การเสริมสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์ สำหรับองค์กรเสมือนขนาดใหญ่โดยใช้ตลาดหลักทรัพย์แห่งประเทศไทยเป็นกรณีศึกษา

นางสาว ณิศรา ศิริพรกุลทรัพย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2546
ISBN 974-17-5085-4

THE HARDENING OF LIBERTY ALLIANCE SINGLE SIGN-ON ARCHITECTURE FOR LARGE-SCALE VIRTUAL ORGANIZATION USING THE STOCK EXCHANGE OF THAILAND ENVIRONMENT AS A CASE STUDY

Miss Nissara Siripornkulasup

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2003

ISBN 974-17-5085-4

หัวข้อวิทยานิพนธ์	การเสริมสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้ แอลไลเอนซ์สำหรับองค์กรเสมือนขนาดใหญ่โดยใช้ตลาดหลักทรัพย์แห่งประเทศไทยเป็นกรณีศึกษา
โดย	นางสาวณิศรา ศิริพรกุลทรัพย์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

..... กรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

..... กรรมการ
(อาจารย์ ธงชัย โรจน์กังสดาล)

ณิศรา ศิริพรกุลทรัพย์ : การเสริมสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์สำหรับองค์กรเสมือนขนาดใหญ่โดยใช้ตลาดหลักทรัพย์แห่งประเทศไทยเป็นกรณีศึกษา (THE HARDENING OF LIBERTY ALLIANCE SINGLE SIGN-ON ARCHITECTURE FOR LARGE-SCALE VIRTUAL ORGANIZATION USING THE STOCK EXCHANGE OF THAILAND ENVIRONMENT AS A CASE STUDY) อ. ที่ปรึกษา : อาจารย์ ดร. ณัฐวุฒิ หนูไพโรจน์, 63 หน้า.
ISBN 974-17-5085-4.

ความร่วมมือกันในการทำงานระหว่างองค์กรได้รับความนิยมมากขึ้น และมีแนวโน้มที่จะอยู่ในรูปแบบของการเชื่อมต่อกันระหว่างระบบงานกับระบบงาน ดังนั้นการอนุญาตให้องค์กรอื่นๆ เข้าใช้ระบบงานภายในบริษัทต้องการมาตรการการรักษาความปลอดภัยที่มีความเข้มแข็งและยืดหยุ่นในเวลาเดียวกัน นอกจากนี้ ยังต้องสามารถใช้งานร่วมกับระบบงานต่างๆ ซึ่งอยู่ในองค์กรเสมือนเดียวกัน หรือองค์กรเสมือนที่มีความเชื่อถือซึ่งกันและกันได้ เพื่อสนับสนุนความต้องการดังกล่าว ลิเบอร์ตี้แอลไลเอนซ์จึงได้เสนอสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวมาใช้กับการพิสูจน์ตัวจริงในองค์กรเสมือน แต่เนื่องจากสถาปัตยกรรมที่ลิเบอร์ตี้สร้างขึ้นนั้นยังไม่รองรับการทำงานที่ซับซ้อน เช่น การพิสูจน์ตัวจริงข้ามองค์กรเสมือน จึงทำให้ไม่ยืดหยุ่นพอที่จะรองรับรูปแบบการทำงานที่เปลี่ยนไปได้

วิทยานิพนธ์นี้มีจุดประสงค์ที่จะศึกษาและออกแบบสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับองค์กรเสมือนที่มีการรักษาความปลอดภัยในการเข้าใช้งานระบบโดยวิธีการพิสูจน์ตัวจริงข้ามองค์กร ซึ่งงานวิจัยนี้ได้นำแนวคิดสถาปัตยกรรมของลิเบอร์ตี้แอลไลเอนซ์มาใช้เป็นพื้นฐานและทำการขยายขีดความสามารถ โดยพิจารณาทั้งการออกแบบโครงสร้างพื้นฐานขององค์กรเสมือน ออกแบบ โพรโทคอลของการพิสูจน์ตัวจริงข้ามองค์กร และออกแบบเนมสเปซของแต่ละองค์กรเสมือน นอกจากนี้งานวิจัยยังได้ทำการทดลองพัฒนาการลงบันทึกเข้าระบบของตลาดหลักทรัพย์ด้วยสถาปัตยกรรมที่สร้างขึ้น เพื่อเป็นกรณีศึกษาในการพัฒนา สถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวที่ออกแบบขึ้นสามารถใช้ในการพิสูจน์ตัวจริงระหว่างองค์กรเสมือนที่มีความเชื่อถือกันตั้งแต่ 2 องค์กรขึ้นไป

ภาควิชา.....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....
สาขาวิชา.....วิทยาศาสตร์คอมพิวเตอร์...ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา 2546

4470306021 : MAJOR COMPUTER SCIENCE

KEY WORD: SINGLE SIGN-ON / LIBERTY ALLIANCE / CROSS-VIRTUAL ORGANIZATION / AUTHENTICATION

NISSARA SIRIPORNKULASUP : THE HARDENING OF LIBERTY ALLIANCE SINGLE SIGN-ON ARCHITECTURE FOR LARGE-SCALE VIRTUAL ORGANIZATION USING THE STOCK EXCHANGE OF THAILAND ENVIRONMENT AS A CASE STUDY. THESIS ADVISOR : .NATAWUT NUPAIROJ , Ph.D., 63 pp. ISBN 974-17-5085-4.

Cross organization coordination becomes increasingly popular and tends to require system to system integration. To allow other companies to access internal systems require security policies, which are both strong and flexible at the same time. Furthermore, the policies must be applicable to all systems in this virtual organization. To satisfy these requirements, Liberty Alliance has proposed single sign-on architecture as a standard authentication method within a virtual organization. As this architecture does not support some features such as cross virtual organization authentication, it is not flexible enough to support complex working environments.

The objective of this thesis is to study and design a single sign-on architecture for cross-virtual organization authentication. We utilize Liberty Alliance architecture as a foundation and extend its features by considering virtual organization architecture, cross-organization authentication protocol, and namespaces for each virtual organization. In addition, this thesis has developed an authentication application of the Stock Exchange of Thailand based on our architecture and used it as a case study in developing single sign-on architecture for authenticating users among trusted virtual organizations.

Department Computer Engineering Student's signature.....

Field of study Computer Science Advisor's signature.....

Academic year 2003

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยความกรุณา และความช่วยเหลืออย่างดียิ่งจาก อ.ดร.ณัฐวุฒิ หนูไพโรจน์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาในการให้คำปรึกษาและแนะนำข้อคิดเห็นต่างๆ ตลอดจนช่วยตรวจแก้ไขวิทยานิพนธ์ด้วยความเอาใจใส่อย่างดียิ่ง

ขอขอบคุณ อ.ดร. ยรรยง เต็งอำนวย ซึ่งช่วยแนะนำแนวคิดต่างๆ ที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์นี้ รวมถึง อ. จารุมาตร ปิ่นทอง และ อ. ธงชัย โรจน์กังสดาล ซึ่งเป็นกรรมการสอบวิทยานิพนธ์นี้

ขอขอบคุณ นางสาวรัศมีทิพย์ วิตา นายรังสรรค์ เกียรติ์ภานนท์ นายกิตติพิชญ์ คุปตะวาณิช และนายกัน อุตะเดช เพื่อนร่วมกลุ่มการวิจัยการออกแบบและพัฒนาโปรแกรมประยุกต์แบบกระจายโดยใช้เทคโนโลยีเชิงวัตถุของตลาดหลักทรัพย์ที่คอยช่วยเหลือข้าพเจ้าในทุกๆ เรื่องตลอดการทำวิทยานิพนธ์นี้

ขอขอบคุณ นางสาวนงเยาว์ จินดาสวัสดิ์ นายชาติชาย ดวงสอาด และพี่ศิรส สุภาวิตา ซึ่งให้ความช่วยเหลือตอบข้อซักถามต่างๆ ด้วยความเต็มใจ

ขอขอบคุณ เพื่อนๆ พี่ๆ น้องๆ ในห้องปฏิบัติการวิศวกรรมสารสนเทศ และห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ทุกท่านที่ให้ความช่วยเหลือและคลายเครียดอย่างดีมาตลอด

สุดท้ายนี้ ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ และพี่ของข้าพเจ้าที่ช่วยเป็นกำลังใจ และให้การสนับสนุนข้าพเจ้า จนสำเร็จการศึกษา

สารบัญ

หน้า

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเริ่มมีการดำเนินธุรกิจแบบใหม่ โดยการทำงานร่วมกันระหว่างองค์กรหลายๆ องค์กรเพื่อจุดมุ่งหมายเดียวกันตามแนวความคิดขององค์กรเสมือน (Virtual Organization) ซึ่งแต่ละองค์กรติดต่อสื่อสารกันโดยใช้อินเทอร์เน็ต ทั้งนี้เพื่อความคล่องตัวขององค์กรที่ทำงานร่วมกันในองค์กรเสมือน องค์กรต่างๆ มักจะเปิดบริการหรือโปรแกรมประยุกต์ภายในองค์กรให้ผู้ใช้ขององค์กรอื่นๆ สามารถเข้าใช้บริการได้ โดยองค์กรต่างๆ จะเตรียมวิธีการที่น่าเชื่อถือสำหรับการพิสูจน์ตัวจริง (Authentication) ของผู้ใช้ โดยก่อนที่ผู้ใช้จะเข้าใช้บริการเหล่านั้น ผู้ใช้ต้องแสดงหลักฐานอ้างอิงตัวผู้ใช้ (Credential) ในการพิสูจน์ตัวจริงก่อน นอกจากนี้ผู้ใช้จะต้องผ่านการตรวจสอบสิทธิ (Authorization) เพื่อให้มั่นใจว่าผู้ที่มีสิทธิสามารถเข้าใช้ระบบได้เท่านั้น เพื่อความสะดวกในการเข้าใช้บริการที่มีการรักษาความปลอดภัยต่างๆ ในองค์กรเสมือน จึงมีการนำแนวคิดของการลงบันทึกเข้าระบบเพียงครั้งเดียว (Single Sign-On - SSO) มาใช้ โดยแนวคิดนี้ทำให้ผู้ใช้สามารถพิสูจน์ตัวจริงกับองค์กรที่ทำหน้าที่พิสูจน์ตัวจริง (Authentication Authority) เพียงครั้งเดียวแล้วสามารถเข้าใช้ทรัพยากรที่มีการรักษาความปลอดภัยอื่นๆ ได้โดยไม่ต้องทำการพิสูจน์ตัวจริงกับผู้ให้บริการทรัพยากรอีกครั้ง [1]

แนวคิดของการลงบันทึกเข้าระบบเพียงครั้งเดียวในปัจจุบันมีหลายแนวคิด เช่น ไมโครซอฟต์พาสปอร์ต (Microsoft Passport) ที่มีการใช้งานจริงในปัจจุบัน จะทำงานอยู่บนระบบแบบรวมศูนย์ (Centralized System) โดยอนุญาตให้ผู้ใช้สร้างด็อทเน็ตพาสปอร์ต (.Net Passport) จากนั้นผู้ใช้สามารถลงบันทึกเข้ากับเว็บไซต์ใดๆ ที่รองรับหลักฐานอ้างอิงตัวผู้ใช้แบบด็อทเน็ตพาสปอร์ตได้ [2] ส่วนโครงสร้างการรักษาความปลอดภัยเชิงกริด (Grid Security Infrastructure - GSI) จะทำการลงบันทึกเข้าระบบระหว่างโดเมนภายในองค์กรเสมือนเดียวกัน ซึ่งมีข้อดีคือเป็นระบบที่เหมาะสำหรับการติดต่อกันระหว่างองค์กรที่มีระบบการรักษาความปลอดภัยที่แตกต่างกัน โดยมีการมอบอำนาจโดยการสร้างตัวแทนเพื่อให้ผู้ใช้สามารถใช้งานระบบภายในโดเมนอื่นๆ ขององค์กรเสมือนได้ และส่วนข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์ (Liberty Alliance) ทำงานบนระบบแบบกระจาย (Distributed System) โดยองค์กรที่อยู่ในวงแห่งความเชื่อถือเดียวกันจะเชื่อถือซึ่งกันและกันและต้องรู้จักกันหมด เป็นต้น แต่แนวคิดของการลงบันทึกเข้าระบบเพียงครั้งเดียวเหล่านี้มีขอบเขตการใช้งานภายในองค์กรเสมือนเดียวกันเท่านั้น ซึ่งไม่เหมาะกับความต้องการขององค์กรที่ต้องการความอิสระในการกำหนดนโยบายด้านการรักษาความ

ปลอดภัยและการจัดการเกี่ยวกับผู้ใช้ ดังนั้น จึงควรมีแนวคิดของการลงบันทึกเข้าระบบเพียงครั้งเดียวซึ่งสามารถใช้งานระหว่างองค์กรเสมือนตั้งแต่ 2 องค์กรขึ้นไปได้

ดังนั้นผู้วิจัยเห็นว่ามีความจำเป็นในการศึกษาถึงแนวทางในการออกแบบสถาปัตยกรรมการลงบันทึกเข้าใช้ระบบเพียงครั้งเดียวเพื่อใช้ในการทำงานร่วมกันขององค์กรเสมือนตั้งแต่ 2 องค์กรขึ้นไป โดยนำแนวคิดการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์มาใช้ แต่เนื่องจากข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์เวอร์ชันล่าสุด (1.2) [3] มีการกล่าวถึงเพียงวิธีการที่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้แนะนำผู้ให้บริการทรัพยากรภายในองค์กรเสมือนเดียวกันให้รู้จักกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้บริการเป็นสมาชิก แต่ยังขาดการกำหนดขั้นตอนและโพรโทคอลการโต้ตอบที่ชัดเจนเพื่อแลกเปลี่ยนและใช้ข้อมูลสำหรับการระบุผู้ใช้ร่วมกัน นอกจากนี้จะศึกษาวิธีการรักษาความปลอดภัยในการเข้าใช้ระบบในปัจจุบัน แล้วนำไปวิเคราะห์และออกแบบวิธีที่เหมาะสมกับการใช้งานขององค์กรเสมือนในรูปแบบต่างๆ เพื่ออำนวยความสะดวกและแก้ปัญหาที่เกิดขึ้นกับผู้ใช้งานในปัจจุบัน โดยนำสถาปัตยกรรมที่ออกแบบขึ้นมาทดลองใช้กับการลงบันทึกเข้าระบบของตลาดหลักทรัพย์ โดยตลาดหลักทรัพย์ถือเป็นตัวอย่างหนึ่งขององค์กรเสมือนที่มีการติดต่อกันระหว่างองค์กรต่างๆ เช่น บริษัทนายหน้าซื้อขายหลักทรัพย์ (Broker Company) บริษัทจดทะเบียน (Listed Company) เป็นต้น

1.2 วัตถุประสงค์ของการวิจัย

เพื่อทำการศึกษาและออกแบบสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับระบบขององค์เสมือนที่มีการรักษาความปลอดภัยในการเข้าใช้งานระบบ ด้วยวิธีการพิสูจน์ตัวจริงและพิสูจน์สิทธิในการเข้าใช้ของผู้ใช้ระบบ

1.3 ขอบเขตของการวิจัย

ในงานวิจัยนี้ ได้มีการกำหนดขอบเขตไว้ดังต่อไปนี้

1. ศึกษาแนวคิดของการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์ และโครงสร้างการรักษาความปลอดภัยเชิงกริด
2. พิจารณาตลาดหลักทรัพย์แห่งประเทศไทยและบริษัทนายหน้าซื้อขายหลักทรัพย์เป็นองค์กรเสมือนต้นแบบ
3. ทำการลงบันทึกเข้าระบบเฉพาะระบบงานที่อยู่ภายในองค์กรเสมือนเดียวกันเท่านั้น
4. ทดลองสร้างระบบต้นแบบสำหรับสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียว

1.4 ขั้นตอนการดำเนินงานวิจัย

การกำหนดขั้นตอนและวิธีการดำเนินงาน มีรายละเอียดดังนี้

1. ศึกษาจุดอ่อนที่เกิดขึ้นจากการรักษาความปลอดภัยของตลาดหลักทรัพย์ในปัจจุบันและการพัฒนาระบบในอนาคต
2. ศึกษาแนวคิดในการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์ และโครงสร้างการรักษาความปลอดภัยเชิงกริด
3. ศึกษาความรู้เกี่ยวกับการออกแบบสถาปัตยกรรมในการลงบันทึกเข้าระบบเพียงครั้งเดียว
4. วิเคราะห์และออกแบบสถาปัตยกรรมในการลงบันทึกเข้าระบบเพียงครั้งเดียว
5. ทดลองพัฒนาระบบต้นแบบจากสถาปัตยกรรมในการลงบันทึกเข้าระบบเพียงครั้งเดียว
6. สรุปผลการวิจัย และจัดทำรายงานวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัยมีดังต่อไปนี้

1. ได้วิธีการที่เหมาะสมสำหรับการรักษาความปลอดภัยในการเข้าใช้ระบบงานขององค์กรเสมือน
2. เพิ่มความสะดวกแก่ผู้ใช้บริการในการจัดการหลักฐานยืนยันตัวผู้ใช้แต่ละองค์กร

1.6 โครงสร้างวิทยานิพนธ์

ในบทต่อไปของวิทยานิพนธ์นี้จะกล่าวถึงทฤษฎีที่นำมาประยุกต์ใช้ และงานวิจัยที่เกี่ยวข้อง บทที่ 3 จะกล่าวถึงการออกแบบสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน ในบทที่ 4 จะแสดงตัวอย่างการทดลองพัฒนาการลงบันทึกเข้าระบบของตลาดหลักทรัพย์โดยใช้สถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน และในบทสุดท้ายจะเป็นการสรุปผลของงานวิทยานิพนธ์และข้อเสนอแนะในการออกแบบสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวและแนวทางในการพัฒนาต่อไป

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

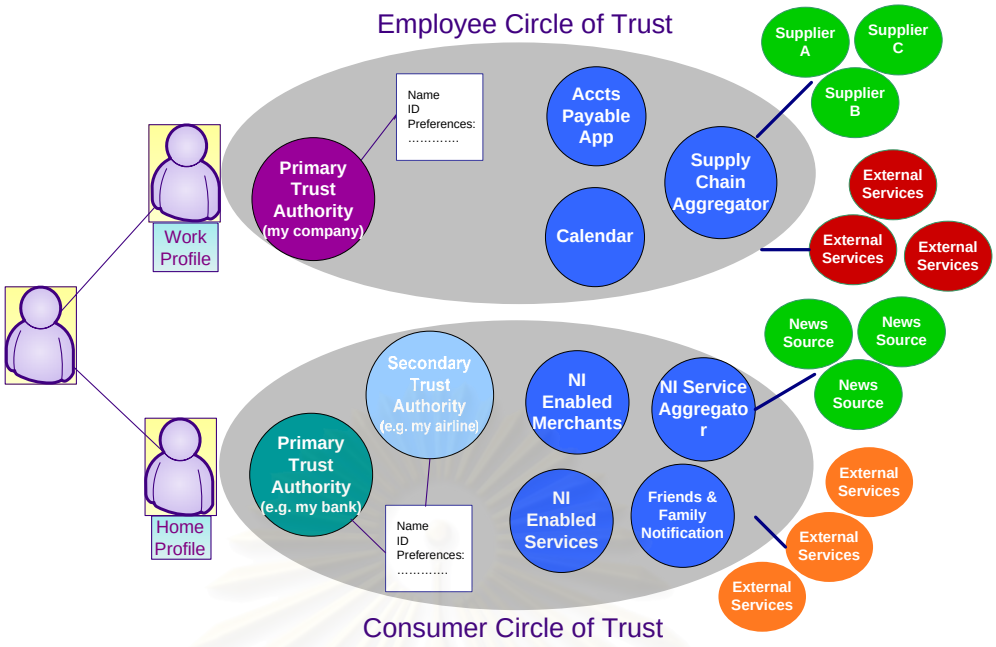
2.1 ทฤษฎีที่เกี่ยวข้อง

ทฤษฎีที่เกี่ยวข้องในงานวิจัยนี้ ได้แก่ แนวคิดในการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลแอนซ์ ภาษาเอสเอเอ็มแอล (Security Assertion Markup Language - SAML) แนวคิดโครงสร้างการรักษาความปลอดภัยเชิงกริด การรักษาความปลอดภัยของตลาดหลักทรัพย์ในปัจจุบัน และการบริการไดเรกทอรี (Directory Services) ซึ่งมีรายละเอียดดังต่อไปนี้

2.1.1 ลิเบอร์ตี้แอลไลแอนซ์ [3, 4]

ข้อมูลสำหรับระบุผู้ใช้บนเครือข่าย (Network Identity) คือ กลุ่มของแอททริบิวท์ต่างๆ ซึ่งประกอบขึ้นมาจากข้อมูลส่วนบุคคลของผู้ใช้ เช่น ชื่อผู้ใช้ ที่อยู่อีเมล์ หมายเลขบัตรเครดิต เป็นต้น โดยข้อมูลสำหรับระบุผู้ใช้บนเครือข่ายเหล่านี้จะกระจายอยู่ตามผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ (Identity Provider - IDP) ต่างๆ ในปัจจุบัน เนื่องจากผู้ให้บริการเหล่านี้มีอิสระในการกำหนดหลักฐานการเข้าใช้ระบบเอง จึงทำให้เกิดปัญหาในกรณีที่ผู้ใช้ติดต่อกับผู้ให้บริการหลายแห่ง ซึ่งผู้ใช้จะต้องรักษาหลักฐานการเข้าใช้ระบบเหล่านี้หลายชุด เช่น ถ้าผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 5 แห่งใช้วิธีการพิสูจน์ตัวจริงโดยการใช้ชื่อผู้ใช้และรหัสผ่าน แล้วผู้ใช้ที่ติดต่อกับผู้ให้บริการทั้ง 5 แห่งนี้จะได้รับชื่อผู้ใช้และรหัสผ่านทั้งหมด 5 ชุด ซึ่งโดยส่วนใหญ่แล้วชื่อผู้ใช้และรหัสผ่านสำหรับผู้ให้บริการแต่ละแห่งจะไม่เหมือนกัน ทำให้ผู้ใช้ต้องจำชื่อผู้ใช้และรหัสผ่านทั้งหมด เพื่อให้สามารถเข้าใช้บริการของแต่ละผู้ให้บริการได้

ข้อกำหนดของลิเบอร์ตี้แอลไอเอนซ์ เสนอแนวคิดที่ใช้ในการรวบรวมข้อมูลสำหรับระบุตัวผู้ใช้บนเครือข่ายให้อยู่ในรูปแบบเดียวกัน เพื่อลดความหลากหลายดังกล่าว โดยนำเทคโนโลยีของการลงบันทึกเข้าระบบเพียงครั้งเดียวมาใช้ในการรวมระบบการพิสูจน์ตัวจริงของแต่ละองค์กรที่เป็นอิสระจากกันในองค์กรเสมือนให้อยู่ในรูปแบบเดียวกัน โดยการสร้างวงแห่งความเชื่อถือ (Circle of Trust) เพื่อรวบรวมผู้ให้บริการทรัพยากร (Service Provider - SP) และผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่มีความสัมพันธ์ทางธุรกิจต่อกันบนพื้นฐานของสถาปัตยกรรมลิเบอร์ตี้แอลไอเอนซ์ และมีข้อตกลงด้านการดำเนินงานร่วมกัน นอกจากนี้ผู้ใช้สามารถดำเนินธุรกรรมอย่างปลอดภัยได้ ส่วนการกำหนดข้อตกลงด้านการดำเนินงานนั้นอยู่นอกเหนือขอบเขตของข้อกำหนดลิเบอร์ตี้



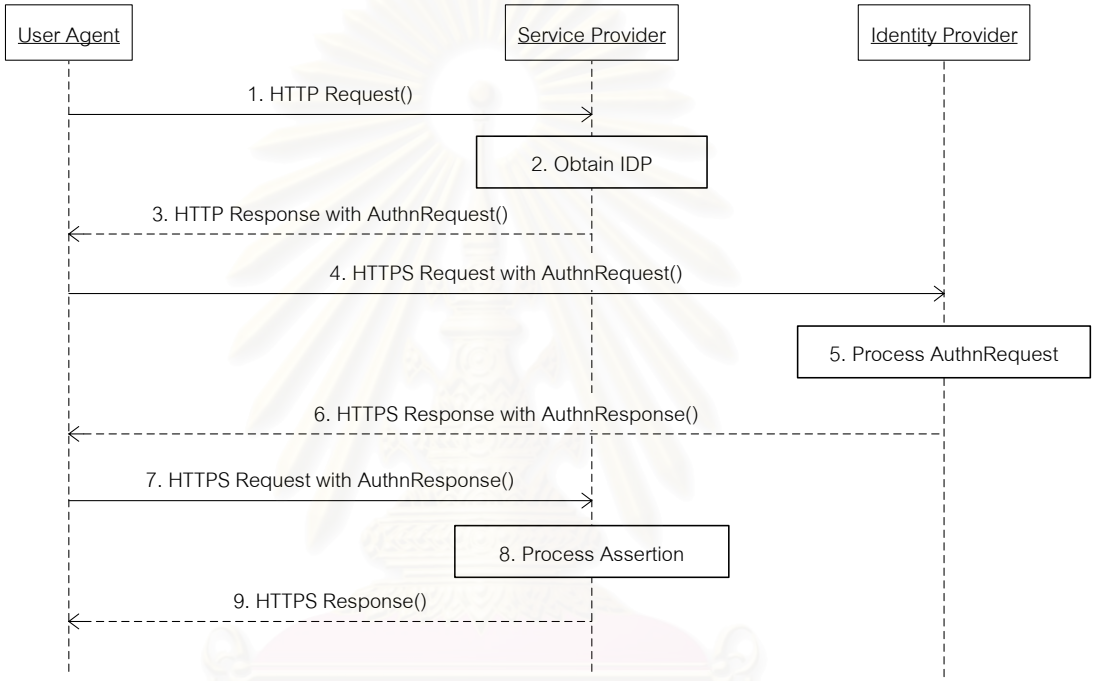
รูปที่ 2.1 วงแห่งความเชื่อถือและการใช้งานข้อมูลสำหรับระบุผู้ใช้บนเครือข่าย [3]

