน 9](#_Toc425342095)

[รูปที่ 2.3 แผนภาพแสดงการเชื่อมต่อทั้งแบบมี และไม่มีแคช 10](#_Toc425342096)

[รูปที่ 2.4 แสดงแผนภาพระบบแบบมีลำดับขั้น 10](#_Toc425342097)

[รูปที่ 2.5 แสดงแผนภาพข้อกำหนดเรสต์แบบเขียนตามต้องการ 11](#_Toc425342098)

[รูปที่ 2.6 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการ และบริการเรเดียสของสำนักบริการเทคโนโลยี 12](#_Toc425342099)

[รูปที่ 2.7 แผนภาพการชื่อฟังก์ชัน และตัวแปร ของส่วนบริการเรสต์เอพีไอ สำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ 15](#_Toc425342100)

[รูปที่ 3.1 แผนภาพยูสเคสของส่วนบริการเกตเวย์ยืนยันตัวตน 20](#_Toc425342101)

[รูปที่ 3.2 แผนภาพกิจกรรมแสดงการยืนยันตัวตนของผู้ใช้ และการส่งข้อมูลระหว่างระบบ 25](#_Toc425342102)

[รูปที่ 3.3 แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของผู้ใช้งาน 27](#_Toc425342103)

[รูปที่ 3.8 แผนภาพขั้นลำดับแสดงระบบจัดการการส่งการบ้านปฏิบัติร้องขอข้อมูลผู้ใช้งาน 29](#_Toc425342104)

# บทที่ 1 บทนำ

ส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ ช่วยในการยืนยันตัวตนของนักศึกษา อาจารย์ และผู้ดูแลระบบ ผู้ใช้แต่ละคนมีชื่อผู้ใช้ (Username) ที่ไม่เหมือนกัน คือ ผู้ใช้ทุกคน มีชื่อผู้ใช้งานสารสนเทศของมหาวิทยาลัยเชียงใหม่เฉพาะตัว ใช้ยืนยันตัวตนผู้ใช้เพื่อเข้าใช้งานระบบได้ ซึ่งในบทนี้จะกล่าวถึงภาพรวมของการจัดทำโครงงานดังนี้ ได้แก่ หลักการและเหตุผล วัตถุประสงค์ของโครงงาน ขอบเขต ประโยชน์ของการทำโครงงานนี้ และแผนการดำเนินงานและระยะเวลาดำเนินงานในการจัดทำระบบ

## หลักการและเหตุผล

ระบบสารสนเทศสำหรับส่งการบ้านปฏิบัติการของภาควิชาวิทยาการคอมพิวเตอร์ เป็นระบบช่วยการเรียนการสอนปฏิบัติการเพื่อเพิ่มความสะดวกแก่การทำงานกับเอกสารอิเล็กทรอนิกส์ ในแต่ละวิชาผู้สอนสามารถให้ นักศึกษาทำงานแต่ละปฏิบัติการ ส่งภายในระหว่างการเรียน หรือนอกเวลา ช่วยจัดเก็บเพิ่มความสะดวกต่อการตรวจงานของอาจารย์ และการจัดการเอกสารภายในระบบ

แต่เดิมระบบส่งการบ้านสำหรับปฏิบัติการ ของภาควิชาวิทยาการคอมพิวเตอร์ ใช้การแจกรหัสตัวเลขเฉพาะให้นักศึกษา และอาจารย์แต่ละคนเพื่อเข้าใช้งานระบบ ปัญหาที่เกิดคือ นักศึกษาบางคนลืมรหัส หรือการขโมยรหัสเข้าใช้งานเพื่อเปลี่ยนแปลงข้อมูลบนระบบในนามของเจ้าของบัญชี

ด้วยเหตุนี้โครงงานจึงได้มุ่งเน้นที่จะปรับปรุงระบบให้นักศึกษา อาจารย์ และผู้ดูแลระบบ เข้าใช้ระบบโดยใช้ บัญชีผู้ใช้ไอที (IT Account) ของมหาวิทยาลัยเชียงใหม่ ซึ่งประกอบด้วยชื่อบัญชีผู้ใช้ไอที (Username) ไม่เติม @cmu.ac.th และรหัสผ่านของมหาวิทยาลัยเชียงใหม่ 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

1. การติดตั้ง ตั้งค่าปรับแต่งเครื่องแม่ข่ายบนระบบลินุกซ์โครงสร้างพื้นฐานด้านการส่งข้อมูลที่มีความปลอดภัยของระบบจัดการสารสนเทศสำหรับส่งการบ้านปฏิบัติการที่ใช้อยู่
2. ความรู้การเชื่อมต่อเพื่อยืนยันตัวตนโดยใช้ เรเดียสเซอร์วิส (RADIUS service) และเรสต์เอพีไอ
3. การส่งผ่านข้อมูลแบบปลอดภัยผ่านเครือข่ายอินเทอร์เน็ตประสานระหว่างผู้ใช้งาน

## ขอบเขตของโครงงาน/วิธีการวิจัย

### ขอบเขตของสถาปัตยกรรม

1. เครื่องคอมพิวเตอร์ที่รองรับระบบปฏิบัติการวินโดวส์ 7 32 บิต
2. ฮาร์ดดิสก์ (Hard disk) ขนาดความจุ 500 กิกะไบต์
3. หน่วยความจำหลักขนาด 2 กิกะไบต์

### ซอฟต์แวร์ (Software) และเครื่องมือที่ใช้ในการพัฒนาระบบประกอบด้วย

1. ระบบปฏิบัติการวินโดวส์ 7 32 บิต
2. มายเอสคิวแอล (MySQL) ใช้จัดการกับฐานข้อมูล
3. พีเอชพีมายแอดมิน (phpMyAdmin) ใช้ในการบริหารฐานข้อมูล
4. อาปาเช (Apache) และพีเอชพี (PHP) รุ่น 5.6.2 ใช้ในทดสอบระบบ
5. ฟาลคอนเฟรมเวิร์ค (Phalcon Framework)

### ระบบที่ติดตั้ง

1) ระบบปฏิบัติการอุบุนตูเซิร์ฟเวอร์ (Ubuntu Server) รุ่น 14.04 64 บิต

2) ฮาร์ดดิสก์ ขนาดความจุ 500 กิกะไบต์

3) หน่วยความจำหลักขนาด 8 กิกะไบต์

### ขอบเขตของระบบงาน

1. ติดตั้งปรับแต่งระบบความปลอดภัยสำหรับเครื่องแม่ข่ายระบบจัดการสารสนเทศสำหรับปฏิบัติการ
2. ติดตั้งโครงสร้างพื้นฐานความปลอดภัยในการส่งข้อมูลสำหรับส่วนบริการ
3. ทำการเชื่อมต่อส่วนบริการกับระบบจัดการการส่งการบ้านปฏิบัติการเพื่อพิสูจน์ตัวตน และดึงข้อมูลผู้ใช้งานผ่านระบบ บัญชีผู้ใช้ไอทีเดียวกันกับของมหาวิทยาลัยเชียงใหม่

### ขอบเขตของข้อมูล

* 1. ชื่อบัญชีผู้ใช้ไอทีมหาวิทยาลัยเชียงใหม่ และรหัสผ่าน ของนักศึกษา อาจารย์ และผู้ดูแลระบบ
  2. ข้อมูลทั่วไปของผู้ใช้งาน เช่น ชื่อ นามสกุล รหัสนักศึกษา
  3. 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 เอสทีทีพี (HTTP) เอฟทีพี (FTP) เอสเอ็มทีพี (SMTP) โดยปกติมักถูกใช้บนเว็บที่ต้องการความปลอดภัยเข้าใช้งานของผู้ใช้งาน และเว็บซื้อขายบนอินเทอร์เน็ต เครื่องแม่ข่ายและลูกข่ายจะสามารถใช้เอสเอสแอล ได้เมื่อมีการตกลงที่จะใช้เหมือนกัน คือ วิธีการจับมือกัน (Handshake) โดยระหว่างการจับมือทั้งเครื่องแม่ข่ายและลูกข่ายต้องตกลงกันในแต่ละเงื่อนไขเพื่อความปลอดภัยของการเชื่อมต่อโดยมีขั้นตอนดังนี้

1. เครื่องลูกข่ายส่ง หมายเลขรุ่นของเอสเอสแอล รายละเอียดการตั้งค่าเข้ารหัส (Cipher Settings) ข้อมูลของช่องสื่อสารที่ได้รับ 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. ในกรณีเครื่องแม่ข่ายร้องขอการยืนยันตัวตนจากลูกข่าย เครื่องลูกค่ายต้องสร้างข้อมูลอื่นซึ่งจะเป็นที่เด่นชัดว่าเป็นเครื่องที่ควรส่งข้อมูลหากันอยู่จริง ซึ่งกรณีนี้เครื่องลูกข่ายต้องส่งเอกสารใหม่ พร้อมใบรับรองเครื่อง และส่งรหัสลับพื้นฐานที่ถูกเข้ารหัสให้กับแม่ข่าย
6. ในกรณีเครื่องแม่ข่ายร้องขอการยืนยันตัวตนจากลูกข่าย เครื่องแม่ข่ายยืนยันลูกข่ายว่าเข้าใช้งาน
   1. ถ้าไม่สามารถยืนยันตัวตนของลูกข่ายให้ทำการปิดช่องสื่อสารกับลูกข่าย
   2. ถ้ายืนยันลูกข่ายได้สำเร็จ เครื่องแม่ข่ายทำการถอดรหัสลับพื้นฐานโดยใช้กุญแจลับ (Private Key) ที่มีเฉพาะเครื่องแม่ข่าย และทำงานพร้อมเครื่องลูกข่ายเพื่อสร้าง รหัสลับหลัก (Master Secret)
7. ทั้งเครื่องแม่ข่ายและลูกข่ายใช้รหัสลับหลักเพื่อสร้าง กุญแจสื่อสาร (Session Key) ซึ่งเป็นกุญแจใช้ร่วมกันของแม่ข่ายและลูกข่าย เพื่อการเข้ารหัสและถอดรหัสข้อมูลสื่อสารแลกเปลี่ยนระหว่างช่วงเปิดเอสเอสแอล และเพื่อยืนยันความเป็นบูรณภาพของข้อมูล
8. เครื่องลูกข่ายส่งข้อความให้แก่เครื่องแม่ข่ายเพื่อบอกว่าในอนาคตข้อมูลจะถูกส่งโดยถูกเข้ารหัสด้วยกุญแจสื่อสาร จากนั้นจึงบอกว่าการจับมือด้านเครื่องลูกข่ายได้เสร็จสิ้น
9. เครื่องแม่ข่ายส่งข้อความให้แก่เครื่องลูกข่ายเพื่อบอกว่าในอนาคตข้อมูลจะถูกส่งโดยถูกเข้ารหัสด้วยกุญแจสื่อสาร จากนั้นจึงบอกว่าการจับมือด้านเครื่องแม่ข่ายได้เสร็จสิ้น



รูปที่ 2.1 แสดงการส่งข้อมูลบนทีแอลเอสระหว่างลูกข่ายและแม่ข่าย

หมายเหตุ

- ถึงขั้นตอนสุดท้ายถือเป็นการเสร็จสิ้นของการจับมือของเอสเอสแอล และเริ่มการเปิดช่องการสื่อสาร ทั้งสองด้านใช้กุญแจสื่อสารเข้ารหัสและแกะรหัสข้อมูล

- ถ้ามีขั้นตอนด้านบนขั้นตอนใดล้มเหลว จะไม่มีการเชื่อมต่อระหว่างสองฝั่ง

## เรเดียส

เรเดียส [2] ย่อมาจาก Remote Access Dial In User Service เป็นโพรโทคอลเครือข่าย บนพื้นฐาน เอเอเอ (AAA) คือ การตรวจสอบ (Authentication) การอนุมัติ (Authorization) และการจัดการการบัญชี (Accounting) เป็นโครงสร้างความปลอดภัยสำหรับระบบที่กระจายการบริการใช้งานเพื่อควบคุมผู้ใช้ที่จะเข้าใช้งาน จากส่วนกลาง สำหรับคอมพิวเตอร์ที่เชื่อมต่อและใช้บริการเครือข่าย

เรเดียสเป็นโพรโทคอลแบบไคลเอ็นต์/เซิร์ฟเวอร์ที่วิ่งในชั้นโปรแกรมประยุกต์ ใช้ยูดีพีเป็นช่องทางขนส่ง  
หลักการของเอเอเอ

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

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*

โปรแกรมวี ทุกชื่อโหมดการทำงานไม่สามารถใช้พิมพ์ใหญ่แทนพิมพ์เล็ก หรือเล็กแทนใหญ่ก็ไม่ได้ โดยแสดงที่กำลังทำงานอยู่ในโหมดทางด้านล่างซ้าย การบันทึกและออกจากไฟล์ให้ใช้: (Semi-colon) นำหน้าคำสั่งนั้น

ตารางที่ 2.1 ตารางแสดงคำสั่งบนโปรแกรม Vi

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

### 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

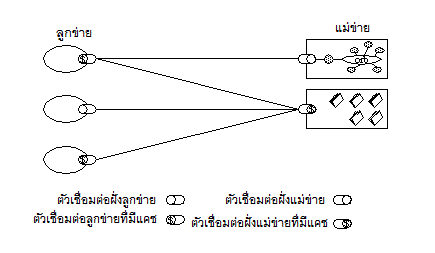
## เรสต์ (REST)

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)

การกำหนดส่วนต่อประสานระหว่างลูกข่าย และแม่ข่ายไม่ขึ้นต่อกัน ซึ่งทำให้แต่ละส่วนแยกจากกันอย่างชัดเจน ดังรูปที่ 2.2 แสดงอิสระในการเชื่อมต่อของลูกข่าย และแม่ข่าย โดยส่วนต่อประสานแบบเดียวกันในที่นี้หมายถึงการทำงานบนเอชทีทีพีโพรโทคอล ซึ่งมีกริยาที่เป็นมาตรฐาน เช่น GET, POST, HEAD, DELETE และ PUT หลักการมีอยู่ 4 ข้อ



รูปที่ . แสดงแผนภาพส่วนต่อประสานแบบเดียวกัน

#### การขึ้นกับทรัพยากร (Resource-Based)

ตัวแปรทรัพยากรที่ร้องขอกำหนดไว้ในยูอาร์ไอ โดยแม่ข่ายจะส่งข้อมูลที่ได้จากฐานข้อมูลในรูปแบบ เอกซ์เอ็มแอล (XML) หรือเจสัน (JSON) 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)**

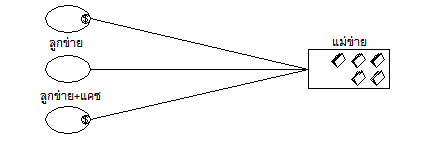
เครื่องลูกข่ายส่งสถานะผ่านเนื้อหาส่วนหลัก (Body Contents) ตัวแปรข้อความสอบถาม (Query-string Parameters) หัวเรื่องร้องขอ (Request Headers) และยูอาร์ไอร้องขอ (Requested URI) ส่วนบริการส่งสถานะให้กับลูกข่ายผ่านเนื้อหาส่วนหลัก เลขรหัสตอบกลับ และส่วนหัวข้อความตอบกลับ

