การออกแบบและพัฒนาระบบจัดการสิทธิแบบกลุ่มคนในสภาพแวดล้อมของกริดจีทีสาม

นายปฏิภาณ คงสิริกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2547

ISBN 974-17-6991-1

THE DESIGN AND DEVELOPMENT OF COMMUNITY-BASED AUTHORIZATION MANAGEMENT SYSTEM IN THE GRID GT3 ENVIRONMENT

Mr. Patipan Kongsirikul

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering in Computer Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2004

ISBN 974-17-6991-1

หัวข้อวิทยานิพนธ์	การออกแบบและพัฒนาระบบจัดการสิทธิแบบกลุ่มคนในสภาพแวดล้อมของกริดจีทีสาม
โดย	นายปฏิภาณ คงสิริกุล
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	ดร.ณัฐวุฒิ หนูไพโรจน์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

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

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

..... กรรมการ
(ดร.วีระ เหมืองสิน)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ภุชงค์ อุทโยภาศ)

นายปฏิภาณ คงสิริกุล : การออกแบบและพัฒนาระบบจัดการสิทธิแบบกลุ่มคนในสภาพแวดล้อมของกริดจีทีสาม. (THE DESIGN AND DEVELOPMENT OF COMMUNITY-BASED AUTHORIZATION MANAGEMENT SYSTEM IN THE GRID GT3 ENVIRONMENT) อ. ที่ปรึกษา : ดร.ณัฐวุฒิ หนูไพโรจน์, 113 หน้า. ISBN 974-17-6991-1.

กริดได้รับความนิยมอย่างมากสำหรับการนำไปใช้เป็นสภาพแวดล้อมของงานทดลองทางวิทยาศาสตร์ ซึ่งจะประกอบไปด้วยผู้ใช้และทรัพยากรเป็นจำนวนมาก และการที่ระบบจัดการสิทธิของกริดสำหรับผู้ใช้จะทำบนแต่ละทรัพยากรแยกกัน ทำให้ระบบกริดมีความสามารถในการขยายตัวของระบบที่ไม่ดี ในช่วงสองปีที่ผ่านมา แนวคิดในการรวมหรือเชื่อมต่อองค์กรเสมือนต่างๆเข้าด้วยกันได้รับความนิยมเพิ่มมากขึ้น แต่ในปัจจุบันก็ยังไม่มีระบบจัดการสิทธิใดๆที่รองรับการทำงานขององค์กรเสมือนที่เชื่อมต่อกันได้

วิทยานิพนธ์นี้มีจุดประสงค์ที่จะออกแบบและพัฒนาระบบจัดการสิทธิการใช้ทรัพยากรแบบกลุ่มคนในกริดที่รองรับการทำงานบนสภาพแวดล้อมที่มีองค์กรเสมือนเชื่อมต่อกันได้ ซึ่งในงานวิจัยนี้ได้นำแนวคิดสถาปัตยกรรมของงานวิจัยซีเอเอสมาใช้เป็นพื้นฐานและขยายขีดความสามารถ โดยพัฒนาให้สามารถทำงานร่วมกันกับบริการแกรมซึ่งเป็นบริการหลักในโกลบัสทูลคิด และพัฒนาบริการจัดการสิทธิดังกล่าวให้รองรับการทำงานบนสภาพแวดล้อมที่มีองค์กรเสมือนเชื่อมต่อกันได้ โดยเสนอแนวคิดไว้ 2 แนวคิดได้แก่ แนวคิดการทำหนังสือเดินทางและแนวคิดการเปลี่ยนบัตร จากผลการทดลองแสดงให้เห็นระบบที่ได้พัฒนาจะสามารถรองรับการทำงานบนสภาพแวดล้อมที่องค์กรเสมือนเชื่อมต่อกันได้อย่างถูกต้อง ถ้าผู้ใช้เลือกหลักฐานอ้างอิงผู้ใช้ตัวแทนที่เหมาะกับสภาพแวดล้อมของการเชื่อมต่อนั้นๆ

ภาควิชา.... วิศวกรรมคอมพิวเตอร์.....ลายมือชื่อนิสิต.....
สาขาวิชา....วิศวกรรมคอมพิวเตอร์.....ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา .....2547.....

45704652 : MAJOR Computer Engineering

KEY WORD: GRID / AUTHORIZATION / COMMUNITY / GLOBUS TOOLKIT / VIRTUAL ORGANIZTIONS

PATIPAN KONGSIRIKUL : THE DESIGN AND DEVELOPMENT OF COMMUNITY-BASED AUTHORIZATION MANAGEMENT SYSTEM IN THE GRID GT3 ENVIRONMENT. THESIS ADVISOR : NATAWUT NUPAIROJ, Ph.D, 113 pp.

ISBN 974-17-6991-1.

Grid becomes popular for enabling scientific experiment environment, consisting of many users and resources. Grid authorization management is performed on each individual resource. This causes grid system poor scalability. In the past two year, the concept of integrated VOs has become increasingly popular. However, there is no authorization framework that can support multiple VOs at the moment.

The objective of this thesis is to design and develop the community-based authorization management system that support integrated VOs environment. We utilize Community Authorization Service as a foundation and extend its features to support Globus Resource Allocation Manager (GRAM), which is the main component in Globus toolkit. This thesis also proposes two solutions for integrated VOs problems, passport concept and exchange credential concept. Our experiments indicate that our authorization framework work well in the integrated VOs environments, given that user choose the proxy credential scheme that is apropriate to the integrated VOs environments.

Department…. Computer Engineering…. Student's.....
Field of study…. Computer Engineering…Advisor's.....
Academic year …2004…….

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จออกมาได้ด้วยความกรุณาของ ดร.ณัฐวุฒิ หนูไพโรจน์ อาจารย์ที่ปรึกษา ซึ่งนอกจากจะช่วยให้คำแนะนำและความคิดเห็นเกี่ยวกับงานวิจัยแล้ว ยังสอนความรู้อื่น ๆ อีกมากมายซึ่งมีส่วนในการเปิดโลกทัศน์การเรียนรู้ของข้าพเจ้า

ขอขอบคุณเพื่อน ๆ พี่ ๆ และน้อง ๆ ทุกคนในห้องปฏิบัติการระบบสารสนเทศและเพื่อนร่วมรุ่นของข้าพเจ้าทุกคนที่ช่วยแก้ปัญหาเบ็ดเตล็ดในงานวิจัย

เหนือสิ่งอื่นใดข้าพเจ้าคงไม่มีทางทำงานวิจัยนี้สำเร็จถ้าขาดพระคุณของคุณพ่อและคุณแม่ที่ให้กำเนิด อบรมเลี้ยงดู สอนความรู้ ให้โอกาส และห่วงใยข้าพเจ้าเสมอมา

สารบัญ

หน้า

สารบัญ(ต่อ)

สารบัญ(ต่อ)

สารบัญภาพ

หน้า

สารบัญภาพ(ต่อ)

สารบัญภาพ(ต่อ)

สารบัญภาพ(ต่อ)

สารบัญตาราง

หน้า

บทที่1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

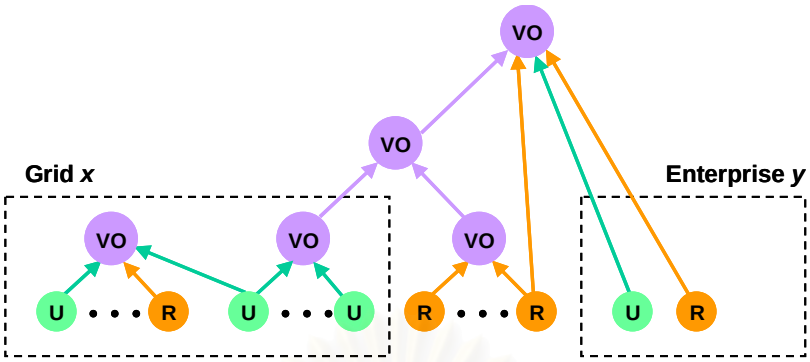
แนวความคิดของกริดคือความพยายามที่จะสร้างองค์กรเสมือน(VOs: Virtual Organizations) โดยการรวบรวมองค์กร (PO: Physical Organization) ต่างๆเข้ามาด้วยกันเพื่อให้เกิดโครงสร้างที่สามารถใช้ทรัพยากรร่วมกันระหว่างองค์กรได้ โดยแต่ละองค์กรภายในองค์กรเสมือนเดียวกันจะมีความเชื่อถือกัน ทำให้ผู้ใช้ต่างองค์กรกันสามารถเข้าไปใช้ทรัพยากรในอีกองค์กรได้ การที่มีโครงสร้างที่สามารถใช้ทรัพยากรร่วมกันได้ทำให้เกิดประโยชน์หลายอย่างด้วยกัน เช่น งานที่ใช้การประมวลผลมากก็จะสามารถนำกริดมาใช้งานซึ่งจะส่งผลให้งานเสร็จเร็วขึ้น เนื่องจากมีจำนวนหน่วยประมวลผลที่มากขึ้น นอกจากนี้ งานที่ใช้หน่วยเก็บข้อมูลจำนวนมาก เช่น แฟ้มขนาด 1 เทระไบต์ขึ้นไป จะไม่สามารถเก็บไว้ในหน่วยเก็บข้อมูลปกติได้ และการเคลื่อนย้ายข้อมูล (FTP: File Transfer Protocol) ทำได้ไม่สะดวกซึ่งจะพบมากในงานประเภทการทดลองทางวิทยาศาสตร์ ดังนั้นนักวิทยาศาสตร์ส่วนใหญ่จึงให้ความสนใจที่จะลองใช้ระบบกริดซึ่งสามารถใช้ทรัพยากรการเก็บข้อมูลร่วมกันได้กล่าวคือกริดสามารถแบ่งแฟ้มออกเป็นแฟ้มย่อยๆไปเก็บยังหน่วยเก็บข้อมูลบนต่างเครื่องกันได้ และยังมีการจัดการเกี่ยวกับการเคลื่อนย้ายข้อมูลขนาดใหญ่ที่มีประสิทธิภาพ ตัวอย่างการใช้งานกริดในปัจจุบันได้แก่ การพยากรณ์อากาศ การออกแบบยารักษาโรค และการวิเคราะห์ลักษณะทางพันธุกรรม เป็นต้น ซึ่งในส่วนของประเทศไทยเองก็ได้ให้ความสนใจในเทคโนโลยีของกริด เช่น โครงการอีไซน์ไทยแลนด์(eScience)[1] ซึ่งเป็นโครงการที่ต้องการสร้างสภาพแวดล้อมของการคำนวณสำหรับนักวิทยาศาสตร์สาขาต่างๆโดยใช้โครงสร้างของกริด และ โครงการไทยกริด(ThaiGrid)[2] ซึ่งเป็นโครงการที่สร้างขึ้นมาเพื่อรวมกลุ่มของผู้พัฒนาระบบกริดระหว่างมหาวิทยาลัยต่างๆและห้องปฏิบัติการวิจัยกริดในไทย เป็นต้น

เนื่องจากแนวความคิดในการใช้ทรัพยากรร่วมกันระหว่างองค์กรของกริดนั้นได้รับความนิยมอย่างมากในกลางทศวรรษที่ 90 และต่อเนื่องมาจนถึงปัจจุบัน จึงได้มีผู้พัฒนาระบบสำหรับทำกริดเป็นจำนวนมากตัวอย่างเช่น โกลบัสทูลคิด (Globus toolkit)[3] อีโคกริด (EcoGRID)[4] และจีฟาร์ม (Gfram)[5] เป็นต้น ซึ่งทุกระบบนั้นต่างก็ให้ความสำคัญกับการรักษาความปลอดภัยบนกริดทั้งสิ้น และระบบที่ได้รับความนิยมมากที่สุดอย่างโกลบัสทูลคิดได้พัฒนาระบบความปลอดภัยเชิงกริด(GSI: Grid Security Infrastructure)[6, 7] ซึ่งจะเน้นในด้านการยืนยันตัวตนของบุคคลและทรัพยากร(authentication) ความปลอดภัยของข้อความ(message protection)