สถาปัตยกรรมของลิเบอร์ตี้แอลไอเอนซ์ประกอบด้วยผู้กระทำ (Actor) 3 ประเภท ได้แก่ ผู้ใช้ ผู้ให้บริการทรัพยากรและผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งผู้ให้บริการทรัพยากรมีหน้าที่ให้บริการแก่ผู้ใช้ เช่น อินเทอร์เน็ตศูนย์รวม (Internet portals) ผู้ค้าปลีก (Retailer) สถาบันทางการเงิน เป็นต้น ส่วนผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้มีหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ให้กับผู้ใช้ และเสนอสิ่งจูงใจทางธุรกิจเพื่อให้ผู้ให้บริการทรัพยากรรายอื่นๆ เข้ามากลุ่มเดียวกัน ซึ่งการสร้างความสัมพันธ์แบบนี้ทำให้เกิดความสัมพันธ์แบบวงแห่งความเชื่อถือ เช่น ในรูปที่ 2.1 วงแห่งความเชื่อถือของลูกค้า (Consumer Circle of Trust) ธนาคารเป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ให้กับผู้ใช้ของธนาคาร และธนาคารมีความสัมพันธ์ทางธุรกิจกับผู้ให้บริการทรัพยากรหลายราย เมื่อผู้ใช้ต้องการเข้าใช้บริการของผู้ให้บริการทรัพยากร ผู้ใช้สามารถนำหลักฐานอ้างอิงตัวผู้ใช้ที่ธนาคารออกให้แสดงต่อผู้ให้บริการทรัพยากรเหล่านั้นเพื่อใช้ในการยืนยันตัวผู้ใช้ได้

เมื่อผู้ใช้ผ่านพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะออกข้อความยืนยันการพิสูจน์ตัวจริง (Authentication Assertion) ให้กับผู้ใช้ เพื่อให้ผู้ใช้นำไปแสดงต่อผู้ให้บริการทรัพยากร ถ้าผู้ให้บริการทรัพยากรเชื่อถือข้อความยืนยันนี้ ผู้ใช้ก็จะผ่านการพิสูจน์ตัวจริงจากผู้ให้บริการทรัพยากรด้วย การเฟ็ดเดอเรชันของข้อมูลสำหรับระบุผู้ใช้ (Identity Federation) ระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ให้บริการทรัพยากรเกิดขึ้นเมื่อผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ออกข้อความยืนยันให้กับผู้ใช้

ลิเบอร์ตี้โพรไฟล์ (Liberty Profile) คือ การรวมเนื้อหาแมสเซจ (Message content) ซึ่งได้แก่ แมสเซจการร้องขอ และแมสเซจการตอบสนอง และกลไลของการส่งแมสเซจ (Message

Transport mechanism) สำหรับผู้ใช้ โดยรูปที่ 2.2 จะอธิบายถึงแผนภาพการโต้ตอบของโพรไฟล์บราวเซอร์/โพสของการลงบันทึกเข้าระบบเพียงครั้งเดียว โดยโพรไฟล์นี้อธิบายการทำงานเริ่มตั้งแต่ผู้ให้บริการทรัพยากรได้รับข้อความยืนยันการพิสูจน์ตัวจริงของผู้ใช้จากผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ เพื่อทำให้เกิดการลงบันทึกเข้าระบบเพียงครั้งเดียว นอกจากนี้ยังอธิบายถึงวิธีการรวมข้อมูลสำหรับการระบุผู้ใช้ ของผู้ให้บริการทรัพยากรและผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งมีรายละเอียดดังนี้



รูปที่ 2.2 แผนภาพแสดงแผนภาพของการโต้ตอบของโพรไฟล์บราวเซอร์ / โพสของการลงบันทึกเข้าระบบเพียงครั้งเดียว [5]

แผนภาพแสดงการโต้ตอบในรูปที่ 2.2 มีการตั้งสมมติฐานว่าผู้ใช้ผ่านการพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้แล้ว ขั้นตอนแรกเมื่อผู้ใช้ร้องขอบริการจากผู้ให้บริการทรัพยากร ผู้ให้บริการทรัพยากรส่งผู้ใช้ไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิกอยู่ พร้อมส่งแมสเซจร้องขอการพิสูจน์ตัวจริง (AuthnRequest) ไปด้วย จากนั้นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นำหลักฐานการพิสูจน์ตัวจริงของผู้ใช้มาสร้างเป็นข้อความยืนยันการพิสูจน์ตัวจริง แล้วใส่ลงในแมสเซจตอบสนองการพิสูจน์ตัวจริง (AuthnResponse) แล้วส่งกลับมายังผู้ให้บริการทรัพยากร เมื่อได้รับแมสเซจตอบสนองการพิสูจน์ตัวจริงแล้ว ผู้ให้บริการทรัพยากรจะนำข้อความยืนยันที่ได้ไปตรวจสอบสิทธิในการใช้งาน ถ้าผู้ใช้มีสิทธิสามารถเข้าใช้งานได้ ผู้ให้บริการทรัพยากรก็จะส่งผลลัพธ์ของการเรียกใช้บริการนั้นกลับไปยังผู้ใช้ต่อไป

จากรูปที่ 2.2 ตัวอย่างแมสเซจร้องขอการพิสูจน์ตัวจริงในขั้นตอนที่ 3 และ4 แสดงในรูปที่ 2.3 และตัวอย่างแมสเซจตอบสนองการพิสูจน์ตัวจริงในขั้นตอนที่ 6 และ7 แสดงในรูปที่ 2.4

```
<AuthnRequest RequestID="RPCUk2ll+GVz+t1lLURp51oFvJXk" MajorVersion="1"
    MinorVersion="2" IssueInstant="2003-09-18T14:20:30Z"
    lib:consent="urn:liberty:consent:obtained">
    <ProviderID>http://ServiceProvider.com</ProviderID>
    <NameIDPolicy>federated</NameIDPolicy>
    <ForceAuthn>false</ForceAuthn>
    <IsPassive>false</IsPassive>
    <ProtocolProfile>http://projectliberty.org/profiles/brws-post</ProtocolProfile>
    <AuthnContext>
        <AuthnContextClassRef>
            http://projectliberty.org/schemas/authctx/classes/Password-ProtectedTransport
        </AuthnContextClassRef>
        <AuthnContextComparison>exact</AuthnContextComparison>
    </AuthnContext>
    <RelayState>R0lGODlhcgGSALMAAAQCAEMmCZtuMFQxDS8b</RelayState>
    <ProxyAuthn>
        <ProxyCount>1</ProxyCount>
    </ProxyAuthn>
</AuthnRequest>
```

รูปที่ 2.3 ตัวอย่างแมสเซจร้องขอการพิสูจน์ตัวจริง

```
<AuthnResponse MinorVersion="2" InResponseTo="Zon3WjJ2KL7j+bJu7MuIr4Pt2go5"
        IssueInstant="2003-09-18T14:52:14Z" Recipient=http://ServiceProvider.com
        ResponseID="hhuuja1bc744hGJn5Q9A5yvEIgS" xmlns:lib="urn:liberty:iff:2003-08"
        lib:consent="urn:liberty:consent:obtained">
    <samlp:Status>
        <samlp:StatusCode Value="samlp:Success"/>
    </samlp:Status>
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      AssertionID="e06e5a28-bc80-4ba6-9ecb-712949db686e" MajorVersion="1" MinorVersion="2"
      Issuer="http://IdentityProvider.com" IssueInstant="2003-09-18T14:52:14Z"
      xsi:type="lib:AssertionType" InResponseTo="4e7c3772-4fa4-4a0f-99e807d719ff6067c">
        <saml:Conditions NotBefore="2003-09-18T14:52:14Z"
                        NotOnOrAfter="2003-09-18T14:57:14Z">
            <saml:AudienceRestrictionCondition>
                <saml:Audience>http://ServiceProvider.com</saml:Audience>
            </saml:AudienceRestrictionCondition>
        </saml:Conditions>
        <saml:AuthenticationStatement
                AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
                AuthenticationInstant="2003-09-18T14:52:15Z"
                xsi:type="AuthenticationStatementType" SessionIndex="3"
                ReauthenticateOnOrAfter="2003-09-18T16:52:14Z">
            <saml:Subject xsi:type="SubjectType">
                <saml:NameIdentifier Format="urn:liberty:iff:nameid:federated">
                342ad3d8-93ee-4c68-be35-cc9e7db39e2b</saml:NameIdentifier>
                <saml:SubjectConfirmation>
                    <saml:ConfirmationMethod>
                        urn:oasis:names:tc:SAML:1.0:cm:artifact-01
                    </saml:ConfirmationMethod>
                </saml:SubjectConfirmation>
                <IDPProvidedNameIdentifier Format="urn:liberty:iff:nameid:federated">
```

รูปที่ 2.4 ตัวอย่างแมสเซจตอบสนองการพิสูจน์ตัวจริง

```
                342ad3d8-93ee-4c68-be35-cc9e7db39e2b</IDPProvidedNameIdentifier>
            </saml:Subject>
        </saml:AuthenticationStatement>
        <ds:Signature>
            <ds:SignedInfo>
                <ds:CanonicalizationMethod
                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod
                    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <ds:Reference URI="">
                    <ds:Transforms>
                        <ds:Transform
                            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <ds:Transform
                            Algorithm=' Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"'/>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>ZbscbqHTX9H8bBftRlWlG4Epv1A=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
        <ds:SignatureValue>
            H+q3nC3jUalj1uKUVkcC4iTFClxeZQIFF0nvHqPS5oZhtkBaDb9qITA7gIkotaB584w
            XqTXwsfsuIrwT5uL3r85Rj7IF6NeCeiy3K0+z3uewxyeZPz8wna449VNm0qNHYkgN
            ak9ViNCp0/ks5MAttoPo2iLOfaKu3wWG6d1G+DM=
        </ds:SignatureValue>
    </ds:Signature>
</saml:Assertion>
```

รูปที่ 2.4 ตัวอย่างแมสเซจตอบสนองการพิสูจน์ตัวจริง (ต่อ)

ในครั้งแรกที่ผู้ใช้ทำการลงบันทึกเข้าระบบกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เพื่อเข้าใช้บริการที่ผู้ให้บริการทรัพยากร ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะเสนอทางเลือกในการเฟ็ดเดอเรชันข้อมูลสำหรับระบุผู้ใช้เฉพาะที่ (Local identity) ที่อยู่ในผู้ให้บริการทรัพยากรกับข้อมูลที่ใช้ลงบันทึกเข้าระบบกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ เพื่อเก็บรักษาข้อมูลของผู้ใช้ที่ใช้ในการลงบันทึกเข้าระบบเพียงครั้งเดียว ซึ่งการลงบันทึกเข้าระบบเพียงครั้งเดียวเป็นวิธีที่ผู้

ให้บริการทรัพยากรหรือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ส่งความจริงว่าผู้ใช้ผ่านการพิสูจน์ตัวจริงแล้วไปให้กับผู้ให้บริการทรัพยากรหรือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อื่นๆ การลงบันทึกเข้าระบบเพียงครั้งเดียวเกิดขึ้นเมื่อมีการเฟ็ดเดอเรดข้อมูลสำหรับระบุผู้ใช้ทั้งที่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ให้บริการทรัพยากร ซึ่งวิธีที่ทำให้ผู้ใช้ผ่านการพิสูจน์ตัวจริงเรียกว่ากลไกของการพิสูจน์ตัวจริง ตัวอย่างของกลไกของการพิสูจน์ตัวจริงเช่น การใช้ชื่อผู้ใช้และรหัสผ่าน หรือการใช้ใบรับรองผ่านโพรโทคอลเอสเอสแอลในการลงบันทึกเข้าระบบ เป็นต้น

นอกจากนี้สถาปัตยกรรมของลิเบอร์ตี้แอลไลเอนซ์จะต้องมีความสามารถในการทำกิจกรรมต่อไปนี้

1. นามแฝง (Pseudonyms)

นามแฝงเป็นชื่อที่ใช้แทนชื่อผู้ใช้ โดยนามแฝงที่ใช้ในการเฟ็ดเดอเรชันระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ให้บริการทรัพยากรทั้งหมดจะต้องไม่ซ้ำกัน

2. การปิดบังชื่อ (Anonymity)

ผู้ให้บริการทรัพยากรสามารถร้องขอต่อผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ให้สร้างนามแฝงเพื่อปิดบังชื่อของผู้ใช้ โดยนามแฝงนี้สามารถนำไปร้องขอข้อมูลสำหรับผู้ใช้หรือข้อมูลของผู้ใช้ได้แต่ไม่อยู่ในข้อกำหนดของลิเบอร์ตี้

3. การลงบันทึกออกแบบครอบคลุม (Global Logout)

เมื่อผู้ใช้ลงบันทึกออกที่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะต้องมีการแจ้งการลงบันทึกมายังผู้ให้บริการทรัพยากรที่ผู้ใช้ติดต่ออยู่

2.1.2 ภาษาเอสเอเอ็มแอล [6]

ภาษาเอสเอเอ็มแอลกำหนดไวยากรณ์และความหมายสำหรับข้อความยืนยัน (Assertion) โพรโทคอลการร้องขอ (Protocol Request) และโพรโทคอลการตอบสนอง (Protocol Response) โดยข้อมูลที่สร้างขึ้นจะถูกฝังลงในแมสเซจรูปแบบอื่น เช่น โซพแมสเซจ (SOAP Message) เพื่อส่งต่อไปยังผู้รับแมสเซจ เช่น ฟอร์มโพสของเอชทีทีพี (HTTP form POST) และโซพแมสเซจที่เข้ารหัสภาษาเอ็กซ์เอ็มแอล (eXtensible Markup Language - XML) เป็นต้น

ภาษาเอสเอเอ็มแอลเป็นโครงร่าง (Framework) ของภาษาเอ็กซ์เอ็มแอลสำหรับการแลกเปลี่ยนข้อมูลความปลอดภัยบนอินเทอร์เน็ต ซึ่งข้อมูลความปลอดภัยนี้แสดงความหมายในรูปแบบของข้อความยืนยันเกี่ยวกับผู้กระทำ โดยที่ผู้กระทำ คือ เอนทิตีที่มีข้อมูลสำหรับระบุผู้ใช้ในบางโดเมนของการรักษาความปลอดภัย ตัวอย่างของผู้กระทำได้แก่ บุคคลซึ่งบ่งชี้โดยอีเมลในโดเมนของอินเทอร์เน็ตดีเอ็นเอส (Domain Name System - DNS)

ข้อความยืนยันเป็นข้อมูลเกี่ยวกับการพิสูจน์ตัวจริงของผู้กระทำ รวมถึงแอททริบิวท์ของผู้กระทำและผลของการพิสูจน์สิทธิ (Authorization Decision) ว่าผู้กระทำได้รับการอนุญาตให้เข้าใช้ทรัพยากรนั้นๆ หรือไม่ ข้อความยืนยันออกโดยองค์กรที่มีอำนาจกำหนดข้อความยืนยันของเอสเอเอ็มแอล (SAML Authority) ได้แก่ องค์กรที่ทำหน้าที่พิสูจน์ตัวจริง (Authentication Authority) องค์กรเกี่ยวกับแอททริบิวท์ (Attribute Authority) และองค์กรตัดสินใจเกี่ยวกับนโยบาย (Policy Decision Point) เอสเอเอ็มแอลนิยามโพรโทคอลที่ผู้ใช้สามารถร้องขอข้อความยืนยันจากองค์กรที่มีอำนาจกำหนดข้อความยืนยันของเอสเอเอ็มแอลและรับผลการตอบสนองได้ โพรโทคอลนี้ประกอบด้วยรูปแบบแมสเซจของการร้องขอและการตอบสนอง ซึ่งสามารถผูกเข้ากับรูปแบบของแมสเซจและโพรโทคอลที่ใช้สื่อสารกันได้หลายรูปแบบ

เป้าหมายหลักของเอสเอเอ็มแอล คือ การลงบันทึกเข้าระบบเพียงครั้งเดียว เพื่อให้ผู้ใช้พิสูจน์ตัวจริงเพียงครั้งเดียวภายในหนึ่งโดเมนและสามารถใช้ทรัพยากรในโดเมนอื่นๆ ได้โดยไม่ต้องทำการพิสูจน์ตัวจริงอีก

2.1.3 โครงสร้างการรักษาความปลอดภัยเชิงกริด [7-9]

โครงสร้างการรักษาความปลอดภัยเชิงกริดเป็นแนวคิดหนึ่งสำหรับการรักษาความปลอดภัยระหว่างองค์กร ซึ่งพัฒนาภายใต้โครงการการวิจัยโกลบัส (Globus) เพื่อสนับสนุนสภาพแวดล้อมของคอมพิวเตอร์ที่มีการทำงานแบบกระจาย โครงสร้างการรักษาความปลอดภัยเชิงกริดนี้ประกอบด้วยโพรโทคอล ไลบรารี (Library) และเครื่องมือ ซึ่งอนุญาตให้ผู้ใช้และโปรแกรมประยุกต์สามารถเข้าใช้งานทรัพยากรกริดได้อย่างปลอดภัย โครงสร้างการรักษาความปลอดภัยเชิงกริดมีหน้าที่จัดการเกี่ยวกับการทำงานระหว่างองค์กรต่างๆ และเชื่อมต่อโซลูชั่นของการรักษาความปลอดภัยที่แตกต่างกันระหว่างองค์กร โดยโครงสร้างการรักษาความปลอดภัยเชิงกริดสร้างขึ้นเพื่อรองรับความต้องการดังต่อไปนี้

1. ความต้องการที่จะมีวิธีการสื่อสารที่ปลอดภัยระหว่างอิลิเมนต์ของกริดเชิงคำนวณ (Computational Grid)
2. ความต้องการที่จะสนับสนุนการรักษาความปลอดภัยข้ามขอบเขตขององค์กร โดยไม่มีระบบการรักษาความปลอดภัยส่วนกลาง
3. ความต้องการที่จะสนับสนุนการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับผู้ใช้งานกริด รวมถึงการส่งต่อข้อมูลสำหรับระบุผู้ใช้เพื่อใช้ในการทำงานร่วมกันของทรัพยากร

โครงสร้างการรักษาความปลอดภัยเชิงกริดประกอบด้วยลักษณะที่สำคัญดังต่อไปนี้

2.1.3.1 **โครงสร้างของกุญแจสาธารณะ** (Public Key Infrastructure - PKI)

โครงสร้างการรักษาความปลอดภัยเชิงกริดใช้พื้นฐานของโครงสร้างของกุญแจสาธารณะโดยกำหนดชื่อเฉพาะ (Distinguished Name - DN) ให้กับเอนทิตีของผู้ใช้และทรัพยากร วิธีการพิสูจน์ตัวจริงด้วยการรักษาความปลอดภัยเชิงกริดนี้ทำโดยการพิสูจน์ว่าผู้ใช้หรือทรัพยากรนั้นเป็นเอนทิตีที่ถูกระบุด้วยชื่อเฉพาะหรือไม่ โดยการแสดงหลักฐานอ้างอิงตัวผู้ใช้ และพิสูจน์ความเป็นเจ้าของกุญแจส่วนบุคคล (Private Key) แต่ละเอนทิตีจะมีหลักฐานรับรองเชิงกริด ซึ่งประกอบด้วยหลักฐานอ้างอิงตัวผู้ใช้ และกุญแจในการเข้ารหัสลับ (กุญแจส่วนบุคคล) หลักฐานอ้างอิงตัวผู้ใช้จะใช้มาตรฐานเอ็กซ์ 509 เวอร์ชัน 3 (X.509v3) โดยหลักฐานอ้างอิงตัวผู้ใช้เป็นการเชื่อมกันระหว่างชื่อเฉพาะของเอนทิตีกับกุญแจส่วนบุคคลโดยจะลงลายเซ็นดิจิทัล (Digital Signature) จากองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ (Certificate Authority - CA) เอนทิตีสามารถพิสูจน์ตัวจริงได้โดยการแสดงหลักฐานอ้างอิงตัวผู้ใช้และพิสูจน์ให้เห็นว่าเอนทิตีนั้นเป็นเจ้าของกุญแจส่วนบุคคล

2.1.3.2 **หลักฐานอ้างอิงตัวผู้ใช้**

แนวคิดหลักของการพิสูจน์ตัวจริงของโครงสร้างการรักษาความปลอดภัยเชิงกริด คือ หลักฐานอ้างอิงตัวผู้ใช้ โดยผู้ใช้และบริการบนกริดจะใช้หลักฐานอ้างอิงตัวผู้ใช้ในการแสดงตัว ซึ่งหลักฐานอ้างอิงตัวผู้ใช้นี้เก็บข้อมูลที่จำเป็นสำหรับการแสดงตัวและการพิสูจน์ตัวจริงของผู้ใช้ ถ้าผู้ให้บริการเชื่อถือหลักฐานอ้างอิงตัวผู้ใช้ขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้แล้ว ผู้รับจะเชื่อถือหลักฐานอ้างอิงตัวผู้ใช้ของผู้กระทำด้วย โดยหลักฐานอ้างอิงตัวผู้ใช้ประกอบด้วยข้อมูลสำคัญ 4 ส่วนได้แก่

1. ชื่อผู้กระทำใช้ ระบุบุคคล หรือ อ็อบเจกต์ (Object) ที่เป็นเจ้าของหลักฐานอ้างอิงนี้
2. กุญแจสาธารณะซึ่งผู้กระทำเป็นเจ้าของ
3. หลักฐานขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ใช้เพื่อรับรองว่าผู้กระทำเป็นเจ้าของหลักฐานอ้างอิงตัวผู้ใช้จริง
4. ลายเซ็นดิจิตอลขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้

2.1.3.3 **ขั้นตอนวิธีการพิสูจน์ตัวจริง** (Authentication Algorithm)

โครงสร้างการรักษาความปลอดภัยเชิงกริดใช้เอสเอสแอล เวอร์ชัน 3 (Secure Socket Layer Version3 – SSLv3) สำหรับโพรโทคอลการพิสูจน์ตัวจริงร่วมกัน โดยเมื่อ 2 ฝ่ายต่างก็มี

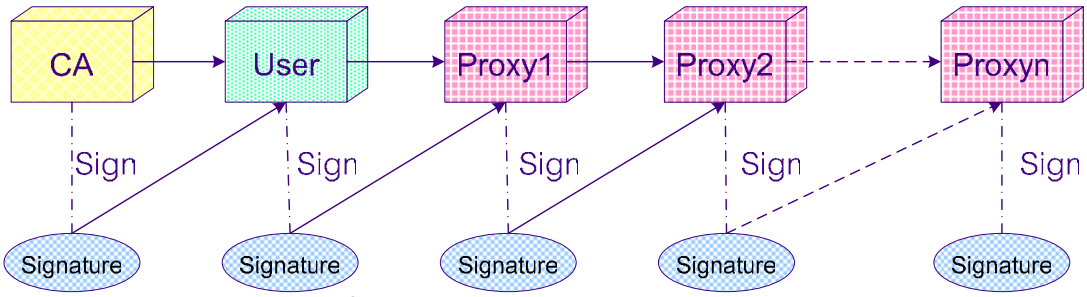
หลักฐานอ้างอิงตัวผู้ใช้และต่างก็เชื่อถือในองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ซึ่งเซ็นหลักฐานอ้างอิงตัวผู้ใช้ของทั้งคู่แล้วทั้งสองฝ่ายก็สามารถพิสูจน์อีกฝ่ายว่าเป็นตัวจริงได้

การรักษาความปลอดภัยของกุญแจส่วนบุคคลทำโดยเข้ารหัสไฟล์กุญแจส่วนบุคคลโดยใช้วลีผ่าน (Pass Phrase) เมื่อต้องการใช้งานกุญแจส่วนบุคคล ผู้ใช้จะต้องใส่วลีผ่าน เพื่อถอดรหัสไฟล์ที่เก็บกุญแจส่วนบุคคล

โพรโทคอลการพิสูจน์ตัวจริงจะตรวจสอบเอนทิตี และทำการเปลี่ยนชื่อของเอนทิตี จากชื่อลงบันทึกเข้า (Login Name) เป็นชื่อผู้ใช้เฉพาะที่ (Local username) เพื่อให้ระบบการรักษาความปลอดภัยรู้จักเอนทิตีนั้น โครงสร้างการรักษาความปลอดภัยเชิงกริดใช้แมบไฟล์ (Map file) เชิงข้อความในการแปลงระหว่างชื่อผู้ใช้ส่วนกลางและชื่อผู้ใช้เฉพาะที่

2.1.3.4 การมอบอำนาจ (Delegation) และการลงบันทึกเข้าระบบเพียงครั้งเดียว

สิ่งที่สำคัญสำหรับโปรแกรมประยุกต์แบบกระจาย คือ การประมวลผลของโปรแกรมประยุกต์ที่มีความสามารถในการทำงานแทนผู้ใช้บนกริดได้ ซึ่งการทำงานแทนผู้ใช้ดังกล่าวอาจจะต้องถูกพิสูจน์ตัวจริงหลายครั้งในระยะเวลาสั้นๆ เช่น การเก็บผลของการคำนวณไว้ในระบบการจัดเก็บข้อมูล ดังนั้นโครงสร้างการรักษาความปลอดภัยเชิงกริดจึงเตรียมความสามารถในการมอบอำนาจให้กับการประมวลผลที่อยู่บนแม่ข่ายระยะไกล (Remote host) โดยการสร้างตัวแทน (Proxy) เพื่อลดจำนวนครั้งที่ผู้ใช้จะต้องใส่วลีผ่านเพื่อถอดรหัสกุญแจส่วนบุคคลในการพิสูจน์ตัวจริง ตัวแทนประกอบด้วยหลักฐานอ้างอิงตัวผู้ใช้ใหม่ซึ่งบรรจุกุญแจสาธารณะใหม่ และกุญแจส่วนบุคคลใหม่ หลักฐานอ้างอิงตัวผู้ใช้ใหม่ประกอบด้วยหลักฐานเกี่ยวกับผู้ใช้ของเจ้าของ ซึ่งแตกต่างจากเดิมเพียงเล็กน้อยเพื่อบ่งชี้ว่าเป็นตัวแทน เจ้าของตัวแทนจะเซ็นหลักฐานอ้างอิงตัวผู้ใช้ใหม่นี้แทนองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ ดังแสดงในรูปที่ 2.5 เนื่องจากตัวแทนมีอายุการใช้งานจำกัด ดังนั้นหลักฐานอ้างอิงตัวผู้ใช้ใหม่จึงต้องบอกระยะเวลาที่สามารถใช้งานตัวแทนไว้ด้วย การเก็บรักษากุญแจส่วนบุคคลของตัวแทนสามารถเก็บโดยไม่ต้องเข้ารหัสไว้ในระบบแฟ้มข้อมูล (File System) ซึ่งมีการป้องกันแฟ้มข้อมูลนี้โดยใช้การอนุญาตของระบบแฟ้มข้อมูล โดยคนที่ไม่ใช่เจ้าของไม่สามารถเข้าถึงแฟ้มข้อมูลได้ ผู้ใช้สามารถใช้หลักฐานอ้างอิงตัวผู้ใช้ตัวแทนและกุญแจส่วนบุคคลสำหรับการพิสูจน์ตัวจริงร่วมกัน (Mutual Authentication) ได้โดยไม่ต้องใส่วลีผ่านทุกครั้งเพื่อเอากุญแจส่วนบุคคลของผู้ใช้มาทำการพิสูจน์ตัวจริง