#### การไม่จดจำสถานะ (Stateless)

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

#### สามารถแคชได้ (Cacheable)

เมื่อข้อความตอบกลับระบุว่าสามารถแคชได้ เครื่องลูกข่ายสามารถใช้ข้อมูลในข้อความตอบกลับเพื่อการร้องขอครั้งต่อไปได้ ช่วยลดเวลาแฝงในการส่งข้อมูลได้ ดังแสดงในรูป 2.3



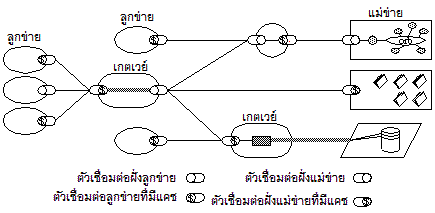
รูปที่ . แผนภาพแสดงการเชื่อมต่อทั้งแบบมี และไม่มีแคช

#### เครื่องลูกข่าย และเครื่องแม่ข่าย (Client-Server)

ส่วนต่อประสานแบบเดียวกันทำให้เครื่องลูกข่าย และเครื่องแม่ข่ายแยกจากกันชัดเจน ส่งผลให้เครื่องลูกข่ายไม่ยุ่งกับส่วนจัดเก็บข้อมูล การเคลื่อนย้ายทำได้ง่าย เครื่องแม่ข่ายไม่ยุ่งเกี่ยวกับส่วนต่อประสานผู้ใช้ หรือสถานะของผู้ใช้ ทำให้ง่ายต่อการสร้าง และขยายได้ดี ทำให้ทั้งสองส่วนถูกพัฒนาโดยไม่ขึ้นต่อกัน

#### ระบบมีลำดับชั้น (Layered System)

เครื่องลูกข่ายไม่จำเป็นต้องทราบว่ากำลังเชื่อมต่อกับแม่ข่ายโดยตรง หรือผ่านตัวกลาง ทำให้ตัวกลางสามารถเพิ่มความสามารถในการจัดเก็บแคช และการกระจายงาน (Load Balancing) ช่วยลดภาระให้กับเครื่องแม่ข่าย



รูปที่ . แสดงแผนภาพระบบแบบมีลำดับขั้น

### 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 ใช้กริยาเอชทีทีพีสำหรับกำหนดการดำเนินงาน

#### เอกซ์เอ็มแอล และเจสัน

เจสัน [8] ควรเป็นตัวเลือกแรกสำหรับข้อมูลส่งกลับ แต่สามารถให้ผู้ใช้บริการเลือกได้ว่าต้องการอย่างใดมากกว่า ระหว่างเอกซ์เอ็มแอล หรือเจสัน

เจสัน ตามมาตรฐานแล้วมีข้อกำหนดที่ต้องการน้อยมาก โดยข้อกำหนดที่ต้องการคือการสร้างข้อความให้ถูกต้อง ไม่เกี่ยวกับการวางรูปแบบ และการวางผัง

ในขณะที่เอกซ์เอ็มแอล [8] ใช้เพื่อต้องการใช้งานป้ายระบุข้อความที่ถูกต้องเท่านั้น

#### คำนึงถึงการเชื่อมต่อ

เอพีไอ สามารถลิงก์ไว้กับข้อความตอบกลับ เพื่อบอกกับเครื่องลูกข่ายถึงข้อมูลก่อนหน้า หรือข้อมูลต่อไปได้ซึ่งง่ายต่อการเรียกใช้กรณีข้อความตอบกลับมีความเชื่อมโยงต่อกัน

#### การสร้างทรัพยากรแบบละเอียด

เมื่อเริ่มต้นสร้างเอพีไอ ควรจะสร้างส่วนบริการขนาดย่อยที่ทำหน้าที่เฉพาะก่อน จากนั้นเมื่อต้องการรวมส่วนบริการให้ใหญ่ขึ้นจึงทำได้ง่าย แทนการสร้างส่วนบริการขนาดใหญ่แล้วแตกออกเป็นส่วนย่อยจำนวนมาก

### ลายเซ็นสำหรับคำขอเรสต์ [9]

ลายเซ็นที่ส่งพร้อมกับคำร้องมีประโยชน์ดังนี้

1. **ยืนยันความน่าเชื่อถือของผู้ร้องขอ** ลายเซ็นช่วยยืนยันว่าคำร้องมาจากระบบที่ได้รับการยอมรับแล้ว ซึ่งมีไอดี และรหัสลับที่ถูกต้อง
2. **ปกป้องข้อมูลในการส่งผ่าน** เพื่อป้องกันการปลอมแปลงคำร้อง ข้อมูลที่ร้องขอถูกใช้เพื่อคำนวณแฮช (Hash) แล้วนำแฮชที่ได้ส่งมาพร้อมกับคำร้อง
3. **ป้องกันการโจมตีแบบรีเพลย์** ถ้าระบบมีการจำกัดว่าเวลาที่ส่งมาพร้อมกับคำร้องต้องมาถึงภายใน 5 นาที เวลาที่คำร้องมาถึงฝั่งแม่ข่าย ถ้าเกินจะถูกปฏิเสธคำขอ

#### ขั้นตอนการสร้างลายเซ็น

สำหรับคำร้องที่หลังได้ลายเซ็นแล้วรูปแบบการร้องขอจะเป็นดังตัวอย่างข้างล่างซึ่งมีทั้งแบบ GET และ POST

ตัวอย่างการร้องขอแบบ POST แบบไม่มีลายเซ็น

POST https://authenurl.com/login/ HTTP/1.1

Host: homeworkurl.com

Content-type: application/x-www-form-urlencoded;   
 charset=utf-8

username=siwaphol\_boonpan&password=12345678&appid=CMUMIS

ตัวอย่างการร้องขอแบบ POST หลังจากสร้างลายเซ็น

POST https://authenurl.com/login/ HTTP/1.1

Host: homeworkurl.com

Content-type: application/x-www-form-urlencoded;   
 charset=utf-8

X-TimeStamp: 1440522123

username=siwaphol\_boonpan&password=12345678&appid=CMUMIS& signature=ced6826de92d2bdeed8f846f0bf508e8559e98e4b0199114b84c54174deb456c

ตัวอย่างการร้องขอแบบ GET แบบไม่มีลายเซ็น

GET https://authenurl.com/userinfo?username=  
siwaphol\_boonpan&access\_token=AGdcE234Sac&appid=CMUMIS HTTP/1.1

Content-type: application/json

Host: homeworkurl.com

ตัวอย่างการร้องขอแบบ GET หลังจากสร้างลายเซ็น

GET https://authenurl.com/userinfo?username=  
siwaphol\_boonpan&access\_token=AGdcE234Sac&appid=CMUMIS&signature=ced6826de92d2bdeed8f846f0bf508e8559e98e4b0199114b84c54174deb456c HTTP/1.1

Content-type: application/json

Host: homeworkurl.com

X-TimeStamp: 1440522123

1. **สร้างสายอักขระคำร้องตามแบบที่กำหนด**

ซึ่งรูปแบบของข้อความก่อนถูกแปลงเป็นลายเซ็นขึ้นอยู่กับผู้พัฒนาระบบ เช่น

StringToSign = HTTPMethod + “\n” +

PATH + “\n” +

Variables + “\n” +

TimeStamp

ซึ่งความหมายของตัวแปร ดังนี้

HTTPMethod คือ กริยาเอชทีทีพีที่ร้องขอ เช่น GET หรือ POST

PATH คือ เส้นทางที่ร้องขอ

Variables คือ ตัวแปรที่ที่ส่งมาพร้อมกับคำร้องเรียงตามลำดับอักขระของ  
 ชื่อตัวแปรคั่นระหว่างตัวแปรด้วยเครื่องหมาย &

TimeStamp คือ ตราเวลาแบบยูนิกซ์เป็นวินาที ใช้ช่วงเวลาของประเทศไทย

ซึ่งถ้าตามคำร้องตัวอย่างแบบ GET ข้างบนจะทำให้ได้ค่าของ StringToSign เป็น

StringToSign = “GET\n” +

“\userinfo\n” +

“access\_token=AGdcE234Sac&appid=CMUMIS&   
 username=siwaphol\_boonpan\n” +

“1440522123”

1. **สร้างลายเซ็นเพื่อส่งพร้อมกับคำร้อง**

ลายเซ็นสุดท้ายที่สำเร็จจะได้เป็นข้อความแฮชโดยเข้าฟังก์ชันเอชแมค (HMAC) และใช้ขั้นตอนวิธีแบบชา 256 (HMAC-SHA256) โดยใช้รหัสลับที่ได้จากระบบที่ต้องการร้องขอเป็นกุญแจสำหรับฟังก์ชันแฮช แล้วแปลงเป็นฐาน 64 จากนั้นจึงนำค่าที่ได้กำหนดให้เป็นค่าของตัวแปร Signature

StringToSign = “GET\nuserinfo\naccess\_token=  
AGdcE234Sac&appid=CMUMIS&username=siwaphol\n1440522123”

SecretKey = “secretkey1234”

Signature = base64encode (HMAC (“SHA256”,   
 SecretKey,StringToSign))

จากนั้นจึงนำตัวแทนข้อมูลสุดท้ายเป็นค่าของ Signature ของคำร้อง และทำการใส่ตราเวลาในส่วนหัวของคำร้องชื่อตัวแปร X-TimeStamp

## เทคโนโลยีการยืนยันตัวตนนักศึกษา ที่มีใช้งานในมหาวิทยาลัยเชียงใหม่

### เรเดียส (RADIUS)

#### การเชื่อมต่อกับการบริการเรเดียส

การเชื่อมต่อกับส่วนบริการเรเดียส ของมหาวิทยาลัยเชียงใหม่มีความต้องการ คือ เครื่องแม่ข่ายใช้ไอพีสาธารณะ การส่งข้อมูลยืนยันใช้ชื่ออีเมล รหัสผ่าน ที่อยู่ของผู้ให้บริการเรเดียส และรหัสลับเข้าใช้งาน โดยสามารถเชื่อมต่อผ่านพีเอชพี โดยการใช้คลังโปรแกรมของ พีอีซีแอลเรเดียส (PECL Radius)

โดย 2 ค่าที่ได้กลับมาคือ Access-Accept ระบบยืนยันว่ามีผู้ใช้ และ Access-Reject คือการยืนยันตัวตนไม่สำเร็จ ตามรูปที่ 2.6



รูปที่ 2.5 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการ และบริการเรเดียสของสำนักบริการเทคโนโลยี

### เรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

#### คำสั่งเพื่อทำงานกับเรสต์เอพีไอ

1. **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 ชื่อบัญชีผู้ใช้ไอที ที่ไม่ใส่ @cmu.ac.th
4. pw คือ รหัสผ่านของบัญชีผู้ใช้ไอทีมหาวิทยาลัยเชียงใหม่
5. **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
5. **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
5. **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 การร้องขอข้อมูลทุกครั้งจะทำให้ค่า access\_token เปลี่ยนไปทุกครั้ง

#### ตัวอย่างรูปแบบข้อมูล เจสัน (JSON) ที่ได้จากเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

1. **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"

}

}

1. **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": "",

"en\_US": ""

},

"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"

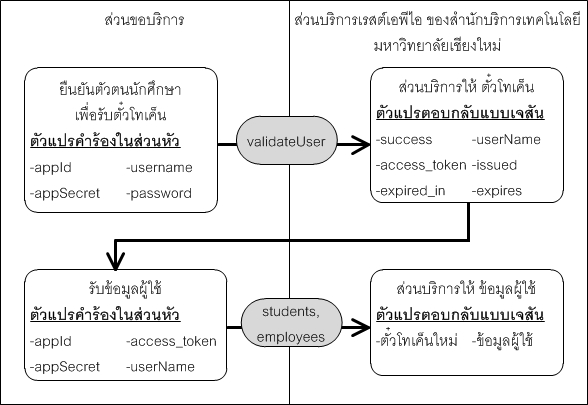
},

"image": null

}

}

โดยค่าของตัวแปร ticket จะถูกสร้างก็ต่อเมื่อการร้องขอสำเร็จ คือ ค่าของ success เป็นจริง



รูปที่ 2.6 แผนภาพการชื่อฟังก์ชัน และตัวแปร ของส่วนบริการเรสต์เอพีไอ สำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่

# 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 เพื่อที่จะนำมาพัฒนาส่วนบริการเกตเวย์

### 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

### แนวทางการออกแบบระบบ

1. ผู้ใช้ทุกคนต้องใช้ชื่อบัญชีผู้ใช้ไอที และรหัสผ่านของมหาวิทยาลัยเชียงใหม่
2. ส่วนบริการใช้โครงสร้างแบบเรสต์ เพื่อให้ง่ายต่อการพัฒนาของส่วนบริการในอนาคต
3. ใช้โพรโทคอลเอสเอสแอลในการรับ-ส่งทุกขั้นตอน เพื่อป้องกันการโจมตีแบบคนกลาง (Man-In-The-Middle Attack)
4. ใช้ลายเซ็นที่มีรูปแบบเป็นข้อความแฮช เพื่อป้องกันการดัดแปลงข้อความคำร้อง และเพื่อแสดงความน่าเชื่อถือของระบบที่ร้องขอส่วนบริการยืนยันตัวตน
5. ส่วนบริการเกตเวย์รับเวลาในตัวแปรส่วนหัวชื่อ X-TimeStamp ไม่น้อยกว่าหรือมากกว่า 5 นาที โดยเทียบกับเวลาที่ส่วนบริการเกตเวย์ได้รับคำร้อง ป้องกันการโจมตีแบบทำซ้ำ (Replay Attack)
6. การทำงานที่มีการส่งรหัสผ่านผู้ใช้งานให้ส่งผ่านแบบ POST เพราะ การที่ส่งข้อมูลแบบ GET ผ่านสายอักขระสอบถามจะทำให้ข้อมูลถูกบันทึกไว้ในล็อกของตัวบริการเว็บ
7. ข้อมูลที่คืนกลับเป็นข้อความรูปแบบเจสันทุกครั้ง
8. ใช้เลขสถานะเอชทีทีพีเป็นตัวบอกถึงสถานะของบริการที่ถูกร้องขอ

### ความต้องการของผู้ใช้

จากการวิเคราะห์ส่วนยืนยันตัวตนของระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ และข้อมูลความต้องการจากคุณถนอม กองใจ ผู้ดูแลระบบ และคำแนะนำจาก อาจารย์ ดร.รัศมีทิพย์ วิตา และคุณปรเมศวร์ พูลประสาธน์พร ผู้ดูแลระบบเรสต์ยืนยันตัวตนของสำนักบริการเทคโนโลยีมหาวิทยาลัยเชียงใหม่ จึงนำความต้องการที่ได้มาพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ จากการวิเคราะห์บทบาทของผู้ใช้แต่ละประเภท ประกอบไปด้วยลักษณะการทำงานหลักๆ ดังนี้

#### กลุ่มผู้ใช้งานเพื่อยืนยันตัวตน (นักศึกษา คณาจารย์ และผู้ดูแลระบบ)

1. ยืนยันตัวตนโดยใช้ชื่อบัญชีผู้ใช้ไอที และรหัสผ่านของมหาวิทยาลัยเชียงใหม่

#### กลุ่มนักพัฒนาระบบนอก

1. ใช้งานส่วนต่อประสานโปรแกรมของส่วนบริการเกตเวย์ยืนยันตัวตน เพื่อใช้บริการยืนยันตัวตน และร้องขอข้อมูลผู้ใช้งานกับส่วนบริการเกตเวย์ยืนยันตัวตน