และการลงทะเบียนเข้าระบบเพียงครั้งเดียว(SSO: Single Sign-On) โดยในส่วนของสิทธิการเข้าใช้ทรัพยากรจะปล่อยเป็นหน้าที่ของผู้ดูแลทรัพยากรเป็นผู้กำหนดเอง

เมื่อองค์กรเสมือนมีขนาดที่ใหญ่ขึ้นมักจะก่อให้เกิดปัญหาแก่ผู้ดูแลระบบกริดโดยเฉพาะอย่างยิ่งปัญหาทางด้านการขยายตัวของระบบ(scalability) เพราะภายหลังทำการพิสูจน์ตัวจริงทั้งสองฝ่ายก่อนเข้าใช้ทรัพยากรเสร็จสิ้นแล้ว ทางทรัพยากรจะมีการใช้กริดแมปไฟล์(Gridmap file) เพื่อทำการตรวจสอบสิทธิการเข้าใช้และเปลี่ยนชื่อผู้ใช้มาเป็นชื่อเฉพาะที่ (local username)ของแต่ละทรัพยากร ซึ่งผู้ใช้จำเป็นที่จะต้องมีชื่อผู้ใช้เฉพาะที่บนทุกๆทรัพยากรในองค์กรเสมือน ทำให้เกิดความยุ่งยากในการดูแลดังนั้น จึงมีแนวคิดที่จะสร้างเครื่องให้บริการขึ้นมาเพื่อจัดการสิทธิของผู้ใช้ในองค์กรเสมือนโดยมีลักษณะเป็นแบบรวมศูนย์ (centralize) โดยงานวิจัยในลักษณะนี้ที่ได้รับความนิยมได้แก่ ซีเอเอส (CAS: Community Authorization Service)[8-10] และ วีโอเอ็มเอส (VOMS: Virtual Organizations Membership Service)[11] ซึ่งจากการสร้างบริการแบบรวมศูนย์ทำให้องค์กรเสมือนมีความสามารถในการขยายตัวที่ดีขึ้นกว่าเดิม โดยที่ทั้งซีเอเอส และ วีโอเอ็มเอส ได้พัฒนาขึ้นเพื่อทำงานร่วมกันกับโกลบัสทูลคิด โดยซีเอเอสนั้นสนับสนุนการทำงานโกลบัสทูลคิดรุ่น 2.x และ โกลบัสทูลคิดรุ่น 3.x ในส่วนของกริดเอฟทีพี (GridFTP)เท่านั้นซึ่งเป็นเพียงส่วนย่อยของโกลบัสทูลคิด ทางด้านวีโอเอ็มเอสนั้นสนับสนุนการทำงานของโกลบัสทูลคิดรุ่น 2.x เท่านั้นยังไม่รองรับการทำงานของโกลบัสทูลคิดรุ่น 3.x ขึ้นไป

งานวิจัยนี้จะเป็นการนำแนวความคิดของการสร้างเครื่องให้บริการเพื่อจัดการสิทธิของผู้ใช้ในองค์กรเสมือนแบบรวมศูนย์ โดยการพัฒนาจะมุ่งเน้นในการปรับปรุงบริการจัดการสิทธิของผู้ใช้ในองค์กรเสมือนและปรับปรุงแกรม (GRAM: Globus Rersource Allocation Manager) ของโกลบัสทูลคิดรุ่น3.2.1 เพื่อให้สามารถทำงานร่วมกันได้ นอกจากการทำงานร่วมกันกับโกลบัสทูลคิดรุ่น 3.2.1 ภายในองค์กรเสมือนเดียวกันแล้วงานวิจัยนี้จะคลอบคลุมถึงการพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรข้ามองค์กรเสมือน (Cross VOs Authorization) ซึ่งมีแนวโน้มที่จะเกิดมากขึ้นเห็นได้จากหลายโครงการที่ให้ความสนใจของการทำงานหรือการร่วมมือกันระหว่างองค์กรเสมือนเพื่อให้ได้ประสิทธิภาพของทรัพยากรที่ดีกว่าเดิมเช่น โครงการ โอเพ่นไซน์กริด (OSG: Open Science Grid) [12] โดยการพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรข้ามองค์กรเสมือนนี้ จะทำการแก้ไขเพิ่มเติมจากระบบที่สามารถใช้งานในองค์กรเสมือนเดียวกัน และจะต้องสนับสนุนการทำงานของโกลบัสทูลคิดรุ่น 3.2.1 ในส่วนของแกรมเช่นเดียวกัน



รูปที่ 1.1 แสดงโครงสร้างแบบลำดับขั้นขององค์กรเสมือนในโอเพ่นไซน์กริด

1.2 วัตถุประสงค์

เพื่อพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรในกริดที่มีความสามารถในการขยายตัวของระบบที่ดีขึ้น และสามารถทำงานร่วมกันกับแกรมในโกลบัสทูลคิดรุ่น 3.2.1 ได้ทั้งในองค์กรเสมือนเดียวกัน และต่างองค์กรเสมือนกันได้

1.3 ขอบเขตงานวิจัย

1. งานวิจัยนี้จะทำการสร้างระบบจัดการสิทธิแบบกลุ่มคนบนกริดบนซอร์ฟแวร์ โกลบัสทูลคิดรุ่น 3.2.1 ทั้งภายในองค์กรเสมือนเดียวกัน และสามารถใช้งานข้ามองค์กรเสมือนได้
2. สภาพแวดล้อมขององค์กรเสมือนสององค์กรที่จะนำมาทดสอบในงานวิจัยนี้จะต้องเชื่อถือตัวกลางร่วมกันอย่างน้อย 1 ตัว
3. งานวิจัยนี้จะพัฒนาจากซีเอเอสรุ่นโกลบัสทูลคิดรุ่น 3.2.1 ให้มีความสามารถทำงานร่วมกันกับแกรมของโกลบัสทูลคิดรุ่น 3.2.1 ได้ คือจะทดสอบคำสั่ง managed-job-globusrun
4. ภาษาที่ใช้ในการพัฒนาระบบการจัดการสิทธิแบบกลุ่มคนนี้จะใช้ภาษาจาวาและชุดคำสั่งของยูนิกต์ (UNIX Script) เป็นหลัก

1.4 ขั้นตอนและวิธีดำเนินงานวิจัย

1. ทำการศึกษาเทคโนโลยีกริด และงานวิจัยอื่นๆที่เกี่ยวข้องกับกริดที่เกิดขึ้นในปัจจุบันเพื่อดูแนวโน้มของกริดในอนาคต

2. ทำการติดตั้งกริดซอร์ฟแวร์ลงบนเซิร์ฟเวอร์ที่ได้เตรียมไว้ เพื่อศึกษาลักษณะการทำงาน โดยในงานวิทยานิพนธ์นี้ได้ตัดสินใจเลือกใช้โกลบัสทูลคิดรุ่น 3.2.1 ซึ่งเป็นกริดซอร์ฟแวร์ที่ทางผู้พัฒนาอนุญาตให้นักวิจัยที่สนใจทางด้านเทคโนโลยีกริดสามารถนำไปติดตั้งได้โดยไม่คิดค่าใช้จ่ายแต่ประการใด
3. ทำการศึกษาจีเอสไอ แกรม ซีเอเอส และงานวิจัยอื่นๆที่เกี่ยวข้อง เช่น อาร์แบค เอสเอเอมแอล เป็นต้น
4. ทำการออกแบบระบบจัดการสิทธิแบบกลุ่มคนในระบบกริดสำหรับโกลบัสทูลคิดรุ่น 3.2.1
5. ทำการพัฒนาระบบการจัดการสิทธิแบบกลุ่มคนในระบบกริดสำหรับโกลบัสทูลคิดรุ่น 3.2.1 เพื่อศึกษาผลกระทบต่อระบบเดิมและดูผลลัทธ์ว่าเป็นไปตามที่คาดไว้หรือไม่
6. ทำการออกแบบระบบจัดการสิทธิการเข้าใช้ทรัพยากรในระบบกริดให้สามารถทำงานข้ามองค์กรเสมือนได้โดยประยุกต์ใช้ระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับในองค์กรเสมือนเดียวกันเป็นต้นแบบ ให้มีความสามารถในการทำงานร่วมกับองค์กรเสมือนอื่นได้
7. ทำการพัฒนาระบบการจัดการสิทธิการเข้าใช้ทรัพยากรในระบบกริดที่มีความสามารถทำงานข้ามองค์กรเสมือนได้ เพื่อศึกษาผลกระทบต่อระบบเดิมและดูผลลัทธ์ว่าเป็นไปตามที่คาดไว้หรือไม่
8. ทำการวิเคราะห์ และสรุปผล พร้อมข้อเสนอแนะ
9. จัดทำรายงานวิทยานิพนธ์ฉบับสมบูรณ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ระบบจัดการสิทธิการเข้าใช้ทรัพยากรที่มีความสามารถในด้านการขยายตัวของระบบที่ดีขึ้นทั้งภายในองค์กรเดียวกัน และระบบที่มีองค์กรเสมือนมากกว่าหนึ่ง
2. ได้ระบบจัดการสิทธิการเข้าใช้ทรัพยากรที่มีสามารถใช้งานได้ทั้งในองค์กรเสมือนเดียวกันและต่างองค์กรเสมือนกันได้
3. สามารถทำงานร่วมกันกับเครื่องทรัพยากรที่ยังไม่ได้ถูกแก้ไขให้เข้าใจนโยบายที่ได้ออกโดยระบบจัดการสิทธิแบบกลุ่มคนนี้ได้ (Backward Compatibles)

1.6 โครงสร้างวิทยานิพนธ์

ในบทต่อไปของวิทยานิพนธ์นี้จะกล่าวถึงทฤษฎีที่นำมาประยุกต์ใช้ และงานวิจัยที่เกี่ยวข้อง บทที่ 3 จะกล่าวถึงการออกแบบและพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับโกลบัสทูลคิดรุ่น 3.2 ภายในองค์กรเสมือนเดียวกัน ในบทที่ 4 จะแสดงรายละเอียดการออกแบบและพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับโกลบัสทูลคิดรุ่น 3.2 บนสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือน ในบทที่5 จะแสดงถึงการทดสอบระบบจัดการสิทธิแบบกลุ่มคนนี้ และในบทสุดท้ายจะเป็นการสรุปผลงานวิทยานิพนธ์และข้อเสนอแนะในการออกแบบระบบจัดการสิทธิการเข้าใช้ทรัพยากรบนโกลบัสทูลคิดและแนวทางในการพัฒนาต่อไป

1.7 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความทางวิชาการในหัวข้อเรื่อง “GAS: Grid Authorization Service in GT3.x Environment” โดย ปฏิภาณ คงสิริกุล และ ณัฐวุฒิ หนูไพโรจน์ ในงานประชุมวิชาการ “The 8th National Computer Science and Engineering Conference (NCSEC 2004)” ซึ่งจัดโดย มหาวิทยาลัยสงขลานครินทร์ ณ โรงแรม เจบี หาดใหญ่ สงขลา ในระหว่างวันที่ 21-22 ตุลาคม 2547