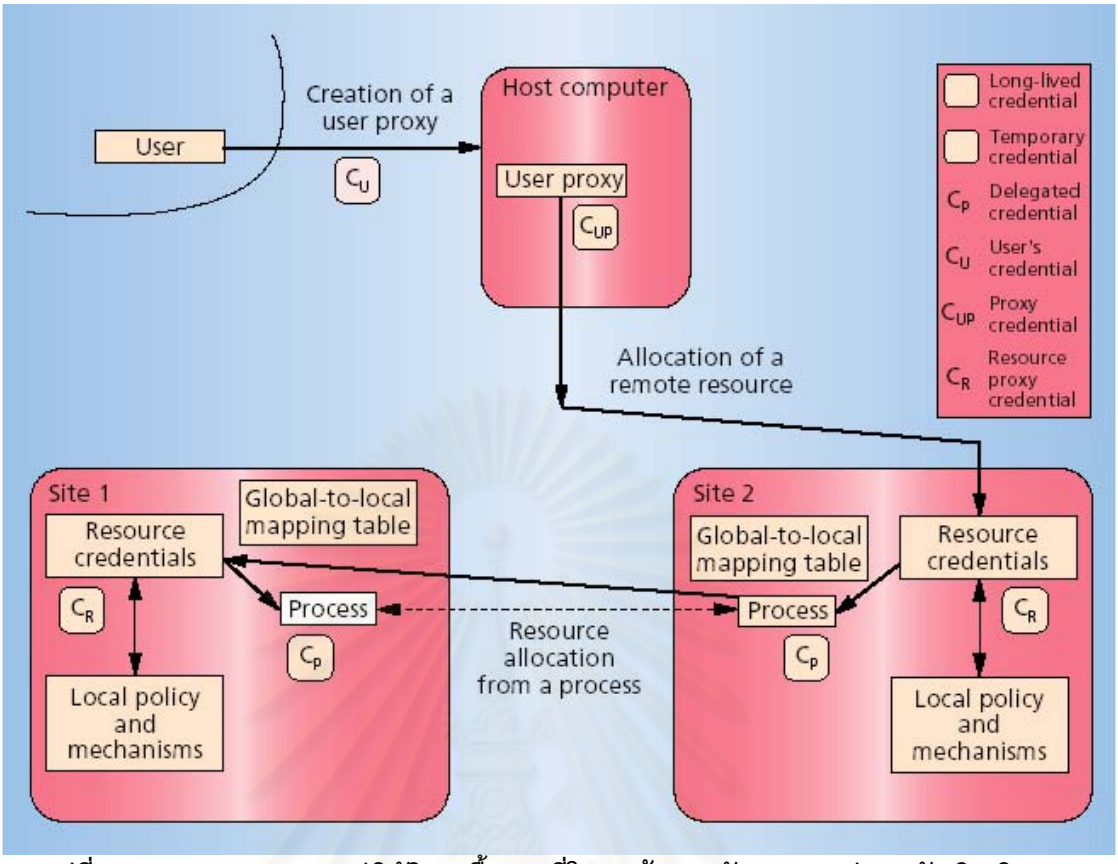
รูปที่ 2.5 **ลำดับการเซ็นหลักฐานอ้างอิงตัวผู้ใช้**

การพิสูจน์ตัวจริงร่วมกันโดยฝ่ายหนึ่งใช้ตัวแทนจะมีวิธีการที่แตกต่างจากเดิมเล็กน้อย คือ ฝ่ายที่ทำการพิสูจน์ตัวจริงของตัวแทนจะได้รับทั้งหลักฐานอ้างอิงตัวผู้ใช้ของตัวแทนและหลักฐานอ้างอิงตัวผู้ใช้ของเจ้าของตัวแทน ซึ่งระหว่างการพิสูจน์ตัวจริงจะใช้กุญแจสาธารณะของเจ้าของที่บรรจุในหลักฐานอ้างอิงตัวผู้ใช้ของเจ้าของในการตรวจสอบลายเซ็นบนหลักฐานอ้างอิงตัวผู้ใช้ของตัวแทน ส่วนกุญแจสาธารณะขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้จะใช้เพื่อตรวจสอบลายเซ็นของหลักฐานอ้างอิงตัวผู้ใช้ของเจ้าของ ซึ่งทำให้เกิดลูกโซ่ของความเชื่อถือ (Trust chain) จากองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ไปยังตัวแทนผ่านเจ้าของ

2.1.3.5 การกำหนดนโยบายสำหรับการตรวจสอบสิทธิ

ทรัพยากรแต่ละทรัพยากรสามารถกำหนดนโยบายขั้นต้นในการอนุญาตให้ผู้ร้องขอเข้าใช้ระบบหรือไม่ โครงสร้างการรักษาความปลอดภัยเชิงกริดกำหนดสิทธิในการเข้าใช้ระบบของผู้ใช้ลงในรายการควบคุมการเข้าถึง (Access Control List – ACL)

จากรูปที่ 2.6 แสดงขั้นตอนในการมอบหมายสิทธิให้กับการประมวลผลที่แม่ข่ายระยะไกล โดยผู้ใช้จะทำการพิสูจน์ตัวจริงด้วยวิธีกุญแจสาธารณะ เมื่อผ่านการพิสูจน์จะได้หลักฐานอ้างอิงตัวผู้ใช้ของผู้ใช้ (C_U) จากนั้นเมื่อต้องการมอบหมายสิทธิให้กับการประมวลผลจะสร้างหลักฐานอ้างอิงตัวผู้ใช้ของตัวแทน (C_{UP}) แล้วส่งการร้องขอไปยังทรัพยากรระยะไกล ซึ่งมีหลักฐานอ้างอิงตัวผู้ใช้แทนของทรัพยากร (C_R) และทำการตรวจสอบสิทธิในการเข้าใช้ พร้อมทั้งทำการแปลงหลักฐานที่แสดงตัวผู้ใช้จากสาธารณะให้กลายเป็นหลักฐานเฉพาะที่ เมื่อผ่านการตรวจสอบสิทธิแล้วจะสามารถสร้างการประมวลผลขึ้นที่ทรัพยากรระยะไกลดังกล่าวได้โดยจะมีหลักฐานอ้างอิงตัวผู้ใช้ในการมอบสิทธิของการประมวลผลของตัวเอง (C_P)

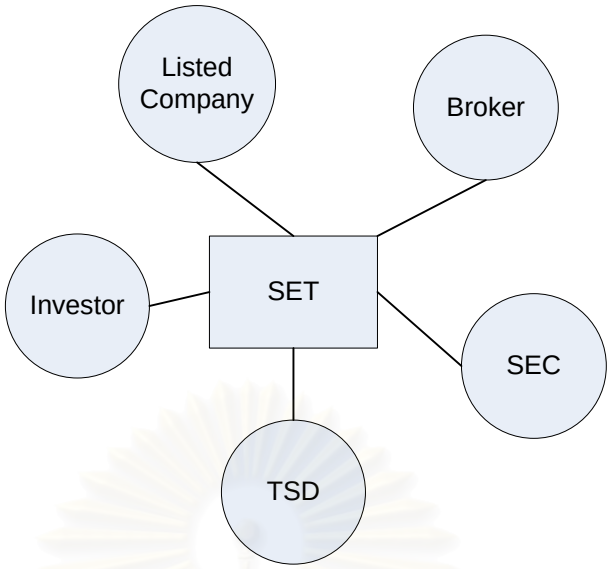


รูปที่ 2.6 แผนภาพแสดงการปฏิบัติการพื้นฐานที่โครงสร้างการรักษาความปลอดภัยเชิงกริด [7]

2.1.4 การรักษาความปลอดภัยของตลาดหลักทรัพย์ในปัจจุบัน

การดำเนินธุรกิจของตลาดหลักทรัพย์มีความจำเป็นต้องติดต่อกับองค์กรอื่นๆ เมื่อมีการติดต่อกันระหว่างองค์กร ตลาดหลักทรัพย์จำเป็นที่จะต้องมีระบบการรักษาความปลอดภัยเพื่อป้องกันการบุกรุกของผู้ที่ไม่มีสิทธิที่จะใช้งาน ซึ่งการทำงานของตลาดหลักทรัพย์ในปัจจุบันมีการติดต่อกับองค์กรต่างๆ ได้แก่

1. ศูนย์รับฝากหลักทรัพย์ (Thailand Security Depository - TSD)
2. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (Securities and Exchange Commission - SEC)
3. บริษัทนายหน้าซื้อขายหลักทรัพย์ (Broker)
4. บริษัทจดทะเบียน (Listed Company)
5. ผู้ลงทุน (Investor)



รูปที่ 2.7 องค์กรที่ติดต่อกับตลาดหลักทรัพย์ในปัจจุบัน

2.1.4.1 รูปแบบการรักษาความปลอดภัยของตลาดหลักทรัพย์

ตลาดหลักทรัพย์มีลักษณะการทำงานเหมือนรูปแบบขององค์กรเสมือน ซึ่งมีการติดต่อธุรกิจกับองค์กรต่างๆ โดยทางตลาดหลักทรัพย์ได้เปิดให้บริการแก่ผู้ใช้ทั้งภายในและภายนอกตลาด ดังนั้นเพื่อการรักษาความปลอดภัย ตลาดหลักทรัพย์ต้องเตรียมมาตรการสำหรับการเข้าใช้ระบบเพื่อป้องกันการบุกรุกจากผู้ที่ไม่มีสิทธิ โดยมีการแบ่งระดับการตรวจสอบสิทธิออกเป็น 2 ประเภท ได้แก่ ระดับเครือข่าย และระดับโปรแกรมประยุกต์ ซึ่งมีรายละเอียดดังนี้

1. ระดับเครือข่าย (Network Level)

การป้องกันในระดับเครือข่ายนี้ ระบบจะอนุญาตให้เครื่องของผู้ใช้ที่มีสิทธิสามารถเข้าถึงระบบที่ให้บริการของตลาดหลักทรัพย์ได้เท่านั้น โดยกำหนดระเบียบวิธีการในการควบคุมตามประเภทของผู้ใช้ที่ติดต่อกับระบบงานในตลาดหลักทรัพย์ออกเป็น 2 ประเภท ได้แก่

2. ผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์

3. กำหนดกลุ่มเลขที่อยู่ไอพี (IP address) ให้กับระบบของบริษัทนายหน้าซื้อขายหลักทรัพย์แต่ละรายเท่า ๆ กัน ตัวอย่างเช่น ระบบของนายหน้าซื้อขายหลักทรัพย์เอได้รับกลุ่มเลขที่อยู่ไอพีที่สามารถใช้ได้ คือ ตั้งแต่ 10.10.10.10 ถึง 10.10.10.20

4. กำหนดโพรโทคอลที่อนุญาตให้ระบบของนายหน้าซื้อขายหลักทรัพย์สามารถติดต่อเข้ามาได้ เช่น อนุญาตให้บริษัทเอสามารถติดต่อกับตลาดหลักทรัพย์ได้ผ่านทางเทลเน็ต (Telnet) แต่ไม่อนุญาตให้บริษัทบีติดต่อกับตลาดหลักทรัพย์ในวิธีเดียวกันนี้ได้

การป้องกันในระดับนี้ ระบบของตลาดหลักทรัพย์จะตรวจสอบเพียงว่าเลขที่อยู่ไอพีของเครื่องที่ติดต่อเข้ามานั้นอยู่ในกลุ่มเลขที่อยู่ไอพีของบริษัทนายหน้าซื้อขายหลักทรัพย์รายนั้นหรือไม่

ถ้าเลขที่อยู่ไอพีของเครื่องถูกต้องตามที่ตลาดหลักทรัพย์กำหนดระบบจะอนุญาตให้ติดต่อกับระบบของตลาดหลักทรัพย์ได้ แต่ถ้าไม่ถูกต้องจะไม่สามารถติดต่อกับระบบของตลาดหลักทรัพย์ได้

1. ผู้ใช้ระบบภายในตลาดหลักทรัพย์ จะมีการกำหนดเลขที่อยู่ไอพีของเครื่องที่สามารถเข้าใช้ระบบได้ มักจะทำเฉพาะระบบที่ต้องการความปลอดภัยสูง

2. ระดับโปรแกรมประยุกต์ (Application Level)

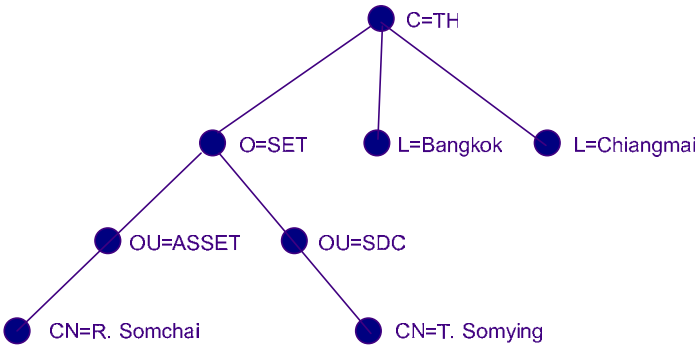
การอนุญาตในระดับโปรแกรมประยุกต์ ทำโดยกำหนดชื่อผู้ใช้และรหัสผ่านให้กับผู้ใช้งานทั้งระบบภายในตลาดหลักทรัพย์และระบบบริษัทนายหน้าซื้อขายหลักทรัพย์ที่ติดต่อเข้ามาในตลาดหลักทรัพย์เพื่อใช้ในการลงบันทึกเข้าระบบ และมีการกำหนดโควตาจำนวนชื่อผู้ใช้ของแต่ละแผนก นอกจากนี้ชื่อผู้ใช้แต่ละชื่อจะมีลำดับความสำคัญไม่เท่ากันขึ้นอยู่กับตำแหน่งและหน้าที่ในองค์กรของผู้ใช้ โดยลำดับความสำคัญเป็นตัวกำหนดการกระทำที่ผู้ใช้สามารถทำได้ เช่น อ่านอย่างเดียว อ่านและแก้ไข แก้ไขเท่านั้น หรือส่งข้อมูลได้เท่านั้น ทั้งนี้การกระทำของผู้ใช้แต่ละคนยังมีความแตกต่างกันอีกด้วย เช่น ผู้ใช้ที่เป็นผู้จัดการสามารถแก้ไขข้อมูลของแผนกได้ทั้งหมด แต่พนักงานสามารถแก้ไขข้อมูลได้เพียง 2 ข้อมูลเท่านั้น

2.1.4.2 **การกำหนดนโยบายของการใช้ระบบงานต่าง ๆ**

การกำหนดนโยบายของการใช้ระบบงานจะถูกกำหนดโดยผู้อำนวยการฝ่ายซึ่งเป็นหัวหน้าของแต่ละฝ่ายงาน แต่ถ้าเป็นนโยบายที่เกี่ยวข้องกับหลายฝ่ายงานจะตั้งคณะทำงานขึ้นมาเพื่อกำหนดนโยบายขององค์กร

2.1.5 **เนมสเปซของไดเรกทอรีเอ็กซ์** 500 [10]

การกำหนดเนมสเปซของไดเรกทอรีได้มีการกำหนดโครงสร้างของเนมสเปซให้มีความคล่องตัวในการออกแบบ โครงสร้างการกำหนดเนมสเปซของไดเรกทอรีโพรโทคอลเอ็กซ์ 500 จะกำหนดประเทศ (Country) หรือตัวอักษรซี (c) ไว้ที่ส่วนบนสุดของไดเรกทอรีถัดจากประเทศ จะเป็นชื่อขององค์กร (Organization) หรือ ตัวอักษรโอ (o) ตัวอย่างของโครงสร้างการกำหนดเนมสเปซดังรูปที่ 2.8



รูปที่ 2.8 โครงสร้างการกำหนดเนมสเปซในเอ็กซ์ 500

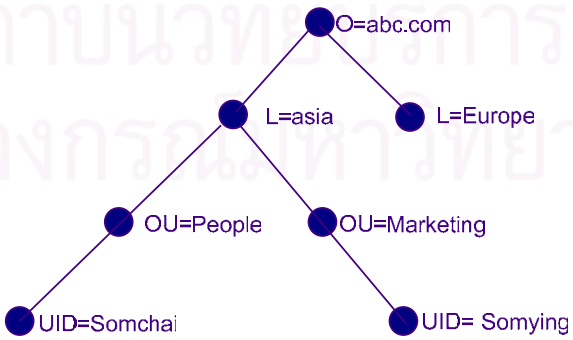
โครงสร้างพื้นฐานของไดเรกทอรีเป็นแบบลำดับขั้น (Hierachical) หรือโครงสร้างแบบต้นไม้ (Tree Structure) ไดเรกทอรีสามารถกำหนดเนมสเปซแบบชั้นเดียว (One-level Hierarchical) ได้โดยจะอาศัยการอ้างชื่อ (alias) โดยรูปแบบของการกำหนดเนมสเปซที่มีใช้กันอยู่ในระบบของไดเรกทอรีสามารถที่จะแบ่งออกเป็น 3 ประเภท ได้แก่

1. ไดเรกทอรีเอ็กซ์ 500 (Traditional X.500)

การกำหนดเนมสเปซของไดเรกทอรีตามรูปแบบนี้ เนมสเปซที่อยู่บนสุดจะใช้ประเทศเป็นตัวกำหนด ใช้อักษรย่อซี (c) แล้วตามด้วยชื่อองค์กร ตัวอย่างการกำหนดเนมสเปซในรูปแบบนี้เช่น o=SET,c=TH และ L=Bangkok,c=TH เป็นต้น ตัวอย่างการกำหนดเนมสเปซแบบไดเรกทอรีเอ็กซ์ 500 แสดงดังรูปที่ 2.8

2. โดเมนเนม (Domain Name Alignment)

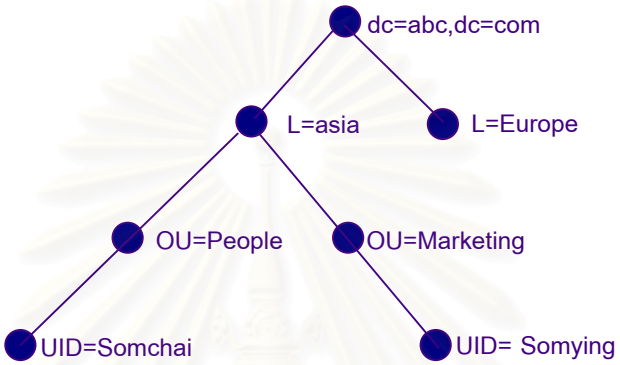
การกำหนดเนมสเปซของไดเรกทอรีตามรูปแบบของโดเมนเนม เริ่มมีการใช้ในไดเรกทอรีโพรโทคอลแอลแดบเวอร์ชัน 3 (LDAPv3) การกำหนดเนมสเปซแบบโดเมนเนมเป็นที่นิยมในการใช้งานเนื่องจากสามารถที่จะจำได้ง่าย รูปแบบเนมสเปซแบบนี้ จะใช้องค์กรอยู่ส่วนบนสุดของไดเรกทอรี เช่น o=abc.com เป็นต้น ตัวอย่างการกำหนดเนมสเปซแสดงดังรูปที่ 2.9



รูปที่ 2.9 การกำหนดเนมสเปซรูปแบบโดเมนเนม

3. โดเมนคอมโพเนนท์ (Domain Component)

รูปแบบของการกำหนดเนมสเปซแบบโดเมนคอมโพเนนท์ เริ่มมีการนำมาใช้งานตั้งแต่ไดเรกทอรีโพรโทคอลแอบแดบเวอร์ชัน 2 (LDAPv2) โดยจะใช้ตัวอักษรดีซี (dc) นำหน้าและจะใช้เครื่องหมายจุลภาค (,) คั่นระหว่างชื่อโดเมน เช่น โดเมน abc.com เมื่อเขียนอยู่ในรูปของโดเมนคอมโพเนนท์จะได้ dc=abc,dc-com ตัวอย่างการกำหนดเนมสเปซแบบโดเมนคอมโพเนนท์แสดงดังรูปที่ 2.10



รูปที่ 2.10 การกำหนดเนมสเปซแบบโดเมนคอมโพเนนท์

ไดเรกทอรีเอ็กซ์ 500 กำหนดชนิดของแอททริบิวท์ที่นิยมใช้ในการกำหนดเนมสเปซ ดังตารางที่ 2.1

ตารางที่ 2.1 ชนิดของแอททริบิวท์ที่นิยมใช้ในการกำหนดเนมสเปซ

Attribute Type	Strings
CommonName	cn
LocalityName	l
StateOrProvinceName	st
OrganizationName	o
OrganizationUnitName	ou
CountryName	c
StreetAddress	street
DomainComponent	dc
UserID	uid

2.2 งานวิจัยที่เกี่ยวข้อง

จากการศึกษาเบื้องต้นพบว่ามีงานวิจัยที่เกี่ยวข้องจำนวนทั้งสิ้น 2 งานวิจัย โดยแบ่งออกเป็นงานวิจัยที่เกี่ยวข้องกับการตั้งเนมสเปซ (Namespace) และงานวิจัยที่เกี่ยวข้องกับการพิสูจน์ตัวจริงและการพิสูจน์สิทธิ ได้แก่

งานวิจัยที่เกี่ยวข้องกับการกำหนดเนมสเปซ ได้แก่

"Distributed Security Manangement Using LDAP Directories": *Edgard Jamhour*

งานวิจัยที่เกี่ยวข้องกับการกับการพิสูจน์ตัวจริงและการพิสูจน์สิทธิ ได้แก่

"A Community Authorization Service for Group Collaboration": *Laura Pearlman, Von Welch, Ian Foster, Carl Kesselman and Steven Tuecke* มีรายละเอียดดังต่อไปนี้

2.2.1 งานวิจัย "Distributed Security Management Using LDAP Directories" [12]

งานวิจัยนี้เกี่ยวข้องกับการจัดการการเข้าถึงของเครือข่ายขนาดใหญ่ซึ่งแต่ละองค์กรภายในเครือข่ายมีการจัดการที่เป็นอิสระจากกัน โดยการกำหนดกลยุทธ์ในการจัดการองค์กรเสมือนจากมุมมองแบบรวมศูนย์ โดยปราศจากการเอาภาวะอิสระของการบริหาร (Administration Autonomy) ของแต่ละสมาชิกออก

งานวิจัยนี้ทำการกำหนดเค้าร่างของอ็อบเจกต์คลาสของแอลแดบสำหรับการติดต่อกันระหว่างองค์กรในองค์กรเสมือน โดยแนวคิดของงานวิจัยนี้คือองค์กรเสมือนเป็นกลุ่มของโดเมนที่ได้รับการป้องกัน (Protected Domains) ซึ่งกลุ่มโดเมนที่ได้รับการป้องกันประกอบด้วยกลุ่มแม่ข่ายที่รักษาความปลอดภัยโดยเครื่องมือป้องกัน เช่น ไฟร์วอลล์ (Firewall) และโดเมนที่ได้รับการป้องกันสามารถบรรจุโดเมนที่ได้รับการป้องกันอื่นๆ ได้ โดยงานวิจัยได้นิยามอ็อบเจกต์คลาส ดังตารางด้านล่างนี้

ตารางที่ 2.2 อ็อบเจกต์คลาสที่ใช้ในองค์กรเสมือน

Class	Description
Virtual Organization RDN=O	Represents a collection of corporate networks that cooperates by sharing resources.
Protected Domain RDN=PD	Represents a collection of one or more hosts protected by the same enforcer device.
Enforcer Device RDN=ED	Typically, a firewall implemented in a host with multiple interfaces or a router.

Class	Description
Directory Enabler RDN=DE	Computer responsible for offering directory enabled capabilities for other devices in the network.
Server RDN=S	A computer that hosts a shared resource.
Shared Resource RDN=SR	Any sharable resource such as files, printers and services (e.g. email, web servers and databases).
Access Control Entry RDN=ACE	An explicit permission for a client or a group of clients to access a shared resource (e.g. “group A”, “read, write, execute”).
Client RDN=C	A user or service that can access a shared resource in the protected domain.
Group RDN=G	A group of clients with similar access rights.