### การเปรียบเทียบบริการยืนยันตัวตนจากสำนักบริการเทคโนโลยีที่มีอยู่

ส่วนบริการยืนยันตัวตนของสำนักบริการเทคโนโลยีที่ให้มีดังนี้ โดยการเปรียบเทียบดูจากตารางที่ 3.1

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 3.1 ตารางเปรียบเทียบคุณสมบัติของเรเดียสยืนยันตัวตน และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

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

จากการวิเคราะห์แล้ว พบว่าการใช้เรสต์เอพีไอสำหรับยืนยันตัวตนมีความเหมาะสมที่สุดเพราะฟังก์ชันที่มีให้ตรงความต้องการ สามารถยืนยันตัวตน และให้ข้อมูลผู้ใช้ต่อคน ง่ายต่อการใช้งานเพราะเป็นการส่งข้อมูลแบบเรสต์ ไม่จำกัดเครื่องที่ร้องขอจะต้องมีไอพีภายนอก ทำให้ส่วนบริการเกตเวย์ยืนยันตัวตนที่สร้างขึ้นง่ายต่อการนำไปใช้ และรองรับการปรับเพิ่มในอนาคต

## แผนภาพยูเอ็มแอล (UML)

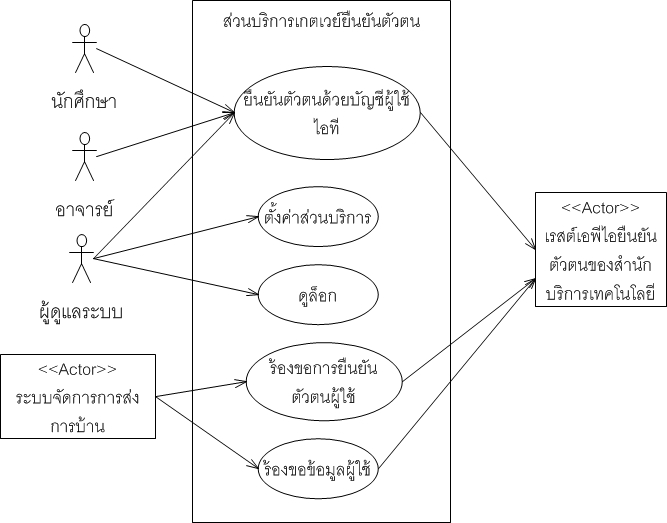
แผนภาพยูเอ็มแอล [7] ของการวิเคราะห์เพื่อการออกแบบส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอนั้น ทางผู้ออกแบบได้ใช้แผนภาพแบบยูเอ็มแอลเพื่อแสดงการทำงานในภาพรวมระดับสูง เช่น แผนภาพยูสเคส (Use Case Diagram) ที่แสดงให้เห็นว่าผู้ใช้งานกับระบบภายนอกมีส่วนทำงานประสานกับส่วนบริการเกตเวย์ ทำงานอะไรบ้างเพื่อง่ายต่อการแสดงความต้องการของส่วนบริการเกตเวย์แผนภาพกิจกรรม (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 3.2

ตารางที่ 3.2 ตารางสัญลักษณ์แผนภาพยูสเคส

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



รูปที่ 3.1 แผนภาพยูสเคสของส่วนบริการเกตเวย์ยืนยันตัวตน

**ชื่อการใช้งาน:** ยืนยันตัวตนด้วยบัญชีผู้ใช้ไอที

**คำอธิบาย:** นักศึกษา อาจารย์ และผู้ดูแลระบบ ทำการยืนยันตัวตนกับส่วนบริการเกตเวย์โดยใช้ชื่อบัญชีผู้ใช้ไอที และรหัสผ่าน ที่ใช้ภายในมหาวิทยาลัยเชียงใหม่ โดยส่วนบริการเกตเวย์นำชื่อบัญชีผู้ใช้ และรหัสผ่านที่ได้ตรวจสอบกับเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี ทำให้ผู้ใช้งานสามารถเข้าใช้ระบบที่ต้องการ เช่น ระบบจัดการการส่งการบ้านปฏิบัติการ

**จุดสำคัญของเหตุการณ์:** ชื่อบัญชีผู้ใช้ไอที และรหัสผ่าน ถูกต้อง

**เงื่อนไขก่อน:** ผู้ใช้กรอกชื่อบัญชีผู้ใช้ไอที และรหัสผ่าน ให้กับระบบนอก จากนั้นข้อมูลถูกส่งมาให้ส่วนบริการเกตเวย์ยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ใช้ยืนยันตัวตนสำเร็จ

**ชื่อการใช้งาน:** ตั้งค่าส่วนบริการ

**คำอธิบาย:** ผู้ดูแลระบบ กำหนดค่าการทำงานภายในส่วนบริการ ผ่านไฟล์เฉพาะสำหรับการตั้งค่าของส่วนบริการเกตเวย์ยืนยันตัวตน กำหนดที่อยู่ของเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี โดยแก้ไขผ่านไฟล์ตั้งค่าของส่วนบริการ

**จุดสำคัญของเหตุการณ์:** ผู้ใช้งานมีสิทธิเป็นผู้ดูแลระบบ

**เงื่อนไขก่อน:** ผู้ใช้ตั้งค่าส่วนบริการมีสิทธิเป็นผู้ดูแลระบบ

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบแก้ไข การตั้งค่าของส่วนบริการได้สำเร็จ

**ชื่อการใช้งาน:** ดูล็อก

**คำอธิบาย:** ผู้ดูแลระบบ สามารถติดตามล็อก (Log) ซึ่งไฟล์ล็อกถูกจัดเก็บไว้ในโฟลเดอร์ชื่อว่า log เปิดใช้งานโดยใช้โปรแกรมแก้ไขข้อความทั่วไป กรณีที่เกิดปัญหาขึ้นกับระบบ นอกจากดูล็อกข้อผิดพลาดแล้ว ยังมีล็อกเข้าใช้งานเมื่อผู้ใช้ยืนยันตัวตนสำเร็จ ส่วนบริการจัดเก็บชื่อบัญชีผู้ใช้ไอที กับเวลาที่สำเร็จไว้ในล็อก โดยผู้ดูแลระบบดูล็อกผ่านส่วนต่อประสานของส่วนบริการเกตเวย์ยืนยันตัวตน

**จุดสำคัญของเหตุการณ์:** ผู้ใช้งานมีสิทธิเป็นผู้ดูแลระบบ

**เงื่อนไขก่อน:** ผู้ใช้งานมีสิทธิเป็นผู้ดูแลระบบ

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบ สามารถเห็นล็อกของส่วนบริการเกตเวย์ยืนยันตัวตน

**ชื่อการใช้งาน:** ร้องขอการยืนยันตัวตนผู้ใช้

**คำอธิบาย:** ระบบนอก ในที่นี้ คือ ระบบจัดการการส่งการบ้านปฏิบัติการ ร้องขอการยืนยันตัวตนให้กับผู้ใช้งาน

**จุดสำคัญของเหตุการณ์:** คำสั่งร้องขอถูกต้อง และตัวแปรนำเข้ามีรูปแบบที่ถูกต้อง

**เงื่อนไขก่อน:** ระบบนอกทำการรับชื่อผู้ใช้ กับรหัสผ่าน แล้วส่งข้อมูลให้ส่วนบริการเกตเวย์ยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ผลลัพธ์การยืนยันตัวตนของผู้ใช้งานถูกส่งกลับให้กับระบบนอก

**ชื่อการใช้งาน:** ร้องขอข้อมูลผู้ใช้

**คำอธิบาย:** ระบบนอก ร้องขอข้อมูลผู้ใช้งานหลังจากยืนยันตัวตนผู้ใช้สำเร็จและได้โทเค็น

**จุดสำคัญของเหตุการณ์:** ผู้ใช้งานยืนยันตัวตนกับส่วนบริการเกตเวย์ยืนยันตัวตนสำเร็จ และระบบนอกมีโทเค็นของผู้ใช้งานนั้น

**เงื่อนไขก่อน:** ผู้ใช้งานยืนยันตัวตนได้สำเร็จ

**ผลลัพธ์เมื่อสำเร็จ:** ข้อมูลผู้ใช้งานในรูปแบบเจสัน

### แผนภาพกิจกรรม

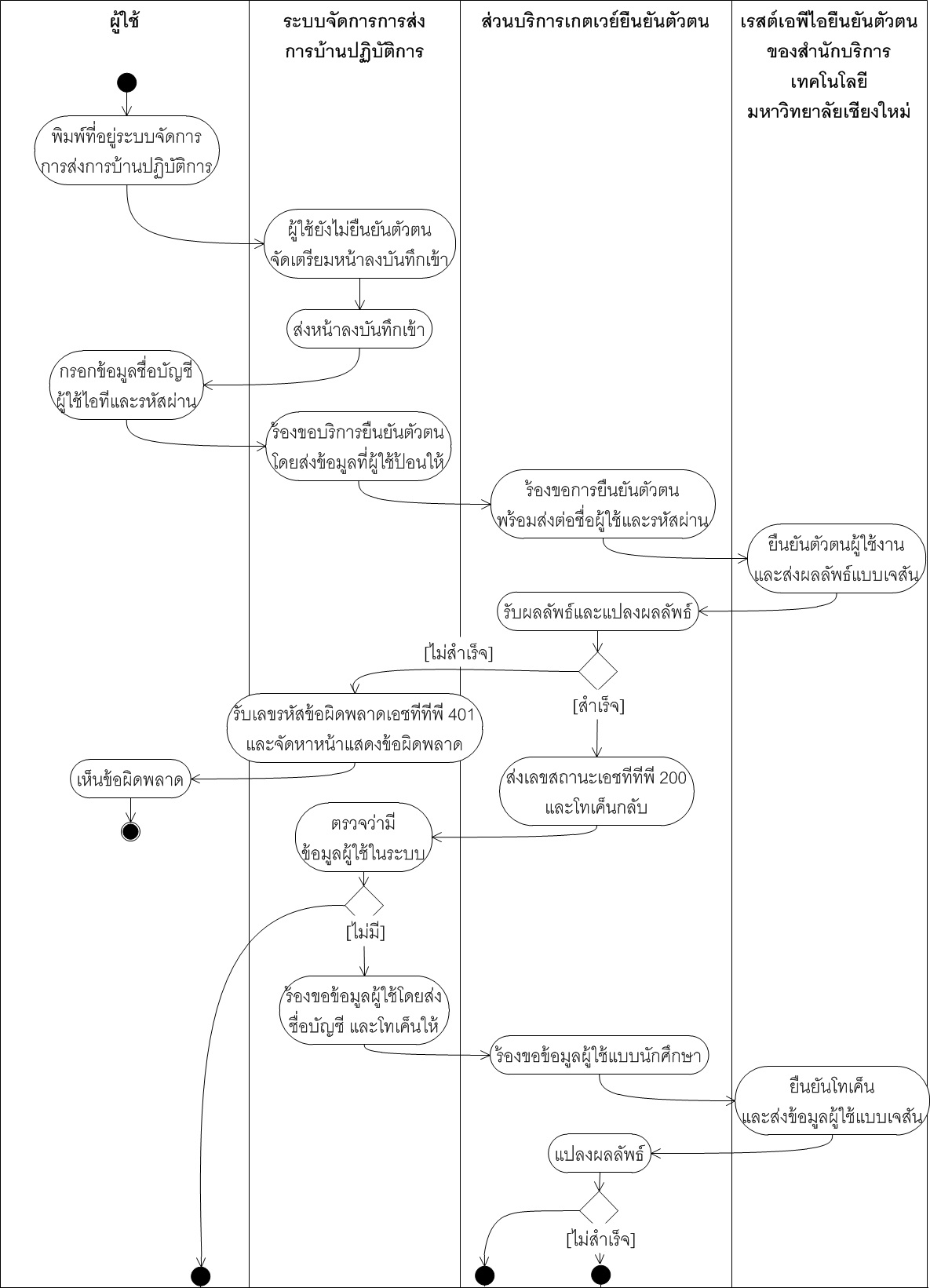
การใช้แผนภาพกิจกรรม [7] เป็นไปเพื่อแสดงขั้นตอนการส่งข้อมูล การทำงานแสดงความสัมพันธ์ระหว่างผู้ใช้ระบบนอก เช่น ระบบจัดการการส่งการบ้านปฏิบัติการ และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี ที่มีต่อส่วนบริการเกตเวย์ยืนยันตัวตน โดยมีการรวมการใช้งานในบางแผนภาพเพื่อให้เห็นการทำงานร่วมกันของผู้ใช้และระบบ ซึ่งแผนภาพนี้ใช้สัญลักษณ์ดังตาราง 3.3

ตารางที่ 3.3 ตารางสัญลักษณ์แผนภาพกิจกรรม

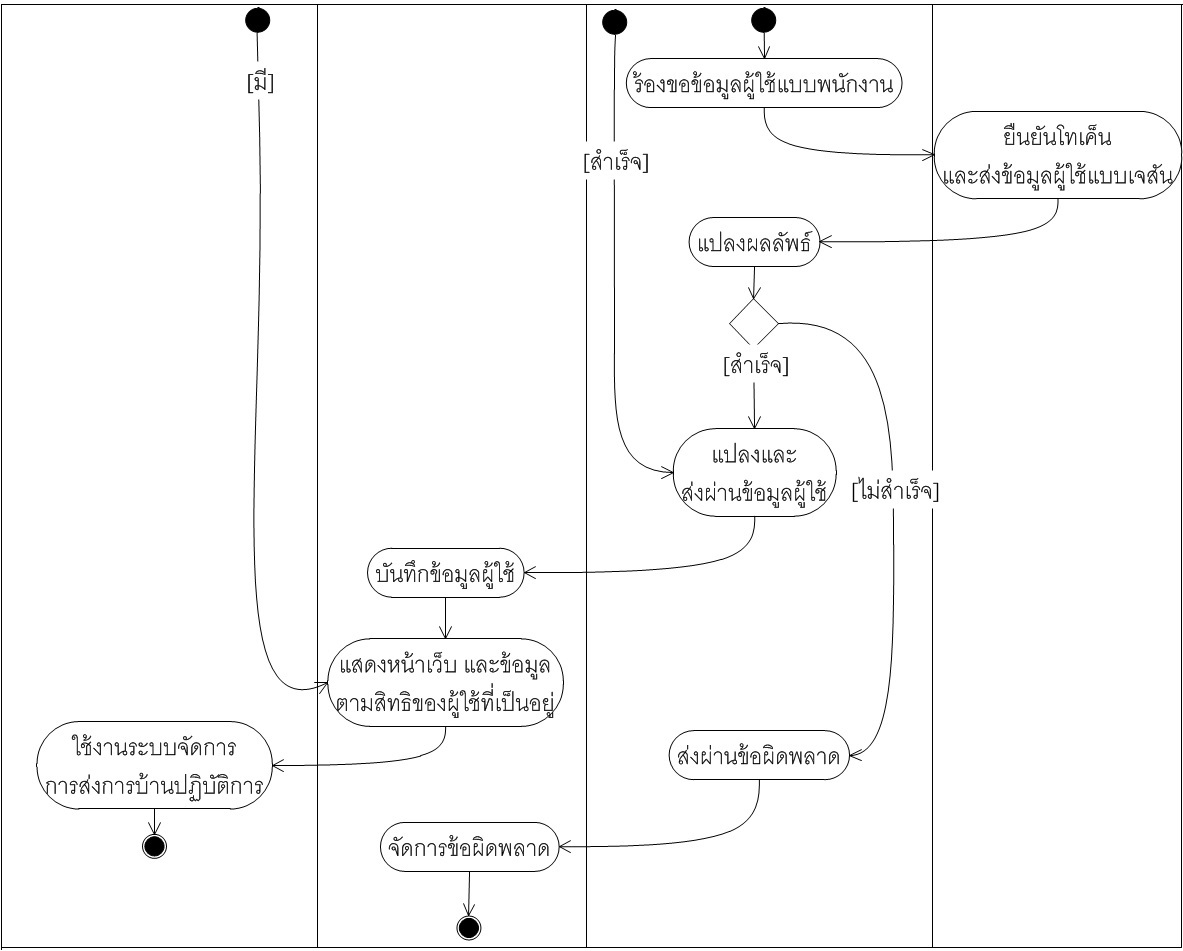
|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Start State | สัญญาลักษณ์สถานะเริ่มต้นในระบบ |
|  | Final State | สัญญาลักษณ์สถานะสุดท้ายในระบบ แสดงถึงการจบการทำงาน |
|  | State | สัญญาลักษณ์แสดงสถานะของระบบ |
|  | Decision | สัญญาลักษณ์การตัดสินใจเลือกสถานะของระบบ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