บทที่2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 กริด (Grid) [13]

กริดเป็นระบบกระจายรูปแบบหนึ่งที่เกิดจากการรวบรวมทรัพยากรต่างๆเข้ามาสร้างเป็นองค์กรเสมือน ซึ่งทรัพยากรที่อยู่ในองค์กรเสมือนนี้จะเป็นทรัพยากรที่อยู่ในองค์กรเดียวกันจริงๆ หรือจะอยู่ต่างองค์กรกันก็ได้ โดยทรัพยากรในองค์กรเสมือนนี้จะไม่ขึ้นกับโครงสร้างการเชื่อมต่อจริงของแต่ละองค์กรและทรัพยากรทั้งหมดในองค์กรเสมือนจะต้องมีความเชื่อถือซึ่งกันและกัน (Trust) การที่ทรัพยากรในองค์กรเสมือนนี้ไม่ขึ้นอยู่กับโครงสร้างการเชื่อมต่อจริงและสามารถทำงานข้ามองค์กรกันได้ จึงจำเป็นที่จะต้องมีระบบจัดการที่ดีพอ โดยคุณสมบัติที่จำเป็นจะต้องมีสำหรับในการสร้างองค์กรเสมือนได้แก่ ความสามารถในการลงทะเบียนเข้าระบบเพียงครั้งเดียว (Single Sign-on) หรือการยืนยันฐานะของผู้ใช้แต่ละคนโดยใช้โครงสร้างการเข้ารหัสสาธารณะ (PKI : Public-Key Infrastructure) ที่จำเป็นต้องมีการกำหนดหน่วยดูแลส่วนกลาง (CA :Central Authorization) เพื่อรับผิดชอบในการสร้างใบยืนยันตัวตนของผู้ใช้ในการขอเข้าไปใช้ทรัพยากรต่างๆในองค์กรเสมือน

2.1.2 โกลบัสทูลคิด (Globus Toolkit) [3]

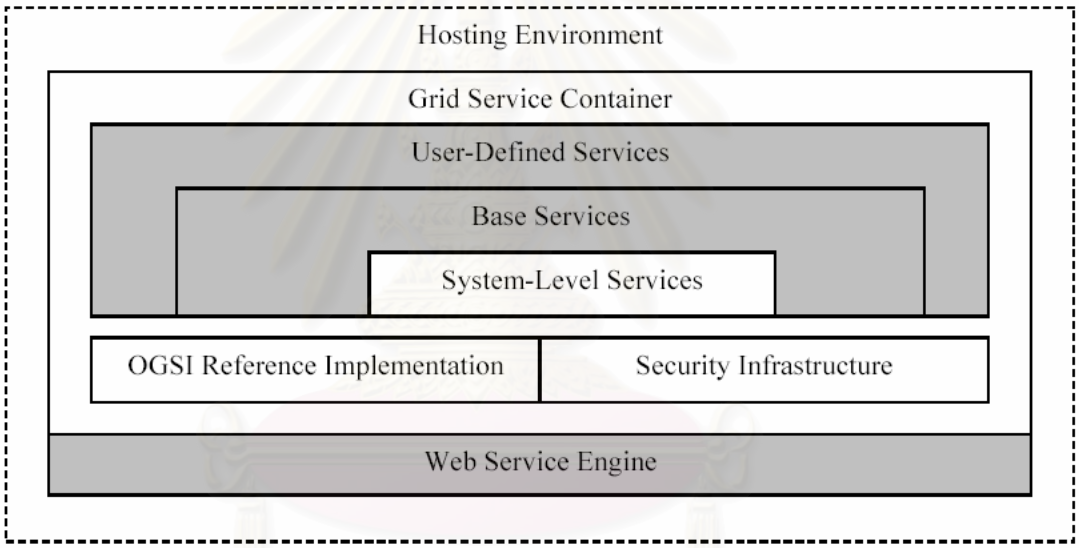
โกลบัสทูลคิท ถูกพัฒนาขึ้นสำหรับเป็นซอฟต์แวร์พื้นฐานสำหรับการสร้างและให้บริการทรัพยากรและบริการต่างๆของระบบกริด การพัฒนาโกลบัสทูลคิทเกิดจากความร่วมมือของบุคคลที่เกี่ยวข้องในวงการกริดในรูปแบบของโอเพ่นซอร์ส ทำให้มีการนำโกลบัสทูลคิทไปใช้เป็นพื้นฐานสำหรับการสร้างระบบกริดสำหรับการทำงานในรูปแบบต่างๆกันเป็นจำนวนมาก

โกลบัสทูลคิทมีส่วนประกอบที่สำคัญได้แก่

- ส่วนกำหนดและจัดการทรัพยากรกริด หรือ แกรม (GRAM: Grid Resource Allocation Manager) ทำหน้าที่สร้างและจัดการการเข้าใช้ทรัพยากร โดยใช้จีเอสไอในการจัดการด้านความปลอดภัย
- ส่วนให้บริการข้อมูล(Information Services) ทำหน้าที่ให้บริการข้อมูลรายละเอียดของทรัพยากรและบริการต่างๆ รวมถึงข้อมูลอื่นๆ ที่เกี่ยวข้อง เช่น สถานะของเครือข่าย หรือ รายละเอียดของข้อมูลในการทำดาต้ากริด เป็นต้น

- โครงสร้างความปลอดภัยกริด หรือ จีเอสไอ (GSI: Grid Security Infrastructure) ทำหน้าที่จัดการด้านความปลอดภัยในการเข้าใช้ทรัพยากรและบริการต่างๆของกริด โดยใช้หลักการการลงทะเบียนเข้าระบบเพียงครั้งเดียวและการมอบสิทธิ (Delegation) จีเอสไอใช้มาตรฐานเอ็กซ์509ซึ่งถูกนำมาใช้ในโครงสร้างการเข้ารหัสสาธารณะเป็นหลักในการยืนยันบุคคล

โกลบัสทูลคิทได้รับการพัฒนาออกมาหลายเวอร์ชั่น จนมาถึงโกลบัสทูลคิทเวอร์ชั่น 3(Globus Toolkit3) ที่ได้นำสถาปัตยกรรมกริดเซอร์วิสแบบเปิด (Open Grid Service Architecture) และแนวคิดของกริดเซอร์วิสมาใช้ และสามารถแสดงสถาปัตยกรรมของโกลบัสทูลคิท 3 ได้ดังรูปที่ 2.1



รูปที่ 2.1 สถาปัตยกรรมของโกลบัสทูลคิท 3

จากรูปที่ 2.1 โกลบัสทูลคิทจะประกอบไปด้วยส่วนประกอบดังต่อไปนี้

- เครื่องมืออ้างอิงของโอจีเอสไอ (OGSI Reference Implementation) ได้นำอินเตอร์เฟสต่างๆของโอจีเอสไอมาสร้างให้อยู่ในรูปแบบของเอพีไอ (API) เพื่ออำนวยความสะดวกทั้งในการสร้างและเรียกใช้งานกริดเซอร์วิส
- โครงสร้างพื้นฐานความปลอดภัย (Security Infrastructure) ทำหน้าที่จัดการการยืนยันบุคคลและการควบคุมสิทธิการเข้าใช้ โดยใช้จีเอสไอเป็นพื้นฐาน
- บริการระดับระบบ (System-Level Services) ให้บริการรันไทม์ (Run-time Services) สำหรับบริการที่ต้องการจะสร้างขึ้น

- บริการพื้นฐาน (Base Services) ทำหน้าที่ให้บริการแก่ผู้ใช้ที่ต้องการเรียกใช้ความสามารถที่มีอยู่เดิมในโกลบัสทูลคิท 2 เช่น บริการการจัดการทรัพยากร บริการข้อมูล เป็นต้น ในรูปแบบของกริดเซอร์วิส
- บริการที่ผู้ใช้สร้างขึ้น (User-Defined Services) เป็นส่วนที่ให้ผู้ใช้ ได้ทำการสร้างบริการต่างๆในรูปแบบของกริดเซอร์วิสที่ผู้ใช้ ต้องการขึ้นเอง
- คอนเทนเนอร์กริดเซอร์วิส (Grid Services Container) เป็นสภาวะแวดล้อมจำลอง (Abstract Environment) ที่โกลบัสทูลคิทสร้างขึ้นมา เพื่อให้กริดเซอร์วิสสามารถทำงานได้อย่างถูกต้อง โดยไม่ขึ้นกับระบบการทำงานที่ระบบทำงานอยู่จริง
- เครื่องมือจัดการเว็บเซอร์วิส (Web Services Engine) ทำหน้าที่จัดการการรับส่งข้อมูลการเรียกใช้กริดเซอร์วิสในรูปแบบเอ็กซ์เอ็มแอล (XML)

ผลของการที่โกลบัสทูลคิท 3 ได้แบ่งแยกส่วนประกอบต่างๆออกจากกันอย่างชัดเจน ทำให้เกิดความสะดวกและง่ายดายทั้งต่อการสร้างและให้บริการต่างๆที่อยู่ในรูปกริดเซอร์วิส รวมถึงการสร้างส่วนประกอบหรือบริการย่อยๆเพื่อรองรับการสร้างและให้บริการกริดเซอร์วิสต่อไป

สำหรับแกรมที่มีในโกลบัสทูลคิท จะอยู่ในรูปแบบของกริดเซอร์วิสเช่นเดียวกับบริการอื่นๆ โดยเมื่อผู้ใช้ต้องการจะเข้าใช้ทรัพยากรจะต้องทำการสร้างคำอธิบายทรัพยากรที่จะใช้ให้อยู่ในรูปของภาษาข้อกำหนดทรัพยากรหรืออาร์เอสแอล (RSL: Resource Specification Language) จากนั้นจึงทำการส่งไปยังกริดเซอร์วิสที่ทำหน้าที่จัดการทรัพยากร เพื่อนำอาร์เอสแอลที่ส่งไปจัดการเรียกใช้ทรัพยากรนั้นต่อไป

2.1.3 **เว็บเซอร์วิส** (Web Services)

เว็บเซอร์วิสเป็นระบบการสร้างและเรียกใช้บริการต่าง ๆ (Service) ผ่านทางระบบเครือข่าย โดยใช้การส่งข้อมูลในรูปแบบของ XML (eXtensible Mark-up Language) การส่งข้อมูลในรูปแบบมาตรฐานนี้ทำให้เว็บเซอร์วิสสามารถถูกสร้างหรือเรียกใช้ด้วยภาษาโปรแกรมภาษาใดก็ได้ (Language Independent) หรือทำงานอยู่บนเครื่องหรือระบบใดก็ได้ (Platform Independent) นอกจากนี้การเรียกใช้เว็บเซอร์วิสก็ทำได้โดยง่าย เปรียบเสมือนการเรียกใช้ส่วนประกอบ(Component) ที่อยู่ภายในเครื่องเดียวกัน อาจกล่าวได้ว่าเว็บเซอร์วิสทำให้เกิดการสร้างระบบกระจาย (Distributed System) ได้อีกด้วย โดยการกระจายงานไปทำในระบบหรือส่วนอื่น ไม่จำเป็นต้องทำที่เครื่องใดเครื่องหนึ่งเพียงอย่างเดียว