2.2.2 งานวิจัย “A Community Authorization Service for Group Collaboration” [13, 14]

งานวิจัยนี้จึงเสนอวิธีการใหม่ในการใช้แทน (Representation), การบำรุงรักษา (Maintenance), และสร้างนโยบายสำหรับการบังคับใช้ที่สามารถปรับขนาด (Scalable) ของวิธีการระบุและบังคับใช้นโยบายเหล่านี้ วิธีการนี้อนุญาตให้ผู้ให้บริการทรัพยากรสามารถมอบสิทธิสำหรับการรักษานโยบายการควบคุมการเข้าถึงอย่างละเอียด (Fine-grained Access Control Policy) ในชุมชน และยังคงรักษาการควบคุมทรัพยากรทั้งหมดของผู้ให้บริการทรัพยากรได้

ในงานวิจัยนี้ สร้างเซิร์ฟเวอร์ซีเอเอส (Community Authorization Service Server - CAS Server) มีหน้าที่รับผิดชอบในการจัดการนโยบายควบคุมการเข้าถึงทรัพยากรในชุมชน เซิร์ฟเวอร์ซีเอเอสบรรจุหน่วยข้อมูล (Entries) สำหรับองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้, ผู้ใช้, เซิร์ฟเวอร์ และทรัพยากรที่ประกอบกันเป็นชุมชน นอกจากนี้ เซิร์ฟเวอร์ซีเอเอสยังบรรจุข้อความสั่งนโยบาย (Policy Statements) ที่กำหนดว่าจะอนุญาตผู้ใช้หรือกลุ่มใด, ทรัพยากรหรือกลุ่มของทรัพยากรไหนที่ได้รับการอนุญาตให้ใช้และการอนุญาตอะไรที่สามารถใช้งานได้

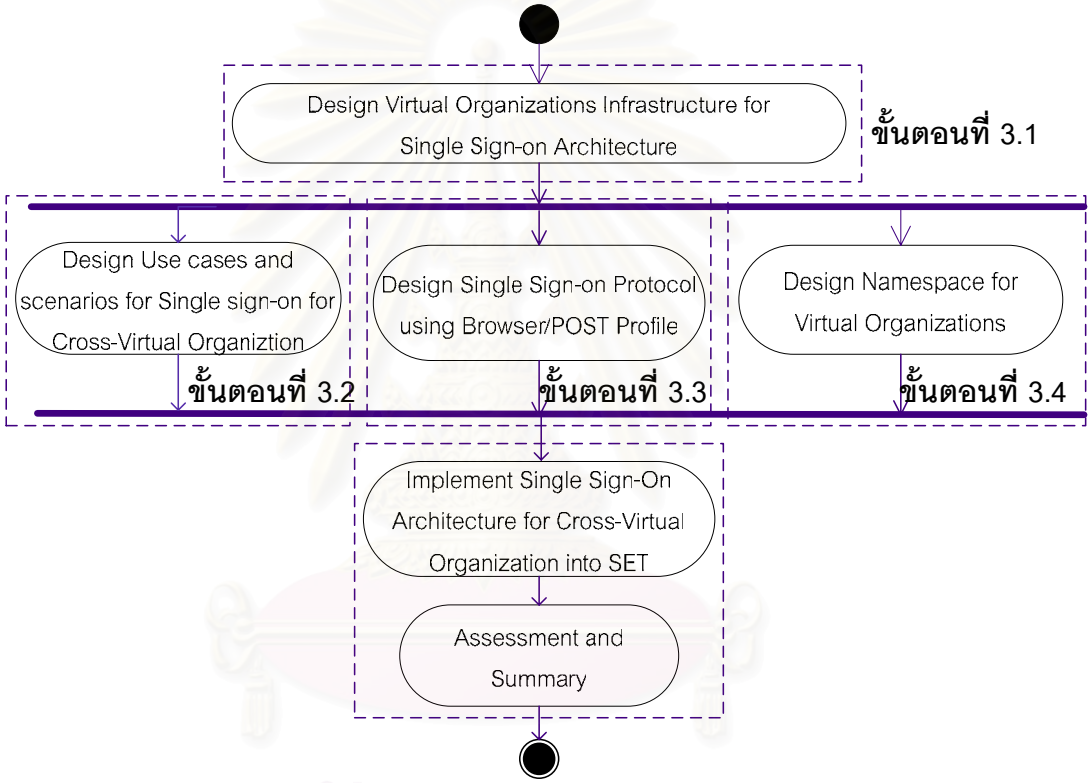
เซิร์ฟเวอร์ซีเอเอสให้สิทธิแก่สมาชิกในชุมชนโดยใช้กลไกของการมอบอำนาจของโครงสร้างการรักษาความปลอดภัยเชิงกริด โดยการให้หลักฐานอ้างอิงตัวผู้ใช้แทนและเพิ่มความสามารถในการมอบอำนาจให้สนับสนุนการกำหนดนโยบายเพื่ออนุญาตให้ผู้มอบอำนาจ

สามารถจำกัดสิทธิที่จะอนุญาตได้ ที่เรียกว่า ตัวแทนจำกัด (Restricted Proxy) ซึ่งเซิร์ฟเวอร์ซีเอเอสจะมอบตัวแทนจำกัดนี้ให้แต่ละผู้ใช้เฉพาะสิทธิที่ได้รับการอนุญาตภายใต้นโยบายชุมชน

จากงานวิจัยนี้ เซิร์ฟเวอร์ซีเอเอสสามารถนำไปดัดแปลงใช้กับโครงสร้างของข้อความยืนยันที่ได้รับจากผู้ให้บริการทั้งผู้ให้บริการหลักฐานที่พิสูจน์ว่าเป็นคนเดียวกันและผู้ให้บริการทรัพยากรอื่นๆ ที่สามารถกำหนดหรือจำกัดสิทธิที่จะอนุญาตได้

บทที่ 3
การออกแบบสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน

งานวิจัยนี้ได้แบ่งขั้นตอนในการดำเนินงานวิจัยออกเป็น 4 ส่วน ได้แก่ การออกแบบแผนภาพยูสเคส การออกแบบโครงสร้างพื้นฐานขององค์กรเสมือน การออกแบบโพรโทคอลที่ใช้ในการพิสูจน์ตัวจริง และการออกแบบเนมสเปซสำหรับองค์กรเสมือน ซึ่งแนวทางการดำเนินการวิจัยดังกล่าวสามารถแสดงได้ด้วยแผนภาพแอคทิวิตีดังแสดงในรูปที่ 3.1



รูปที่ 3.1 แผนภาพขั้นตอนการดำเนินงานวิจัย

ขั้นตอนที่ 3.1 แสดงการออกแบบโครงสร้างพื้นฐานขององค์กรเสมือน ขั้นตอนที่ 3.2 แสดงการออกแบบแผนภาพยูสเคสของการพิสูจน์ตัวจริงและการตรวจสอบสิทธิระหว่างองค์กรเสมือน ขั้นตอนที่ 3.3 แสดงการออกแบบโพรโทคอลในการลงบันทึกเข้าระบบเพียงครั้งเดียวและการตรวจสอบสิทธิ ขั้นตอนที่ 3.4 แสดงวิธีการกำหนดเนมสเปซ รายละเอียดของแต่ละขั้นตอนแสดงในหัวข้อที่ 3.1 3.2 3.3 และ 3.4 ตามลำดับ

3.1 องค์ประกอบต่าง ๆ ของสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียว

ก่อนกล่าวถึงขั้นตอนการออกแบบสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียว จะกล่าวถึงองค์ประกอบต่างๆ ในการสร้างสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียว ประกอบด้วย โครงสร้างพื้นฐานขององค์กรเสมือน โพรโทคอลของการลงบันทึกเข้าระบบเพียงครั้งเดียว และเนมสเปซของการลงบันทึกเข้าระบบเพียงครั้งเดียว ซึ่งมีรายละเอียดดังนี้

3.1.1 โครงสร้างพื้นฐานขององค์กรเสมือน

โครงสร้างพื้นฐานขององค์กรเสมือนประกอบด้วย ผู้ใช้ ผู้ให้บริการทรัพยากร และผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ดังรูปที่ 3.2 ซึ่งแต่ละองค์ประกอบมีรายละเอียดดังนี้

1. ผู้ใช้ (Client)

ผู้ใช้เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และสามารถเข้าใช้งานผู้ให้บริการทรัพยากรได้ตามสิทธิของผู้ใช้

2. ผู้ให้บริการทรัพยากร (Service Provider)

ผู้ให้บริการทรัพยากรจะให้บริการแก่ผู้ใช้ตามที่ผู้ใช้ร้องขอ โดยผู้ใช้ที่ต้องการเข้าใช้บริการจะต้องผ่านการพิสูจน์ตัวจริงจากผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เสียก่อน ผู้ให้บริการทรัพยากรจะทำการพิสูจน์สิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอได้หรือไม่

3. ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ (Identity Provider)

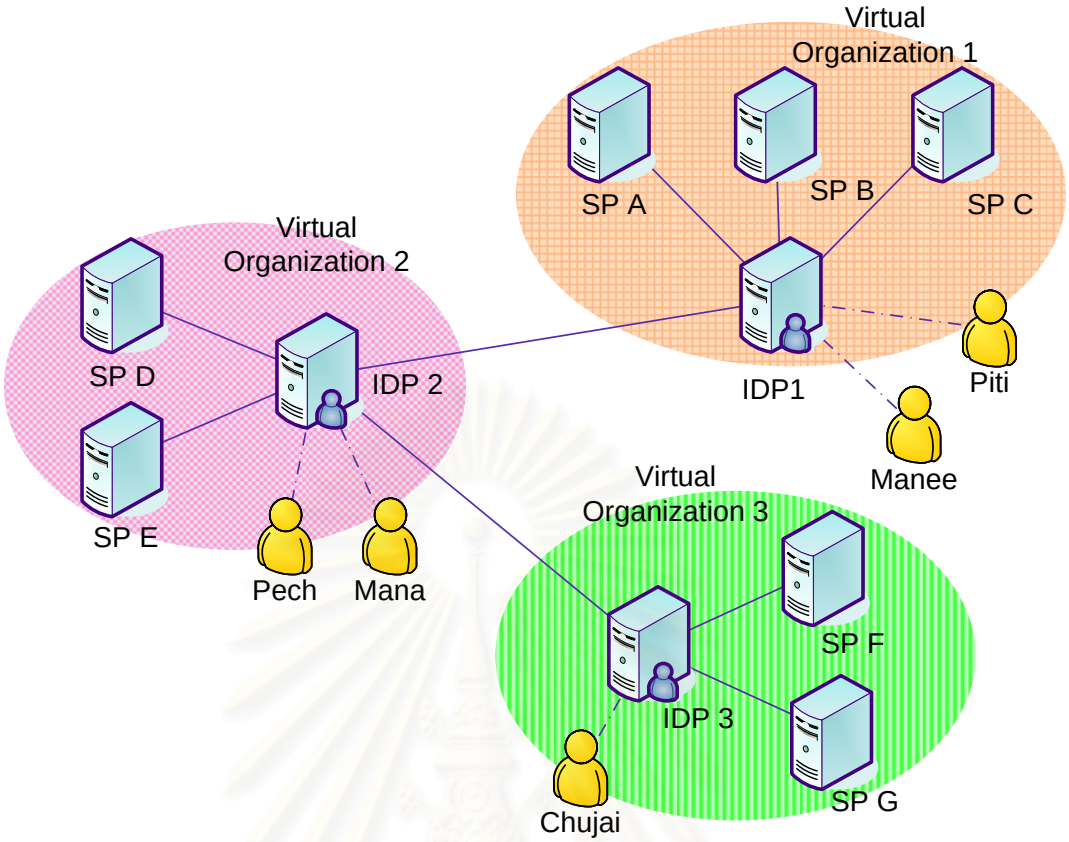
ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ให้บริการการพิสูจน์ตัวจริงแก่ผู้ใช้ และบริการข้อมูลเกี่ยวกับการพิสูจน์ตัวจริงให้กับผู้ให้บริการทรัพยากรอื่นๆ เช่น บริการข้อความยืนยันของผู้ใช้ให้กับผู้ให้บริการทรัพยากร โดยผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะมีเพียงหนึ่งผู้ให้บริการต่อหนึ่งองค์กรเสมือน

4. โพรโทคอลของการลงบันทึกเข้าระบบเพียงครั้งเดียว

โพรโทคอลของการลงบันทึกเข้าระบบเพียงครั้งเดียวจะกล่าวถึงวิธีการที่ผู้ใช้ร้องขอข้อความยืนยันจากองค์กรที่ทำหน้าที่พิสูจน์ตัวจริง และวิธีการได้รับผลตอบสนองจากองค์กรนั้น รายละเอียดของการออกแบบโพรโทคอลของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนจะกล่าวถึงในหัวข้อที่ 3.3

5. เนมสเปซสำหรับองค์กรเสมือน

เนมสเปซสำหรับองค์กรเสมือนใช้ในการค้นหาพาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ (Identity Provider path) และใช้ในการระบุผู้ให้บริการข้อมูลสำหรับระบุของผู้ใช้ โดยรายละเอียดของการออกแบบเนมสเปซของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนจะกล่าวถึงในหัวข้อที่ 3.4



รูปที่ 3.2 โครงสร้างพื้นฐานของสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน

จากรูปที่ 3.2 แสดงโครงสร้างพื้นฐานของสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน ประกอบด้วยองค์กรเสมือน 3 องค์กรได้แก่ องค์กรเสมือน1 (Virtual Organization1) องค์กรเสมือน2 และองค์กรเสมือน3 ซึ่งภายในแต่ละองค์กรเสมือนจะมีผู้ให้บริการข้อมูลสำหรับผู้ใช้ เช่น ไอดีพี1 (IDP1) และผู้ให้บริการทรัพยากร เช่น เอสพี เอ (SP A) เอสพี ดี เป็นต้น นอกจากนี้ยังมีผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของแต่ละองค์กรเสมือน เช่น มานี มานะ ชูใจ เป็นต้น โดยความสัมพันธ์ของความเชื่อถือของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของแต่ละองค์กรเสมือน ได้แก่ ไอดีพี1กับไอดีพี2 มีความเชื่อถือซึ่งกันและกัน และไอดีพี2 กับไอดีพี3

เมื่อผู้ใช้ต้องการเข้าใช้บริการของผู้ให้บริการทรัพยากร ผู้ใช้จะต้องทำการพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ให้บริการทรัพยากรเชื่อถือ เช่น ในรูปที่ 3.2 ผู้ให้บริการทรัพยากรเอ (SP A) ผู้ให้บริการทรัพยากรบี (SP B) และผู้ให้บริการทรัพยากรซี (SP C) จะเชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 1 หรือ ไอดีพี 1 เมื่อผ่านขั้นตอนการพิสูจน์ตัวจริง ผู้ใช้จะได้รับข้อความยืนยันเพื่อนำไปยื่นให้กับผู้ให้บริการทรัพยากร ถ้าผู้ให้บริการทรัพยากรเชื่อถือในข้อความยืนยันของผู้ใช้ ผู้ใช้จะถือว่าผ่านการพิสูจน์ตัวจริงกับผู้ให้บริการทรัพยากรด้วย ต่อจากนั้นผู้ให้บริการทรัพยากรจะทำการพิสูจน์สิทธิของผู้ใช้ก่อนอนุญาตให้ผู้ใช้สามารถเข้าใช้บริการต่อไป

ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของแต่ละองค์กรเสมือนสามารถสร้างความเชื่อถือซึ่งกันและกันได้ เพื่อทำให้เกิดการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน เมื่อองค์กรเสมือนสององค์กรสร้างความเชื่อถือซึ่งกันและกัน ผู้ใช้ขององค์กรเสมือนหนึ่งจะสามารถเรียกใช้บริการที่อยู่ในอีกองค์กรเสมือนที่มีความเชื่อถือกันได้ แต่การพิสูจน์ตัวจริงยังคงเป็นหน้าที่ของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ซึ่งผู้ใช้เป็นสมาชิกอยู่ ตัวอย่างการเรียกใช้งานข้ามองค์กรเสมือนของผู้ใช้ เช่น ไอดีพี1 และไอดีพี2 มีความเชื่อถือซึ่งกันและกัน เมื่อปิติซึ่งเป็นสมาชิกของไอดีพี1 ร้องขอการให้บริการจากผู้ให้บริการทรัพยากรดี (SP D) ในองค์กรเสมือน2 ผู้ให้บริการทรัพยากรดีจะส่งผู้ใช้ไปให้กับไอดีพี2 เพื่อทำการพิสูจน์ตัวจริง แต่ไอดีพี2ไม่รู้จักผู้ใช้คนนี้ และทราบว่าผู้ใช้เป็นสมาชิกของไอดีพี1 ก็จะส่งผู้ใช้กลับไปให้ไอดีพี1ทำการพิสูจน์ตัวจริง เมื่อผู้ใช้ผ่านการพิสูจน์ตัวจริงแล้ว ไอดีพี1จะส่งผู้ใช้กลับมาให้ไอดีพี2พร้อมกับข้อความยืนยัน ไอดีพี2ตรวจสอบข้อความยืนยันนั้น ถ้าไอดีพี 2 เชื่อว่าข้อความยืนยันเป็นความจริงก็จะส่งผู้ใช้กลับไปให้ผู้ให้บริการทรัพยากรดีเพื่อทำการพิสูจน์สิทธิของผู้ใช้ต่อไป

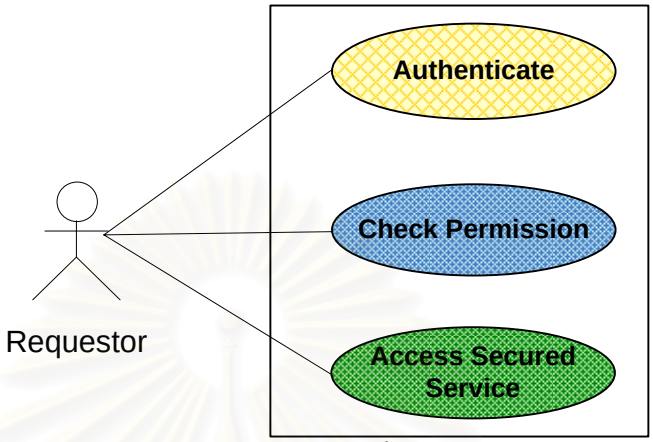
3.2 แผนภาพยูสเคสของการพิสูจน์ตัวจริงและการตรวจสอบสิทธิระหว่างองค์กรเสมือน

องค์กรหนึ่งๆ มักจะมีการเปิดให้บริการสาธารณะแก่องค์กรอื่นๆ ในองค์กรเสมือนเดียวกันเพื่อความสะดวกในการทำงานร่วมกัน โดยการเปิดบริการสาธารณะให้ผู้ใช้บริการประเภทต่างๆ ได้แก่ ผู้ใช้บริการในองค์กรของตนเอง ผู้ใช้บริการที่อยู่ภายนอกองค์กรแต่อยู่ภายในองค์กรเสมือนเดียวกัน และผู้ใช้บริการที่อยู่ภายนอกองค์กรเสมือนใช้ จึงจำเป็นที่จะต้องมีการจำกัดสิทธิที่ผู้ใช้ทั้งหลายพึงจะมีเพื่อความปลอดภัยของระบบงานและข้อมูลในองค์กรนั้นๆ การจำกัดสิทธิในการเข้าถึงบริการต่างๆ ขององค์กรส่วนใหญ่ในปัจจุบันมักจะใช้การพิสูจน์ตัวจริงและการพิสูจน์สิทธิของผู้ใช้นั้นๆ ก่อนจะอนุญาตให้เข้าถึงบริการต่างๆ ได้ โดยสามารถแบ่งประเภทของการเข้าใช้บริการขององค์กรต่างๆ ออกเป็น 2 ประเภท ดังนี้

3.2.1 การใช้บริการภายในหนึ่งองค์กรเสมือน

โดยปกติแล้ว ผู้ใช้มักจะเข้าถึงบริการที่มีการรักษาความปลอดภัยโดยไม่ได้ผ่านการลงบันทึกเข้าระบบ ดังนั้นผู้ให้บริการทรัพยากรจึงต้องส่งผู้ใช้ไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้งานเพื่อทำการลงบันทึกเข้าระบบ เพื่อทำการพิสูจน์ตัวจริงก่อนที่จะให้บริการต่อไป เมื่อผ่านการพิสูจน์ตัวจริงแล้ว ผู้ใช้จะต้องผ่านการพิสูจน์สิทธิกับผู้ให้บริการทรัพยากรว่าสามารถเข้าใช้งานได้หรือไม่ การใช้บริการภายในหนึ่งองค์กรเสมือนมีฟังก์ชันการทำงานหลักอยู่ 3 ฟังก์ชัน คือ ฟังก์ชันการพิสูจน์ตัวจริง ฟังก์ชันการพิสูจน์สิทธิ และฟังก์ชันการให้บริการที่มีการรักษาความปลอดภัย ดังแสดงในรูปที่ 3.3 ประกอบด้วย

1. ฟังก์ชันการพิสูจน์ตัวจริง รับข้อมูลเข้าเป็นแมสเซจร้องขอการพิสูจน์ตัวจริง ชื่อผู้ใช้และรหัสผ่าน และตรวจสอบว่าชื่อผู้ใช้และรหัสผ่านนั้นถูกต้องหรือไม่ ผลที่ได้คือ แมสเซจตอบสนองการพิสูจน์ตัวจริง



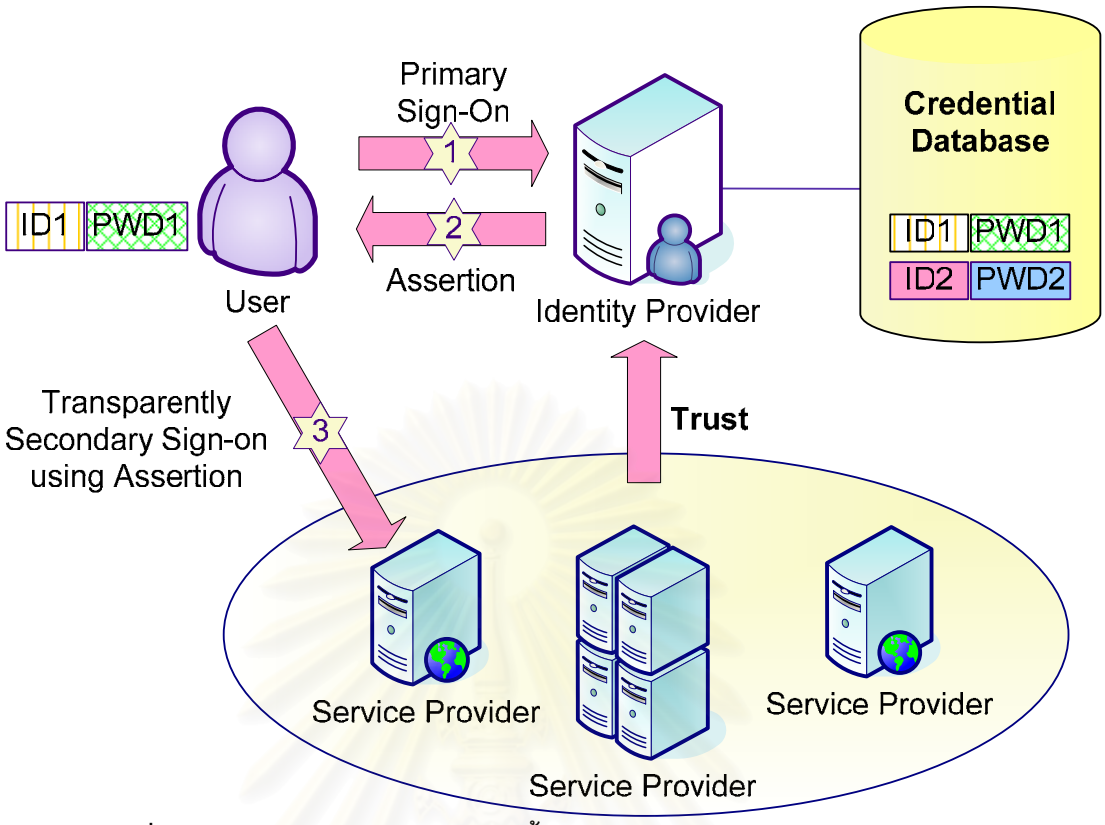
รูปที่ 3.3 **แผนภาพยูสเคสของการลงบันทึกเข้าระบบเพียงครั้งเดียวเพื่อใช้บริการภายในองค์กรเสมือน**

2. ฟังก์ชันการพิสูจน์สิทธิ รับข้อมูลเข้าเป็นแมสเซจตอบสนองการพิสูจน์ตัวจริง แล้วตรวจสอบสิทธิของผู้ใช้

3. ฟังก์ชันการให้บริการที่มีการรักษาความปลอดภัย บริการที่ผู้ให้บริการทรัพยากรเปิดให้ผู้ใช้ภายในองค์กรเสมือนสามารถใช้บริการได้ โดยผู้ใช้ต้องผ่านขั้นตอนการพิสูจน์ตัวจริงก่อนการเข้าใช้งาน

3.2.1.1 เหตุการณ์ตัวอย่าง (Scenario) ของการลงบันทึกเข้าระบบเพียงครั้งเดียวกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ภายในองค์กรเสมือน

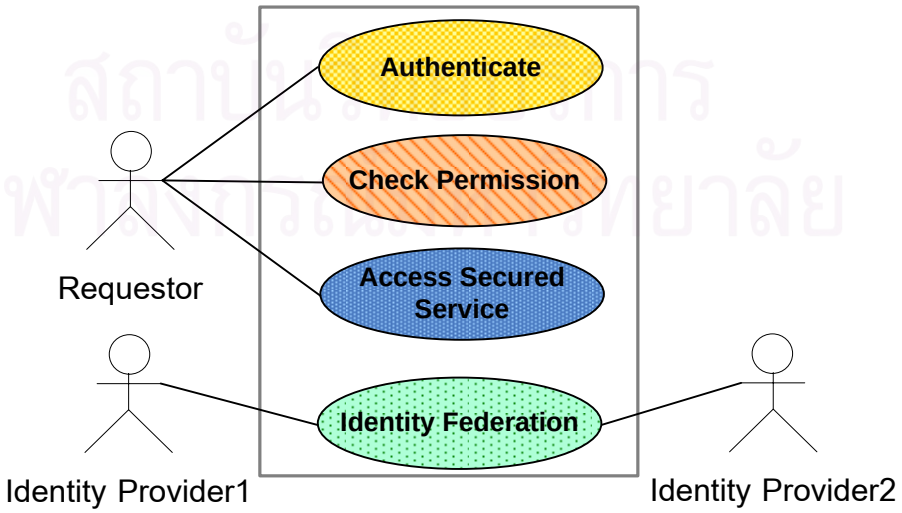
ในขั้นตอนของการพิสูจน์ตัวจริง ดังรูปที่ 3.4 ผู้ใช้แสดงหลักฐานอ้างอิงตัวผู้ใช้ (1) ซึ่งในที่นี้คือ ชื่อผู้ใช้และรหัสผ่านแก่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ โดยผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ตรวจสอบหลักฐานอ้างอิงตัวผู้ใช้กับข้อมูลที่เก็บไว้ในฐานข้อมูลหลักฐานอ้างอิงตัวผู้ใช้ (Credential Database) ถ้าหลักฐานอ้างอิงตัวผู้ใช้ที่ผู้ใช้แสดงและหลักฐานอ้างอิงตัวผู้ใช้ที่เก็บอยู่ในฐานข้อมูลตรงกัน จะถือว่าผู้ใช้นั้นผ่านการพิสูจน์ตัวจริงแล้ว เมื่อผู้ใช้ผ่านการพิสูจน์ตัวจริงแล้ว ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะออกข้อความยืนยันส่งกลับไปให้ผู้ใช้ (2) ซึ่งข้อความยืนยันนี้ใช้เพื่อแสดงให้ผู้ให้บริการทรัพยากรทราบว่าผู้ใช้ผ่านการพิสูจน์ตัวจริงแล้ว จากนั้นผู้ใช้แสดงข้อความยืนยันต่อผู้ให้บริการทรัพยากรเพื่อพิสูจน์สิทธิในการเข้าใช้บริการ (3)