ตารางที่ 3.4 ตารางอธิบายคำศัพท์เฉพาะภายในแผนภาพยูเอ็มแอล

|  |  |
| --- | --- |
| **คำศัพท์** | **คำอธิบาย** |
| ระบบจัดการการส่งการบ้านปฏิบัติการ | เป็นระบบนอกในกรณีนี้ ที่ทำการร้องขอการยืนยันตัวผู้ใช้งาน เพื่อจะให้สิทธิเข้าใช้งานกับผู้ใช้งานแต่ละคนได้ |
| เรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ | เป็นผู้ให้บริการยืนยันตัวตนปลายทางที่เกตเวย์จะส่งข้อมูลไปให้ ทำงานบน เอชทีทีพี ส่งผ่านข้อมูลแบบ GET ซึ่งให้การบริการดังนี้   * + ยืนยันตัวตนผู้ใช้งาน * ให้ข้อมูลผู้ใช้งาน |
| ข้อมูลผู้ใช้งาน | ข้อมูลนักศึกษา ประกอบไปด้วย ชื่อ นามสกุล เลขที่ประจำตัวนักศึกษาเป็นต้น  อาจารย์ และผู้ดูแลระบบ ประกอบด้วย ชื่อ นามสกุล |
| สถานะเอชทีทีพี | เป็นสถานะที่ส่วนบริการเกตเวย์ส่งกลับให้ผู้ร้องขอ   * + 200 คือ ทุกอย่างเรียบร้อย   + ขึ้นต้นด้วยเลข 4 คือ ปัญหาเกิดระหว่างระบบนอกกับส่วนบริการเกตเวย์   + ขึ้นต้นด้วยเลข 5 คือ ปัญหาเกิดภายในของส่วนบริการเกตเวย์ยืนยันตัวตน |



รูปที่ 3.2 แผนภาพกิจกรรมแสดงการยืนยันตัวตนของผู้ใช้ และการส่งข้อมูลระหว่างระบบ



รูปที่ 3.2 แผนภาพกิจกรรมแสดงการยืนยันตัวตนของผู้ใช้ และการส่งข้อมูลระหว่างระบบ (ต่อ)

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

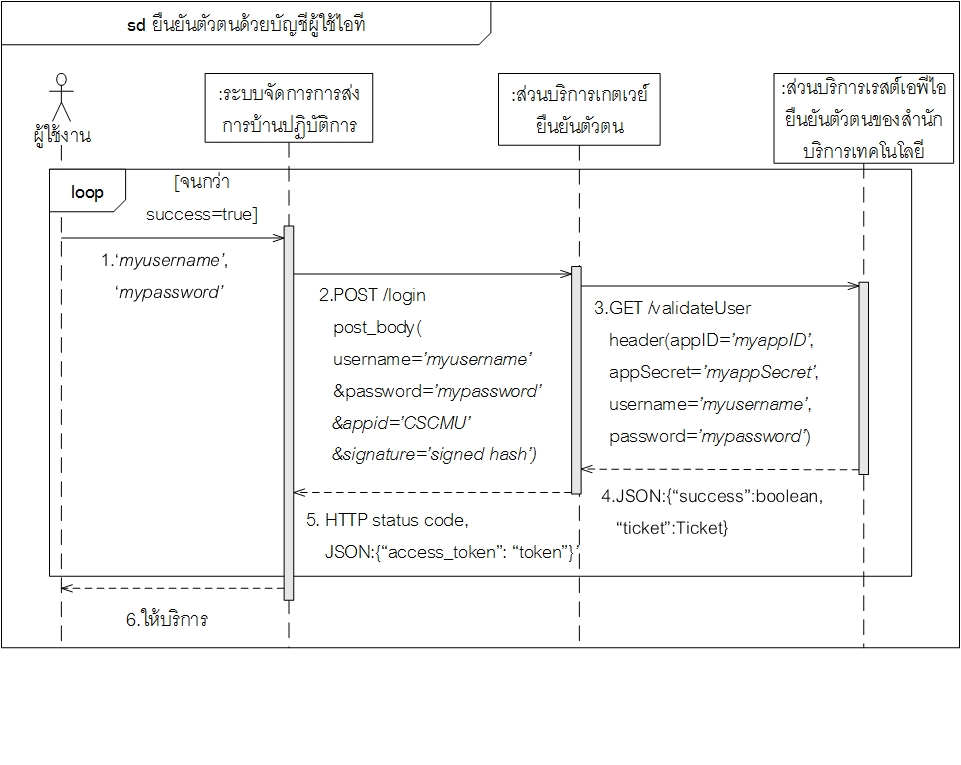
สำหรับข้อมูลที่ผู้ใช้งานยืนยันตัวตน คือ ชื่อบัญชีผู้ใช้ไอที และรหัสผ่าน ของมหาวิทยาลัยเชียงใหม่ โดยส่วนบริการเกตเวย์ยืนยันตัวตน ส่งผ่านข้อมูลตัวตนให้กับเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี โดยข้อความตอบกลับที่ได้ทุกครั้งเป็นแบบเจสัน เมื่อส่วนบริการเกตเวย์ยืนยันตัวตนสำเร็จ จากนั้นระบบจัดการการส่งการบ้านปฏิบัติการจึงตรวจสอบว่ามีข้อมูลผู้ใช้ที่ยืนยันตัวตนสำเร็จในระบบหรือไม่ ถ้าไม่มีให้ทำการร้องขอข้อมูลโดยใช้โทเค็นของผู้ใช้ที่ได้รับจากส่วนบริการเกตเวย์ ต่อไปส่วนบริการเกตเวย์ยืนยันตัวตนจึงส่งให้เรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีอีกครั้ง โดยร้องขอสองครั้ง ครั้งแรกเพื่อตรวจว่าเป็นนักศึกษา ถ้าไม่ใช่ครั้งครั้งที่สองตรวจสอบว่าเป็นพนักงานของมหาวิทยาลัยเชียงใหม่ เมื่อระบบจัดการการส่งการบ้านได้รับข้อมูลสำเร็จ บันทึกข้อมูลผู้ใช้ และให้บริการแก่ผู้ใช้งาน

### แผนภาพขั้นลำดับ

แผนภาพแสดงลำดับการทำงานของระบบ [7] โดยมีวัตถุและเวลาเป็นตัวกำหนดลำดับของงาน และเน้นไปที่ การแสดงปฏิสัมพันธ์ ระหว่างวัตถุ ตามลำดับของเหตุการณ์ที่เกิดขึ้น ณ เวลาที่กำหนด ข้อความที่เกิดขึ้นระหว่างวัตถุ ซึ่งแผนภาพนี้ใช้สัญลักษณ์ดังตาราง 3.5

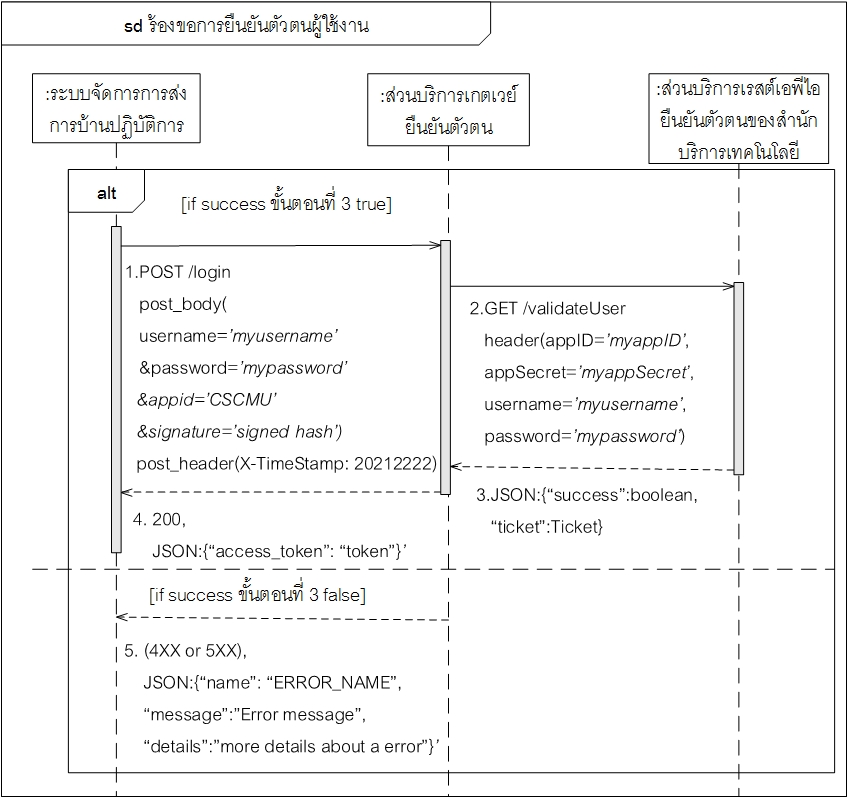
ตารางที่ 3.5 ตารางสัญลักษณ์แผนภาพขั้นลำดับ

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Actor | สัญลักษณ์แสดงผู้ใช้งานที่เกี่ยวข้องกับระบบ |
|  | Instance | สัญลักษณ์แทนแต่ละระบบ |
|  | Lifeline | สัญลักษณ์เส้นแสดงถึงขอบเขตของแต่ละส่วนเกี่ยวข้อง |
|  | Message | สัญลักษณ์แสดงคำสั่งหรือการสั่งการ |
|  | Message Return | สัญลักษณ์แสดงถึงค่าส่งกลับจากระบบด้านขวาไปหาด้านซ้ายของแผนภาพ |
|  | Focus of Control/Activation | สัญลักษณ์จุดเริ่มต้นและจุดสิ้นสุดของแต่ละกิจกรรมในระหว่างการทำงาน |



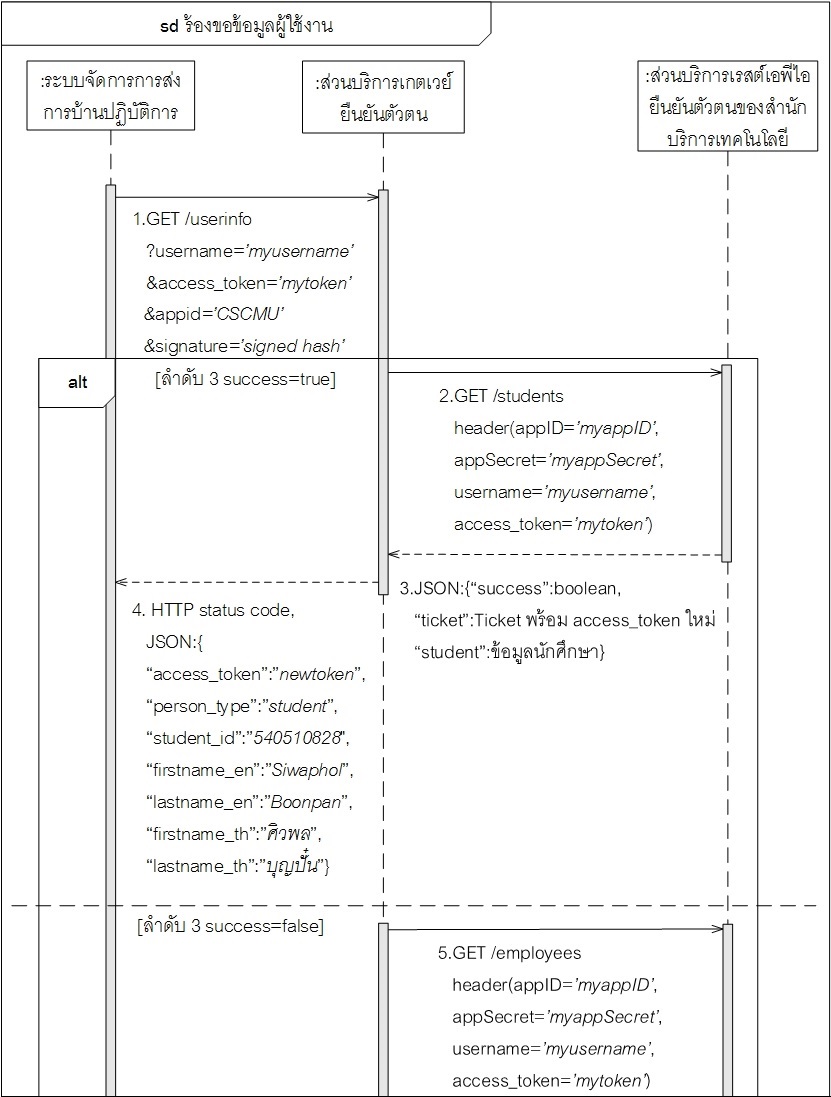
รูปที่ 3.3 แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของผู้ใช้งาน

จากแผนภาพขั้นลำดับแสดงการยืนยันตัวตนกับระบบของผู้ใช้งาน โดยป้อนข้อมูลชื่อบัญชีผู้ใช้ไอที และรหัสผ่านให้กับระบบจัดการการส่งการบ้าน ระบบจัดการการส่งการบ้านจึงร้องขอยืนยันตัวตนกับส่วนบริการเกตเวย์แบบ POST โดยค่าของ signature จะพูดถึงในบทที่ 5 จากนั้นส่วนบริการเกตเวย์ยืนยันตัวตนส่งข้อมูลผู้ใช้ให้กับส่วนบริการเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี โดยร้องขอแบบ GET โดยที่ appID และ appSecret เป็นตัวระบุหมายเลขเอพีไอที่ต้องการใช้งาน และรหัสเพื่อขอใช้งาน ต่อด้วยชื่อผู้ใช้ และรหัสผ่าน การตอบกลับสำหรับส่วนบริการเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี จะเป็นข้อมูลแบบเจสัน ตัวแปรที่สำคัญ คือ success ที่จะบอกว่าผู้ใช้มีตัวตน และ ticket ตัวแปรส่วนบริการเกตเวย์ต้องการคือ access\_token ซึ่งจะถูกใช้ในการร้องขอการบริการครั้งต่อไป โดย access\_token จะถูกส่งให้กับระบบจัดการการบ้านเพื่อใช้ร้องขอบริการอื่นในอนาคต