เว็บเซอร์วิสได้ทำการกำหนดรูปแบบที่จะใช้ในการบรรยายรายละเอียดของส่วนประกอบหรือบริการต่างๆ รูปแบบการเรียกใช้บริการ รวมไปถึงการจัดเก็บและค้นหาบริการต่างๆ รูปแบบต่างๆเหล่านี้ได้มีการกำหนดเป็นมาตรฐานที่แน่นอน อันได้แก่ ดับบลิวเอสดีแอล (WSDL – Web Services Description Language) โซป (SOAP – Simple Object Access Protocol) และ ยูดีดีไอ (UDDI – Universal Description Discovery and Integration) นอกจากนั้นส่วนประกอบพื้นฐานเหล่านี้แล้ว องค์กรธุรกิจต่างๆ ยังได้มีการสร้างข้อกำหนด (Specification) เพื่อเพิ่มความสามารถต่างๆให้แก่เว็บเซอร์วิสและนำเว็บเซอร์วิสไปใช้ในงานเฉพาะด้าน เช่น ดับบลิวเซเคียวริตี้ (WS-Security) ดับบลิว-ทรานแซ็คชั่น (WS-Transaction) เป็นต้น ทำให้เว็บเซอร์วิสได้รับความนิยมและถูกนำไปใช้อย่างกว้างขวาง

2.1.4 **กริดเซอร์วิส** (Grid Service)

กริดเซอร์วิสเกิดจากความต้องการในการสร้างมาตรฐานการสร้างและให้บริการต่างๆ ที่อยู่ในระบบกริดให้เป็นรูปแบบเดียวกัน จึงได้มีการออกแบบของสถาปัตกรรมกริดเซอร์วิสแบบเปิดหรือโอจีเอสเอ (OGSA – Open Grid Services Architecture) [14] เพื่อเป็นสถาปัตยกรรมพื้นฐานสำหรับการทำงานร่วมกันภายในระบบกริด และมีการกำหนดขึ้นมาเป็นมาตรฐานที่เรียกว่าโครงสร้างกริดเซอร์วิสแบบเปิด หรือ โอจีเอสไอ (OGSI - Open Grid Services Infrastructure) [15]ดังนั้นจึงอาจกล่าวได้ว่า กริดเซอร์วิสหมายถึงบริการที่สร้างตามมาตรฐานของเรียกว่าโครงสร้างกริดเซอร์วิสแบบเปิด และมีการอธิบายการเข้าใช้บริการไว้ในรูปแบบของดับบลิวเอสดีแอล

สถาปัตกรรมกริดเซอร์วิสแบบเปิดหรือโอจีเอสเอ ได้ออกแบบกริดเซอร์วิสจากพื้นฐานของสถาปัตยกรรมเว็บเซอร์วิส จะเห็นได้จากมีการนำมาตรฐานของเว็บเซอร์วิสมาใช้ในการบรรยายและการเรียกใช้กริดเซอร์วิส อันได้แก่ ดับบลิวเอสดีแอลและโซปนอกจากนั้นยังได้กำหนดกลไกข้อกำหนด และคุณสมบัติพื้นฐานเพิ่มเติมสำหรับกริดเซอร์วิสนอกเหนือจากที่มีในระบบเว็บเซอร์วิสพื้นฐาน ได้แก่ การจัดการสถานะ (State Management) การสร้างตัวแปรของบริการ (Service Instances) กลไกการอ้างอิงชื่อบริการ (Service References) แนวคิดข้อมูลของบริการ (Service Data) กลไกการแจ้งข่าว (Notification Mechanisms) ความสามารถที่เพิ่มขึ้นมาเหล่านี้ทำให้กริดเซอร์วิสเหมาะกับการนำไปใช้สร้างบริการที่ต้องการความปลอดภัยในการเข้าใช้ มีความคงทนต่อความผิดพลาด และเหมาะสมกับบริการที่มีการทำงานเป็นเวลานาน ทำให้กริดเซอร์วิสมีความสามารถที่มากกว่า และเหมาะสมมากกว่ากับการนำมาใช้ในระบบกริด

2.1.5 **ภาษาเอสเอเอ็มแอล** [16, 17]

ภาษาเอสเอเอ็มแอลเป็นโครงร่าง (Framework) ของภาษาเอ็กซ์เอ็มแอลสำหรับการแลกเปลี่ยนข้อมูลความปลอดภัยบนอินเทอร์เนต ซึ่งข้อมูลความปลอดภัยนี้แสดงความหมายในรูปแบบของข้อความยืนยันเกี่ยวกับผู้กระทำ โดยที่ผู้กระทำ คือ เอนทิตีที่มีข้อมูลสำหรับระบุผู้ใช้ในบางโดเมนของการรักษาความปลอดภัย ตัวอย่างของผู้กระทำได้แก่ บุคคลซึ่งบ่งชี้โดยอีเมลในโดเมนของอินเทอร์เนตดีเอ็นเอส (DNS - Domain Name Service)

ข้อความยืนยันเป็นข้อมูลเกี่ยวกับการพิสูจน์ตัวจริงของผู้กระทำ รวมถึงแอททริบิวต์ของผู้กระทำและผลของการพิสูจน์สิทธิ (Authorization Decision) ว่าผู้กระทำได้รับการอนุญาตให้เข้าใช้ทรัพยากรนั้นๆ หรือไม่ ข้อความยืนยันออกโดยองค์กรที่มีอำนาจกำหนดข้อความยืนยันของเอสเอเอ็มแอล (SAML Authority) ได้แก่องค์กรที่ทำหน้าที่พิสูจน์ตัวจริง (Authentication Authority) และองค์กรตัดสินใจเกี่ยวกับนโยบาย (PDP - Policy Decision Point) เอสเอเอ็มแอลนิยามโพรโทคอลที่ผู้ใช้สามารถร้องขอข้อความยืนยันจากองค์กรที่มีอำนาจกำหนดข้อความยืนยันของเอสเอเอ็มแอล และรับผลการตอบสนองได้ โพรโทคอลนี้ประกอบไปด้วยรูปแบบแมสเซจของการร้องขอและการตอบสนอง ซึ่งสามารถผูกเข้ากับรูปแบบของแมสเซจและโพรโทคอลที่ใช้สื่อสารกันได้หลายรูปแบบ

เป้าหมายหลักของเอสเอเอ็มแอล คือ การลงบันทึกเข้าระบบเพียงครั้งเดียว เพื่อให้ผู้ใช้พิสูจน์ตัวจริงเพียงครั้งเดียวภายในหนึ่งโดเมน และสามารถใช้ทรัพยากรในโดเมนอื่นๆได้โดยไม่ต้องพิสูจน์ตัวจริงอีก แต่ก็มีผู้วิจัยจำนวนหนึ่งนำเอสเอเอ็มแอลไปใช้แสดงนโยบายการเข้าใช้ทรัพยากร โดยเพิ่มเติมสิทธิการเข้าใช้ไว้ในข้อความตอบสนองการร้องขอเข้าใช้แบบเอสเอซีเอ็มแอล (SAML response) เพื่อนำมาสร้างสิ่งอ้างสิทธิการเข้าใช้แบบเอสเอเอ็มแอล (SAML Assertion) ดังรูปที่ 2.2


```
<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="e0ccf105-9878-4c1b-9168-ae30c08efdc4"
IssueInstant="2005-01-18T07:34:07Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1"
MinorVersion="0"><Conditions NotBefore="2005-01-18T07:34:07Z" NotOnOrAfter="2005-01-
19T07:34:07Z"></Conditions><AuthorizationDecisionStatement Decision="Permit"
Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier
Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo
CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-
PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action
Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">
```

```
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">
here()/ancestor::signs:Assertion[1]
</xfilter2b:XPath>
<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">
here()/ancestor::ds:Signature[1]
</xfilter2b:XPath>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd
xsi"></ec:InclusiveNamespaces></ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>4Wiu3vcEbUVhsZDrfOO6GDP0lok=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
HuPswDw1eW4NRniedFcmbDU6EipIYkcD2rbZ9UiCF0/TlhYVDzqow4GxGocAKFBRQ5oBljzOWz5w
nIEw3QhEPqy6umS0IuuistFg9Wgn3oBKjLOzJQ4ULGCAMZaVxIljRjgaxH728SZbAIh4/Rpl7iy/
LTUv/fxLI1rUEDgVK6s=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIB6zCCAVQCAQQwDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1
bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDIwNDA4MTBaFw0xNDExMzAwNDA4MTBaMEkx
DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMSgwJgYDVQQDEx9jYXMvYXBvbGxvMTAuY3Au
ZW5nLmNodWxhLmFjLnRoMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKbvxw2FhR1awR+tmJ
li90IUIwK/YaTN4pCof6149RmcETYslrmHs+umWT26g8faF3ZHWTIoggX1J5RkbrrC9/097z8yaZ
NMhZnb1JQRS89T0E12IcAvnlmSB+LVHWS7h+8WT+gZlYJSMhq6Xzl9HdGYimNfNmBxR6/fojPtYQ
7wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHJtaMwxFJ4ZMuq5KOa4qmh0N+/z2E4z8FBqfKCVG/9f
tS5wgbPf3ja4ST7Zq/NLmIEiM2docXw6z95hi6kUmB6Q8DzzewrBNTijGt2SgIrc8SbM75tJ87xQ
WpquzY/ytj6vaL0hUiMN/lemSBSfpRkZul4R1bDCJg5y1zceFBlG
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></ds:Signature></Assertion>
```

รูปที่ 2.2 แสดงนโยบายการเข้าใช้ทรัพยากรในรูปแบบของ เอสเอเอ็มแอล

2.1.6 โครงสร้างระบบจัดการสิทธิการเข้าใช้ทรัพยากร

ระบบจัดการสิทธิการเข้าใช้ทรัพยากรโดยทั่วไปมักจะพบองค์ประกอบที่สำคัญอยู่สองส่วน ได้แก่ ส่วนการตัดสินใจเกี่ยวกับนโยบาย (PDP – Policy Decision Point) และ ส่วนการบังคับใช้นโยบาย (PEP – Policy Enforcement Point) ซึ่งแต่ละส่วนมีรายละเอียดดังนี้

ส่วนการตัดสินใจเกี่ยวกับนโยบาย จะเป็นส่วนที่ผู้ดูแลระบบของแต่ละองค์กรจะต้องกำหนดสิทธิการใช้งานของผู้ใช้ที่อยู่ภายในองค์กร โดยส่วนมากแล้วนโยบายจะถูกจัดเก็บอยู่ในฐานข้อมูล เมื่อผู้ใช้ต้องการเข้าใช้ทรัพยากรจะทำการส่งข้อความร้องขอเข้าใช้ ซึ่งส่วนมากจะอยู่ในรูปแบบของเอ็กซ์เอ็มแอล เช่น ข้อความร้องขอเข้าใช้แบบเอ็กซ์เอซีเอ็มแอล (XACML request) หรือ ข้อความร้องขอเข้าใช้แบบเอสเอเอ็มแอล (SAML request) มาเพื่อพิสูจน์ตัวตนหลังจากนั้นส่วนตัดสินใจเกี่ยวกับนโยบายจะพิจารณาจากนโยบายที่เก็บไว้ในฐานข้อมูลแล้วจัดทำข้อความตอบสนองการร้องขอเข้าใช้กลับไปยังผู้ใช้ ตัวอย่างข้อความตอบสนอง เช่น ข้อความตอบสนองการร้องขอเข้าใช้แบบเอ็กซ์เอซีเอ็มแอล (XACML response) หรือ ข้อความตอบสนองการร้องขอเข้าใช้แบบเอสเอซีเอ็มแอล (SAML response)