รูปที่ 3.4 การลงบันทึกเข้าระบบเพียงครั้งเดียวกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ภายในองค์กรเสมือน

3.2.2 การใช้บริการระหว่างองค์กรเสมือน

การใช้บริการระหว่างองค์กรเสมือนมีฟังก์ชันการทำงานหลักอยู่ 4 ฟังก์ชัน คือ ฟังก์ชันการพิสูจน์ตัวจริง ฟังก์ชันการพิสูจน์สิทธิ ฟังก์ชันการให้บริการที่มีการรักษาความปลอดภัย และฟังก์ชันเฟ็ดเดอเรชัน ดังแสดงในรูปที่ 3.5



รูปที่ 3.5 แผนภาพยูสเคสของการลงบันทึกเข้าระบบเพียงครั้งเดียวเพื่อใช้บริการระหว่างองค์กรเสมือน

1. ฟังก์ชันการพิสูจน์ตัวจริง รับข้อมูลเข้าเป็นแมสเซจร้องขอการพิสูจน์ตัวจริง (AuthnRequest) ชื่อผู้ใช้ และรหัสผ่านจากผู้ใช้ และตรวจสอบว่าชื่อผู้ใช้และรหัสผ่านนั้นถูกต้องหรือไม่ ผลที่ได้คือ แมสเซจตอบสนองการพิสูจน์ตัวจริง (AuthnResponse)

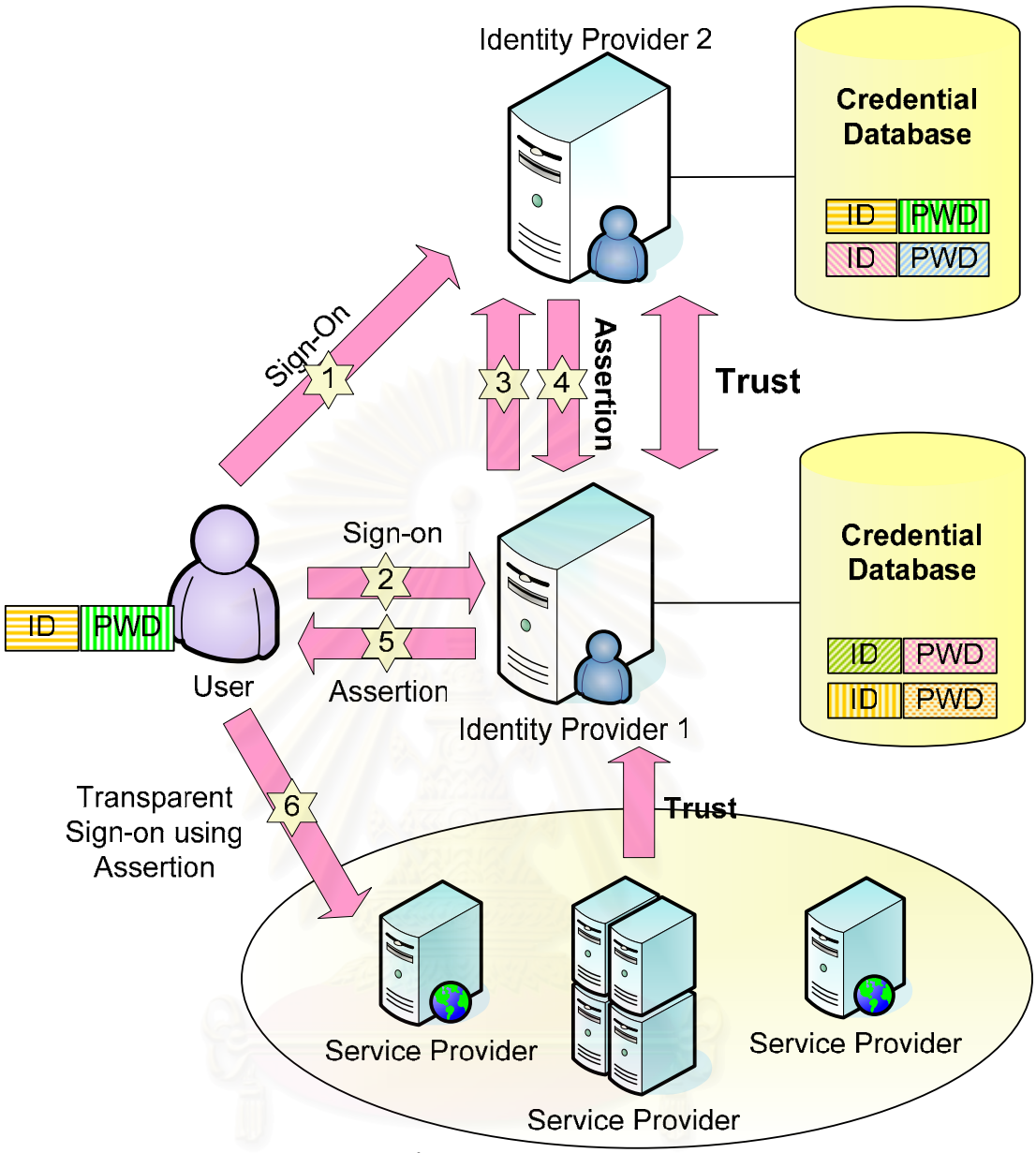
2. ฟังก์ชันการพิสูจน์สิทธิ รับข้อมูลเข้าเป็นแมสเซจตอบสนองการพิสูจน์ตัวจริง แล้วตรวจสอบสิทธิของผู้ใช้

3. ฟังก์ชันการให้บริการที่มีการรักษาความปลอดภัย บริการที่ผู้ให้บริการทรัพยากรเปิดให้ผู้ใช้ภายในองค์กรเสมือนสามารถใช้บริการได้ โดยผู้ใช้ต้องผ่านขั้นตอนการพิสูจน์ตัวจริงก่อนการเข้าใช้งาน

4. ฟังก์ชันการเฟ็ดเดอเรชันของข้อมูลสำหรับระบุผู้ใช้ เกิดขึ้นเมื่อผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ออกข้อความยืนยันให้กับผู้ใช้

3.2.2.1 เหตุการณ์ตัวอย่างของการลงบันทึกเข้าระบบเพียงครั้งเดียวกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ภายนอกองค์กรเสมือนของผู้ให้บริการทรัพยากร

ในขั้นตอนของการพิสูจน์ตัวจริง ดังแสดงในรูปที่ 3.6 ตั้งสมมติฐานว่าผู้ใช้ทำการพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 2 (Identity Provider2) (1) มาก่อนแล้ว โดยขั้นตอนการพิสูจน์ตัวจริงจะเริ่มที่ผู้ใช้ทำการพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 1 (2) ซึ่งผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 1 ทราบว่าผู้ใช้เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 2 จึงร้องขอข้อความยืนยันของผู้ใช้จากผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้2 (3) โดยผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะตรวจสอบว่าผู้ใช้ผ่านการพิสูจน์ตัวจริงหรือยัง ถ้าผู้ใช้ผ่านการพิสูจน์ตัวจริงเรียบร้อยแล้ว ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้จะส่งข้อความยืนยันกลับไปให้ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้1 (4) ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ 1 ตรวจสอบข้อความยืนยันที่ได้รับมา ถ้าผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เชื่อถือข้อความยืนยันที่ได้รับมา ผู้ให้บริการนี้จะถือว่าผู้ใช้ได้ผ่านการพิสูจน์ตัวจริงมาแล้ว และผู้ให้บริการจะออกข้อความยืนยันของผู้ใช้ใหม่ ก่อนจะส่งข้อความยืนยันใหม่นี้กลับไปให้ผู้ใช้ (5) ผู้ใช้จะยื่นข้อความยืนยันนี้ต่อผู้ให้บริการทรัพยากร (6) ซึ่งข้อความยืนยันนี้ใช้เป็นข้อพิสูจน์ต่อผู้ให้บริการทรัพยากรว่าผู้ใช้ผ่านการพิสูจน์ตัวจริงแล้ว จากนั้นผู้ให้บริการทรัพยากรทำการพิสูจน์สิทธิของผู้ใช้ก่อนจะอนุญาตหรือไม่อนุญาตให้เข้าใช้บริการ



รูปที่ 3.6 การลงบันทึกเข้าระบบเพียงครั้งเดียวกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ภายนอกองค์กรเสมือนของผู้ให้บริการทรัพยากร

3.3 การออกแบบโพรโทคอลที่ใช้ในการลงบันทึกเข้าระบบเพียงครั้งเดียวและการตรวจสอบสิทธิของผู้ใช้

ลิเบอร์ตี้แอลไลเอนซ์ระบุข้อกำหนดพื้นฐานของโพรโทคอลที่ใช้ในการติดต่อเพื่อทำการลงบันทึกเข้าระบบเพียงครั้งเดียว ดังนี้

1. การติดต่อโดยใช้โพรโทคอลเอชทีทีพีเอส (HTTPS) สำหรับยูอาร์แอล (URL) จะต้องใช้โพรโทคอลการรักษาความปลอดภัย (Security Protocol) แบบเอสเอสแอลเวอร์ชัน 3.0 หรือ ทีเอสแอลเวอร์ชัน 1.0

2. ข้อความที่ส่งระหว่างผู้ให้บริการต่างๆจะต้องมีการป้องกันสภาพบูรณภาพ (Integrity protected) และต้องเป็นความลับ (Confidentiality) นอกจากนี้ผู้รับจะต้องพิสูจน์ตัวจริงกับผู้ส่ง

3. ผู้ให้บริการจะต้องใช้การขนส่งอย่างปลอดภัยโดยใช้เอชทีทีพีเอส เพื่อรักษาความลับและป้องกันสภาพบูรณภาพ โดยที่ผู้เริ่มการติดต่อจะต้องพิสูจน์ตัวจริงกับเซิร์ฟเวอร์โดยใช้ใบรับรองฝั่งเซิร์ฟเวอร์แบบเอ็กซ์ 509 (Server-side X.509 certificates)

4. ข้อมูลการพิสูจน์ตัวจริงของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เก็บรักษาอย่างปลอดภัยไว้เพื่อให้กับผู้ใช้ ก่อนที่ผู้ใช้จะแสดงข้อมูลการพิสูจน์ตัวจริงของตนแก่ผู้ให้บริการข้อมูลสำหรับการพิสูจน์ตัวจริง

5. ใบรับรองและกุญแจส่วนบุคคลใช้สำหรับลายเซ็นดิจิตอลระยะยาว (long-term signature) โดยผู้ให้บริการทรัพยากรและผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ควรใช้ใบรับรองและกุญแจส่วนบุคคลสำหรับเซ็นลายเซ็นดิจิตอลและการทวนสอบ (Verification) ของข้อความที่ส่งระหว่างกันตามโพรโทคอลที่แตกต่างจากใบรับรองและกุญแจส่วนบุคคลที่ใช้สำหรับการติดต่อด้วยเอสเอสแอลหรือทีเอสแอล

6. ผู้ให้บริการจะต้องป้องกันการใช้ข้อความร้องขอซ้ำและผู้รับข้อความตอบสนองจะต้องตรวจสอบว่าข้อความที่ได้รับนี้สอดคล้องกับข้อความร้องขอหรือไม่ โดยการจัดเตรียมข้อมูลเชิงเวลาเพื่อยืนยันความใหม่

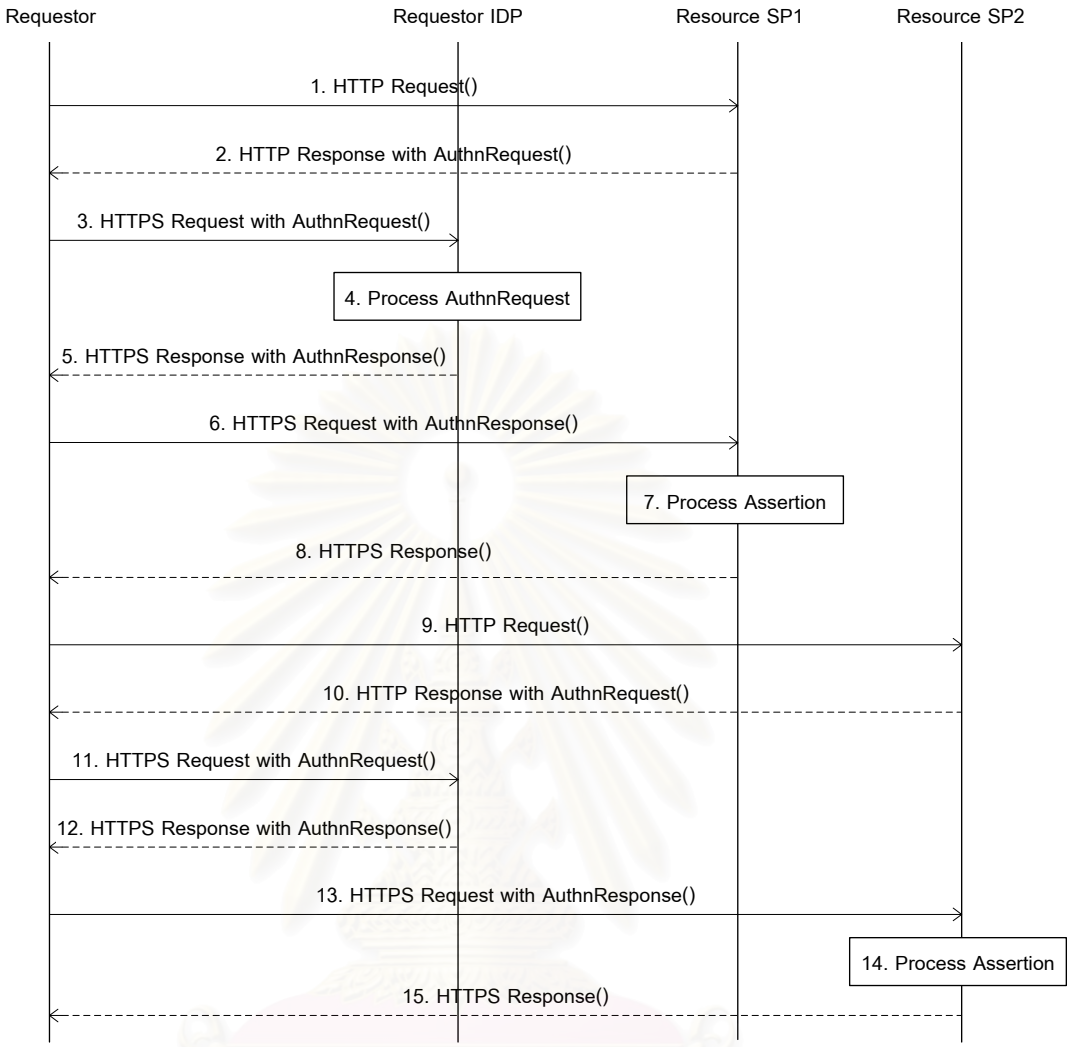
การออกแบบโพรโทคอลที่ใช้ในการลงบันทึกเข้าระบบเพียงครั้งเดียวและการตรวจสอบสิทธิของผู้ใช้ ผู้วิจัยแบ่งโพรโทคอลออกเป็น 2 ส่วนตามประเภทของการใช้งาน ได้แก่ การใช้งานภายในองค์กรเสมือน และการใช้งานระหว่างองค์กรเสมือนตั้งแต่ 2 องค์กรขึ้นไป ซึ่งมีรายละเอียดดังนี้

3.3.1 **การใช้งานภายในองค์กรเสมือน**

บริการที่ผู้ให้บริการทรัพยากรเปิดให้ใช้มีการรักษาความปลอดภัย ถ้ามีผู้ต้องการใช้งานจะต้องทำการพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ภายในองค์กรเสมือนก่อน เมื่อผ่านการพิสูจน์ตัวจริงแล้ว ผู้ให้บริการทรัพยากรจะตรวจสอบว่าผู้ใช้ดังกล่าวมีสิทธิที่จะใช้งานตามที่ผู้ใช้ร้องขอหรือไม่ ซึ่งมีการทำงานดังรูปที่ 3.7 ขั้นตอนการทำงานของโพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการภายในองค์กรเสมือน มีรายละเอียดดังนี้

1. ขั้นตอนแรก ผู้ใช้ร้องขอการเข้าใช้บริการกับ Resource SP1 ซึ่งต่อไปจะเรียกว่า ผู้ให้บริการที่1 โดยยังไม่ได้ทำการลงบันทึกเข้าระบบ

2. ในขั้นตอนที่ 2-3 ผู้ให้บริการที่ 1 สร้างแมสเซจร้องขอการพิสูจน์ตัวจริงโดยระบุข้อมูลในอิลิเมนต์ <ProviderID> เป็นชื่อเฉพาะของผู้ให้บริการที่ 1 แล้วส่งผู้ใช้ไปยังบริการการลงบันทึกเข้าระบบเพียงครั้งเดียวที่ Resource IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร
3. ในขั้นตอนที่ 4 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร ทำการพิสูจน์ตัวจริงของผู้ใช้แล้วสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงที่บรรจุข้อความยืนยันการพิสูจน์ตัวจริงของผู้ใช้
4. ขั้นตอนที่ 5-6 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร ส่งแมสเซจตอบสนองการพิสูจน์ตัวจริงกลับไปยังผู้ให้บริการที่ 1
5. ในขั้นตอนที่ 7 ผู้ให้บริการที่ 1 ทำการตรวจสอบแมสเซจการตอบสนองการพิสูจน์ตัวจริงที่ได้รับมาว่าผู้ใช้ที่ร้องขอการใช้บริการผ่านการพิสูจน์ตัวจริงหรือไม่ ถ้าผ่านการพิสูจน์ตัวจริงผู้ให้บริการที่ 1 ทำการประมวลผลข้อความยืนยันตามข้อกำหนดของลิเบอร์ตี้ [4] จากนั้นตรวจสอบสิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอมาได้หรือไม่ ถ้าผ่านการตรวจสอบสิทธิก็จะให้เข้าใช้บริการ และส่งผลลัพธ์ของการร้องขอกลับไปยังผู้ใช้ในขั้นตอนที่ 8



รูปที่ 3.7 โพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการภายในองค์กรเสมือน

ขั้นตอนต่อจากนี้จะสันนิษฐานว่าผู้ใช้ร้องขอบริการที่มีการรักษาความปลอดภัยอีกครั้งหนึ่ง ซึ่งคราวนี้ ผู้ใช้ได้ผ่านการพิสูจน์ตัวจริงเรียบร้อยแล้ว และข้อความยืนยันการพิสูจน์ตัวจริงนั้นยังไม่หมดอายุ ผู้ใช้ก็สามารถเข้าใช้บริการได้โดยไม่ต้องทำการพิสูจน์ตัวจริงอีกครั้ง ดังขั้นตอนที่ 9 ถึง15 ในรูปที่ 3.7

6. ขั้นตอนที่ 9 ผู้ใช้ทำการร้องขอการใช้บริการที่ Resource SP2 ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการที่ 3 ซึ่งอยู่ภายในองค์กรเสมือนเดียวกันผู้ให้บริการที่ 1
7. ขั้นตอนที่ 10 - 11 เหมือนกับขั้นตอนที่ 2-3
8. ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร ตรวจสอบดูว่ามีข้อความยืนยันของผู้ใช้ที่ร้องขอการใช้บริการหรือไม่ แล้วข้อความยืนยันนั้นหมดอายุหรือยัง ถ้าพบว่ามีข้อความยืนยันของ

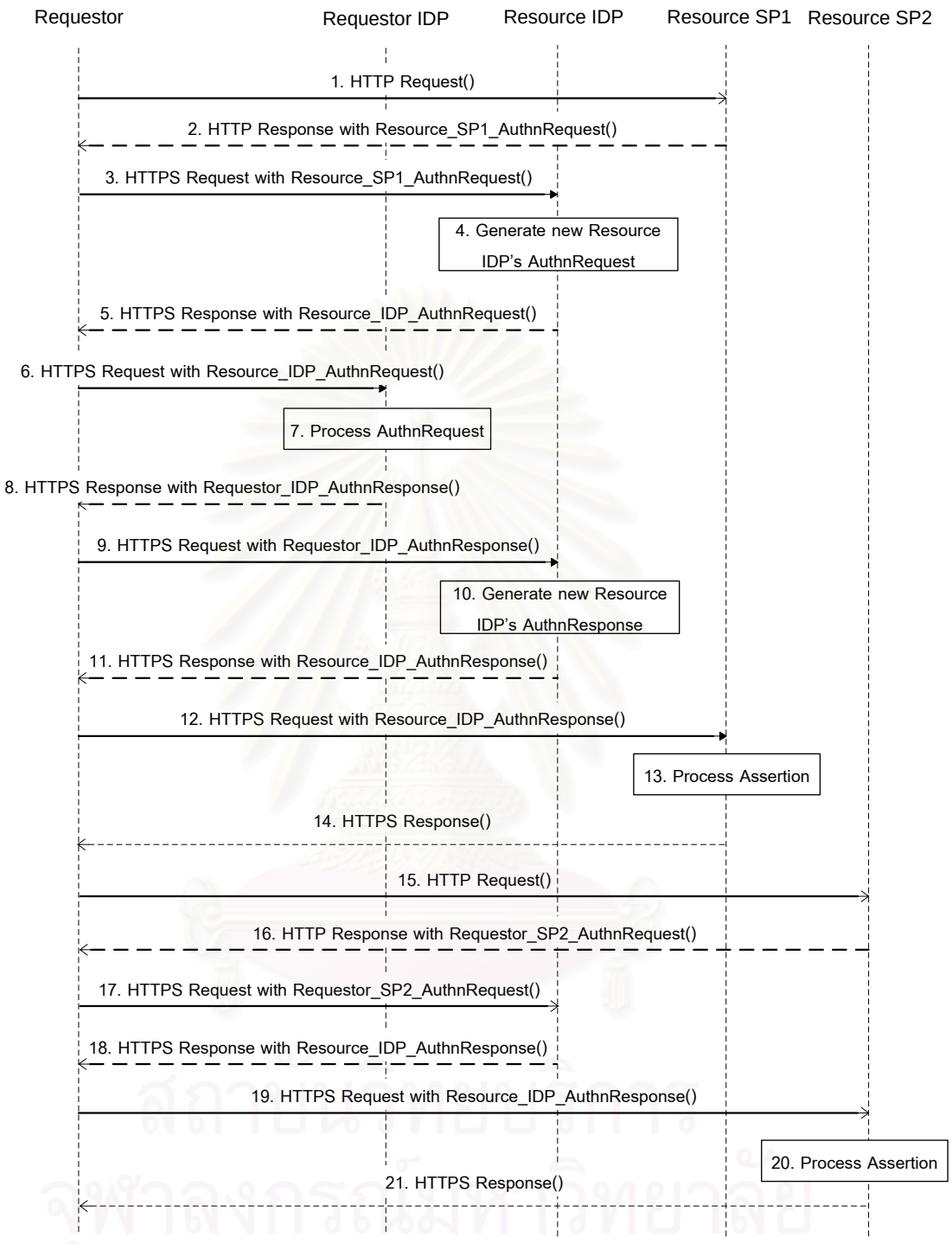
ผู้ใช้ยังไม่หมดอายุ จะสร้างแมสเซจการตอบสนองการพิสูจน์ตัวจริง เพื่อส่งกลับไปให้ผู้ให้บริการที่ 2ในขั้นตอนที่ 12 และ 13

9. ขั้นตอนที่ 14 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร ทำการตรวจสอบแมสเซจตอบสนองการพิสูจน์ตัวจริงที่ได้รับมาว่าผู้ใช้ที่ร้องขอการใช้บริการผ่านการพิสูจน์ตัวจริงหรือไม่ ถ้าผ่านการพิสูจน์ตัวจริงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร จะประมวลผลข้อความยืนยันตามข้อกำหนดของลิเบอร์ตี้ จากนั้นตรวจสอบสิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอมาได้หรือไม่ ถ้าผ่านการตรวจสอบสิทธิก็จะให้เข้าใช้บริการ และส่งผลลัพธ์ของการร้องขอกลับไปยังผู้ใช้ในขั้นตอนที่ 15

3.3.2 การใช้งานระหว่างองค์กรเสมือนตั้งแต่ 2 องค์กรขึ้นไป

การเรียกใช้บริการระหว่างองค์กรเสมือนจำเป็นต้องพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ขององค์กรเสมือนของผู้ให้บริการทรัพยากร โดยองค์กรเสมือนที่ติดต่อกันนั้นมีความเชื่อถือกันอยู่แล้ว ขั้นตอนการทำงานของโพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการระหว่างองค์กรเสมือนในรูปที่ 3.8 มีรายละเอียดดังนี้

1. ขั้นตอนแรก ผู้ใช้ร้องขอการเข้าใช้บริการกับ Resource SP1 ซึ่งต่อไปจะเรียกว่า ผู้ให้บริการที่1 โดยยังไม่ได้ทำการลงบันทึกเข้าระบบ
2. ในขั้นตอนที่ 2-3 ผู้ให้บริการที่ 1 สร้างแมสเซจร้องขอการพิสูจน์ตัวจริงโดยระบุข้อมูลในอิลิเมนต์ <ProviderID> เป็นชื่อเฉพาะของผู้ให้บริการที่ 1 พร้อมทั้งติดต่อกับผู้ใช้เพื่อให้เลือกผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิกอยู่ และส่งผู้ใช้ไปยังบริการการลงบันทึกเข้าระบบเพียงครั้งเดียวที่ Resource IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร
3. ในขั้นตอนที่ 4 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากรตรวจสอบข้อมูลชื่อเฉพาะของผู้ให้บริการที่ผู้ใช้ระบุมาให้ว่าตรงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร หรือไม่ ถ้าไม่ตรงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากรต้องสร้างแมสเซจร้องขอการพิสูจน์ตัวจริงใหม่โดยคัดลอกแมสเซจร้องขอการพิสูจน์ตัวจริงเดิม แต่เปลี่ยนข้อมูลของผู้ร้องขอที่กำหนดในอิลิเมนต์ <AudienceRestrictionCondition> ให้เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากรเองและเก็บบันทึกผู้ร้องขอเดิมไว้ แล้วส่งไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งระบุมากับแมสเซจร้องขอการพิสูจน์ตัวจริง



รูปที่ 3.8 โพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการระหว่างองค์กรเสมือน