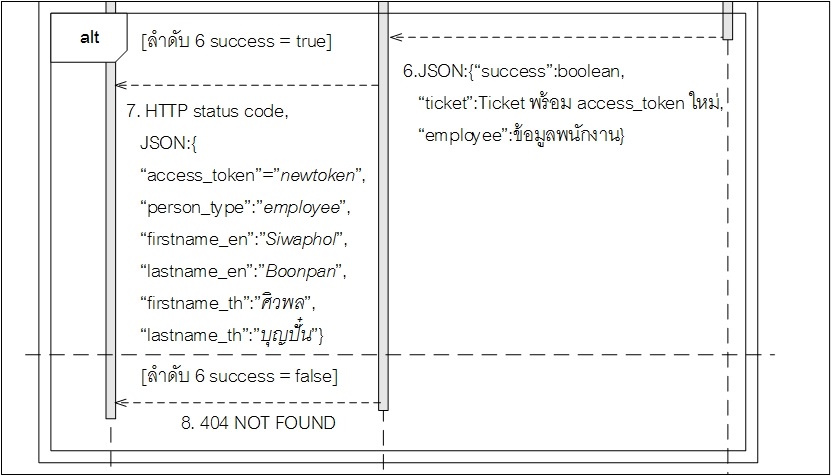


รูปที่ . แผนภาพขั้นลำดับสำหรับการร้องขอการยืนยันตัวตนผู้ใช้งาน

จากแผนภาพ 3.4 ขั้นลำดับการร้องขอการยืนยันตัวตนสำหรับผู้ใช้งาน จะเกิดหลังจากระบบนอกได้รับชื่อบัญชีผู้ใช้ไอที และรหัสผ่านของผู้ใช้งานแล้ว ใช้ข้อมูลที่มีอยู่แปลงเป็นลายเซ็น ที่กำหนดค่าให้กับตัวแปร signature จากนั้นกำหนดตราเวลาเดียวกันที่ใช้ทำลายเซ็นให้กับตัวแปร X-TimeStamp จากนั้นส่งข้อมูลทั้งหมดให้กับส่วนบริการเกตเวย์ยืนยันตัว เพื่อให้ส่วนบริการยืนยันตัวตนกับเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีอีกขั้นตอนหนึ่ง ถ้าการยืนยันตัวตนสำเร็จจะได่ค่าตอบกลับเลขสถานะเอชทีทีพี 200 และโทเค็นที่ได้จากเรสต์เอพีไอยืนยันตัวตน ถ้าไม่สำเร็จจะได้เลขขึ้นต้นด้วย 4 หรือ 5 ขึ้นอยู่กับประเภทของข้อผิดพลาดที่เกิดขึ้น พร้อมกับค่าตอบกลับเจสันอธิบายถึงปัญหาที่เกิดขึ้น



**รูปที่ 3.5 แผนภาพขั้นลำดับแสดงระบบจัดการการส่งการบ้านปฏิบัติร้องขอข้อมูลผู้ใช้งาน**



รูปที่ 3.6 แผนภาพขั้นลำดับแสดงระบบจัดการการส่งการบ้านปฏิบัติร้องขอข้อมูลผู้ใช้งาน (ต่อ)

เมื่อระบบภายนอกต้องการข้อมูลผู้ใช้งาน จึงต้องมีการร้องขอข้อมูลกับส่วนบริการเกตเวย์ยืนยันตัวตน โดยที่สามารถร้องขอได้ทีละผู้ใช้ โดยที่จะต้องมีชื่อผู้ใช้ และ access\_token ปัจจุบันของผู้ใช้งาน

# บทที่ 4 การออกแบบฐานข้อมูล

ส่วนบริการเกตเวย์ยืนยันตัวตน มีการจัดเก็บข้อมูลของผู้ขอบริการ และรหัสลับที่ใช้ร่วมกันไว้ในฐานข้อมูล ส่วนของล็อกจะถูกใช้จัดเก็บสถานะ ทั้งการขอยืนยันตัวตนให้กับผู้ใช้งาน ข้อผิดพลาดที่เกิดขึ้นภายในส่วนบริการ และข้อผิดพลาดที่เกิดจากการร้องขอบริการจากเรสต์เอพีไอยืนยันตัวตนสำนักบริการเทคโนโลยี

## การออกแบบฐานข้อมูล

ขั้นตอนแรกในการออกแบบฐานข้อมูล คือ การวิเคราะห์ข้อมูลที่จะถูกจัดเก็บ และประเมินการใช้งานของข้อมูล โดยส่วนบริการเกตเวย์ยืนยันตัวตนมีการเชื่อมต่อกับระบบอื่น ดังนั้น ควรจัดเก็บข้อมูลเกี่ยวกับระบบอื่น ไว้ภายในฐานข้อมูลของส่วนบริการเกตเวย์ยืนยันตัวตน ให้ง่ายต่อการจัดการ และเปลี่ยนแปลงข้อมูล

เพื่อความง่ายต่อการจัดการของข้อมูล และตาราง แต่ละตารางจะมีอย่างน้อยหนึ่งสดมภ์ที่มีค่าแต่ละระเบียนต่างกัน โดยหลักการแล้วสดมภ์ที่มีค่าเฉพาะมักจะถูกซ่อนไม่ให้เห็นโดยผู้ใช้งาน แต่ข้อมูลจะเข้าถึงได้โดยผู้ดูแลระบบเพื่อการติดตามดูแลข้อมูล

### ตาราง Applications

ตาราง Applications ถูกสร้างเพื่อจัดเก็บข้อมูลของระบบภายนอกที่ต้องการร้องขอใช้บริการ โดยจะจัดเก็บชื่อระบบที่ขอใช้บริการ และรหัสลับที่ใช้ร่วมกันระหว่างส่วนบริการเกตเวย์ยืนยันตัวตนกับระบบอื่น จำนวนคำร้องที่กำหนดให้รับได้สูงสุดภายในช่วงเวลาหนึ่งเริ่มนับตั้งแต่ได้รับคำร้องแรก ส่วนบริการถือว่าคำร้องนั้นเป็นคำร้องแรกเมื่อไม่ได้รับคำร้องใหม่นานเกิน 20 นาที

ตารางที่ . แสดงรายละเอียดของตารางชื่อว่า Applications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ชื่อสดมภ์** | **ประเภท** | **สดมภ์แบบดัชนี** | **อนุญาตค่าว่าง** | **คำอธิบาย** |
| appid | varchar(50) | Unique  Index | ไม่ | เลขที่ถูกสร้างเองโดยโปรแกรม ใช้สำหรับอ้างอิงถึงระเบียนนั้น |
| secret | varchar(50) |  | ไม่ | รหัสลับที่ใช้ร่วมกัน สำหรับการเข้ารหัสข้อมูลที่สำคัญ เช่น รหัสของผู้ใช้งาน |
| time\_window | int |  |  | เวลาเป็นวินาที สำหรับช่วงเวลาที่จำกัดจำนวนคำร้อง ค่าตั้งต้น 0 คือ ไม่จำกัด |
| max\_request | int |  |  | จำนวนคำร้องสูงสุดภายในช่วงเวลาหนึ่ง |
| wait\_second | int |  |  | จำนวนเวลาเป็นวินาทีที่ถูกบังคับให้รอ |

### ตาราง Waitlist

ตาราง Waitlist ใช้สำหรับควบคุมการร้องขอจากระบบภายนอกที่มีการเรียกใช้งานส่วนบริการเกตเวย์ยืนยันตัวตน โดยจะถูกใช้เมื่อระบบนอกร้องขอเกินจำนวนที่กำหนดตามตารางที่ 4.1 อาจจะหยุดการทำงานเฉพาะบางบริการ หรือหยุดให้บริการจากทุกส่วน โดยจะหยุดเพียงช่วงเวลาหนึ่ง เพื่อให้การประมวลผลคำร้องก่อนหน้าเสร็จก่อนที่จะประมวลผลคำร้องใหม่มีสดมภ์ตามตารางที่ 4.2

ตารางที่ . แสดงรายละเอียดของตาราง Waitlist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ชื่อสดมภ์** | **ประเภท** | **สดมภ์แบบดัชนี** | **อนุญาตค่าว่าง** | **คำอธิบาย** |
| appid | varchar(50) | Unique  Index | ไม่ | เลขที่ถูกสร้างเองโดยโปรแกรม ใช้สำหรับอ้างอิงถึงระเบียนนั้น |
| service\_url | Varchar(50) |  |  | ยูอาร์แอลของฟังก์ชันที่หยุดให้บริการ |
| block\_until | int |  |  | เป็นตราเวลายูนิกซ์แบบวินาทีที่บอกถึงระยะเวลาที่ระบบนอกถูกจำกัดการร้องขอ จะร้องขอได้อีกครั้งก็ต่อเมื่อเวลาในตัวแปร X-TimeStamp เกินค่าในส่วนนี้ |

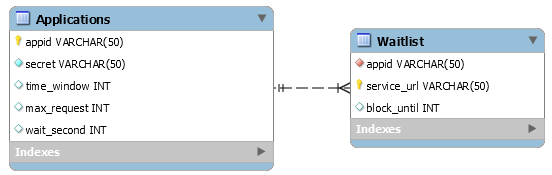
### แผนภาพความสัมพันธ์ระหว่างเอนทิตี

การออกแบบฐานข้อมูลของส่วนบริการเกตเวย์ยืนยันตัวตน อ้างอิงจากข้อมูลเป็นหลัก จากการศึกษาข้อมูลสามารถสร้างความสัมพันธ์ของข้อมูล โดยใช้แผนภาพแสดงความสัมพันธ์ของเอนทิตี (Entity Relationship Diagram: ER - Diagram) แสดงความสัมพันธ์ระหว่างเอนทิตี โดยมีการแทนความสัมพันธ์ของข้อมูลโดยใช้สัญลักษณ์ดังตารางที่ 4.3 และรูปที่ 4.1 แสดงภาพความสัมพันธ์ของเอนทิตี

การออกแบบฐานข้อมูลของส่วนบริการเกตเวย์ยืนยันตัวตน อ้างอิงจากข้อมูลที่เกี่ยวกับการเชื่อมต่อกับระบบนอกเป็นหลัก

ตารางที่ 4.3 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) |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ 1 : N (One to Many Relationship) |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ M : N (Many to Many Relationship) |



รูปที่ . แผนภาพความสัมพันธ์ระหว่างเอนทิตีต่างภายในส่วนบริการเกตเวย์ยืนยันตัวตน

จากแผนภาพแสดงความสัมพันธ์ดังรูปที่ 4.1 สามารถอธิบายความสัมพันธ์ระหว่างเอนทิตีได้ว่า แต่ละเลขโปรแกรมจะถูกหยุดให้บริการได้หลายฟังก์ชันในช่วงเวลาหนึ่ง เมื่อจำนวนคำร้องเกินที่ระบุไว้ในสดมภ์ max\_request

## การออกแบบล็อก

ในขั้นตอนการออกแบบล็อก สิ่งที่ต้องคำนึงก่อนคือการแยกประเภทของล็อก ซึ่งแยกได้เป็น 2 ประเภท คือ ล็อกบันทึกการเข้าใช้ (Access Log) และล็อกบันทึกข้อผิดพลาด (Error Log)

### ล็อกบันทึกการเข้าใช้

เป็นล็อกบันทึกข้อมูลทำงานระหว่างส่วนบริการเกตเวย์ยืนยันตัวตนกับระบบนอก โดยข้อความที่บันทึกมีโครงสร้าง โดยเก็บข้อมูล ดังต่อไปนี้

1. คำร้องของระบบนอก และผลลัพธ์จากส่วนบริการเกตเวย์ยืนยันตัวตน
2. ข้อมูลการใช้งาน เช่น จำนวนที่ร้องขอในช่วงเวลาหนึ่ง ขนาดของรายการเปลี่ยนแปลง

โดยล็อกบันทึกการเข้าใช้งานมีโครงสร้างดังต่อไปนี้

**$client\_ip $app\_id $timestamp “$HTTP\_method $request $protocol” $HTTP\_status\_code $response\_size**

$client\_ip คือ หมายเลขไอพีของระบบนอกที่ขอใช้บริการ

$app\_id คือ เลขประจำโปรแกรม ที่ถูกส่งมาพร้อมกับส่วนร้องขอ

$timestamp คือ วัน และเวลาที่ทำการร้องขอ

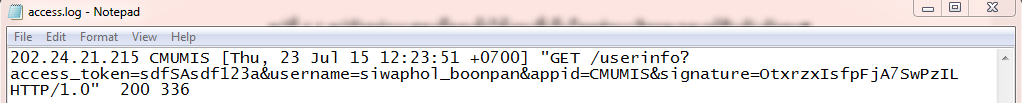
$HTTP\_method คือ รูปแบบเอชทีทีพีที่ใช้

$request คือ ประกอบไปด้วยยูอาร์แอลที่เรียก ในกรณีร้องขอแบบ GET จะรวมถึงตัวแปรที่ส่งมา

$protocol คือ โพรโทคอลที่ใช้ในการส่งข้อมูล

$HTTP\_status\_code คือ ค่าสถานะเอชทีทีพีที่ส่งคืนหลังจากการประมวลผลคำร้องเสร็จสิ้น

$response\_size คือ ขนาดข้อความตอบกลับขนาดเป็นไบต์ (Byte)



รูปที่ . รูปตัวอย่างแสดงล็อกเข้าใช้งานที่เก็บโดยส่วนบริการเกตเวย์ยืนยันตัวตน

### ล็อกบันทึกข้อผิดพลาด

เป็นล็อกบันทึกข้อผิดพลาดหลายกรณีที่เกิดจากภายในส่วนบริการเกตเวย์ และการรับ ส่งข้อมูลกับภายนอกของส่วนบริการเกตเวย์ยืนยันตัวตน เช่น การทำงานของส่วนบริการล้มเหลว มีข้อผิดพลาดจากการตั้งค่าในส่วนบริการ การเชื่อมต่อกับเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีไม่สำเร็จ โดยข้อความที่บันทึกมีโครงสร้างดังนี้

**$timestamp $error $file\_name $client\_ip: $message**

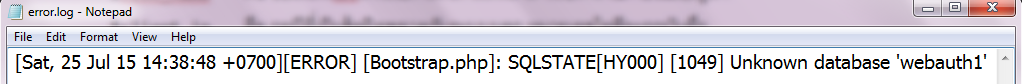
$timestamp คือ วัน และเวลาที่เกิดข้อผิดพลาด