ส่วนการบังคับใช้นโยบาย จะเป็นส่วนที่ผู้ดูแลระบบของแต่ละองค์กรต้องทำขึ้นมาเพิ่มเติมเพื่อที่จะได้ทำความเข้าใจกับนโยบายที่ส่วนการตัดสินใจเกี่ยวกับนโยบายเป็นผู้ออกมาให้โดยที่ทุกๆทรัพยากรที่ต้องการจะใช้นโยบายจำเป็นที่จะต้องมีส่วนนี้

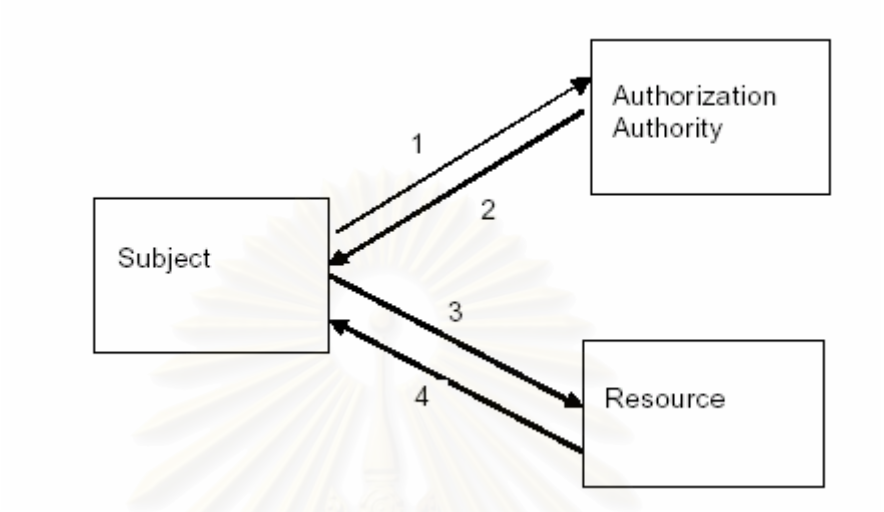
โครงสร้างระบบจัดการสิทธิการเข้าใช้ทรัพยากรในปัจจุบันมีอยู่ 2 โครงสร้างด้วยกันได้แก่ ระบบจัดการสิทธิการเข้าใช้ทรัพยากรแบบพุช (Push Model) และ ระบบจัดการสิทธิการเข้าใช้ทรัพยากรแบบพูล (Pull Model) ซึ่งมีรายละเอียดดังต่อไปนี้

2.1.6.1 **ระบบจัดการสิทธิการเข้าใช้ทรัพยากรแบบพุช** (Push Model)

ระบบจัดการสิทธิการเข้าใช้ทรัพยากรแบบพุชนี้จะมีการทำงานแบ่งเป็นสองขั้นคือ

- ขั้นแรก ผู้ใช้งานระบบจะต้องมายืนยันเพื่อพิสูจน์ตัวจริงว่าเป็นผู้ที่ได้รับอนุญาตให้ใช้ระบบจริงๆ ที่ ส่วนการตัดสินใจเกี่ยวกับนโยบาย หลังจากพิสูจน์ตัวจริงได้แล้ว ส่วนการตัดสินใจเกี่ยวกับนโยบาย จะทำการค้นหานโยบายการเข้าใช้ทรัพยากรของผู้ใช้คนนั้นมาสร้างนโยบายซึ่งอาจจะอยู่รูปแบบเอ็กซ์เอ็มแอลแบบใดแบบหนึ่งที่ได้กล่าวไว้ตอนข้างต้นแล้วจึงส่งนโยบายนั้นกลับคืนให้ผู้ใช้ โดยนโยบายจะมีลายเซ็นดิจิตอลเพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตจากส่วนการตัดสินใจเกี่ยวกับนโยบาย
- ขั้นสอง ผู้ใช้งานระบบจะนำนโยบายการใช้งานที่ส่วนการตัดสินใจเกี่ยวกับนโยบาย เป็นผู้ออกให้ ไปยื่นแสดงความจำนงขอใช้ทรัพยากรที่แต่ละทรัพยากร โดยทรัพยากรจะต้องตรวจสอบก่อนว่าส่วนการตัดสินใจเกี่ยวกับนโยบาย เป็นผู้ออกนโยบายนั้นๆจริงและไม่ได้ถูกเปลี่ยนแปลงใดๆ ถ้าตรวจสอบพบว่านโยบายนั้นมีความถูกต้องและส่วนการตัดสินใจ

เกี่ยวกับนโยบาย ให้สิทธิผู้ใช้มาใช้งานบนทรัพยากรนี้ได้ก็จะยินยอมให้ผู้ใช้สามารถใช้งานตามคำขอได้ต่อไป



รูปที่ 2.3 แสดงการทำงานของระบบจัดการสิทธิแบบพุช

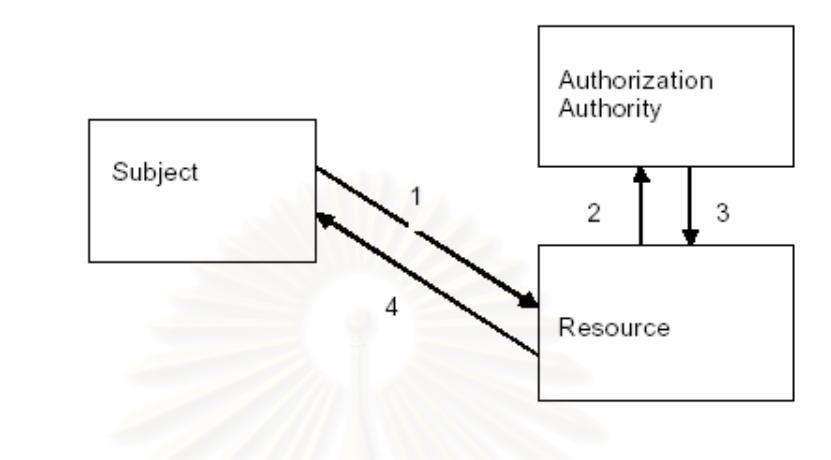
สำหรับการใช้ระบบจัดการสิทธิการเข้าใช้แบบพุชผู้ใช้จำเป็นที่จะต้องรู้ว่าทรัพยากรที่จะไปขอใช้งานนั้นเชื่อถืออยู่กับส่วนการตัดสินใจเกี่ยวกับนโยบาย ตัวไหน เพราะถ้าไปขอนโยบายการเข้าใช้กับส่วนการตัดสินใจเกี่ยวกับนโยบายที่ทรัพยากรไม่เชื่อถือจะไม่สามารถเข้าไปใช้งานได้

2.1.6.2 **ระบบจัดการสิทธิการเข้าใช้ทรัพยากรแบบพูล** (Pull Model)

ระบบจัดการสิทธิการเข้าใช้ทรัพยากรแบบพูลนี้ก็จะมีขั้นตอนสองขั้นเช่นเดียวกับแบบพุช คือ

- ขั้นแรก ผู้ใช้จะไปที่ทรัพยากรที่จะใช้งานแล้วทำการพิสูจน์ตัวจริงกับทรัพยากร หลังจากนั้นทรัพยากรจะส่งข้อความร้องขอเข้าใช้ซึ่งจะมีชื่อผู้ใช้อยู่ภายในไปยังส่วนการตัดสินใจเกี่ยวกับนโยบายที่ทรัพยากรนั้นเชื่อถือเอง
- ขั้นสอง ส่วนการตัดสินใจเกี่ยวกับนโยบายจะทำการค้นหานโยบายการเข้าใช้ทรัพยากรของผู้ใช้คนนั้นมาสร้างนโยบายซึ่งอาจจะอยู่รูปแบบเอ็กซ์เอ็มแอลแบบใดแบบหนึ่งที่ได้กล่าวไว้ตอนข้างต้นแล้วจึงส่งนโยบายนั้นกลับคืนให้ผู้ใช้ในรูปแบบของข้อความตอบสนองการร้องขอเข้าใช้ โดยนโยบายจะมีลายเซ็นดิจิตอลเพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตจากส่วนการตัดสินใจเกี่ยวกับนโยบาย แล้วทำการส่งมายังเครื่องทรัพยากร โดยทรัพยากรจะต้องตรวจสอบก่อนว่าส่วนการตัดสินใจเกี่ยวกับนโยบายเป็นผู้ออกนโยบายนั้นๆจริงและไม่ได้ถูกเปลี่ยนแปลงใดๆ ถ้าตรวจสอบพบว่านโยบายนั้นมีความ

ถูกต้องและส่วนการตัดสินใจเกี่ยวกับนโยบายให้สิทธิผู้ใช้มาใช้งานบนทรัพยากรนี้ได้ก็จะยินยอมให้ผู้ใช้สามารถใช้งานตามคำขอได้ต่อไป



รูปที่ 2.4 แสดงการทำงานของระบบจัดการสิทธิแบบพูล

สำหรับการใช้ระบบจัดการสิทธิการเข้าใช้แบบพูลผู้ใช้ไม่จำเป็นที่จะต้องรู้ว่าทรัพยากรที่เราจะไปขอใช้งานนั้นเชื่อถืออยู่กับส่วนการตัดสินใจเกี่ยวกับนโยบายตัวไหนแต่ทรัพยากรเองจะต้องจำว่าตนเองเชื่อถือส่วนการตัดสินใจเกี่ยวกับนโยบายตัวไหนแทน

2.1.7 **โครงสร้างรักษาความปลอดภัยเชิงกริด หรือ จีเอสไอ** (GSI - Grid Security Infrastructure)

โครงสร้างรักษาความปลอดภัยเชิงกริดหรือจีเอสไอถูกพัฒนาภายใต้โครงงานวิจัยโกลบัส (Globus) เพื่อสนับสนุนสภาพแวดล้อมของคอมพิวเตอร์ที่มีการทำงานแบบกระจาย โดยจีเอสไอมีหน้าที่จัดการเกี่ยวกับการทำงานระหว่างองค์กรต่างๆและเชื่อมต่อโซลูชั่นของการรักษาความปลอดภัยที่แตกต่างกันระหว่างองค์กร โดยจีเอสไอสร้างขึ้นเพื่อรองรับความต้องการดังต่อไปนี้

1. ความต้องการที่จะมีวิธีการสื่อสารอย่างปลอดภัยระหว่างอิลิเมนต์ (element) บนกริด
2. ความต้องการที่สนับสนุนการรักษาความปลอดภัยข้ามขอบเขตขององค์กรโดยไม่มีระบบการรักษาความปลอดภัยส่วนกลาง
3. ความต้องการที่จะสนับสนุนการลงบันทึกเข้าระบบเพียงครั้งเดียวสำหรับผู้ใช้งานกริด รวมถึงการส่งต่อข้อมูลสำหรับระบุผู้ใช้เพื่อใช้ในการทำงานร่วมกันของทรัพยากร

จีเอสไอประกอบไปด้วยลักษณะที่สำคัญดังต่อไปนี้

2.1.7.1 **โครงสร้างของกุญแจสาธารณะ** (PKI – Public Key Infrastructure)