4. ขั้นตอนที่ 5-6 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากรส่งผู้ใช้ไปยังบริการการลงบันทึกเพียงครั้งเดียวของ Requestor IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ 1 ซึ่งผู้ใช้เป็นสมาชิกอยู่พร้อมแนบแมสเซจร้องขอการพิสูจน์ตัวจริงที่เพิ่งสร้างใหม่ไปด้วย

5. ขั้นตอนที่ 7 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ 1 ทำการพิสูจน์ตัวจริงให้กับผู้ใช้ จากนั้นสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงที่บรรจุข้อความยืนยันการพิสูจน์ตัวจริงของผู้ใช้
6. ขั้นตอนที่ 8-9 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ 1 ส่งแมสเซจตอบสนองการพิสูจน์ตัวจริงกลับไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร
7. เมื่อได้รับแมสเซจตอบสนองกลับมา ในขั้นตอนที่10 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร จะสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงใหม่ โดยผู้ร้องขอในอิลิเมนต์ <AudienceRestrictionCondition> กำหนดเป็นผู้ร้องขอเดิมซึ่งเก็บไว้เมื่อขั้นตอนที่ 4 พร้อมทั้งเพิ่มอิลิเมนท์ <AuthnContext> ซึ่งระบุผู้ให้บริการที่ทำการพิสูจน์ตัวจริงให้กับผู้ใช้
8. ขั้นตอนที่ 11-12 ผู้ให้บริการในขั้นตอนที่ 10 ส่งผู้ใช้กลับไปยังผู้ให้บริการที่ร้องขอการพิสูจน์ตัวจริงครั้งแรก (ผู้ให้บริการที่ 1) พร้อมทั้งส่งแมสเซจการตอบสนองการพิสูจน์ตัวจริงใหม่ไปให้
9. ขั้นตอนที่ 13 เมื่อได้รับแมสเซจ ผู้ให้บริการที่ 1 ตรวจสอบแมสเซจการตอบสนองการพิสูจน์ตัวจริงใหม่ว่าผู้ใช้ที่ร้องขอการใช้บริการผ่านการพิสูจน์ตัวจริงหรือไม่ ถ้าผ่านการพิสูจน์ตัวจริงผู้ให้บริการที่ 1 ทำการประมวลผลข้อความยืนยันตามข้อกำหนดของลิเบอร์ตี้ จากนั้น ตรวจสอบสิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอมาได้หรือไม่ ถ้าผ่านการตรวจสอบสิทธิจะให้เข้าใช้บริการ และส่งผลกลับไปยังผู้ใช้ในขั้นตอนที่ 14

ถ้าผู้ใช้ต้องการเข้าใช้บริการภายในองค์กรเสมือนเดิม ซึ่งผู้ใช้ผ่านขั้นตอนการพิสูจน์ตัวจริงมาแล้ว และข้อความยืนยันที่ได้รับมานั้นยังไม่หมดอายุ ผู้ใช้ก็สามารถเข้าใช้บริการได้โดยไม่ต้องทำการพิสูจน์ตัวจริงอีกครั้ง ดังขั้นตอนที่ 15-21 ในรูปที่ 3.8

10. ขั้นตอนที่ 15 ผู้ใช้ทำการร้องขอการเข้าใช้บริการที่ Resource SP2 ซึ่งต่อไปนี้เรียกว่า ผู้ให้บริการที่ 3 ซึ่งอยู่ภายในองค์กรเสมือนเดียวกันกับผู้ให้บริการที่ 1
11. ขั้นตอนที่ 16-17 เหมือนกับขั้นตอนที่ 2-3
12. ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของทรัพยากร ตรวจสอบว่าผู้ใช้ที่ทำการร้องขอผ่านการพิสูจน์ตัวจริงแล้วหรือยัง เมื่อพบว่าผ่านการพิสูจน์ตัวจริงแล้ว และข้อความยืนยันของผู้ใช้นั้นยังไม่หมดอายุ จะทำการสร้างแมสเซจการตอบสนองการพิสูจน์ตัวจริงส่งกลับไปให้ผู้ให้บริการที่ 3 ในขั้นตอนที่ 18-19
13. ขั้นตอนที่ 20 เหมือนกับขั้นตอนที่ 13
14. เมื่อผ่านการตรวจสอบสิทธิ ผู้ให้บริการที่ 3 จะส่งผลลัพธ์ของการร้องขอบริการกลับไปให้ผู้ใช้ในขั้นตอนที่ 21

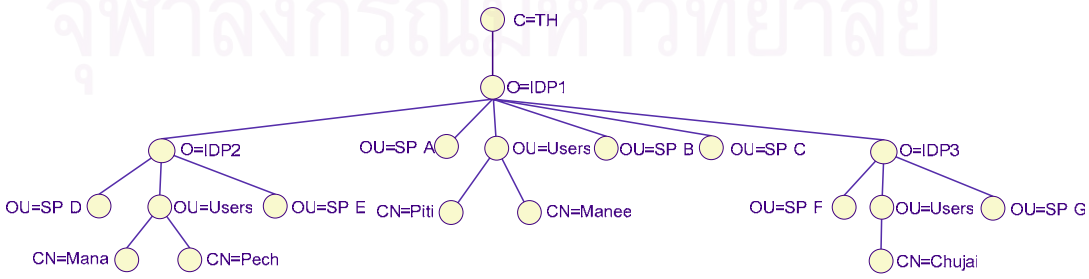
3.4 การออกแบบเนมสเปซสำหรับองค์กรเสมือน

สถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนกำหนดให้ผู้ใช้จะต้องพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิกอยู่เท่านั้น เนมสเปซสำหรับองค์กรเสมือนใช้ในการแก้ปัญหาการใช้บริการระหว่างองค์กรเสมือน ดังนั้น เมื่อผู้ใช้สามารถเรียกใช้บริการข้ามองค์เสมือนได้ จึงเกิดปัญหาในการระบุผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิกอยู่ และวิธีการค้นหาพาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นั้น เนื่องจากผู้ให้บริการทรัพยากรที่ผู้ใช้ร้องขอบริการนั้น อาจจะไม่อยู่ในองค์กรเสมือนเดียวกันกับผู้ใช้ ซึ่งตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์ยังไม่ได้ระบุถึงวิธีการค้นหาพาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ข้ามองค์กรเสมือน

ดังนั้น ผู้วิจัยจึงออกแบบเนมสเปซสำหรับองค์กรเสมือนตามรูปแบบของการกำหนดเนมสเปซของไดเรกทอรีเอ็กซ์ 500 โดยจะอิงตามโครงสร้างพื้นฐานขององค์กรเสมือนและความเชื่อถือกันระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งประกอบด้วย องค์กรเสมือน ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ผู้ให้บริการทรัพยากร และผู้ใช้ โดยแอททริบิวท์ที่ใช้ในการกำหนดเนมสเปซในรูปแบบนี้ ประกอบด้วยแอททริบิวท์ต่างๆ ซึ่งจะเรียงตามลำดับขั้นดังนี้

- ประเทศ
- องค์กร
- ระบบงาน
- บุคคล

เนมสเปซองค์กรใช้กำหนดผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ เช่น O=IDP1 เนมสเปซระบบงานใช้กำหนดผู้ให้บริการทรัพยากรต่างๆ เช่น OU=SP A และเนมสเปซบุคคลใช้กำหนดผู้ใช้ซึ่งจะอยู่ภายใต้เนมสเปซระบบงานผู้ใช้ (OU=Users) เช่น CN=Manee,OU=Users นอกจากนี้การเชื่อมต่อของเนมสเปซองค์กร จะอิงตามความเชื่อถือกันระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ขององค์กรเสมือนทั้งสอง เช่น ไอดีพี1 มีความเชื่อถือกันกับไอดีพี 2 และไอดีพี3 ดังรูปที่ 3.9



รูปที่ 3.9 ตัวอย่างการออกแบบเนมสเปซสำหรับองค์กรเสมือน

วิธีการค้นหาผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิก มี 3 วิธีดังนี้

1. ผู้ใช้รู้พาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ตนเป็นสมาชิก เมื่อผู้ใช้ร้องขอบริการจากผู้ให้บริการทรัพยากรที่อยู่คนละองค์กรเสมือน ผู้ใช้จะแนบพาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ตนเป็นสมาชิกไปด้วย

2. ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้รู้ภาพรวมขององค์กรเสมือน เมื่อผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้รู้ว่าองค์กรเสมือนทั้งหมดมีองค์กรใดบ้าง ผู้ให้บริการนั้นก็จะทราบถึงวิธีที่ไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้

3. การใช้โพรโทคอลการแยก (Resolution protocol) เลียนแบบระบบดีเอ็นเอส วิธีนี้ผู้ใช้และผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ไม่จำเป็นต้องมีข้อมูลเกี่ยวกับองค์กรเสมือนอื่นๆ โดยเมื่อต้องการติดต่อกับผู้ให้บริการที่ไม่รู้จักก็จะถามไปยังเซิร์ฟเวอร์กลางที่รู้ภาพรวมขององค์กรเสมือนทั้งหมด ก็จะได้ผลลัพธ์เป็นพาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้

3.5 การเปรียบเทียบระหว่างสถาปัตยกรรมที่ออกแบบกับเทคโนโลยีอื่นๆ

สถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน (Cross-Virtual Organization Single Sign-On) ที่สร้างขึ้นเมื่อเปรียบเทียบกับแนวคิดการลงบันทึกเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์และโครงสร้างการรักษาความปลอดภัยเชิงกริดแล้วมีข้อแตกต่างกันดังนี้

1. กลไกของการลงบันทึกเข้าระบบเพียงครั้งเดียว (Single Sign-On Mechanism)

กลไกของการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์เกิดจากการเฟ็ดเดอเรชันของข้อมูลสำหรับระบุผู้ใช้ระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้กับผู้ให้บริการทรัพยากร เมื่อผู้ให้บริการ 2 ฝ่ายเฟ็ดเดอเรดกันแล้วผู้ใช้สามารถเข้าใช้บริการของผู้ให้บริการทั้งสองได้โดยไม่ต้องทำการพิสูจน์ตัวจริงกับผู้ให้บริการทั้งคู่อีก ส่วนโครงสร้างการรักษาความปลอดภัยเชิงกริดจะใช้วิธีมอบอำนาจให้กับตัวแทน เมื่อผู้ใช้ต้องการใช้บริการที่แม่ข่ายระยะไกล ผู้ใช้จะส่งตัวแทนไปให้กับแม่ข่ายระยะไกล โดยตัวแทนที่สร้างขึ้นมีความสามารถในการพิสูจน์ตัวจริงแทนผู้ใช้ได้ ส่วนสถาปัตยกรรมที่สร้างขึ้นทำตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์

2. ความสามารถในการรองรับการพิสูจน์ตัวจริงภายในองค์กรเสมือน (Single Virtual Organization Authentication)

ข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์มีการกำหนดวิธีการพิสูจน์ตัวจริงภายในองค์กรเสมือน เช่นการใช้ชื่อผู้ใช้และรหัสผ่าน โครงสร้างการรักษาความปลอดภัยเชิงกริดใช้การพิสูจน์ตัวจริงร่วมกันโดยการแสดงหลักฐานอ้างอิงของตน แล้วให้อีกฝ่ายตรวจสอบ ส่วนสถาปัตยกรรมที่สร้างขึ้นทำตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์

3. ความสามารถในการรองรับการพิสูจน์ตัวจริงระหว่างองค์เสมือน (Cross Virtual Organization Authentication)

ทั้งข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์และโครงสร้างการรักษาความปลอดภัยเชิงกริดไม่ได้กล่าวถึงการพิสูจน์ตัวจริงระหว่างองค์กรเสมือน ส่วนสถาปัตยกรรมที่สร้างขึ้นรองรับการพิสูจน์ตัวจริงระหว่างองค์กรเสมือน โดยการพิสูจน์ตัวจริงจะทำตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์ โดยเพิ่มโพรโทคอลในการส่งข้อความยืนยันการพิสูจน์ตัวจริงระหว่างองค์กรเสมือนจากข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์เดิม

4. การใช้บริการนามแฝง (Use of pseudonyms)

ข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์มีการกำหนดวิธีการให้บริการนามแฝงในการเฟ็ดเดอเรชันระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ให้บริการทรัพยากรได้ โครงสร้างการรักษาความปลอดภัยเชิงกริดไม่ได้กล่าวถึงการใช้บริการนามแฝง ส่วนสถาปัตยกรรมที่สร้างขึ้นนี้ทำตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์

5. รองรับบริการแบบนิรนาม (Support for Anonymity)

ข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์มีการกำหนดให้ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้สร้างนามแฝงให้กับผู้ใช้เพื่อปกปิดชื่อของผู้ใช้ได้ โครงสร้างการรักษาความปลอดภัยเชิงกริดไม่ได้กล่าวถึงบริการแบบนิรนาม ส่วนสถาปัตยกรรมที่สร้างขึ้นทำตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์

6. การลงบันทึกออกแบบครอบคลุม (Global Logout)

ข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์มีการกำหนดวิธีการแจ้งให้ผู้ให้บริการทรัพยากรทั้งหมดที่ติดต่อกับผู้ใช้ทราบเมื่อผู้ใช้ลงบันทึกออกที่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ โครงสร้างการรักษาความปลอดภัยเชิงกริดไม่ได้กล่าวถึงการลงบันทึกออกแบบครอบคลุม ส่วนสถาปัตยกรรมที่สร้างขึ้นทำตามข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์

7. เส้นทางของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ (Identity Provider Path)

ข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์ไม่ได้ระบุถึงวิธีการค้นหาผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ทั้งภายในองค์กรเสมือนเดียวกัน และระหว่างองค์กรเสมือนอื่นๆ โครงสร้างการรักษาความปลอดภัยเชิงกริดไม่ได้กล่าวถึงวิธีการนี้เช่นกัน ส่วนสถาปัตยกรรมที่สร้างขึ้นใช้เนมสเปซแสดงเส้นทางของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เพื่อใช้ในการค้นหาผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้

บทที่ 4
ตัวอย่างการทดลองพัฒนาการลงบันทึกเข้าระบบของตลาดหลักทรัพย์โดยใช้สถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน

ในงานวิจัยชิ้นนี้ได้มีการทดลองพัฒนาการลงบันทึกเข้าระบบของตลาดหลักทรัพย์โดยใช้สถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน ซึ่งประกอบด้วยขั้นตอนการวิเคราะห์การลงบันทึกเข้าระบบของตลาดหลักทรัพย์ในปัจจุบัน ขั้นตอนการออกแบบโครงสร้างพื้นฐานของตลาดหลักทรัพย์ ขั้นตอนการออกแบบโพรโทคอลที่ใช้ในการลงบันทึกเข้าระบบเพียงครั้งเดียว ขั้นตอนการออกแบบเนมสเปซของตลาดหลักทรัพย์ และตัวอย่างการอิมพลีเมนต์การลงบันทึกเข้าระบบของตลาดหลักทรัพย์ ซึ่งมีรายละเอียดดังนี้

4.1 ขั้นตอนการนำสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนไปใช้งาน

ขั้นตอนการนำสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนไปใช้งานประกอบด้วย 3 ขั้นตอนดังนี้

1. ออกแบบเนมสเปซขององค์กรเสมือน
2. ติดตั้งผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้
3. กำหนดผู้ใช้ของแต่ละผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้

4.2 การวิเคราะห์การลงบันทึกเข้าระบบของตลาดหลักทรัพย์ในปัจจุบัน

4.2.1 ความต้องการในอนาคตของตลาดหลักทรัพย์

จากการศึกษาการทำงานของตลาดหลักทรัพย์ คาดว่าในอนาคตของตลาดหลักทรัพย์มีความต้องการดังต่อไปนี้

1. การนำระบบเอสทีพีมาใช้ (Straight Through Processing - STP)

ความต้องการในการเปลี่ยนแปลงระบบการทำงานให้เป็นระบบเอสทีพี เพื่อลดเวลาในการประมวลผลการซื้อขายหลักทรัพย์ รวมถึงการส่งมอบหลักทรัพย์และชำระราคาหลักทรัพย์ลงจากเดิมที่ใช้เวลา 3 วันทำการ นับจากวันซื้อขายให้เสร็จเรียบร้อยภายในวันที่ทำการซื้อขายหรือหลังจากวันซื้อขาย 1 วัน การเปลี่ยนระบบให้เป็นระบบเอสทีพีนั้นจะช่วยให้ระบบสามารถทำงานโดยอัตโนมัติได้มากขึ้น เพราะมีการลดขั้นตอนที่ใช้คนทำงานมาเป็นให้คอมพิวเตอร์ทำงานแทน ทำให้ช่วงเวลาของการประมวลผลลดลง ระบบจะต้องมีการเปลี่ยนแปลงเทคโนโลยีที่ใช้ เพื่อให้ระบบสามารถทำงานได้โดยไม่ต้องมีบุคลากรเป็นผู้ควบคุม เช่น การนำเทคโนโลยีเว็บเซอร์วิสเข้า

มาใช้ในการติดต่อระหว่างระบบงานภายในและภายนอก ดังนั้นขั้นตอนในการรักษาความปลอดภัยจึงต้องมีการเปลี่ยนแปลงเพื่อให้รองรับกับเทคโนโลยีใหม่ๆ ด้วย เช่น การเข้าใช้ระบบงานควรมีการตรวจสอบความปลอดภัยต่างๆ ที่มีความรวดเร็วและเชื่อถือได้

2. การเพิ่มจำนวนผู้ติดบริษัทนายหน้าซื้อขายหลักทรัพย์และการซื้อขายหลักทรัพย์กับตลาดหลักทรัพย์ต่างประเทศ

การติดต่อกับระบบนายหน้าซื้อขายหลักทรัพย์ในปัจจุบันมีความปลอดภัยมาก เนื่องจากช่องทางที่ติดต่อสื่อสารกันเป็นแบบสายเช่า (Leased Line) แต่ในอนาคต ถ้าตลาดหลักทรัพย์อนุญาตให้มีจำนวนนายหน้าซื้อขายหลักทรัพย์มากขึ้นหรือเพิ่มการซื้อขายหลักทรัพย์กับตลาดหลักทรัพย์ต่างประเทศ ช่องทางที่ติดต่อสื่อสารในปัจจุบันอาจจะไม่เหมาะสม เนื่องจากช่องทางการสื่อสารในปัจจุบันมีราคาสูงและไม่สะดวกสำหรับการติดต่อข้ามประเทศ ทำให้เกิดความต้องการช่องทางการติดต่อสื่อสารที่มีลักษณะเป็นสาธารณะมากขึ้น เช่น การใช้อินเทอร์เน็ตในการติดต่อสื่อสาร

4.2.2 ปัญหาเกี่ยวกับการรักษาความปลอดภัยของตลาดหลักทรัพย์ในปัจจุบัน

การรักษาความปลอดภัยของตลาดหลักทรัพย์ในปัจจุบันไม่รองรับกับการเปลี่ยนแปลงของเทคโนโลยีใหม่ๆ ที่ทางตลาดหลักทรัพย์จะนำมาใช้ในอนาคต ซึ่งปัญหาที่เกิดขึ้นมีดังนี้

1. การรักษาความปลอดภัยในปัจจุบันไม่รองรับเทคโนโลยีใหม่

การตรวจสอบการเข้าใช้ระบบของตลาดหลักทรัพย์สำหรับผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์เป็นเพียงแค่การเช็คเลขที่อยู่ไอพีของเครื่องที่ส่งข้อความเข้ามาว่าอยู่ในกลุ่มเลขที่อยู่ไอพีของบริษัทนายหน้าซื้อขายหลักทรัพย์ที่ตลาดหลักทรัพย์กำหนดให้หรือไม่เท่านั้น โดยผลักภาระให้กับบริษัทนายหน้าซื้อขายหลักทรัพย์เป็นผู้รับผิดชอบการรักษาความปลอดภัยของเลขที่อยู่ไอพีที่จะกำหนดให้แก่ผู้ใช้แต่ละรายของบริษัท แต่ในอนาคต ถ้ามีการเปลี่ยนแปลงเทคโนโลยีที่ใช้ในการสร้างระบบทำให้การรักษาความปลอดภัยที่มีอยู่นั้นอาจจะไม่เพียงพอและไม่ทันท่วงทีเพราะระบบในอนาคตจะมีการประมวลผลที่เร็วขึ้นทำให้การรักษาความปลอดภัยหรือการตรวจสอบต้องมีการพัฒนาให้สามารถทำงานได้ทันกับความต้องการและรองรับกับเทคโนโลยีที่เปลี่ยนแปลงไปด้วย

2. การเพิ่มประเภทของผู้ใช้

ถ้าตลาดหลักทรัพย์นำเทคโนโลยีเว็บเซอร์วิสเข้ามาใช้ในการทำงาน การรักษาความปลอดภัยในปัจจุบันอาจจะไม่เพียงพอ เนื่องจากประเภทของผู้ใช้งานอาจจะเพิ่มจากผู้ใช้งานที่เป็น

คนเปลี่ยนเป็นผู้ใช้งานที่เป็นเซอร์วิสหรือโปรแกรมประยุกต์แทน ดังนั้นวิธีการรักษาความปลอดภัยในการเข้าใช้ระบบงานควรจะครอบคลุมลักษณะของผู้ใช้ที่เพิ่มขึ้น

3. การบริหารจัดการผู้ใช้ทั้งในตลาดหลักทรัพย์และองค์กรอื่นๆ ที่ทำงานร่วมกัน

ปัจจุบัน ตลาดหลักทรัพย์มีหน้าที่จัดการบัญชีผู้ใช้และกำหนดนโยบายการเข้าใช้ระบบของผู้ใช้ทั้งในตลาดหลักทรัพย์และในองค์กรอื่นๆ ที่ติดต่อกัน ซึ่งเป็นงานที่มีความยุ่งยากมาก เช่น เมื่อเกิดการเปลี่ยนแปลงผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์เอเนื่องจากการลาออกหรือเปลี่ยนแปลงตำแหน่งงาน ตลาดหลักทรัพย์จะต้องจัดการปรับปรุงบัญชีผู้ใช้และสิทธิที่ผู้ใช้คนนั้นทำงานให้ถูกต้องตลอดเวลา ดังนั้นเพื่อให้การบริหารจัดการผู้ใช้มีประสิทธิภาพมากขึ้น แต่ละองค์กรควรจะรับผิดชอบในการจัดการบัญชีผู้ใช้และกำหนดนโยบายการเข้าใช้ระบบของตนเอง และตลาดหลักทรัพย์ควรเปลี่ยนรูปแบบการจัดการผู้ใช้จากการใช้บัญชีผู้ใช้ในการระบุสิทธิในการเข้าใช้ระบบมาเป็นบทบาทและหน้าที่ของผู้ใช้แทน

4.3 การออกแบบโครงสร้างพื้นฐานของตลาดหลักทรัพย์

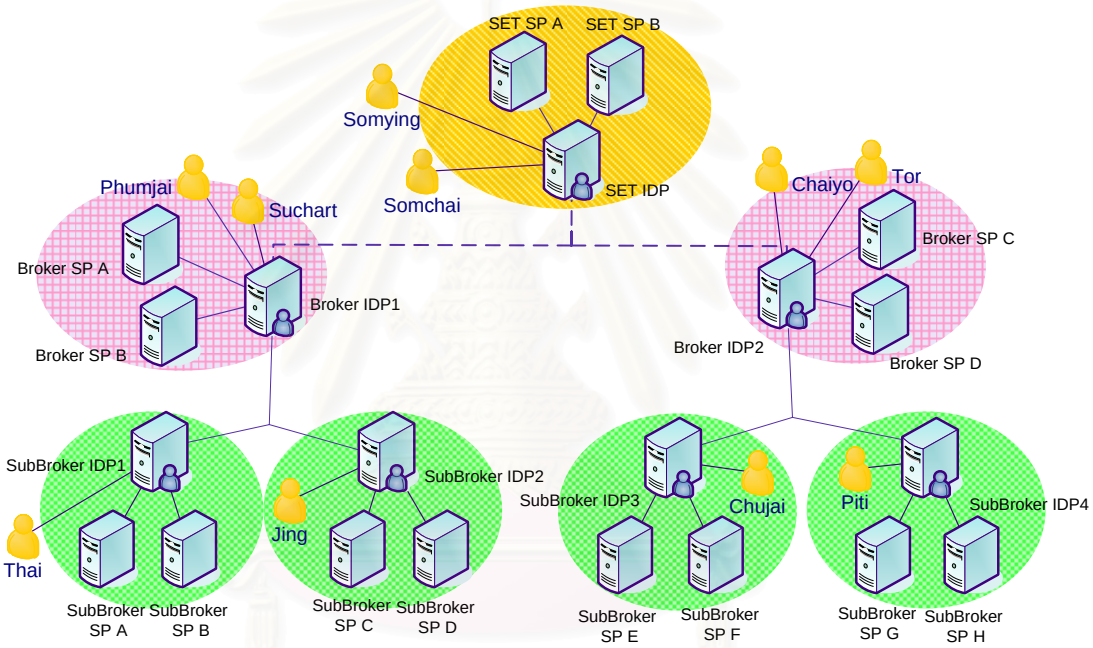
การออกแบบโครงสร้างพื้นฐานของตลาดหลักทรัพย์ จะออกแบบตามหัวข้อที่ 3.2 ซึ่งในสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน องค์กรเสมือนหนึ่งองค์กรประกอบด้วย ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ให้บริการทรัพยากร ผู้วิจัยจึงออกแบบโครงสร้างพื้นฐานของตลาดหลักทรัพย์ ประกอบด้วย 7 องค์กรเสมือน แสดงในรูปที่ 4.1 ซึ่งมีรายละเอียดดังนี้

- องค์กรเสมือนตลาดหลักทรัพย์ ประกอบไปด้วย SETIDP เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ SETSP_A และSETSP_B
- องค์กรเสมือนบริษัทนายหน้าซื้อขายหลักทรัพย์ที่ 1 ประกอบไปด้วย BrokerIDP1 เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ BrokerSP_A และ BrokerSP_B
- องค์กรเสมือนบริษัทนายหน้าซื้อขายหลักทรัพย์ที่ 2 ประกอบไปด้วย BrokerIDP2 เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ BrokerSP_C และ BrokerSP_D
- องค์กรเสมือนบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 1 ประกอบไปด้วย SubBrokerIDP1 เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ SubBrokerSP_A และSubBrokerSP_B

- องค์กรเสมือนบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 2 ประกอบไปด้วย SubBrokerIDP2 เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ SubBrokerSP_C และSubBrokerSP_D