$error คือ ประเภทข้อผิดพลาด

$file\_name คือ ชื่อไฟล์พีเอชพี กรณีการตั้งค่าผิดพลาด หรือทำงานภายในมีปัญหา

$client\_ip คือ กรณีที่เป็นข้อผิดพลาดกับระบบนอก หมายเลขไอพีจะถูกบันทึก

$message คือ ข้อความของข้อผิดพลาดที่เกิดขึ้น



รูปที่ . แผนภาพแสดงตัวอย่างล็อกบันทึกข้อผิดพลาดภายในระบบ

### นโยบายการจัดการล็อก

กระบวนการจัดการล็อก มีดังนี้

1. การหมุนเวียนของล็อก (Log Rotation) และการจัดเก็บไฟล์ล็อกเป็นแบบไฟล์บีบอัด ไฟล์ล็อกจะถูกจัดเก็บเป็นแบบบีบอัดเมื่อไฟล์มีขนาดตั้งแต่ 25 เมกะไบต์ขึ้นไป หรือทุก 1 เดือนจะถูกจัดเก็บเป็นแบบบีบอัด
2. การลบล็อก เมื่อไฟล์ล็อกแบบบีบอัดมีจำนวนเกิน 10 ไฟล์ ไฟล์ที่เก่าที่สุดจะถูกลบ หรือไฟล์ที่มีอายุเกิน 6 เดือนจะถูกลบ
3. การตั้งชื่อไฟล์ล็อกแบบบีบอัด เป็นในรูปแบบ “ชื่อไฟล์ล็อก+ปีเดือนวัน” เป็นไฟล์นามสกุล gz เช่น access20150901.gz

# บทที่ 5 การออกแบบส่วนต่อประสานผู้ใช้

ส่วนต่อประสานโปรแกรมเปรียบเหมือนส่วนต่อประสานผู้ใช้สำหรับนักพัฒนาโปรแกรม ดังนั้นการออกแบบส่วนต่อประสานโปรแกรมสำหรับส่วนบริการเกตเวย์ยืนยันตัวตน จึงจำเป็นต้องออกแบบให้ใช้งานง่ายแต่ยังคงความปลอดภัย เพื่อให้ผู้พัฒนาระบบอื่นสามารถจะใช้งานบริการกับส่วนบริการเกตเวย์ยืนยันตัวตน

## ข้อกำหนดหลักของส่วนต่อประสาน

### ข้อกำหนดของคำร้อง

#### ส่วนหัวของคำร้องต้องมีตัวแปรชื่อ X-TimeStamp

ทุกคำร้องต้องมีตัวแปรชื่อ X-TimeStamp เป็นเวลาที่ใช้ในการสร้างลายเซ็น ตราเวลาใช้เวลา **ยูนิกซ์แบบวินาที** โดยช่วงเวลาที่ใช้เป็น **ช่วงเวลาของประเทศไทย**

เทคนิคสำหรับภาษาพีเอชพีให้ใช้คำสั่งเริ่มต้นบนหัวของไฟล์พีเอชพีว่า date\_default\_timezone\_set('Asia/Bangkok') จะทำให้การเรียกใช้ฟังก์ชันเวลาอื่น ใช้ช่วงเวลาของกรุงเทพเป็นหลัก กรณีที่เวลาของตัวบริการเว็บไม่ใช่ของประเทศไทย จากนั้นสามารถสร้างเวลาเป็นวินาทีแบบยูนิกซ์โดยใช้ฟังก์ชัน เช่น time()

#### ทุกคำร้องจะต้องมีตัวแปรลายเซ็นชื่อ Signature

ลายเซ็นเพื่อยืนยันความน่าเชื่อถือของระบบนอก

โดยรูปแบบของข้อความก่อนจะถูกเข้ารหัสมีส่วนประกอบดังนี้

**StringToSign = HTTPMethod + “\n” +**

**PATH + “\n” +**

**Variables + “\n” +**

**TimeStamp**

โดยที่ HTTPMethod คือ กริยาเอชทีทีพีที่ใช้ เช่น GET หรือ POST

Path คือ ยูอาร์ไอที่เรียก

Variables คือ ตัวแปรพร้อมค่าของตัวแปรที่ส่งมาพร้อมกับคำร้องเรียง   
 ตามลำดับอักขระของชื่อตัวแปร และคั่นระหว่างตัวแปร  
 ด้วยเครื่องหมาย &

TimeStamp คือ รูปแบบเวลาตามข้อ 5.1.1.1

แต่ละส่วนของข้อความก่อนถูกเข้ารหัสคั่นด้วยเครื่องหมายขึ้นบรรทัดใหม่ โดยตัวอย่างของข้อความก่อนถูกเข้ารหัส เช่น

StringToSign= “GET\n” +

“/userinfo” +   
 “access\_token=avdfsdf345AD&appid=CMUMIS   
 &username=siwaphol\_boonpan” +   
 “Thu, 20 Aug 2015 03:45:21 ICT”

ในส่วนของการเข้ารหัสของข้อความเพื่อผลสุดท้ายให้ได้ลายเซ็นส่งให้กับเกตเวย์ยืนยันตัวตนมีขั้นตอนดังนี้

**Signature = Base64Encode (HMAC (“sha256”, Secret\_key, StringToSign))**

1. นำข้อความเข้าฟังก์ชันแฮชแบบเอชแมค โดยใช้อัลกอริทึมแบบชา 256 โดยใช้รหัสลับจากเกตเวย์ยืนยันตัวตนเป็นกุญแจสำหรับแฮชนี้
2. แปลงแฮชที่ได้ให้อยู่ในฐาน 64

### ข้อกำหนดของค่าคืนกลับ

#### ใช้เลขสถานะเอชทีทีพีในการแสดงสถานะของการทำงาน

สำหรับเกตเวย์ยืนยันตัวตนจะใช้เลขสถานะเอชทีทีพีในการระบุความสำเร็จของคำร้อง โดยเลขสถานะขึ้นต้นด้วยเลข 2 การทำงานสำเร็จ ขึ้นต้นด้วยเลข 4 เกิดข้อผิดพลาดจากคำร้องที่ส่งมา หรือการทำงานไม่สำเร็จ ขึ้นต้นด้วยเลข 5 เกิดข้อผิดพลาดภายในเกตเวย์ยืนยันตัวตน โดยเลขสถานะที่ใช้ทั้งหมดกำหนดตามตารางที่ 5.1

ตารางที่ . ตารางแสดงเลขสถานะเอชทีทีพีที่ใช้ในส่วนบริการเกตเวย์ยืนยันตัวตน

|  |  |  |
| --- | --- | --- |
| **เลขสถานะ** | **ความหมาย** | **อธิบาย** |
| 200 | OK | การประมวลผลคำร้องสำเร็จ |
| 400 | Bad Request | ไม่มีบริการที่ร้องขอ หรือขาดตัวแปรที่ต้องการ |
| 401 | Unauthorized Request | ไม่พบลายเซ็นที่ส่งมา หรือตราเวลาใน X-TimeStamp น้อยกว่า หรือมากกว่าเวลาที่คำร้องมาถึงภายใน 5 นาที |
| 404 | Not Found | ไม่พบข้อมูลผู้ใช้ที่ต้องการ หรือไม่สามารถยืนยันตัวตนได้ |
| 429 | Too Many Requests | ผู้ร้องขอส่งคำร้องเกินจำนวนในช่วงเวลาที่กำหนด |
| 500 | Internal Server Error | เกิดปัญหาภายในเกตเวย์ยืนยันตัวตน |

#### รูปแบบเจสันกรณีที่เกิดข้อผิดพลาด

ในกรณีที่เกิดข้อผิดพลาดขึ้นเกตเวย์ยืนยันตัวตนจะทำการส่งข้อมูลเจสันกลับเพื่อบอกถึงข้อผิดพลาดที่เกิดขึ้น โดยในข้อความเจสันมีแต่ละตัวแปรดังนี้

ตารางที่ . แสดงชื่อตัวแปรในข้อความเจสันกรณีเกิดข้อผิดพลาด

|  |  |
| --- | --- |
| **ชื่อตัวแปร** | **อธิบาย** |
| name | ชื่อข้อผิดพลาด |
| message | อธิบายข้อผิดพลาด |
| details | ส่วนอธิบายข้อผิดพลาดเพิ่มเติม |

**ตัวอย่างของข้อความผิดพลาด**

{

“name” : “TIMESTAMP\_REJECTED”,

“message” : “X-Timestamp should be within 5 minute of   
 arrival timestamp.”,

“details” : “”

}

## ส่วนต่อประสานสำหรับการร้องขอยืนยันตัวตน

ใช้ยูอาร์ไอ https://<ที่อยู่ของส่วนบริการ>/login สำหรับการร้องขอยืนยันตัวตนของผู้ใช้งาน

### การดำเนินการ

POST /login โดยหลังจากส่งข้อมูลเสร็จส่วนบริการเกตเวย์ยืนยันตัวตนกับ เรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีโดยที่

### ตัวแปรคำร้อง

โดยคำร้องมีตัวแปรตามตารางที่ 5.3

ตารางที่ . แสดงตัวแปรคำร้องของส่วนต่อประสานร้องขอยืนยันตัวตน

|  |  |
| --- | --- |
| **ตัวแปร** | **อธิบาย** |
| username | ชื่อผู้ใช้งานที่ต้องการยืนยันตัวตน |
| password | รหัสผ่านของผู้ใช้งาน |
| appid | เลขของระบบได้รับจากส่วนบริการเกตเวย์ยืนยันตัวตน |
| signature | ลายเซ็นตามที่กำหนด |
| userinfo (ตัวเลือก) | ในกรณีที่ต้องการค่าตอบกลับเป็นข้อมูลผู้ใช้งานให้เพิ่ม userinfo=true ถ้าไม่มีตัวแปรนี้จะทำการยืนยันตัวตนเพียงอย่างเดียว และคืนค่าเฉพาะโทเค็น |

โดยปกติจะไม่ใส่ตัวแปร userinfo ในคำร้องเพื่อให้เกิดความเร็วในการยืนยันตัวตน เนื่องจากการร้องขอข้อมูลผู้ใช้งานจะเกตเวย์ต้องขอข้อมูลผู้ใช้งานจากเรสต์เอพีไอของสำนักบริการเทคโนโลยีอีกขั้นตอน เกิดความล่าช้าในการรับ-ส่งข้อมูล แต่ควรถูกใช้ในกรณีที่ระบบนอกยังไม่มีข้อมูลผู้ใช้งาน

**ตัวอย่างของการส่งคำร้อง**

curl https://<ที่อยู่ของส่วนบริการ>/login \

-H “X-TimeStamp: Sat, 29 Nov 2014 16:57:56 ICT” \

--data “username=siwaphol\_boonpan&password=password1234&appid=CMUMIS&signature =324SDFsdfadbHwd”

### ค่าตอบกลับ

ค่าคืนกลับในรูปแบบเจสันในกรณีทำงานนได้สำเร็จมีตัวแปรตามตารางที่ 5.4

ตารางที่ . แสดงตัวแปรค่าตอบกลับของส่วนต่อประสานโปรแกรมร้องขอการยืนยันตัวตน

|  |  |
| --- | --- |
| **ตัวแปร** | **อธิบาย** |
| access\_token | โทเค็นของผู้ใช้งานที่ได้จากเรสต์ยืนยันตัวตนของสำนักบริการเทคโนโลยี |

เมื่อกำหนดค่าของ userinfo เป็น true จะได้ค่าตอบกลับตามข้อ 5.3.3

**ตัวอย่างของค่าคืนกลับ**

{

“access\_token”:”โทเค็นของผู้ใช้งาน”

}

## ส่วนต่อประสานสำหรับการร้องขอข้อมูลนักศึกษา

### การดำเนินการ

GET /userinfo?access\_token=<โทเค็นเข้าใช้งาน>&appid=<เลขที่ระบบ>   
 &signature=<ลายเซ็น>&username=<ชื่อบัญชีผู้ใช้งาน>

จะสามารถร้องขอได้ต่อเมื่อผู้ใช้งานยืนยันตัวตนสำเร็จ และได้รับโทเค็นเข้าใช้งานแล้ว

### ตัวแปรคำร้อง

โดยคำร้องมีตัวแปรตามตารางที่ 5.5

ตารางที่ . แสดงตัวแปรคำร้องของส่วนต่อประสานโปรแกรมร้องขอข้อมูลผู้ใช้งาน

|  |  |
| --- | --- |
| **ตัวแปร** | **อธิบาย** |
| username | ชื่อผู้ใช้งานที่ต้องการยืนยันตัวตน |
| appid | เลขของระบบได้รับจากส่วนบริการเกตเวย์ยืนยันตัวตน |
| signature | ลายเซ็นตามที่กำหนด |
| access\_token | โทเค็นเข้าใช้งานที่ได้หลังจากการยืนยันตัวตนสำเร็จ |

**ตัวอย่างของการส่งคำร้อง**

curl –X POST https://<ที่อยู่ของส่วนบริการ>/userinfo? \

-H “X-TimeStamp: Sat, 29 Nov 2014 16:57:56 ICT” \

--data “username=siwaphol\_boonpan&password=password1234&appid=CMUMIS&signature =324SDFsdfadbHwd”

### ค่าตอบกลับ

ค่าคืนกลับจะอยู่ในรูปแบบเจสันมีตัวแปรตามตารางที่ 5.6

ตารางที่ . แสดงตัวแปรค่าตอบกลับของส่วนต่อประสานโปรแกรมร้องขอข้อมูลผู้ใช้งาน

|  |  |
| --- | --- |
| **ตัวแปร** | **อธิบาย** |
| access\_token | โทเค็นของผู้ใช้งานที่ได้จากเรสต์ยืนยันตัวตนของสำนักบริการเทคโนโลยี |
| person\_type | ระดับของผู้ใช้งาน คือ เป็นนักศึกษา “student” หรือพนักงาน “employee” |
| student\_id | รหัสนักศึกษา |
| firstname\_en | ชื่อภาษาอังกฤษ |
| lastname\_en | นามสกุลภาษาอังกฤษ |
| firstname\_th | ชื่อภาษาไทย |
| lastname\_th | นามสกุลภาษาไทย |

**ตัวอย่างของค่าคืนกลับ**

{

“access\_token” : “โทเค็นใหม่ของผู้ใช้งาน”,

“person\_type” : “student”,

“student\_id” : “540510828”

“firstname\_en” : “Siwaphol”,

“lastname\_en” : “Boonpan”,

“firstname\_th” : “ศิวพล”,

“lastname\_th” : “บุญปั๋น”,

}

## ข้อความค่าตอบกลับเจสันกรณีที่เกิดปัญหา

เมื่อเกิดข้อผิดพลาด ส่วนบริการจะคืนค่าข้อความแบบเจสัน เพื่อบอกถึงข้อผิดพลาดที่เกิดขึ้นโดยมีส่วนชื่อข้อผิดพลาด ที่ระบุถึงส่วนที่เกิดข้อผิดพลาด โดยชื่อข้อผิดพลาดเป็นตามตารางที่ 5.7

ตารางที่ . แสดงชื่อและรายละเอียดข้อผิดพลาดที่เกิดกับส่วนบริการเกตเวย์ยืนยันตัวตน

|  |  |
| --- | --- |
| **ชื่อข้อผิดพลาด** | **อธิบาย** |
| INTERNAL\_SERVICE\_ERROR | เกิดข้อผิดพลาดภายในส่วนบริการ |
| INVALID\_REQUEST | ขาดตัวแปรคำร้องที่ต้องการของบริการนั้น |
| NO\_REQUEST\_SERVICE | ไม่มีบริการที่ร้องขอ |
| NO\_SIGNATURE | ไม่มีตัวแปรลายเซ็นในคำร้อง |
| SIGNATURE\_MISMATCH | ลายเซ็นจากคำร้องกับลายเซ็นของส่วนบริการมีค่าไม่ตรงกัน |
| TIMESTAMP\_REJECTED | ตราเวลาในตัวแปรส่วนหัวของคำร้องมากกว่าหรือน้อยกว่า 5 นาที ที่คำร้องมาถึง |
| TOO\_MANY\_REQUESTS | จำนวนที่ร้องขอเกินจำนวนที่กำหนด ในช่วงเวลาหนึ่ง |
| UNAUTHORIZED | การร้องขอบริการกับเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีไม่สำเร็จ เกิดจากค่าของตัวแปรที่ระบบนอกให้ไม่ถูกต้อง |