จีเอสไอใช้พื้นฐานของโครงสร้างของกุญแจสาธารณะ กล่าวคือ ผู้ใช้ระบบกริดจะต้องมีกุญแจสาธารณะ (Public Key) และกุญแจส่วนบุคคล (Private Key) เป็นของตนเองซึ่งโดยปกติแล้วกุญแจทั้งคู่จะเก็บอยู่ในโฮมไดเรกทอรีของผู้ใช้ โดยกุญแจส่วนบุคคลจะถูกตั้งสิทธิให้ผู้ใช้ซึ่งเป็นเจ้าของมีสิทธิอ่านได้อย่างเดียว และกุญแจส่วนบุคคลจะถูกเข้ารหัสด้วยวลีผ่าน (Pass Phrase) อีกครั้งเพื่อความปลอดภัย ส่วนกุญแจสาธารณะของผู้ใช้จะถูกเก็บอยู่ในรูปแบบของหลักฐานอ้างอิงผู้ใช้ตามมาตรฐานเอ็กซ์ 509 เวอร์ชั่น 3 (X.509v3) โดยหลักฐานอ้างอิงผู้ใช้เป็นการเชื่อมกันระหว่างชื่อเฉพาะของเอนทิตีกับกุญแจส่วนบุคคลโดยจะลงลายเซ็นดิจิตอล (Digital Signature) จากองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ และพิสูจน์ให้เห็นว่าเอนทิตีนั้นเป็นเจ้าของกุญแจส่วนบุคคล นอกจากผู้ใช้ระบบกริดแล้วเอนทิตีอื่นที่อยู่ในระบบจำเป็นที่จะต้องมีกุญแจสาธารณะและกุญแจส่วนบุคคลด้วย เพื่อใช้เป็นการพิสูจน์ตัวจริงของทั้งสองฝ่าย (Mutual Authentication)

2.1.7.2 **หลักฐานอ้างอิงตัวผู้ใช้ตามมาตรฐานเอ็กซ์ 509 เวอร์ชั่น 3** (X.509 Certificate)

หลักฐานอ้างอิงตัวผู้ใช้เป็นสิ่งสำคัญสำหรับการแสดงตัวและการพิสูจน์ตัวจริงของผู้ใช้ ถ้าผู้ให้บริการเชื่อถือหลักฐานอ้างอิงตัวผู้ใช้ขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้แล้ว ผู้ให้บริการจะเชื่อถือหลักฐานอ้างอิงตัวผู้ใช้ของผู้กระทำด้วย โดยหลักฐานอ้างอิงตัวผู้ใช้ประกอบด้วยข้อมูลสำคัญดังรูปที่ 2.5

```
Issuer: /C=TH/O=Grid/O=Chula/CN=Apollo CA
Validity
    Not Before: May 31 04:35:25 2004 GMT
    Not After : May 31 15:22:32 2004 GMT
Subject: /C=TH/O=Grid/O=Chula/CN=g46pkn
Subject Public Key Info :
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (512 bit)
    Modulus (512 bit):
        00:e1:08:29:be:ba:5f:99:47:af:03:7d:
        03:26:29:97:ca:08:44:4d:48:f2:f1:92:
        09:f8:85:05:87:59:5b:f4:89:2d:32:34:
    Exponent: 65537 (0x10001)
X509v3 extensions:
    1.3.6.1.4.1.3536.1.222: critical
    0.0
Signature Algorithm: md5WithRSAEncryption
  9b:e4:8c:ee:c6:df:68:5b:56:ac:56:88:53:
  7e:f2:37:35:47:62:e5:03:62:28:96:1f:05:
  42:19:79:de:f9:bd:8f:c2:b6:13:ee:5a:2b:
  a5:cb:6f:6c:bd:b2:6d:f2:e1:76:8e:30:86:
  67:6c:87:38:1d:4a:cf:c8:96:c8:dd:9f:a3
```

รูปที่ 2.5 แสดงรูปแบบหลักฐานอ้างอิงตัวผู้ใช้ตามมาตรฐานเอ็กซ์ 509 เวอร์ชั่น 3

จากรูปที่ 2.5 หลักฐานอ้างอิงตัวผู้ใช้แบบเอ็กซ์ 509 เวอร์ชั่น 3 ประกอบไปด้วยส่วนสำคัญดังนี้

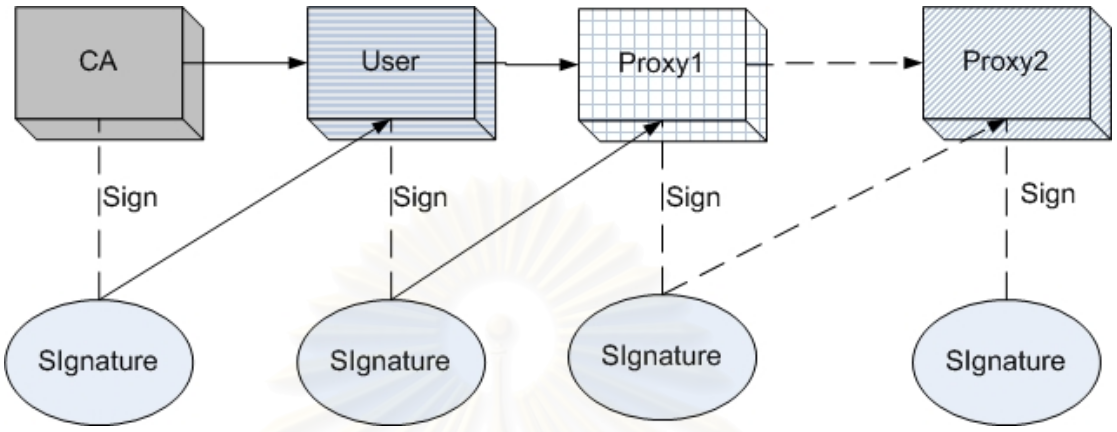
- ชื่อเฉพาะ (DN - Distinguished Name) จะเป็นสิ่งที่ไม่ซ้ำกันทั่วโลกโดยมีลักษณะเป็นลำดับขั้นตามรูปแบบของการสร้างเนมสเปซของไดเรกทอรีเอ็กซ์ 500 ดังนั้นเราจึงนำชื่อเฉพาะนี้มาใช้เป็นชื่อผู้ใช้ในองค์กรเสมือนได้ ตัวอย่างชื่อเฉพาะได้แก่ /C=TH/O=Grid/O=Chula/CN=g46pkn
- ชื่อผู้ออกหลักฐานอ้างอิงตัวผู้ใช้ (Issuer) เป็นชื่อเฉพาะของผู้ที่ทำการออกหลักฐานอ้างอิงตัวผู้ใช้จากในรูปที่ 2.5 คือ /C=TH/O=Grid/O=Chula/CN=Apollo CA
- ช่วงเวลาที่ใช้ได้ (validity) คือช่วงเวลาที่ใบยืนยันตัวตนนี้สามารถใช้งานได้อย่างถูกต้อง ในรูปที่ 2.5 หลักฐานอ้างอิงตัวผู้ใช้นี้จะสามารถใช้ได้ในช่วงเวลาระหว่าง 31 May 2004 เวลา 04:35:25 ถึง 31 May 2004 เวลา 15:22:32
- กุญแจสาธารณะ (public key) เป็นส่วนหนึ่งที่ใช้ในระบบโครงสร้างของกุญแจสาธารณะ
- ส่วนขยายของหลักฐานอ้างอิงผู้ใช้ คือส่วนที่โดยปกติจะถูกเพิกเฉย คือถ้าไม่มีรายละเอียดในส่วนนี้หลักฐานอ้างอิงผู้ใช้ก็ยังสามารถใช้งานได้
- ลายเซ็นดิจิตอล คือ ส่วนที่มีไว้ตรวจสอบว่าหลักฐานอ้างอิงผู้ใช้นี้ได้มีการแก้ไขไปจากสิ่งที่ผู้ออกหลักฐานอ้างอิงผู้ใช้สร้างไว้ตอนแรกหรือไม่

2.1.7.3 การมอบอำนาจ (Delegation) การลงบันทึกเข้าระบบเพียงครั้งเดียว

ในการประมวลผลของโปรแกรมแบบกระจายจะต้องมีความสามารถในการทำงานแทนผู้ใช้บนกริดได้ ซึ่งการทำงานแทนผู้ใช้ดังกล่าวอาจจะต้องถูกพิสูจน์ตัวจริงหลายครั้ง ดังนั้นจีเอสไอจึงเตรียมความสามารถในการมอบอำนาจให้กับการประมวลผลที่อยู่บนแม่ข่ายระยะไกล (remote host) โดยการสร้างตัวแทน (Proxy) เพื่อลดจำนวนครั้งที่ผู้ใช้จะต้องใส่วลีผ่านในการถอดรหัสกุญแจส่วนบุคคลเพื่อพิสูจน์ตัวจริง โดยตัวแทนที่สร้างขึ้นมานั้นจะประกอบไปด้วยหลักฐานอ้างอิงผู้ใช้อันใหม่ซึ่งบรรจุกุญแจสาธารณะใหม่และกุญแจส่วนบุคคลใหม่

โดยหลักฐานอ้างอิงตัวผู้ใช้อันใหม่จะต่างจากอันเดิมเล็กน้อยเพื่อบอกว่าเป็นตัวแทน โดยผู้ที่จะเซ็นหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนใหม่นี้ก็คือตัวผู้ใช้เอง หรือกล่าวได้ว่าเจ้าของตัวแทนจะทำหน้าที่แทนองค์กรที่ออกหลักฐานอ้างอิงตัวผู้ใช้เพื่อสร้างตัวแทน และตัวแทนที่สร้างขึ้นมาจะมีอายุการใช้งานจำกัดถ้าผู้ใช้ไม่ระบุระยะเวลาไว้ตัวแทนจะมีอายุการใช้งาน 12 ชั่วโมง และการเก็บรักษากุญแจส่วนบุคคลของตัวแทนสามารถเก็บโดยไม่ต้องเข้ารหัสไว้ในระบบแฟ้มข้อมูลเดียวกันกับหลักฐานอ้างอิงตัวผู้ใช้อันใหม่แต่ไม่ได้เก็บไว้ในรูปแบบของเอ็กซ์ 509 เพื่อให้ผู้ใช้สามารถใช้หลักฐานอ้างอิงผู้ใช้ตัวแทนและกุญแจส่วนบุคคลตัวแทนสำหรับการพิสูจน์ตัวจริงร่วมกัน (Mutual

Authentication) ได้โดยไม่ต้องใส่วลีผ่านทุกครั้งเพื่อเอากุญแจส่วนบุคคลของผู้ใช้มาทำการพิสูจน์ตัวจริง



รูปที่ 2.6 แสดงลำดับการเซ็นหลักฐานอ้างอิงตัวผู้ใช้เพื่อสร้างตัวแทน

การพิสูจน์ตัวจริงร่วมกันโดยฝ่ายหนึ่งใช้ตัวแทนจะมีวิธีการที่แตกต่างจากปกติเล็กน้อย คือ ฝ่ายที่ทำการพิสูจน์ตัวจริงของตัวแทนจะได้รับทั้งหลักฐานอ้างอิงตัวผู้ใช้ของตัวแทนและหลักฐานอ้างอิงตัวผู้ใช้ของเจ้าของตัวแทน ซึ่งระหว่างการพิสูจน์ตัวจริงจะใช้กุญแจสาธารณะของเจ้าของที่บรรจุในหลักฐานอ้างอิงตัวผู้ใช้ในการตรวจสอบลายเซ็นบนหลักฐานอ้างอิงตัวผู้ใช้ของตัวแทน ส่วนกุญแจสาธารณะขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้จะใช้เพื่อตรวจสอบลายเซ็นของหลักฐานอ้างอิงตัวผู้ใช้ ซึ่งทำให้เกิดลูกโซ่ของความเชื่อถือ (Trust chain) จากองค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ยังตัวแทนผ่านเจ้าของ โดยกุญแจสาธารณะขององค์กรที่ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้จะอยู่ในรูปแบบของหลักฐานอ้างอิงตัวองค์กรเองและจะเก็บอยู่บนทุกเอนทิตีที่ต้องการพิสูจน์ตัวจริง โดยปกติแล้วจะอยู่ในไดเรกทอรี /etc/grid-security/certificates/ และชื่อแฟ้มที่บรรจุหลักฐานอ้างอิงตัวองค์กรจะมีรูปแบบคือ ค่า hash ของหลักฐานอ้างอิงตัวองค์กร.0 เช่น 411204bc.0 เป็นต้น ส่วนหลักฐานอ้างอิงตัวผู้ใช้ของตัวแทนจะถูกเก็บในแฟ้ม /tmp/x509up_u{uid} เช่น /tmp/x509up_u5561 ซึ่งในแฟ้มจะมีรายละเอียดดังต่อไปนี้