- องค์กรเสมือนบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 3 ประกอบไปด้วย SubBrokerIDP3 เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ SubBrokerSP_E และSubBrokerSP_F

- องค์กรเสมือนบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 4 ประกอบไปด้วย SubBrokerIDP4 เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และมีผู้ให้บริการทรัพยากร 2 องค์กรได้แก่ SubBrokerSP_G และSubBrokerSP_H



รูปที่ 4.1 ตัวอย่างการออกแบบโครงสร้างองค์กรเสมือนซึ่งประกอบด้วยตลาดหลักทรัพย์ บริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย

ความเชื่อถือกันระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ขององค์กรเสมือนต่างๆ ในรูปที่ 4.1 แสดงได้ดังตารางที่ 4.1 โดยช่องที่มีเครื่องหมายถูกหมายถึง ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ขององค์กรเสมือนทั้งสองนั้นมีความเชื่อถือกัน

ตารางที่ 4.1 ความเชื่อถือกันระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ขององค์กรเสมือนต่างๆ

Virtual Organization	Broker IDP1	Broker IDP2	SubBroker IDP1	SubBroker IDP2	SubBroker IDP3	SubBroker IDP4
SET IDP	✓	✓				
Broker IDP1			✓	✓		
Broker IDP2					✓	✓

4.4 การออกแบบเนมสเปซของตลาดหลักทรัพย์

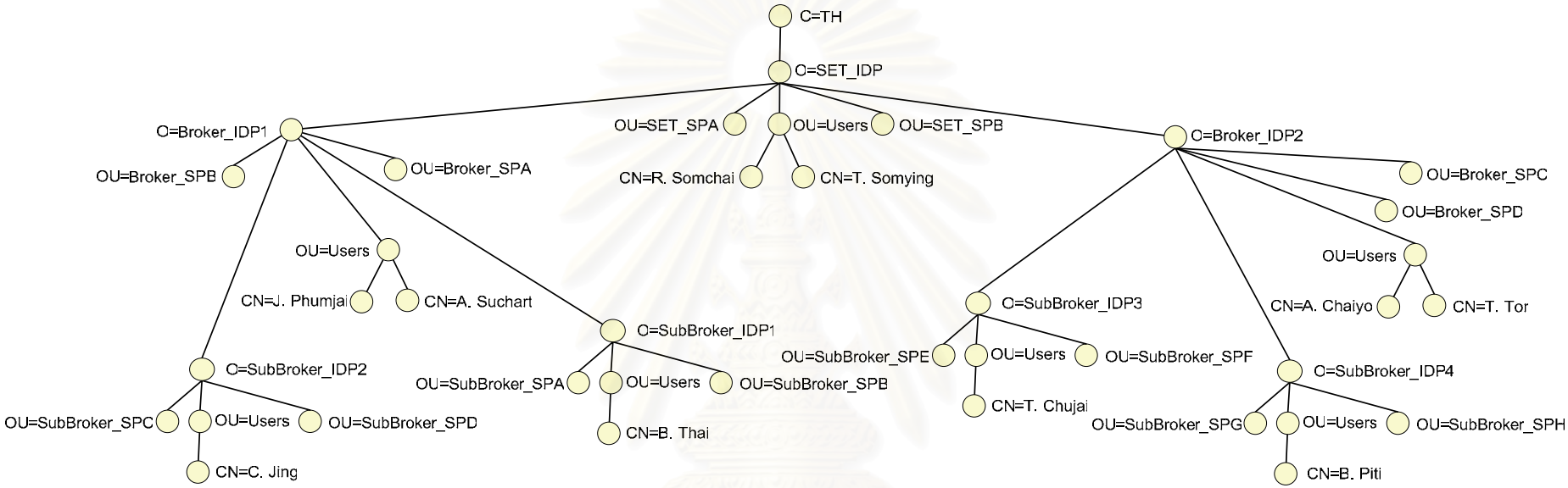
การออกแบบเนมสเปซตามการออกแบบในหัวข้อ 3.3 แสดงดังรูปที่ 4.2 โดยเนมสเปซที่อยู่บนสุด มีค่าเป็น C=TH อธิบายถึงประเทศไทย ในระดับที่ 2 อธิบายถึงโครงสร้างขององค์กรภายในประเทศไทย ซึ่งในที่นี้หมายถึงองค์กรเสมือน ระดับที่ 3 อธิบายถึงหน่วยขององค์กรภายใต้องค์กรระดับที่ 2 ในที่นี้หมายถึงผู้ให้บริการต่างๆ ภายใต้องค์กรเสมือน ระดับที่ 4 อธิบายถึงผู้ใช้ในองค์กรเสมือน ซึ่งมีรายละเอียดดังนี้

- O=SET_IDP หมายถึงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ โดยระดับถัดไปจะเป็นผู้ให้บริการทรัพยากรและผู้ใช้ที่เชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้ ประกอบด้วย
  - OU=SET_SPA หมายถึงผู้ให้บริการทรัพยากรของตลาดหลักทรัพย์ เอ
  - OU=SET_SPB หมายถึงผู้ให้บริการทรัพยากรของตลาดหลักทรัพย์ บี
  - CN=R. Somchai และ CN=T. Somying หมายถึงผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้
- O=Broker_IDP1 หมายถึงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ที่ 1 โดยระดับถัดไปจะเป็นผู้ให้บริการทรัพยากรและผู้ใช้ที่เชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้ ประกอบด้วย
  - OU=Broker_SPA หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ เอ
  - OU=Broker_SPB หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ บี
  - ผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อธิบายโดยใช้ชื่อผู้ใช้ ได้แก่ CN=J. Phumjai และ CN=A. Suchart

- O=SubBroker_IDP1 หมายถึงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 1 โดยระดับถัดไปจะเป็นผู้ให้บริการทรัพยากรและผู้ใช้ที่เชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้ ประกอบด้วย
  - OU=SubBroker_SPA หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย เอ
  - OU=SubBroker_SPB หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย บี
  - ผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อธิบายโดยใช้ชื่อผู้ใช้ ได้แก่ CN=B. Thai
- O=SubBroker_IDP2 หมายถึงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 2 โดยระดับถัดไปจะเป็นผู้ให้บริการทรัพยากรและผู้ใช้ที่เชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้ ประกอบด้วย
  - OU=SubBroker_SPC หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย ซี
  - OU=SubBroker_SPD หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย ดี
  - ผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อธิบายโดยใช้ชื่อผู้ใช้ ได้แก่ CN=C. Jing
- O=Broker_IDP2 หมายถึงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ที่ 2 โดยระดับถัดไปจะเป็นผู้ให้บริการทรัพยากรและผู้ใช้ที่เชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้ ประกอบด้วย
  - OU=Broker_SPC หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ ซี
  - OU=Broker_SPD หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ ดี
  - ผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อธิบายโดยใช้ชื่อผู้ใช้ ได้แก่ CN=T. Tor และ CN=A. Chaiyo
- O=SubBroker_IDP3 หมายถึงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 3 โดยระดับถัดไปจะเป็นผู้ให้บริการทรัพยากรและผู้ใช้ที่เชื่อถือผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้นี้ ประกอบด้วย

- OU=SubBroker_SPE หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย อี
- OU=SubBroker_SPF หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย เอฟ
- ผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อธิบายโดยใช้ชื่อผู้ใช้ ได้แก่ CN=T. Chujai

- O=SubBroker_IDP4 หมายถึงองค์กรเสมือนของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 4 ซึ่งผู้ให้บริการภายใต้องค์กรเสมือนของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยที่ 4ประกอบด้วย
  - OU=SubBroker_SPG หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย จี
  - OU=SubBroker_SPH หมายถึงผู้ให้บริการทรัพยากรของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย เอช
  - ผู้ใช้ที่เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้อธิบายโดยใช้ชื่อผู้ใช้ ได้แก่ CN=B. Piti



รูปที่ 4.2 การออกแบบเนมสเปซของตลาดหลักทรัพย์ บริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย

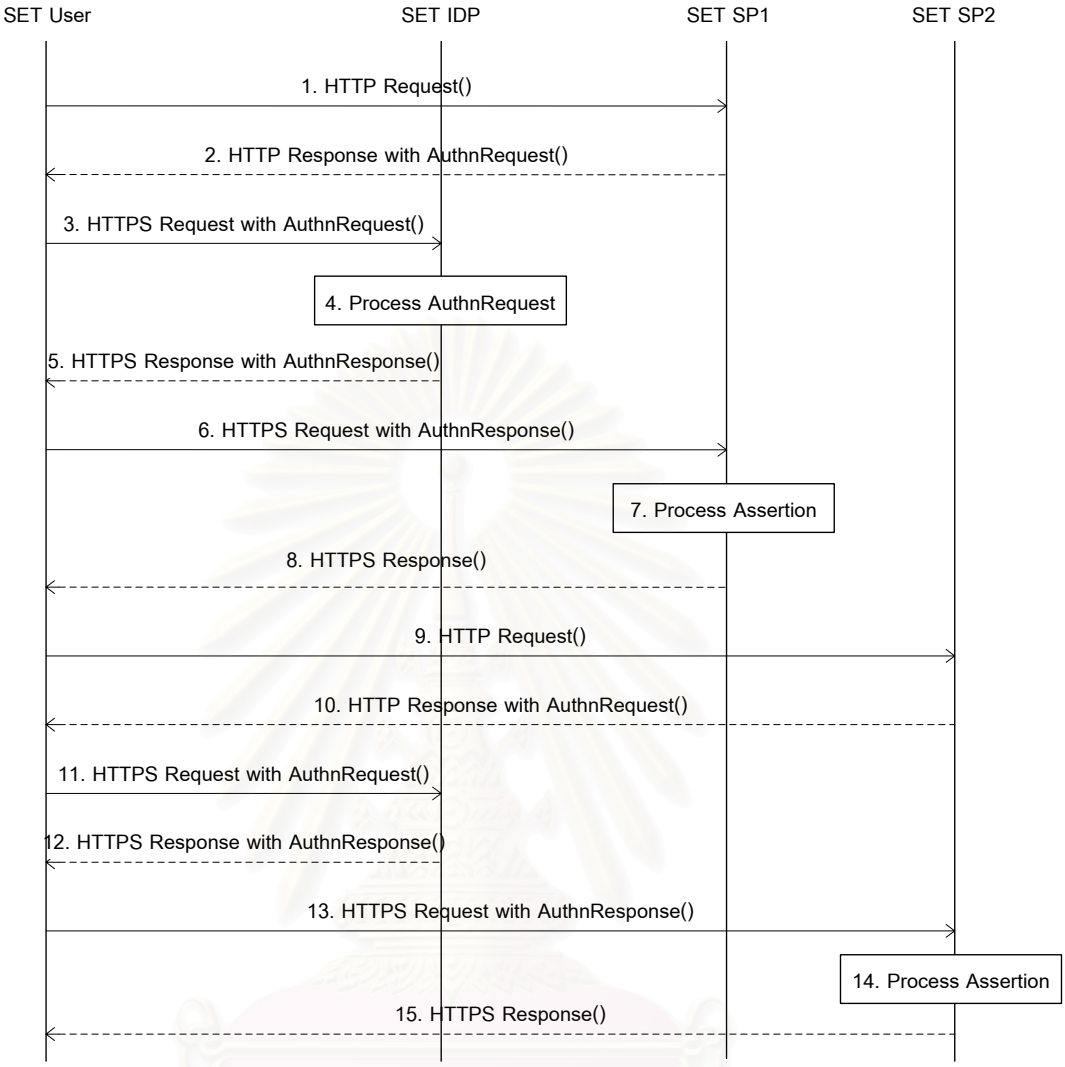
4.5 การออกแบบโพรโทคอลที่ใช้ในการลงบันทึกเข้าระบบเพียงครั้งเดียวและการตรวจสอบสิทธิของผู้ใช้ของตลาดหลักทรัพย์

การออกแบบโพรโทคอลที่ใช้ในการลงบันทึกเข้าระบบเพียงครั้งเดียวและการตรวจสอบสิทธิของผู้ใช้ของตลาดหลักทรัพย์ ผู้วิจัยแบ่งโพรโทคอลออกเป็น 2 ส่วนตามประเภทของการใช้งาน ได้แก่ การใช้งานภายในตลาดหลักทรัพย์ และการใช้บริการระหว่างตลาดหลักทรัพย์ บริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย ซึ่งมีรายละเอียดดังนี้

4.5.1 การใช้บริการภายในตลาดหลักทรัพย์

ตลาดหลักทรัพย์ประกอบด้วยผู้ให้บริการทรัพยากร 2 องค์กรและผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ โดยบริการที่ผู้ให้บริการทรัพยากรเปิดให้ใช้มีการรักษาความปลอดภัย ผู้ใช้ที่ต้องการใช้งานจะต้องทำการพิสูจน์ตัวจริงกับผู้ให้บริการทรัพยากรข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ก่อน เมื่อผ่านการพิสูจน์ตัวจริงแล้ว ผู้ให้บริการทรัพยากรจะตรวจสอบว่าผู้ใช้ดังกล่าวมีสิทธิที่จะใช้งานตามที่ผู้ใช้ร้องขอหรือไม่ ซึ่งมีการทำงานดังรูปที่ 4.5 ขั้นตอนการทำงานของโพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการภายในตลาดหลักทรัพย์ มีรายละเอียดดังนี้

1. ขั้นตอนแรก ผู้ใช้ร้องขอการเข้าใช้บริการกับ SET SP1 ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการที่1 โดยยังไม่ได้ทำการลงบันทึกเข้าระบบ
2. ในขั้นตอนที่ 2-3 ผู้ให้บริการที่ 1 สร้างแมสเซจร้องขอการพิสูจน์ตัวจริงโดยระบุข้อมูลในอิลิเมนต์ <ProviderID> เป็นชื่อเฉพาะของผู้ให้บริการที่ 1 แล้วส่งผู้ใช้ไปยังบริการการลงบันทึกเข้าระบบเพียงครั้งเดียวที่ SET IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์
3. ในขั้นตอนที่ 4 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ทำการพิสูจน์ตัวจริงของผู้ใช้ แล้วสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงที่บรรจุข้อความยืนยันการพิสูจน์ตัวจริงของผู้ใช้
4. ขั้นตอนที่ 5-6 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ส่งแมสเซจตอบสนองการพิสูจน์ตัวจริงกลับไปยังผู้ให้บริการที่ 1



รูปที่ 4.5 โพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการภายในตลาดหลักทรัพย์

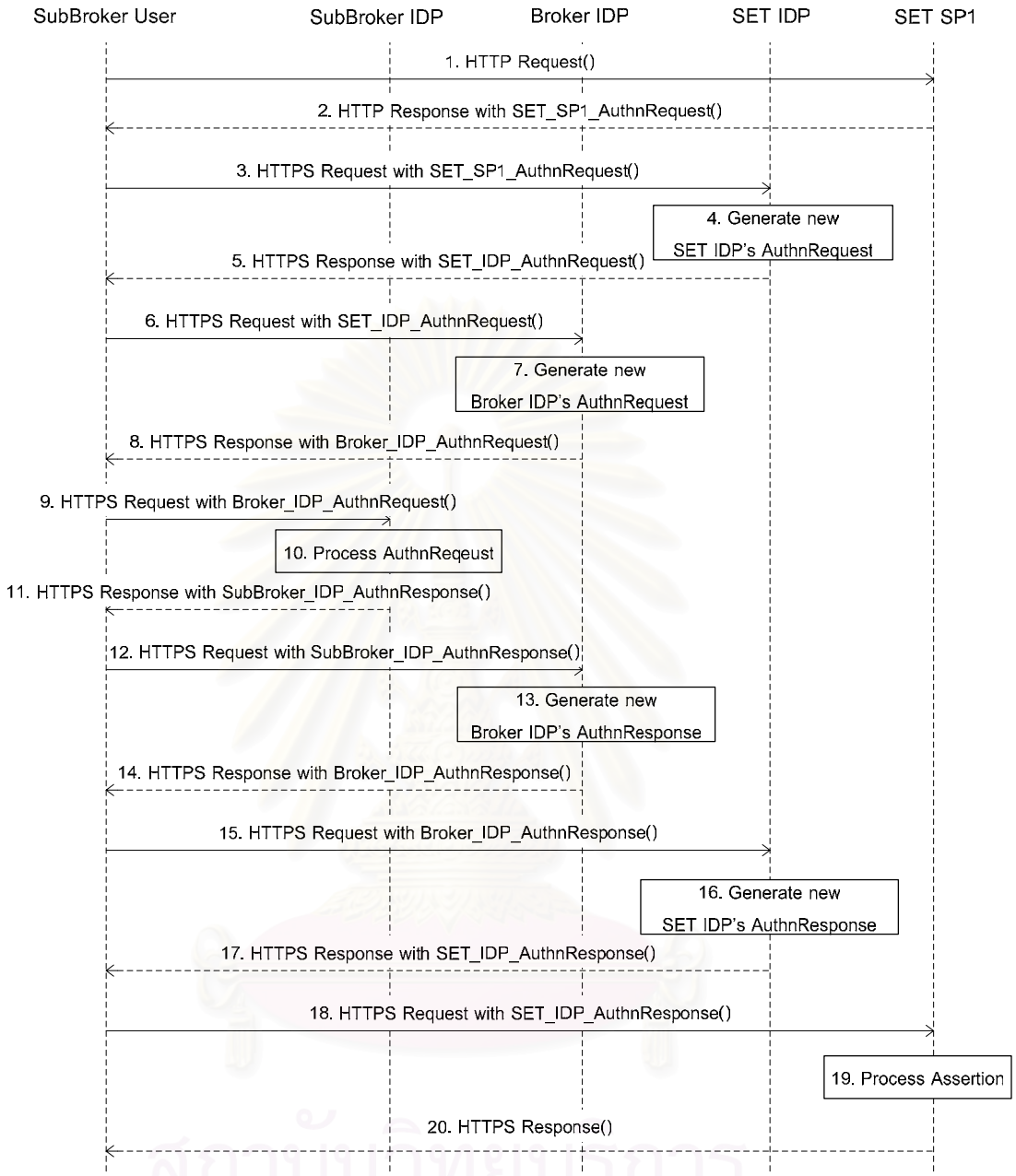
5. ในขั้นตอนที่7 ผู้ให้บริการที่ 1 ทำการตรวจสอบแมสเซจการตอบสนองการพิสูจน์ตัวจริงที่ได้รับมาว่าผู้ใช้ที่ร้องขอการใช้บริการผ่านการพิสูจน์ตัวจริงหรือไม่ ถ้าผ่านการพิสูจน์ตัวจริงผู้ให้บริการที่ 1 ทำการประมวลผลข้อความยืนยันตามข้อกำหนดของลิเบอร์ตี้ จากนั้นตรวจสอบสิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอมาได้หรือไม่ ถ้าผ่านการตรวจสอบสิทธิก็จะให้เข้าใช้บริการ และส่งผลลัพธ์ของการร้องขอกลับไปยังผู้ใช้ในขั้นตอนที่ 8

ขั้นตอนต่อจากนี้จะสันนิษฐานว่าผู้ใช้ร้องขอบริการที่มีการรักษาความปลอดภัยในผู้ให้บริการของตลาดหลักทรัพย์อีกครั้งหนึ่ง โดยผู้ใช้ได้ผ่านขั้นตอนการพิสูจน์ตัวจริงเรียบร้อยแล้ว และข้อความยืนยันการพิสูจน์ตัวจริงนั้นยังไม่หมดอายุ ผู้ใช้ก็สามารถเข้าใช้บริการได้โดยไม่ต้องทำการพิสูจน์ตัวจริงอีกครั้ง โดยแสดงในขั้นตอนที่ 9-15 ของรูปที่ 4.5

6. ขั้นตอนที่ 9 ผู้ใช้ทำการร้องขอการใช้บริการที่ SET SP2 ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการที่ 2 ซึ่งอยู่ภายในตลาดหลักทรัพย์
7. ขั้นตอนที่ 10-11 ผู้ให้บริการที่ 2 สร้างแมสเซจร้องขอการพิสูจน์ตัวจริงโดยระบุข้อมูลในอิลิเมนต์ <ProviderID> เป็นชื่อเฉพาะของผู้ให้บริการที่ 2 แล้วส่งผู้ใช้ไปยังบริการการลงบันทึกเข้าระบบเพียงครั้งเดียวของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์
8. ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ ตรวจสอบดูว่ามีข้อความยืนยันของผู้ใช้ที่ร้องขอการใช้บริการหรือไม่ แล้วข้อความยืนยันนั้นหมดอายุหรือยัง ถ้าพบว่ามีข้อความยืนยันของผู้ใช้ยังไม่หมดอายุ ผู้ให้บริการจะสร้างแมสเซจการตอบสนองการพิสูจน์ตัวจริง เพื่อส่งกลับไปให้ผู้ให้บริการที่ 2 ในขั้นตอนที่ 12 และ 13
9. ขั้นตอนที่ 14 ผู้ให้บริการที่ 2 ทำการตรวจสอบแมสเซจตอบสนองการพิสูจน์ตัวจริงที่ได้รับมาว่าผู้ใช้ที่ร้องขอการใช้บริการผ่านการพิสูจน์ตัวจริงหรือไม่ ถ้าผ่านการพิสูจน์ตัวจริงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ จะประมวลผลข้อความยืนยันตามข้อกำหนดของลิเบอร์ตี้ จากนั้นตรวจสอบสิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอมาได้หรือไม่ ถ้าผ่านการตรวจสอบสิทธิก็จะให้เข้าใช้บริการ และส่งผลลัพธ์ของการร้องขอกลับไปยังผู้ใช้ในขั้นตอนที่ 15

4.5.2 การใช้บริการระหว่างตลาดหลักทรัพย์ บริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย

การเรียกใช้บริการระหว่างองค์กรเสมือนจำเป็นต้องพิสูจน์ตัวจริงกับผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ขององค์กรเสมือนของผู้ให้บริการทรัพยากร โดยองค์กรเสมือนที่ติดต่อกันนั้นมีความเชื่อถือกันอยู่แล้ว ขั้นตอนการทำงานของโพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการระหว่างองค์กรเสมือนในรูปที่ 4.5 มีรายละเอียดดังนี้



รูปที่ 4.5 โพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการระหว่างตลาดหลักทรัพย์ บริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย

1. ขั้นตอนแรก ผู้ใช้ร้องขอการเข้าใช้บริการกับ SET SP1 ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการของตลาดหลักทรัพย์ โดยยังไม่ได้ทำการลงบันทึกเข้าระบบ
2. ในขั้นตอนที่ 2-3 ผู้ให้บริการของตลาดหลักทรัพย์สร้างแมสเซจร้องขอการพิสูจน์ตัวจริงโดยระบุข้อมูลในอิลิเมนต์ <ProviderID> เป็นชื่อเฉพาะของผู้ให้บริการของตลาดหลักทรัพย์พร้อมทั้งติดต่อกับผู้ใช้ เพื่อให้ผู้ใช้เลือกผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิกอยู่

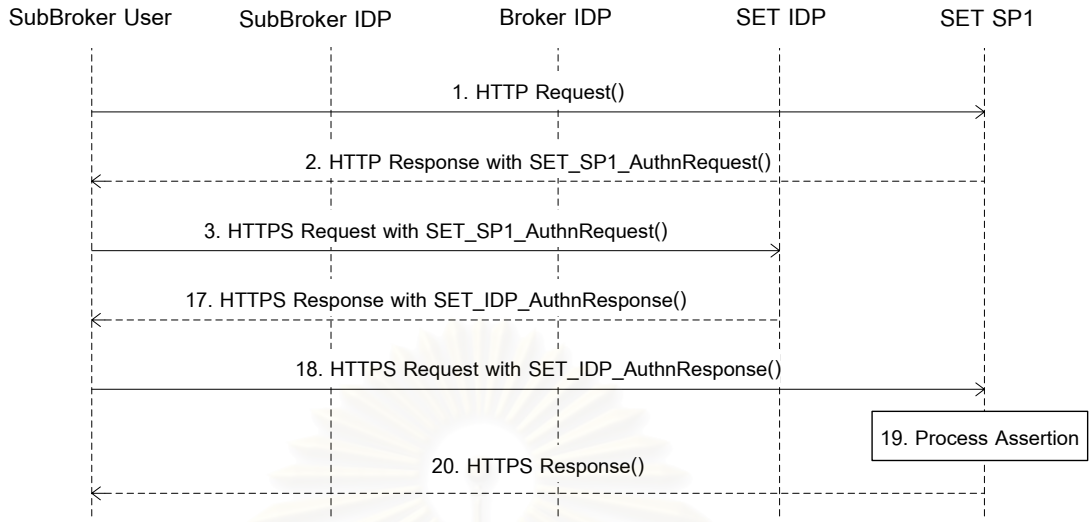
และส่งผู้ใช้ไปยังบริการการลงบันทึกเข้าระบบเพียงครั้งเดียวที่ SET IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์

3. ในขั้นตอนที่ 4 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ตรวจสอบข้อมูลชื่อเฉพาะของผู้ให้บริการที่ผู้ใช้ระบุมาให้ว่าตรงกับชื่อเฉพาะของตนหรือไม่ ถ้าไม่ตรงผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ต้องสร้างแมสเซจร้องขอการพิสูจน์ตัวจริงใหม่โดยคัดลอกแมสเซจร้องขอการพิสูจน์ตัวจริงเดิม แต่เปลี่ยนข้อมูลของผู้ร้องขอที่กำหนดในอิลิเมนต์ <AudienceRestrictionCondition> ให้เป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์เองและเก็บบันทึกผู้ร้องขอเดิมไว้ แล้วส่งไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งระบุมากับแมสเซจร้องขอการพิสูจน์ตัวจริง
4. ขั้นตอนที่ 5-6 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ส่งผู้ใช้ไปยังบริการการลงบันทึกเพียงครั้งเดียวของ Broker IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ ซึ่งผู้ใช้เป็นสมาชิกอยู่พร้อมแนบแมสเซจร้องขอการพิสูจน์ตัวจริงที่เพิ่งสร้างใหม่ไปด้วย
5. ขั้นตอนที่ 7 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ตรวจสอบข้อมูลชื่อเฉพาะของผู้ให้บริการที่ผู้ใช้ระบุมาว่าตรงกับชื่อเฉพาะของตนหรือไม่ ถ้าไม่ตรง ผู้ให้บริการต้องสร้างแมสเซจร้องขอการพิสูจน์ตัวจริงใหม่โดยคัดลอกแมสเซจร้องขอการพิสูจน์ตัวจริงเดิม แต่เปลี่ยนข้อมูลของผู้ร้องขอที่กำหนดในอิลิเมนต์ <AudienceRestrictionCondition> ให้เป็นผู้ให้บริการเอง และเก็บบันทึกผู้ร้องขอเดิมไว้ แล้วส่งไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งระบุมากับแมสเซจร้องขอการพิสูจน์ตัวจริง
6. ขั้นตอนที่ 7-8 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ส่งผู้ใช้ไปยังบริการการลงบันทึกเพียงครั้งเดียวของ SubBroker IDP ซึ่งต่อไปนี้จะเรียกว่า ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย ซึ่งผู้ใช้เป็นสมาชิกอยู่พร้อมแนบแมสเซจร้องขอการพิสูจน์ตัวจริงที่เพิ่งสร้างใหม่ไปด้วย
7. ขั้นตอนที่ 10 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยทำการพิสูจน์ตัวจริงให้กับผู้ใช้ จากนั้นสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงที่บรรจุข้อความยืนยันการพิสูจน์ตัวจริงของผู้ใช้
8. ขั้นตอนที่ 11-12 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยส่งแมสเซจตอบสนองการพิสูจน์ตัวจริงกลับไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์
9. เมื่อได้รับแมสเซจตอบสนองกลับมา ในขั้นตอนที่13 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์จะสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงใหม่ โดยผู้ร้อง