# บทที่ 6 ผลการดำเนินงาน

ในบทนี้จะอธิบายในส่วนของผลการดำเนินงาน และสรุปผลการดำเนินงาน เพื่อเป็นการตรวจสอบการทำงานของระบบที่ได้จัดทำขึ้นนั้นทำงานได้อย่างถูกต้อง และตรงตามความต้องการ โดยการทดสอบระบบเพื่อหาจุดบกพร่อง และแก้ไขจุดเหล่านั้นให้ระบบใช้งานได้อย่างมีประสิทธิภาพ

## การยืนยันตัวตนของผู้ใช้งาน

การทดสอบในส่วนของการยืนยันตัวตนของผู้ใช้งานจะเป็นการทดสอบผ่านระบบอื่น โดยในที่นี้คือหน้ายืนยันตัวตนของระบบจัดการการบ้านปฏิบัติการ การกรอกข้อมูลผู้ใช้แล้วทำการยืนยันตัวตนกับระบบ โดยในการยืนยันตัวตนของผู้ใช้งาน จะกรอกชื่อบัญชีผู้ใช้ไอที และรหัสผ่าน การดำเนินการทดสอบ ดังตารางที่ 6.1

ตารางที่ . ผลการทดสอบการยืนยันตัวของนักศึกษา

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test Case Name | | | ทดสอบการยืนยันตัวตนของผู้ใช้งาน | | | | |
| Test Description | | | เพื่อทดสอบการยืนยันตัวตนให้สำเร็จ | | | | |
| Pre-Condition | | | ผู้ใช้งานกรอกชื่อผู้ใช้ และรหัสผ่านถูกต้อง | | | | |
| Steps | Test Steps | Test Data | | Expected Result | Actual Result | Status | Note |
| 1 | ผู้ใช้งานเข้าสู่หน้ายืนยันตัวของระบบจัดการการส่งการบ้าน | 1.username=  siwaphol\_boonpan  2.password=  (รหัสผ่านของ siwaphol\_boonpan) | | ผู้ใช้งานสามารถเข้าใช้งานระบบจัดการการส่งการบ้านปฏิบัติการได้ | ผู้ใช้งานเข้าไปที่หน้าหลักของระบบจัดการการส่งการบ้านปฏิบัติการ | ผ่าน |  |
| 2 | ผู้ใช้กรอกชื่อผู้ใช้ |  |
| 3 | ผู้ใช้กรอกรหัสผ่าน |  |
| 4 | กดปุ่ม Login |  |

## การร้องขอยืนยันตัวตน

การทดสอบการร้องขอการยืนยันตัวตน โดยระบบนอกจะร้องขอการยืนยันตัวตนให้กับผู้ใช้งาน โดยโปรแกรมที่ใช้ในการทดสอบมีชื่อว่าโพสต์แมน (Postman) เป็นโปรแกรมสำหรับทดสอบเอพีไอ โดยมีการดำเนินการทดสอบระบบดังตารางที่ 6.2

ตารางที่ . ตารางทดสอบการการร้องขอยืนยันตัวตน

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test Case Name | | | ทดสอบการร้องขอยืนยันตัวตน | | | | |
| Test Description | | | เพื่อทดสอบการรับ และส่งค่าสำหรับการยืนยันตัวตนได้สำเร็จ | | | | |
| Pre-Condition | | | ผู้ใช้งานกรอกชื่อผู้ใช้ และรหัสผ่านถูกต้อง ระบบนอกสามารถเชื่อมต่อกับส่วนบริการได้ หมายเลขโปรแกรมถูกต้อง | | | | |
| Steps | Test Steps | Test Data | | Expected Result | Actual Result | Status | Note |
| 1 | รับค่าชื่อผู้ใช้ และรหัสผ่านผู้ใช้ จากหน้ากรอกข้อมูลยืนยันตัวตน | 1.username=  siwaphol\_boopan  2.password=  (รหัสผ่านที่ถูกเข้ารหัส siwaphol\_boonpan)  3.appid=CMUMIS  4.ที่อยู่ GET ที่ร้องขอ คือ /login | | ระบบนอกได้รับข้อมูลเลขเอชทีทีพี 200 และ access\_token ของผู้ใช้งาน | ระบบนอกได้รับเลขสถานะเอชทีทีพี 200 และ ได้ค่าเจสันaccess\_token กลับคืนมา | ผ่าน |  |
| 2 | นำรหัสผ่านไปเข้ารหัสโดยใช้รหัสลับที่ได้จากส่วนบริการเกตเวย์ |  |
| 3 | ส่งค่าทั้งหมดให้แก่ส่วนบริการเกตเวย์ยืนยันตัวตนแบบ GET ไปที่ /login |  |

## การร้องขอข้อมูลผู้ใช้งาน

การทดสอบการร้องขอข้อมูลผู้ใช้งาน โดยระบบนอกร้องขอข้อมูลผู้ใช้งาน หลังจากยืนยันตัวตนสำเร็จและได้รับ access\_token โดยโปรแกรมโพสต์แมน ทดสอบทั้งการส่ง และรับค่า โดยมีการดำเนินการทดสอบระบบดังตารางที่ 6.3

ตารางที่ . ตารางทดสอบการการร้องขอข้อมูลผู้ใช้งาน

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test Case Name | | | ทดสอบการร้องขอข้อมูลผู้ใช้งาน | | | | |
| Test Description | | | เพื่อทดสอบการร้องขอ และรับข้อมูลผู้ใช้ของส่วนบริการเกตเวย์กับระบบนอก | | | | |
| Pre-Condition | | | ชื่อผู้ใช้งาน และ access\_token ถูกต้อง ระบบนอกสามารถเชื่อมต่อกับส่วนบริการได้ หมายเลขโปรแกรมถูกต้อง | | | | |
| Steps | Test Steps | Test Data | | Expected Result | Actual Result | Status | Note |
| 1 | เพิ่มชื่อผู้ใช้กับตัวแปร username | 1.username=  siwaphol\_boopan  2.access\_token=  ค่าโทเค็นที่เก็บอยู่ในเซสชั่นหลังผู้ใช้งานยืนยันตัวตนสำเร็จ  3.appid=CMUMIS  4.ที่อยู่ GET ที่ร้องขอ คือ /getUserInfo | | ระบบนอกได้รับข้อมูลเลขเอชทีทีพี 200 และข้อมูลผู้ใช้งานกับaccess\_token ใหม่ในรูปแบบเจสัน | เลขสถานะ เอชทีทีพี 200 และได้ข้อมูลผู้ใช้กับ access\_tokenใหม่ในรูปแบบเจสัน | ผ่าน |  |
| 2 | นำเอาโทเค็นเก็บในเซสชั่นใส่ตัวแปร access\_token |  |
| 3 | ใส่ค่าหมายเลขโปรแกรมในตัวแปร appid ส่งค่าทั้งหมดให้แก่ส่วนบริการโดยส่งไปที่ /getUserInfo |  |

# บทที่ 7 บทสรุป

การค้นคว้าอิสระนี้ มีวัตถุประสงค์เพื่อพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอเพื่อใช้งานในรูปแบบส่วนบริการแบบเรสต์ ให้ผู้ใช้งานยืนยันตัวตนโดยใช้ชื่อบัญชีผู้ใช้ไอที และรหัสผ่านของมหาวิทยาลัยเชียงใหม่ และผู้พัฒนาระบบอื่นใช้งานบริการยืนยันตัวตน และดึงข้อมูลผู้ใช้งาน โดยสรุปเป็นประเด็นดังนี้

7.1 สรุปผลการศึกษาและพัฒนาระบบ

7.2 ปัญหาและอุปสรรค

7.3 ข้อจำกัดของระบบงาน

7.4 ข้อเสนอแนะ

## สรุปผลการศึกษาและพัฒนาระบบ

การค้นคว้าอิสระนี้ เป็นการพัฒนาส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอ โดยตัวส่วนบริการเองใช้โครงสร้างแบบเรสต์ ในการติดต่อกับระบบนอก มีการให้บริการ 2 ส่วน คือ ให้บริการยืนยันตัวตนผู้ใช้งานโดยใช้ชื่อบัญชีผู้ใช้ไอที และรหัสผ่านของมหาวิทยาลัยเชียงใหม่ และให้ข้อมูลผู้ใช้งาน

การเพิ่มความปลอดภัยในการสื่อสารกับระบบนอก ใช้การรับ และส่งข้อมูลผ่านเอสเอสแอลตลอกเวลา และใช้ระบบลายเซ็นเพื่อป้องกันการเข้าถึงโดยระบบที่ไม่ได้รับอนุญาต

## ปัญหา และอุปสรรค

ปัญหาและอุปสรรคที่เกิดขึ้นในการพัฒนาระบบ มีดังนี้

1. ส่วนบริการเกตเวย์ยืนยันตัวตน ขึ้นอยู่กับเรสต์เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีเป็นหลัก ดังนั้น เมื่อเกิดปัญหากับเรสต์เอพีไอของสำนักบริการเทคโนโลยี จะทำให้การทำงานของส่วนบริการเกตเวย์หยุดทันที
2. ความยากในการทดสอบของโปรแกรมแบบเว็บ เพราะการเขียนโปรแกรมบนเว็บประกอบด้วยหลายภาษาทั้งเอชทีเอ็มแอล จาวาสคริปต์ และพีเอชพี ซึ่งใช้งานร่วมกัน การทดสอบต้องทำในหลายส่วน
3. การเขียนโปรแกรมเพื่อดักจับข้อผิดพลาดที่จะเกิดขึ้นในอนาคต ไม่สามารถครอบคลุมได้ทุกกรณี เพราะการเขียนโปรแกรมที่ทำงานบนเครือข่ายอินเทอร์เน็ต มีความเสี่ยงที่จะถูกโจมตีตลอดเวลา

## ข้อจำกัดของระบบงาน

ส่วนบริการเกตเวย์ยืนยันตัวตนโดยใช้เรสต์เอพีไอมีข้อจำกัดของระบบดังนี้

1. ส่วนของรหัสลับที่ใช้ร่วมกัน จะต้องเหมือนกันตลอด เมื่อเปลี่ยนรหัสลับในฐานข้อมูลของส่วนบริการ ผู้ดูแลส่วนบริการจะต้องแจ้งให้กับนักพัฒนาระบบนอกถึงรหัสลับที่ถูกเปลี่ยนแปลง เพื่อให้การทำงานเป็นไปได้ด้วยดี
2. การส่งข้อมูลระหว่างส่วนบริการเกตเวย์ยืนยันตัวตนกับระบบภายนอกทำผ่านเอชทีทีพี ดังนั้นจะต้องบังคับให้ทำงานกับโพรโทคอลรักษาความปลอดภัยเอสเอสแอลตลอดเวลาเพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
3. เรสต์เอพีไอยืนยันตัวตัวตนของสำนักบริการเทคโนโลยี มีการเปลี่ยนแปลงรุ่นตลอดเวลา ผู้ดูแลระบบจะต้องมีการติดต่อกับผู้ดูแลฝั่งสำนักบริการเทคโนโลยีในกรณีมีการเปลี่ยนแปลงเกิดขึ้น

## ข้อเสนอแนะ

1. การพัฒนาต่อยอดส่วนบริการเกตเวย์ยืนยันตัวตน การเพิ่มส่วนบริการใหม่ หรือแก้ไขให้ใส่หมายเลขระบุรุ่นในส่วนของยูอาร์แอล เพื่อบอกถึงการเปลี่ยนแปลงให้กับนักพัฒนาระบบนอก
2. ใช้เทคโนโลยี อุปกรณ์ และวิธีการพัฒนาโปรแกรมแบบเว็บที่จะช่วยเพิ่มประสิทธิภาพ ความเร็ว และความปลอดภัย โดยอย่างน้อยให้ความสำคัญกับความปลอดภัย เนื่องจากส่วนบริการเกตเวย์จะต้องทำงานกับข้อมูลสำคัญของผู้ใช้งาน

# ภาคผนวก ก การตั้งค่าที่จำเป็น

## 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/gatewayservice

* กำหนดสมนาม (Alias) ให้เพิ่มตัวแปร Alias เช่น

Alias /gatewayservice /home/siwaphol/gatewayservice

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 **ก**  
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/gatewayservice>

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/gatewayservice

* เพิ่มสิทธิอนุญาตให้แก่กลุ่มของเจ้าของไฟล์

Chmod –R 755 /home/siwaphol/gatewayservice

# ภาคผนวก ข การติดตั้งฟาลคอนเฟรมเวอร์ค (Phalcon Framework)

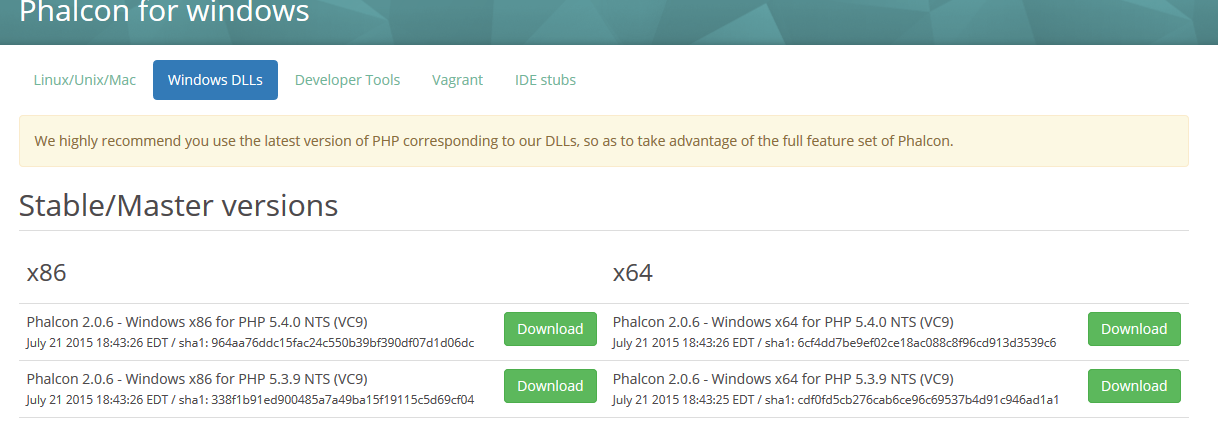
เนื่องจากส่วนบริการเกตเวย์ยืนยันตัวตนถูกพัฒนาโดยใช้ฟาลคอนเฟรมเวอร์ค ดังนั้นก่อนการใช้งานส่วนบริการจะต้องติดตั้งฟาลคอนเฟรมเวอร์ค เพื่อให้ส่วนบริการเกตเวย์ยืนยันตัวตนทำงานได้