หลักฐานอ้างอิงตัวผู้ใช้ตัวแทน

```
-----BEGIN CERTIFICATE-----
MIICDjCCAXegAwIBAgIBAjANBgkqhkiG9w0BAQQFADBnMQ0wCwYDVQQKEwRHcmlk
MQ4wDAYDVQQKEwVDaHVsYTEbMBkGA1UECxMSY3AuZW5nLmNodWxhLmFjLnRoMSkw
JwYDVQQDEyBQYXRpcGFuIEtvbmdzaXJpa3VsICg0NjcwMzU5NTIxKTAeFw0wNTAy
MjEwNTU5NDdaFw0wNTAyMjExODA0NDdaMHcxDTALBgNVBAoTBEdyaWQxDjAMBgNV
BAoTBUNodWxhMRswGQYDVQQLExJjcC5lbmcuY2h1bGEuYWMudGgxKTAnBgNVBAMT
IFBhdGlwYW4gS29uZ3NpcmlrdWwgKDQ2NzAzNTk1MjEpMQ4wDAYDVQQDEwVwcm94
eTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDXpP9l8tyJoi/Zel8i8fvVandc2AEP
ile2JOX79CL9PACninYDiqkmja24QDFtRS2RrgdAiNTmANXwME3rygtlAgMBAAEw
```

กุญแจส่วนบุคคลสำหรับผู้ใช้ตัวแทน

หลักฐานอ้างอิงตัวผู้ใช้

รูปที่ 2.7 แสดงรายละเอียดภายในแฟ้มหลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้รับการมอบอำนาจ

ในหลักฐานอ้างอิงผู้ใช้ผู้แทนที่ได้รับการมอบอำนาจจากผู้ใช้จะประกอบด้วยรายละเอียดของผู้มอบอำนาจทั้งหมดตั้งแต่ผู้ใช้จนถึงตัวแทนล่าสุด กล่าวคือถ้ามีการมอบอำนาจจนถึงตัวแทนผู้ใช้ล่าสุดเป็นจำนวน 3 ครั้งจะต้องมีหลักฐานอ้างอิงผู้ใช้และหลักฐานอ้างอิงผู้ใช้จำนวน 3 อัน นอกจากนี้ในแฟ้มหลักฐานอ้างอิงผู้ใช้ตัวแทนจะเก็บกุญแจส่วนบุคคลของผู้ใช้ตัวแทนล่าสุดไว้ด้วย

2.1.7.4 **ขั้นตอนวิธีการพิสูจน์ตัวจริง**

ในการพิสูจน์ตัวจริงจะทำบนมาตรฐานของโครงสร้างของกุญแจสาธารณะ โดยกำหนดชื่อเฉพาะ ให้กับผู้ใช้และทรัพยากร วิธีการพิสูจน์ตัวจริงด้วยการรักษาความปลอดภัยของกริดนี้ทำโดยการพิสูจน์ว่าผู้ใช้หรือทรัพยากรนั้นเป็นเอนทีตี ที่ถูกระบุโดยชื่อเฉพาะหรือไม่ โดยจะทำการ

ตรวจสอบหลักฐานอ้างอิงผู้ใช้ และกุญแจส่วนบุคคล โดยที่ทั้งผู้ใช้และทรัพยากรจะต้องเชื่อถือผู้ทำหน้าที่ออกหลักฐานอ้างอิงตัวผู้ใช้ของทั้งสองฝ่าย ดังนี้

1. ผู้ใช้สร้างตัวแทนเพื่อลดจำนวนครั้งที่ผู้ใช้จะต้องใส่วลีผ่าน(Grid Passphrase) เพื่อถอดรหัสกุญแจส่วนบุคคลในการพิสูจน์ตัวจริงโดยที่ตัวแทนจะมีหลักฐานอ้างอิงผู้ใช้ตัวแทน(Proxy Certificate) และกุญแจส่วนบุคคลของผู้ใช้ตัวแทน(Proxy Private Key)
2. ผู้ใช้และทรัพยากรจึงทำการแลกเปลี่ยนหลักฐานอ้างอิงผู้ใช้ซึ่งกันและกัน
3. ทรัพยากรทำการตรวจสอบหลักฐานอ้างอิงผู้ใช้ดังนี้
    a. ผู้ที่ออกหลักฐานอ้างอิงผู้ใช้คือใครและทรัพยากรมีความเชื่อถือหรือไม่ ถ้าทรัพยากรไม่มีความเชื่อถือผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ ก็จะพิจารณาผู้ที่ออกหลักฐานอ้างอิงของผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ และทำไปเรื่อยจนกว่าผู้ที่ออกหลักฐานอ้างอิงผู้ใช้นั้นมีความเชื่อถือกันทำให้เกิดลูกโซ่ของความเชื่อถือ (Trust chain)
    b. เมื่อทรัพยากรเชื่อถือในหลักฐานอ้างอิงผู้ใช้แล้ว จึงทำการตรวจสอบความถูกต้องของหลักฐานการอ้างอิงของผู้ใช้กับลายเซ็นดิจิตอลที่แนบมาในหลักฐานอ้างอิงผู้ใช้ โดยนำลายเซ็นดิจิตอลถอดรหัสด้วยกุญแจสาธารณะของผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ และนำไปเทียบกับหลักฐานอ้างอิงผู้ใช้ที่ทำเมสเซจไดเจซ (Massage Digest) ถ้าได้ลักษณะเหมือนกันแสดงว่าข้อความไม่ได้ถูกแก้ไข
    c. พิจารณาระยะเวลาที่สามารถใช้งานได้ในหลักฐานอ้างอิงผู้ใช้
4. ตัวแทนผู้ใช้ทำการพิสูจน์ตัวจริงว่าเป็นเจ้าของหลักฐานอ้างอิงผู้ใช้นั้นโดย
    a. ทรัพยากรสร้างข้อความสุ่มไปยังตัวแทนผู้ใช้เพื่อขอให้ตัวแทนผู้ใช้เข้ารหัสข้อความนั้น
    b. ตัวแทนผู้ใช้เข้ารหัสข้อความนั้นด้วยกุญแจส่วนบุคคลของตัวแทนผู้ใช้ โดยใช้เอสเอสแอล เวอร์ชัน 3 (SSLv3) สำหรับการเข้ารหัส
    c. ทรัพยากรทำการถอดรหัสโดยใช้กุญแจสาธารณะของตัวแทนผู้ใช้ และทำการเปรียบเทียบกับข้อความสุ่มที่ได้ส่งไปยังตัวแทนผู้ใช้
5. ทรัพยากรทำการพิสูจน์ตัวจริงกับผู้ใช้ดังข้อ 3 และ ข้อ 4
6. ในตอนนี้ทรัพยากรจะเชื่อถือตัวแทนผู้ใช้และจะทำการจับระหว่างชื่อเฉพาะในหลักฐานอ้างอิงผู้ใช้กับชื่อผู้ใช้เฉพาะที่ในกริดแมปไฟล์ (grid-mapfile) ดังรูปที่ 2.8

"/…/CN=Patipan Kongsirikul" g46pkn

รูปที่ 2.8 แสดงเนื้อความในกริดแมปไฟล์

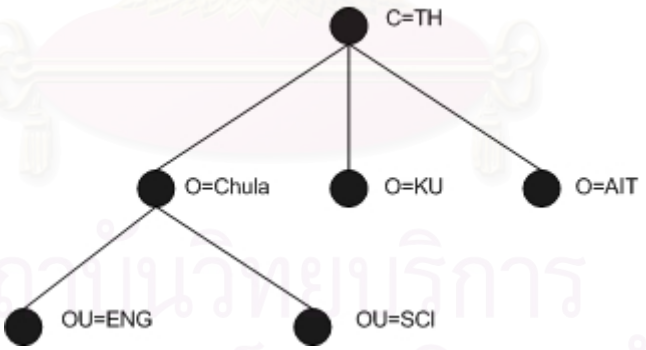
จะเห็นได้ว่าจีเอสไอมีความสามารถในด้านการขยายตัวค่อนข้างแย่ดังสมการต่อไปนี้

ความสามารถในการขยายตัวของระบบ = 1 / (จำนวนผู้ใช้ในองค์กรเสมือน x จำนวนเครื่องทรัพยากรในองค์กรเสมือน)

ดังนั้นในงานวิจัยนี้จึงมุ่งเน้นที่จะเพิ่มความสามารถในการขยายตัวของระบบกริดให้มีความสามารถในการขยายตัวของระบบที่ดีกว่าจีเอสไอ

2.1.8 **เนมสเปซของไดเรกทอรีเอ็กซ์** 500

การกำหนดเนมสเปซของไดเรกทอรีได้มีการกำหนดโครงสร้างของเนมสเปซให้มีความคล่องตัวในการออกแบบ โครงสร้างสร้างการกำหนดเนมสเปซของไดเรกทอรีโพรโทคอลเอ็กซ์ 500 จะกำหนดประเทศ (Country) หรือตัวอักษรซี (c) ไว้ที่ส่วนบนสุดของไดเรกทอรีถัดจากประเทศจะเป็นชื่องค์กร (Organization) หรือตัวอักษรโอ (o) ตัวอย่างของโครงสร้างการกำหนดเนมสเปซดังรูปที่ 2.9



รูปที่ 2.9 โครงสร้างการกำหนดเนมสเปซในเอ็กซ์ 500

ไดเรกทอรีเอ็กซ์ 500 กำหนดชนิดของแอททริบิวท์ที่นิยมใช้ในการกำหนดเนมสเปซ ดังตารางที่ 2.1

ตารางที่ 2.1 แสดงชนิดของแอททริบิวต์ที่นิยมใช้ในการกำหนดเนมสเปซ

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

2.2 งานวิจัยที่เกี่ยวข้อง

จากการศึกษาเบื้องต้นพบว่ามีงานวิจัยที่เกี่ยวข้องทั้งสิ้น 7 งานวิจัย โดยแบ่งออกเป็นงานวิจัยที่เกี่ยวข้องกับระบบจัดการสิทธิภายในองค์กรเสมือนเดียวกัน 6 งานวิจัยและระบบจัดการสิทธิสำหรับสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือน 1 งานวิจัย ซึ่งมีรายละเอียดดังต่อไปนี้

2.2.1 ระบบจัดการสิทธิภายในองค์กรเสมือน

ปัญหาการขยายตัวภายในองค์กรเสมือนจะเกิดขึ้นเมื่อองค์กรเสมือนมีขนาดใหญ่ กล่าวคือสามารถพิจารณาขนาดขององค์กรเสมือนได้จากจำนวนผู้ใช้และจำนวนของทรัพยากรที่อยู่ในองค์กรเสมือน เพราะในระบบกริดนั้นผู้ใช้และทรัพยากรจะมีความสัมพันธ์กันแบบทั่วถึง โดยการสร้างกริดแมปไฟล์บนทุกๆเครื่องทรัพยากร โดยเนื้อหาในกริดแมปไฟล์มีลักษณะเป็นชื่อเฉพาะจับคู่กับชื่อผู้ใช้เฉพาะที่บนเครื่องทรัพยากรนั้น ทำให้มีงานวิจัยที่เข้ามาเสริมระบบกริดให้มีความสามารถในการขยายตัวของระบบที่ดีขึ้นดังนี้