ขอในอิลิเมนต์ <AudienceRestrictionCondition> กำหนดเป็นผู้ร้องขอเดิมซึ่งเก็บไว้เมื่อขั้นตอนที่ 7 พร้อมทั้งเพิ่มอิลิเมนท์ <AuthnContext> ซึ่งระบุเป็นผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ย่อย

10. ขั้นตอนที่ 14-15 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของบริษัทนายหน้าซื้อขายหลักทรัพย์ส่งแมสเซจตอบสนองการพิสูจน์ตัวจริงกลับไปยังผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์
11. เมื่อได้รับแมสเซจตอบสนองกลับมา ในขั้นตอนที่16 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์จะสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริงใหม่ โดยผู้ร้องขอในอิลิเมนต์ <AudienceRestrictionCondition> กำหนดเป็นผู้ร้องขอเดิมซึ่งเก็บไว้เมื่อขั้นตอนที่ 7
12. ขั้นตอนที่ 17-18 ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ส่งแมสเซจตอบสนองการพิสูจน์ตัวจริงกับไปยังผู้ให้บริการของตลาดหลักทรัพย์
13. ขั้นตอนที่ 19 เมื่อได้รับแมสเซจ ผู้ให้บริการของตลาดหลักทรัพย์ ตรวจสอบแมสเซจการตอบสนองการพิสูจน์ตัวจริงใหม่ว่าผู้ใช้ที่ร้องขอการใช้บริการผ่านการพิสูจน์ตัวจริงหรือไม่ ถ้าผ่านการพิสูจน์ตัวจริงผู้ให้บริการของตลาดหลักทรัพย์ ทำการประมวลผลข้อความยืนยันตามข้อกำหนดของลิเบอร์ตี้ จากนั้น ตรวจสอบสิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอมาได้หรือไม่ ถ้าผ่านการตรวจสอบสิทธิจะให้เข้าใช้บริการ และส่งผลกลับไปยังผู้ใช้ในขั้นตอนที่ 20

ถ้าผู้ใช้ต้องการเข้าใช้บริการที่ผู้ให้บริการทรัพยากรของตลาดหลักทรัพย์อีกครั้ง ซึ่งผู้ใช้ผ่านขั้นตอนของการพิสูจน์ตัวจริงมาแล้ว และข้อความยืนยันที่ได้รับมานั้นยังไม่หมดอายุ ผู้ใช้ก็สามารถเข้าใช้บริการได้โดยไม่ต้องทำการพิสูจน์ตัวจริงอีกครั้ง ดังแสดงในรูปที่ 4.5 ซึ่งมีรายละเอียดของขั้นตอนเหมือนในรูปที่ 4.5 ต่างกันเพียงขั้นตอนที่ 3 เมื่อผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ได้รับแมสเซจร้องขอการพิสูจน์ตัวจริงมาแล้ว ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ของตลาดหลักทรัพย์ตรวจสอบว่าผู้ใช้ที่ทำการร้องขอผ่านการพิสูจน์ตัวจริงแล้วหรือยัง เมื่อพบว่าผ่านการพิสูจน์ตัวจริงแล้ว และข้อความยืนยันของผู้ใช้นั้นยังไม่หมดอายุ จะทำการสร้างแมสเซจการตอบสนองการพิสูจน์ตัวจริงจากข้อมูลยืนยันของผู้ใช้ แล้วส่งกลับไปให้ผู้ให้บริการทรัพยากรของตลาดหลักทรัพย์ ในขั้นตอนที่ 17-18



รูปที่ 4.5 โพรโทคอลการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการใช้บริการระหว่างตลาดหลักทรัพย์ บริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อย เมื่อผู้ใช้ผ่านการลงบันทึกเข้าระบบเรียบร้อยแล้ว

4.6 ตัวอย่างการอิมพลีเมนต์การลงบันทึกเข้าระบบของตลาดหลักทรัพย์

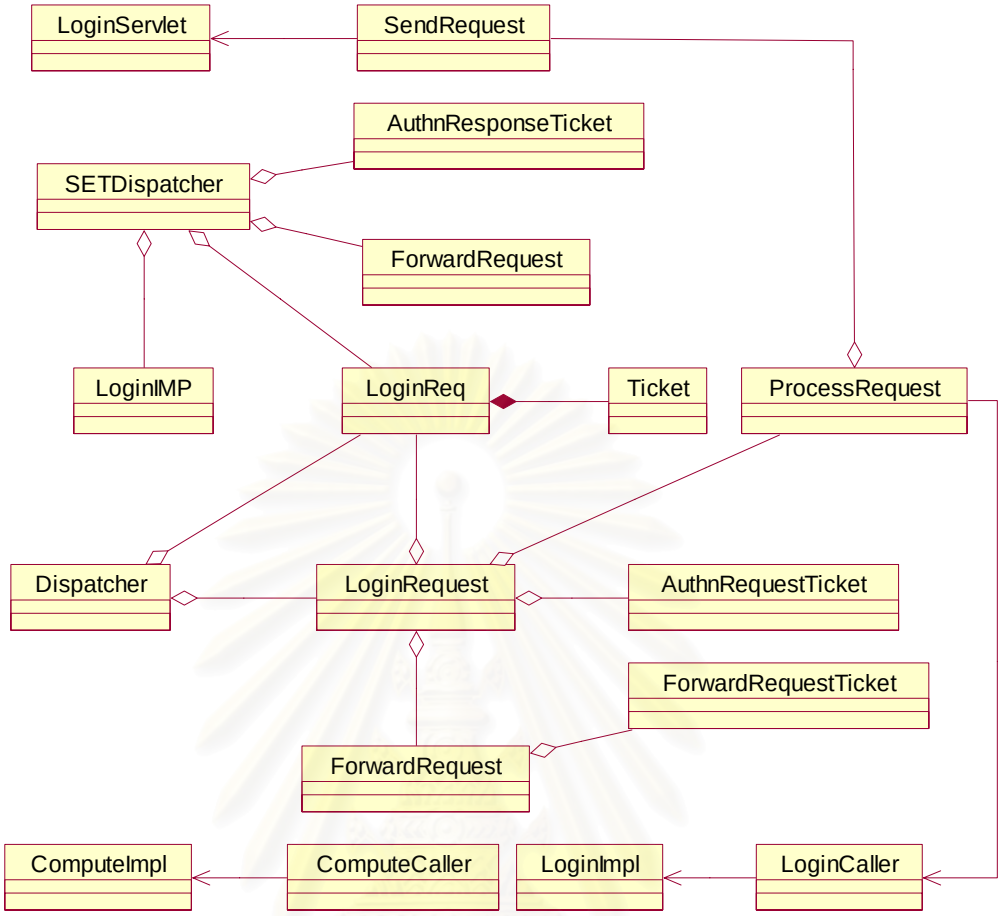
ตัวอย่างการอิมพลีเมนต์การลงบันทึกเข้าระบบของตลาดหลักทรัพย์แบ่งงานออกเป็น 2 ส่วนหลักๆ คือ ส่วนของการลงบันทึกเข้าระบบ และ ส่วนของบริการการรับข้อมูลการขายหุ้น มีรายละเอียดดังนี้

4.6.1 แผนภาพคลาส (Class Diagram)

จากรูปที่ 4.6 แสดงคลาสทั้งหมด 20 คลาส ประกอบด้วย คลาสในส่วนของการลงบันทึกเข้าระบบได้แก่ LoginServlet SendRequest SETDispatcher AuthnResponseTicket LoginIMP LoginReq Ticket ProcessRequest Dispatcher LoginRequest ForwardRequest AuthnRequestTicket ForwardRequestTicket LoginImpl และ LoginCaller และคลาสในส่วนของการบริการการรับข้อมูลการขายหุ้น ได้แก่ ComputeImpl และ ComputeCaller

4.6.1.1 คลาส LoginServlet

คลาส LoginServlet ทำหน้าที่รับการร้องขอมาเพื่อสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริง โดยรับข้อมูลนำเข้าเป็นแมสเซจร้องขอการพิสูจน์ตัวจริงและข้อความยืนยันการพิสูจน์ตัวจริงของผู้ใช้ ซึ่งผ่านขั้นตอนการพิสูจน์ตัวจริง แล้วนำมาประมวลผลเพื่อสร้างแมสเซจ ตอบสนองการพิสูจน์ตัวจริง



รูปที่ 4.6 แผนภาพคลาสของระบบการลงบันทึกเข้าระบบของตลาดหลักทรัพย์

4.6.1.2 **คลาส** SendRequest

คลาส SendRequest ทำหน้าที่ส่งแมสเซจเพื่อร้องขอการสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริง โดยจะทำการส่งข้อมูลยืนยันการพิสูจน์ตัวจริงของผู้ใช้ และแมสเซจร้องขอการพิสูจน์ตัวจริงไปให้กับคลาส LoginServlet

4.6.1.3 **คลาส** SETDispatcher

คลาส SETDispatcher เป็นคลาสหลักของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ โดยเปิดรับทุกการร้องขอ แล้วจะส่งไปให้กับส่วนประมวลผลอื่นๆ ที่เกี่ยวข้อง

4.6.1.4 **คลาส** AuthnResponseTicket

คลาส AuthnResponseTicket เป็นคลาสที่ถ่ายทอดมาจากคลาส Ticket ซึ่งใช้เก็บข้อมูลของแมสเซจตอบสนองการพิสูจน์ตัวจริง และข้อความยืนยันการพิสูจน์ตัวจริง

4.6.1.5 **คลาส** LoginIMP

คลาส LoginIMP ทำหน้าที่ตรวจสอบการพิสูจน์ตัวจริงของผู้ใช้ โดยรับข้อมูลชื่อผู้ใช้และรหัสผ่าน แล้วนำมาตรวจสอบกับข้อมูลผู้ใช้ที่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ถ้าข้อมูลของผู้ใช้ตรงกับข้อมูลที่ผู้ให้บริการทรัพยากร ผู้ให้บริการทรัพยากรจะสร้างข้อความยืนยันการพิสูจน์ตัวจริงส่งกลับไปให้กับคลาสที่เรียกมา

4.6.1.6 **คลาส** LoginReq

คลาส LoginReq เป็นคลาสที่ใช้เก็บรายละเอียดข้อมูลเกี่ยวกับการพิสูจน์ตัวจริง เพื่อใช้ในการพิสูจน์สิทธิของผู้ใช้

4.6.1.7 **คลาส** Ticket

คลาส Ticket เป็นคลาสพื้นฐานของแมสเซจทั้งสองชนิด ได้แก่แมสเซจร้องขอการพิสูจน์ตัวจริง และแมสเซจตอบสนองการพิสูจน์ตัวจริง

4.6.1.8 **คลาส** ProcessRequest

คลาส ProcessRequest เป็นคลาสทำหน้าที่เรียกใช้คลาส LoginCaller เพื่อการพิสูจน์ตัวจริง และเรียกใช้คลาส SendRequest เพื่อร้องขอการสร้างแมสเซจตอบสนองการพิสูจน์ตัวจริง

4.6.1.9 **คลาส** Dispatcher

คลาส Dispatcher เป็นคลาสหลักของผู้ให้บริการทรัพยากร จะเปิดรับทุกการร้องขอจากผู้ใช้ ถ้าผู้ใช้ต้องการเข้าใช้บริการที่มีการรักษาความปลอดภัย คลาสนี้จะสร้างอินสแตนท์ (Instance) ของคลาส LoginRequest เพื่อร้องขอการพิสูจน์ตัวจริงจากผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และสร้างอินสแตนท์ของคลาส AuthnRequestTicket เพื่อใช้เป็นแมสเซจการร้องขอการพิสูจน์ตัวจริงส่งไปให้ด้วย

4.6.10 **คลาส** LoginRequest

คลาส LoginRequest ทำหน้าที่สร้างแมสเซจการร้องขอการพิสูจน์ตัวจริง และส่งผู้ใช้พร้อมกับแมสเซจที่สร้างขึ้น ไปให้ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เพื่อทำการพิสูจน์ตัวจริงตามที่ผู้ใช้ระบุมา

4.6.1.11 **คลาส** ForwardRequest

คลาส ForwardRequest จะตรวจสอบชื่อเฉพาะของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ และสร้างแมสเซจการร้องขอการพิสูจน์ตัวจริงของผู้ให้บริการใหม่ จากนั้นส่งต่อผู้ใช้พร้อมกับแมสเซจที่สร้างขึ้นไปให้กับบริการของผู้ให้บริการนั้นๆ เพื่อทำการพิสูจน์ตัวจริง เมื่อผู้ให้บริการเหล่านั้นทำการพิสูจน์ตัวจริงให้กับผู้ใช้เรียบร้อยแล้วจะส่งกลับแมสเซจตอบสนองการพิสูจน์ตัวจริงกลับมาให้

4.6.1.12 **คลาส** ForwardRequestTicket

คลาส ForwardRequestTicket เป็นคลาสที่ถ่ายทอดมาจากคลาส Ticket ซึ่งใช้เก็บข้อมูลของแมสเซจการร้องขอการพิสูจน์ตัวจริง

4.6.1.13 **คลาส** AuthnRequestTicket

คลาส AuthnRequestTicket เป็นคลาสที่ถ่ายทอดมาจากคลาส Ticket ซึ่งใช้เก็บข้อมูลของแมสเซจการร้องขอการพิสูจน์ตัวจริง

4.6.1.14 **คลาส** LoginImpl

คลาส LoginImpl เป็นคลาสที่อิมพลีเมนต์มาจากอินเทอร์เฟส LoginIF ทำหน้าที่ตรวจสอบการพิสูจน์ตัวจริงของผู้ใช้ โดยรับข้อมูลชื่อผู้ใช้และรหัสผ่าน แล้วนำมาตรวจสอบกับข้อมูลผู้ใช้ที่ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ถ้าข้อมูลของผู้ใช้ตรงกับข้อมูลที่ผู้ให้บริการผู้ให้บริการจะสร้างข้อความยืนยันการพิสูจน์ตัวจริงส่งกลับไปให้กับคลาสที่เรียกมา

4.6.1.15 **คลาส** LoginCaller

คลาส LoginCaller ทำหน้าที่เป็นไคลเอนต์เพื่อเรียกใช้คลาส LoginImpl โดยผู้เรียกคลาสนี้คือ ProcessRequest

4.6.1.16 **คลาส** ComputeImpl

คลาส ComputeImpl เป็นคลาสที่อิมพลีเมนต์มาจากอินเทอร์เฟส ComputeIF ทำหน้าที่รับข้อมูลการขายหุ้นจากผู้ใช้ แล้วส่งข้อมูลยืนยันกลับไปหาผู้ใช้ว่าได้รับข้อความนั้นเรียบร้อยแล้ว

4.6.1.17 **คลาส** ComputeCaller

คลาส ComputeCaller ทำหน้าที่เป็นไคลเอนต์เพื่อเรียกใช้คลาส ComputeImpl

บทที่ 5
สรุปผลการวิจัย และข้อเสนอแนะ

จากการศึกษาการลงบันทึกเข้าระบบเพียงครั้งเดียวพบว่า เป็นแนวคิดที่ช่วยแก้ปัญหาเรื่องความหลากหลายของข้อมูลสำหรับระบุผู้ใช้ในการพิสูจน์ตัวจริงของระบบที่ต่างกัน นอกจากนั้น ยังช่วยอำนวยความสะดวกให้กับผู้ใช้ในการเข้าใช้ระบบที่มีการรักษาความปลอดภัยด้วยการพิสูจน์ตัวจริงอีกด้วย แต่อย่างไรก็ตาม การนำสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์ที่ออกแบบขึ้นไปใช้งานจริงยังขาดความชัดเจนของการพิสูจน์ตัวจริงของผู้ใช้ข้ามองค์กรเสมือน ดังนั้นในงานวิทยานิพนธ์นี้จึงมีจุดประสงค์เพื่อศึกษาสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์ โดยศึกษาวิธีการออกแบบและการทำงานของสถาปัตยกรรมนั้น และออกแบบสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนบนพื้นฐานสถาปัตยกรรมของลิเบอร์ตี้แอลไลแอนซ์ และเพื่อเป็นการทดสอบแนวคิดที่ได้ศึกษามา จึงมีการทดลองไปพัฒนากับระบบการพิสูจน์ตัวจริงของตลาดหลักทรัพย์ที่มีการติดต่อกับองค์กรอื่นๆ เช่น บริษัทนายหน้าซื้อขายหลักทรัพย์ ซึ่งเริ่มพัฒนาระบบตั้งแต่การออกแบบโครงสร้างพื้นฐานให้กับตลาดหลักทรัพย์ จนได้ออกมาเป็นโค้ดที่เสร็จสมบูรณ์ ซึ่งสามารถสรุปผลที่ได้จากการวิจัย อุปสรรคของการพัฒนาสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือน แนวทางการวิจัยในอนาคต รวมถึงข้อเสนอแนะต่างๆ ดังนี้

5.1 สรุปผลการวิจัย

วิทยานิพนธ์นี้ ได้ทำการสร้างสถาปัตยกรรมของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนบนพื้นฐานของแนวคิดการลงบันทึกเข้าระบบเพียงครั้งเดียวของลิเบอร์ตี้แอลไลเอนซ์ ซึ่งเพิ่มเติมความสามารถในส่วนของการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนตั้งแต่ 2 องค์กรเสมือนขึ้นไป โดยการกำหนดโครงสร้างพื้นฐานขององค์กรเสมือนที่ใช้กับสถาปัตยกรรมที่สร้างขึ้น ต่อจากนั้นออกแบบโพรไฟล์บราวเซอร์/โพสของการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับการส่งข้อความยืนยันในการพิสูจน์ตัวผู้ใช้ระหว่างผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ให้บริการทรัพยากรขององค์กรเสมือนตั้งแต่ 2 องค์กรขึ้นไป และออกแบบเนมสเปซให้กับตัวกระทำต่างๆ ขององค์กรเสมือน โดยใช้รูปแบบการกำหนดเนมสเปซของมาตรฐานไดเรกทอรีเอ็กซ์ 500 เพื่อใช้ในการระบุเส้นทางในการค้นหาผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิก จากนั้นทำการทดลองพัฒนาการลงบันทึกเข้าระบบของตลาดหลักทรัพย์ที่มีการติดต่อกับบริษัทนายหน้าซื้อขายหลักทรัพย์ และบริษัทนายหน้าซื้อขายหลักทรัพย์ย่อยโดยใช้สถาปัตยกรรมที่สร้างขึ้น ซึ่งข้อแตกต่างระหว่างสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนกับข้อกำหนดของลิเบอร์ตี้แอลไลเอนซ์ และโครงสร้างการรักษาความ

ปลอดภัยสามารถอธิบายได้ดังตารางที่ 5.1 โดยเครื่องหมายถูก (✓) แปลว่าเทคโนโลยีนั้นๆ มีลักษณะ (Feature) ที่กำหนด และเครื่องหมายผิด (✘) แปลว่าเทคโนโลยีนั้นไม่มีลักษณะที่กำหนด

ตารางที่ 5.1 การเปรียบเทียบลักษณะของสถาปัตยกรรมการลงบันทึกเข้าระบบเพียงครั้งเดียวระหว่างองค์กรเสมือนกับลิเบอร์ตี้แอลไลเอนซ์ และโครงสร้างการรักษาความปลอดภัยเชิงกริด

Features	Single Sign-on Cross Virtual Organizations	Liberty Alliance	Grid Security Infrastructure
Single sign-on mechanism	Identity Federation	Identity Federation	Proxy Credential
Support single virtual organization authentication	✓	✓	✓
Support cross virtual organization authentication	✓	✘	✘
Use of pseudonyms	✓	✓	✘
Support for anonymity	✓	✓	✘
Global logout	✓	✓	✘
Global namespace	✓	✘	✓
Authorization control	Resource and Identity Provider	Resource and Identity Provider	Resource

5.2 แนวทางการวิจัยในอนาคต

จากงานวิจัยนี้ ยังมีประเด็นที่สามารถนำมาทำการวิจัยต่อเนื่องได้ ดังนี้

5.2.1 การสร้างการค้นหาเส้นทางของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้

เทคโนโลยีของการลงบันทึกเข้าระบบของลิเบอร์ตี้แอลไลเอนซ์ยังไม่ได้กล่าวถึงวิธีการระบุผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ถูกต้องของผู้ใช้งาน จะเป็นเพียงการเก็บรายชื่อของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ ซึ่งเคยมีความเชื่อถือกันกับผู้ให้บริการทรัพยากรเท่านั้น โดยผู้พัฒนาระบบจะต้องหาวิธีในการระบุผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้เอาเอง

5.2.2 บริการแอททริบิวท์ (Attribute Service)

เมื่อผู้ใช้ติดต่อกับทรัพยากรของผู้ให้บริการซึ่งอยู่ในขอบเขตของความเชื่อถือต่างกัน ผู้ให้บริการควรจะรู้เกี่ยวกับข้อมูลของผู้ใช้เพื่อที่จะสร้างบริการที่เป็นส่วนตัวให้กับผู้ใช้ โดยบริการ

แอททริบิวท์นี้จะอยู่ภายในโดเมน หรือระหว่างโดเมน ซึ่งให้บริการข้อมูลเกี่ยวกับสิทธิของผู้ใช้ และอนุญาตให้เอนทิตีที่มีสิทธิสามารถใช้ข้อมูลร่วมกันได้

5.3 ข้อเสนอแนะ

1. วิธีการค้นหาผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ที่ผู้ใช้เป็นสมาชิกในงานวิจัยนี้ใช้วิธีการแนบพาธของผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้ไปด้วยซึ่งง่ายต่อการพัฒนา แต่ในการใช้งานจริงนั้นควรจะมีการสร้างเชิร์ฟเวอร์ที่ทำหน้าที่เหมือนดีเอ็นเอสเชิร์ฟเวอร์เพื่อให้ผู้ให้บริการข้อมูลสำหรับระบุผู้ใช้และผู้ใช้สามารถสอบถามพาธของผู้ให้บริการข้อมูลสำหรับผู้ใช้ได้

2. การทำงานร่วมกันระหว่างองค์กรไม่จำเป็นจะต้องใช้เทคโนโลยีเดียวกันในการลงบันทึกเข้าระบบเพียงครั้งเดียว ดังนั้นจึงควรหาวิธีในการใช้งานร่วมกันของการลงบันทึกเข้าระบบเพียงครั้งเดียวของเทคโนโลยีต่างๆ

รายการอ้างอิง

1. Clercq, J.D. Single Sign-On Architectures. Proceedings of the International Conference on Infrastructure Security. 2002.
2. Microsoft .NET Passport Review Guide. (Online). Available from: http://www.microsoft.com/net/services/passport/review_guide.asp: Microsoft, (2004, February 14).
3. Cantor, S. and Kemp, J. Liberty ID-FF Architecture Overview Version: 1.2. (Online). Available from: http://www.projectliberty.org/specs/: Liberty Alliance Project, (2004, February 14).
4. Cantor, S. and Kemp, J. Liberty ID-FF Protocols and Schema Specification Version: 1.2. (Online). Available from: http://www.projectliberty.org/specs/: Liberty Alliance Project, (2004, February 14).
5. Cantor, S. and Kemp, J. Liberty ID-FF Bindings and Profiles Specification Version: 1.2. (Online). Available from: http://www.projectliberty.org/specs/: Liberty Alliance Project, (2004, February 14).
6. Maler, E., et al. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. (Online). Available from: http://www.oasis-open.org/committees/security/: OASIS, (2004, February 14).
7. Butler, R., et al. A National-Scale Authentication Infrastructure. IEEE Computer Society magazine. 2000.
8. Novotny, J., Tuecke, S., and Welch, V. An Online Credential Repository for the Grid: MyProxy. Proceedings of 10th IEEE International Symposium on High Performance Distributed Computing. 2001.
9. Overview of the Grid Security Infrastructure. (Online). Available from: http://www-unix.globus.org/security/overview.html: The Globus Alliance, (2004, February 14).
10. ชัยนันท์ กมลวดี. เพิ่มพลังเครือข่ายเต็มพิกัดด้วย Directory Service. กรุงเทพฯ: สำนักพิมพ์ เอส.พี.ซี บุ๊คส์, 2003.
11. จตุชัย แพงจันทร์และอนุโชต วุฒิพรพงษ์. เจาะระบบ Network ฉบับสมบูรณ์. 1. นนทบุรี: ไอดีซี, 2003.

12. Jamhour, E. Distributed Security Management using LDAP Directories. Proceedings of Computer Science Society, 2001. SCCC 2001. Proceedings. XXI Internatinal Conference of the Chilean. 2001.

13. Pearlman, L., et al. A Community Authorization Service for Group Collaboration. Proceedings of Policies for Distributed Systems and Networks. 2002.

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวณิศรา ศิริพรกุลทรัพย์ เกิดเมื่อวันที่ 31 กรกฎาคม พ.ศ. 2523 ที่กรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาตรีวิทยาศาสตรบัณฑิต คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์ สาขาศาสตร์คอมพิวเตอร์ ในปีการศึกษา 2543 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยในปีการศึกษา 2544