## การติดตั้งฟาลคอนเฟรมเวอร์คสำหรับแซมป์ (XAMPP) บนระบบปฏิบัติการวินโดวส์

โดยรุ่นพีเอชพีที่แสดงวิธีทำคือ 5.6.0 สถาปัตยกรรมคอมพิวเตอร์แบบ 86 บิต และรุ่นของฟาลคอนเฟรมเวอร์คคือ 2.0.5

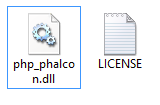
1. ทำการบรรจุลงไฟล์ซิป (zip) ของฟาลคอนเฟรมเวอร์คได้จาก

https://phalconphp.com/en/download /windows



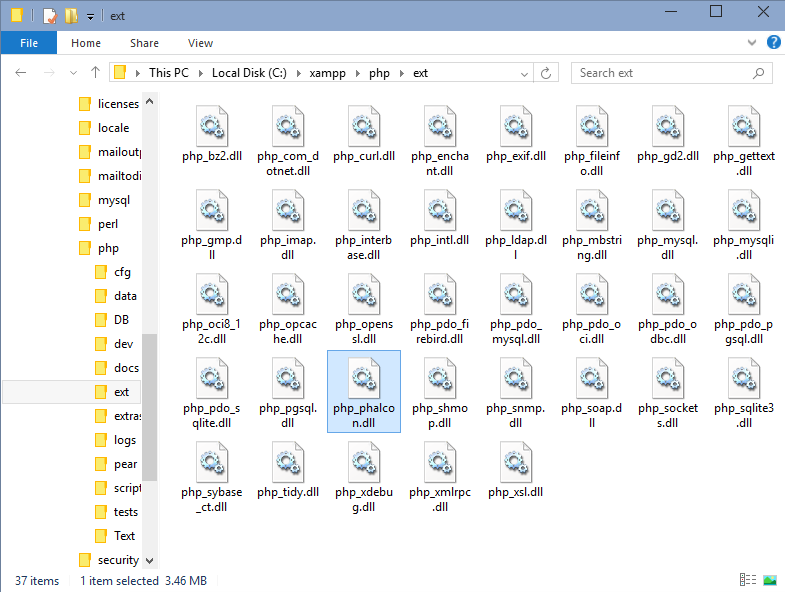
รูปที่ . แสดงตัวเลือกสำหรับการดาวน์โหลดฟาลคอนเฟรมเวอร์คบนระบบปฏิบัติการวินโดวส์

1. เปิดไฟล์ซิปที่บรรจุลงเสร็จ คลายไฟล์ซิปออกมาจะเห็นมีอยู่สองไฟล์



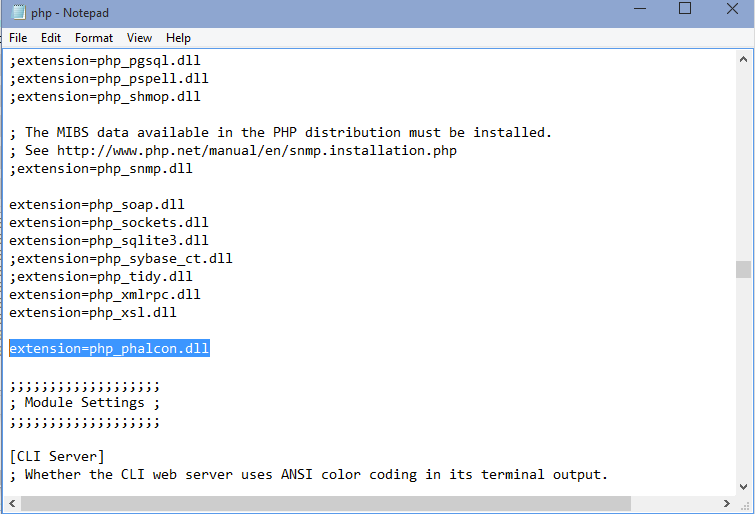
รูปที่ . แสดงไฟล์ php\_phalcon.dll ใช้สำหรับติดตั้งฟาลคอนเฟรมเวอร์ค

1. ให้คัดลอกไฟล์ php\_phalcon.dll ไปไว้ที่โฟลเดอร์ส่วนขยายของพีเอชพีถ้าติดตั้งแซมป์ไว้ที่ c:\xampp โฟลเดอร์ส่วนขยายจะอยู่ที่ c:\xampp\php\ext



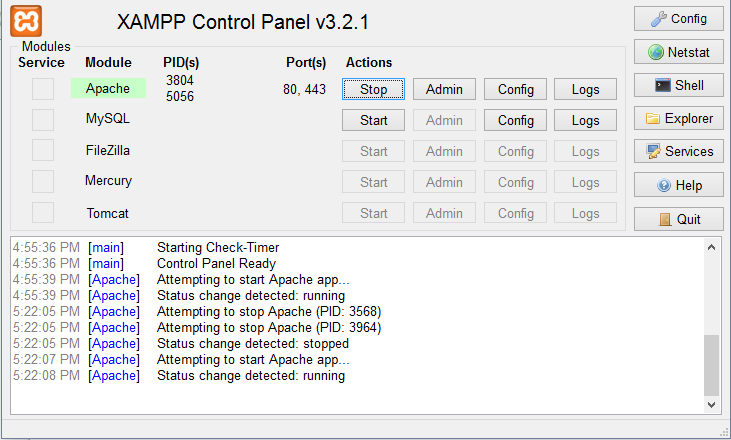
รูปที่ . แสดงโฟลเดอร์สำหรับติดตั้งส่วนขยายพีเอชพี

1. แก้ไขไฟล์ php.ini เพื่อเพิ่มส่วนขยายสำหรับ php\_phalcon.dll โดยปกติตำแหน่งไฟล์ php.ini อยู่ที่ c:\xampp\php



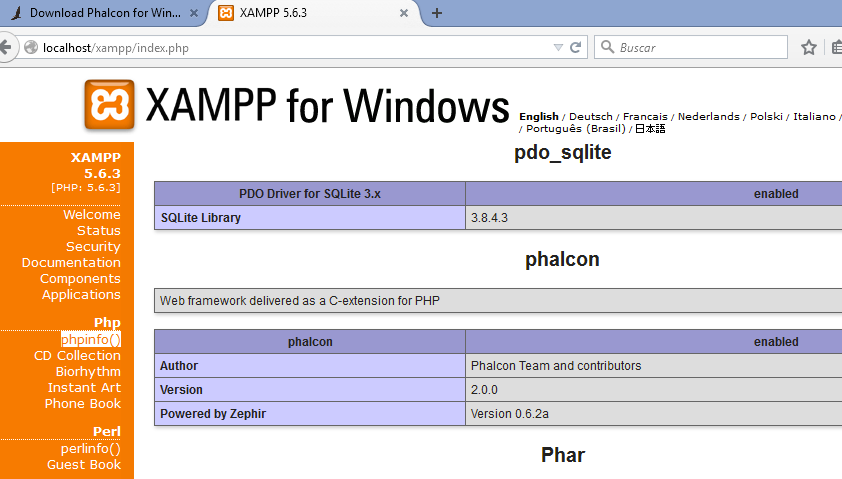
รูปที่ . แสดงการตั้งค่าไฟล์ php.ini เพื่อเพิ่มส่วนขยายฟาลคอนเฟรมเวอร์ค

1. ทำการเริ่มการทำงานตัวบริการเว็บใหม่



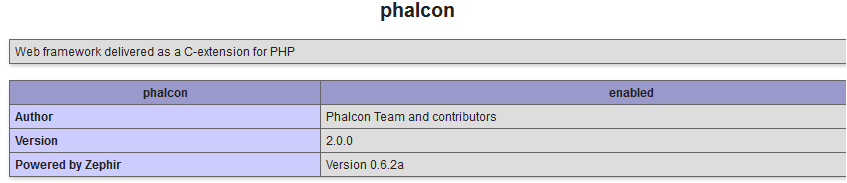
รูปที่ . แสดงการเริ่มตัวบริการเว็บบนแซมป์

1. เปิดเบราว์เซอร์แล้วไปที่ http://localhost โดยจะเป็นหน้าหลักของแซมป์ด้านซ้ายเลือกเมนูว่า phpinfo()



รูปที่ . แสดงหน้าต่างเริ่มต้นของโปรแกรมแซมป์

1. เมื่อติดตั้งฟาลคอนเฟรมเวอร์คสำเร็จจะเห็น ชื่อฟาลคอน และหมายเลขรุ่นที่ใช้งาน



รูปที่ . แสดงหน้าต่างชอง phpinfo เพื่อดูความสำเร็จในการติดตั้งฟาลคอนเฟรมเวอร์ค

## การติดตั้ง ฟาลคอนเฟรมเวอร์ค บนระบบปฏิบัติการอูบุนตู

ก่อนการติดตั้งให้ตรวจสอบว่าพีเอชพีมีส่วนขยายดังต่อไปนี้

1. Mbstring
2. Mcrypt
3. Openssl
4. PDO
5. PDO/Mysql
6. PDO/Postgresql
7. PDO/Sqlite
8. PDO/Oracle
9. Mongo

สำหรับส่วนขยายที่ 5 - 9 สามารถเลือกที่จะติดตั้งแค่อันใดอันหนึ่ง ขึ้นอยู่กับประเภทของฐานข้อมูลที่ใช้

### การติดตั้งผ่านโปรแกรมแอพท์-เกต (apt-get)

1. ทำการเพิ่มที่อยู่ของฟาลคอนเฟรมเวอร์ค

sudo apt-add-repository ppa:phalcon/stable

1. ทำการอัพเดตรายชื่อโปรแกรมสำเร็จ

sudo apt-get update

1. ทำการติดตั้งส่วนขยายชื่อ php5-phalcon

sudo apt-get install php5-phalcon

หมายเหตุ กรณีที่ยังไม่มีคำสั่ง apt-add-repository ในระบบของอูบุนตูตั้งแต่รุ่น 14.04 ให้ใช้

sudo apt-get install software-properties-common

### การติดตั้งผ่านการแปลโปรแกรม

โปรแกรมสำเร็จที่ต้องการก่อนการแปลโปรแกรม

- พีเอชพีแบบพัฒนาตั้งแต่รุ่น 5 เป็นต้นไป

- ตัวแปลโปรแกรมจีซีซี (GCC compiler)

สำหรับอูบุนตูติดตั้งโปรแกรมสำเร็จส่วนพัฒนาข้างต้นได้จากคำสั่ง

sudo apt-get install php5-dev php5-mysql gcc libpcre3-dev

1. ทำการคัดลอกรหัสต้นฉบับมาจากที่เก็บกิต (Git) ของฟาลคอนเฟรมเวอร์ค

git clone git://github.com/phalcon/cphalcon.git

1. เข้าไปที่โฟลเดอร์

cd cphalcon/build

1. ทำการแปลโปรแกรมโดยตัวแปลโปรแกรมจีซีซีจะเป็นตัวตรวจว่าควรใช้สถาปัตยกรรมคอมพิวเตอร์แบบไหน

sudo ./install

1. รอจนการการแปลโปรแกรมเสร็จสิ้น ไฟล์สำเร็จจะถูกเก็บไว้ที่โฟลเดอร์เก็บส่วนขยายของพีเอชพี
2. เพิ่มส่วนขยายในไฟล์ php.ini

สำหรับอูบุนตู หรือดีเบียน

ให้สร้างไฟล์ชื่อว่า 30-phalcon.ini ใน /etc/php5/conf.d/

สำหรับอุบุนตุ หรือดีเบียนที่ใช้ php5-fpm แทนพีเอชพีดั้งเดิม

ให้สร้างไฟล์ชื่อว่า30-phalcon.ini ใน etc/php5/fpm/conf.d/

โดยภายในไฟล์ 30-phalcon.ini และ php.ini ให้ใส่ข้อความดังข้างล่าง

extension=phalcon.so

1. ทำการสร้างไฟล์ phalcon.ini ไว้ในโฟลเดอร์ /etc/php5/mods-available โดยภายในไฟล์กรอก

extension=phalcon.so

1. ทำการเริ่มตัวบริการเว็บใหม่

# ภาคผนวก ค การใช้งานส่วนบริการเกตเวย์ยืนยันตัวตน

## การใช้งานส่วนต่อประสานโปรแกรมของส่วนบริการเกตเวย์ยืนยันตัวตน

### การนำเข้าไฟล์คลังโปรแกรม และใช้งานฟังก์ชันสำเร็จรูป

1. ในโฟลเดอร์ libs มีไฟล์ชื่อ GatewayService.php



รูปที่ . แสดงภาพไฟล์คลังโปรแกรม GatewaySercive.php

1. ในไฟล์พีเอชพีที่ต้องการนำเข้าฟังก์ชันสำหรับทำงานร่วมกับส่วนบริการเกตเวย์

Include ‘libs/GatewayService.php’;

โดยที่ libs แทนที่อยู่ซึ่งไฟล์ GatewayService.php ถูกจัดเก็บอยู่

การเรียกใช้ฟังก์ชันในคลังโปรแกรมให้ใช้คำสั่ง

GatewayService::ชื่อฟังก์ชันที่เรียกพร้อมตัวแปรที่ฟังก์ชันต้องการ

1. เรียกใช้ฟังก์ชันที่ต้องการมีดังนี้

**ฟังก์ชันสร้างลายเซ็น**

Array createSignature (string $httpMethod, string $requestURL,   
 string $parameters, string $secret)

**ตัวแปร**

$httpMethod เอชทีทีพีเมท็อด

$requestURL ที่อยู่ยูอาร์แอลบริการที่ต้องการ

$parameter ตัวแปรส่งเข้าโดยใช้เครื่องหมาย & ขั้นระหว่างตัวแปร ไม่จำเป็นต้องเรียงลำดับ

$secret รหัสลับที่ได้จากส่วนบริการ

**ค่าคืนกลับ**

Array (

[0] => ลายเซ็น

[1] => ตราเวลายูนิกซ์เป็นวินาที่)

**ตัวอย่าง**

$result = GatewayService::createSignature (‘POST’, ‘/login’, ’appid=CMUMIS& username=siwaphol\_boonpan&password=12341234&’, ’app\_secret\_here’);

ผลลัพธ์จากคำสั่งข้างต้นจะได้

$result[0] คือ ลายเซ็น และ $result[1] คือ ตราเวลาแบบยูนิกซ์เป็นวินาที

## การส่งคำร้องไปยังส่วนบริการเกตเวย์ยืนยันตัวตน

ก่อนการส่งคำร้องจะต้องสร้าง ลายเซ็น โดยผู้ใช้งานสามารถที่จะสร้างตามรูปแบบที่ส่วนบริการกำหนด หรือใช้งานคลาสที่ส่วนบริการได้จัดเตรียมไว้ในไฟล์ GatewayService.php โดยทำได้ดังคำสั่งตัวอย่างด้านล่าง

<?php

import “libs/GatewayService.php”

## ร้องขอการยืนยันตัวตน

โดยสามารถเรียกโดยใช้คำสั่ง requestLogin (ที่อยู่ของ)

## ร้องขอข้อมูลผู้ใช้งาน

หกด

## หก

# 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

[9] Amazon AWS, Authenticating REST Requests [ระบบออนไลน์] แหล่งที่มา http://s3.amazonaws.com/doc/s3-developer-guide/RESTAuthentication.html