2.2.1.1 **ซีเอเอส** (CAS - Community Authorization Service) [8-10]

ซีเอเอส(CAS) พัฒนาโดยทีมวิจัยโกลบัสเช่นเดียวกันกับจีเอสไอ เพื่อทำการปรับปรุงระบบการดูแลสิทธิการเข้าใช้ทรัพยากรในระบบกริดซึ่งเป็นปัญหาแก่ผู้ดูแลระบบกริดได้แก่ ปัญหาด้านการขยายตัวของระบบ (Scalability) ความยืดหยุ่นของระบบ(Flexibility) การขาดนโยบายดีพอ (lack of expressiveness) โดยใช้แนวคิดการสร้างเซอร์ฟเวอร์สำหรับดูแลสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ในกลุ่มของผู้ใช้เองและให้ผู้ครอบครองทรัพยากรกำหนดสิทธิการเข้าใช้ของกลุ่มคนแทนการกำหนดสิทธิการเข้าใช้เป็นรายบุคคล แต่ทั้งนี้ผู้ครอบครองทรัพยากรยังสามารถกำหนดสิทธิการเข้าใช้ทรัพยากรให้แก่ผู้ใช้เป็นรายบุคคลได้ด้วย โดยหลักการทำงานของซีเอเอสสามารถอธิบายได้ดังนี้

ขั้นแรกผู้ใช้จะต้องติดต่อไปยังเซอร์ฟเวอร์ที่เก็บสิทธิการใช้งานทรัพยากรและทำการพิสูจน์ตัวจริงและหลังจากนั้นเซอร์ฟเวอร์จะค้นหาสิทธิการเข้าใช้ทรัพยากรจากฐานข้อมูลพร้อมทั้งสร้างสิ่งที่อ้างสิทธิการใช้(Authorization Assertion) พร้อมทั้งทำลายเซ็นดิจิตอลกำกับไว้

ขั้นสองเมื่อผู้ใช้งานต้องการใช้งานทรัพยากรใดๆก็จะนำสิ่งที่อ้างสิทธิไปให้ทรัพยากรพร้อมทั้งยืนยันตัวบุคคลว่าเป็นบุคคลในสิ่งที่อ้างสิทธิจริงสามารถใช้งานทรัพยากรนี้ได้ และทรัพยากรเองก็จะนำชื่อเฉพาะของผู้ใช้และชื่อเฉพาะของเซอร์ฟเวอร์ผู้ออกสิ่งที่อ้างสิทธิไปเปรียบเทียบกับสิทธิที่มีต่อทรัพยากรเองพร้อมทำการอินเทอเซกชันเพื่อให้ได้สิทธิที่ใช้ได้จริงต่อไป

ซีเอเอสได้มีการพัฒนามาหลายเวอร์ชั่นด้วยกันโดยเวอร์ชั่นล่าสุดนั้นสามารถรองรับการทำงานของโกลบัสทูลคิดในรุ่นที่ 3.2 ในส่วนของกริดเอฟทีพี แต่ยังไม่รองรับการทำงานในส่วนอื่นๆของโกลบัสทูลคิดรุ่น3.2 ซึ่งในงานวิจัยนี้จะนำแนวคิดของซีเอเอสมาพัฒนาต่อให้สามารถทำงานร่วมกันกับโกลบัสทูลคิดรุ่น 3.2 ในส่วนของแกรมให้สามารถใช้งานได้ภายในองค์กรเสมือนเดียวกันและสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือน

2.2.1.2 **วีโอเอ็มเอส** (VOMS – Virtual Organizations Membership Service) [11]

งานวิจัยวีโอเอมเอสทำขึ้นเพื่อจุดประสงค์ในการทำระบบจัดการสิทธิการเข้าใช้ทรัพยากรของยุโรปดาต้ากริด (EDG: Europe Data Grid) โดยหลักการของวีโอเอมเอสนี้ก็คือจะทำการสร้างวีโอเอมเอสเซอร์ฟเวอร์ เพื่อทำการเก็บสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ในองค์กรเสมือน เพื่อเพิ่มความสามารถในด้านขยายระบบซึ่งเป็นข้อเสียของระบบเดิมของกริด

ซึ่งในส่วนของงานวิจัยวีโอเอ็มเอสในช่วงแรกสร้างขึ้นเพื่อรองรับการทำงานโกลบัสทูลคิดในรุ่น 2.x ในส่วนของแกรม และเมื่อปลายปีพศ. 2547 ทางผู้พัฒนาได้พัฒนาให้หลักฐานอ้างอิงผู้ใช้แบบแอททริบิวต์ สามารถนำไปใช้กับกริดเซอร์วิสที่รันอยู่บนโกลบัสคอนเทนเนอร์ได้

งานวิจัยวีโอเอ็มเอสต่างจากงานวิจัยนี้ตรงที่ งานวิจัยวีโอเอ็มเอสรองรับการใช้งานแกรมของโกลบัสทูลคิดรุ่น 3.x โดยการเรียกกริดเซอร์วิสผ่าน โกลบัสเกตคีปเปอร์ (Globus Gatekeeper) ของโกลบัสทูลคิดรุ่น 2.x แต่งานวิจัยนี้ผู้ใช้สามารถเรียกใช้กริดเซอร์วิสได้โดยผ่านโกลบัสคอนเทนเนอร์โดยตรงไม่ต้องผ่านโกลบัสเกตคีปเปอร์

2.2.1.3 **พริม่า** (PRIMA - PRIvilege Management Architecture) [18]

งานวิจัยพริม่าทำขึ้นเพื่อมีจุดประสงค์การทำสภาพแวดล้อมสำหรับการทำงานใดๆโดยใช้สิทธิน้อยที่สุดเท่าที่สามารถทำงานนั้นได้ (least privilege execution environment) และการทำรายชื่อผู้ใช้แบบพลวัตร (dynamic accounts) โดยในงานวิจัยนี้มีรูปแบบการใช้สิทธิเข้าใช้ทรัพยากรได้ 3 รูปแบบได้แก่ แบบจับคู่ครีเดนเชียลกับรายชื่อผู้ใช้เฉพาะที่(Credential mapping), แบบผสม (Mixed Mode Authorization) และ แบบใช้ครีเดนเชียลเพียงอย่างเดียว (Full Credential Combination) รูปแบบของพริม่าจะเป็นการทำงานแบบพูลและมีจุดเด่นกว่างานอื่นคือเป็นงานที่ให้ความสนใจสิทธิการใช้งานน้อยสุดที่ทำงานได้และการทำรายชื่อผู้ใช้แบบพลวัตรซึ่งไม่มีในงานวิจัยอื่น

ตัวงานวิจัยพริม่าต่างจากงานวิจัยนี้ตรงที่งานวิจัยพริม่าสนับสนุนโกลบัสทูลคิดในรุ่น 2.x เท่านั้นยังไม่สนับสนุนการทำงานของโกลบัสในรุ่น 3.x

2.2.1.4 **เพอมิส** (PERMIS) [19]

งานวิจัยเพอมิสได้นิยามโครงสร้างของการออกหลักฐานการอ้างอิงผู้ใช้แบบแอททริบิวต์ (AC - Attribute Certificate) โดยเลียนแบบมาจากโครงสร้างการออกหลักฐานอ้างอิงผู้ใช้แบบเอ็กซ์ห้าศูนย์เก้า (X.509 Certificate) ของโครงสร้างกุญแจสาธารณะ โดยให้ชื่อว่าโครงสร้างการจัดการสิทธิ (PMI - Privilege Management Infrastructure) งานวิจัยเพอมิสมุ่งเน้นที่จะบรรยายสิทธิการเข้าใช้ให้อยู่ในพื้นฐานของอาร์แบค (RBAC: Role Based Access Control) โดยสิทธิของผู้ใช้จะมาเก็บในรูปแบบของหลักฐานการอ้างอิงผู้ใช้แบบแอททริบิวต์แล้วนำไปเก็บไว้ในแอลแดป (LDAP: Lightwieght Directory Access Protocol)

ในงานวิจัยเพอมิสแตกต่างจากงานวิจัยนี้ตรงที่ งานวิจัยเพอมิสมีการทำงานเป็นแบบพูล และยังไม่สนับสนุนการทำงานของโกลบัสรุ่น 2.x และ 3.x

2.2.1.5 **อะเคนติ** (Akenti) [20]

งานวิจัยอะเคนติเป็นงานวิจัยที่เกี่ยวกับการจัดการสิทธิบนระบบกระจายงานในช่วงแรก ประมาณปีคศ. 1996 และมีลักษณะเป็นแบบพูลนั่นคือผู้ใช้จะติดต่อไปที่ทรัพยากรและทรัพยากรจะเป็นตัวกลางไปค้นหาสิทธิการเข้าใช้ทรัพยากรของผู้ใช้เอง

งานวิจัยอะเคนติต่างกับงานวิจัยนี้ตรงที่งานวิจัยอะเคนติยังไม่ได้มีการพัฒนามาใช้งานร่วมกันกับโกลบัสทูลคิดรุ่นใดเลย แต่มีแนวโน้มว่าจะพัฒนามาใช้งานร่วมกันกับระบบจัดการสิทธิตัวอื่นเช่น อะเคนติกับซีเอเอส หรือ อะเคนติกับวีโอเอมเอส บนโกลบัสทูลคิดรุ่น 2.x แต่ในงานวิจัยนี้พัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรในกริดสำหรับโกลบัสทูลคิดรุ่น3.x ในส่วนของแกรมให้สามารถใช้งานได้ภายในองค์กรเสมือนเดียวกันและสามารถใช้บนสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือนได้

2.2.1.6 **ดับบลิวเอเอส** (WAS – Workflow Authorization Service) [21]

งานวิจัยดับบลิวเอเอสเป็นงานวิจัยที่ทำเกี่ยวกับสิทธิการเข้าใช้ทรัพยากรในกริดของประเทศเกาหลีใต้ โดยนำมาแก้ปัญหาซึ่งพบได้ในการจัดการสิทธิในกริดแบบเดิมได้แก่ เพิ่มความสามารถในด้านการขยายตัวของระบบเดิมที่มีแต่จีเอสไอ และ นโยบายการใช้งานที่แนบมากับสิ่งยืนยันตัวตนนั้นให้สิทธิมากเกินกว่าสิทธิที่ผู้ใช้ต้องการในการทำงานครั้งนั้นๆ อาจก่อให้เกิดการนำไปใช้ในทางที่ผิดได้โดยง่าย

งานวิจัยดับบลิวเอเอสนี้มีแนวคิดที่ค่อนข้างแตกต่างจากงานวิจัยอื่นอยู่ตรงที่งานวิจัยอื่นๆจะเป็นการค้นหาสิทธิของผู้ใช้ทั้งหมดแต่งานวิจัยนี้จะนำเวิร์กโฟลว์(Workflow) ของผู้ใช้ไปเปรียบเทียบกับสิทธิการเข้าใช้งานของผู้ใช้ ถ้าตรวจแล้วว่าผู้ใช้มีสิทธิจึงทำการเข้ารหัสเวิร์กโฟลว์แทน และงานวิจัยดับบลิวเอเอสนี้รองรับการทำงานของโกลบัสรุ่น2.x เท่านั้นยังไม่มีส่วนที่มารองรับโกลบัสรุ่น3.x

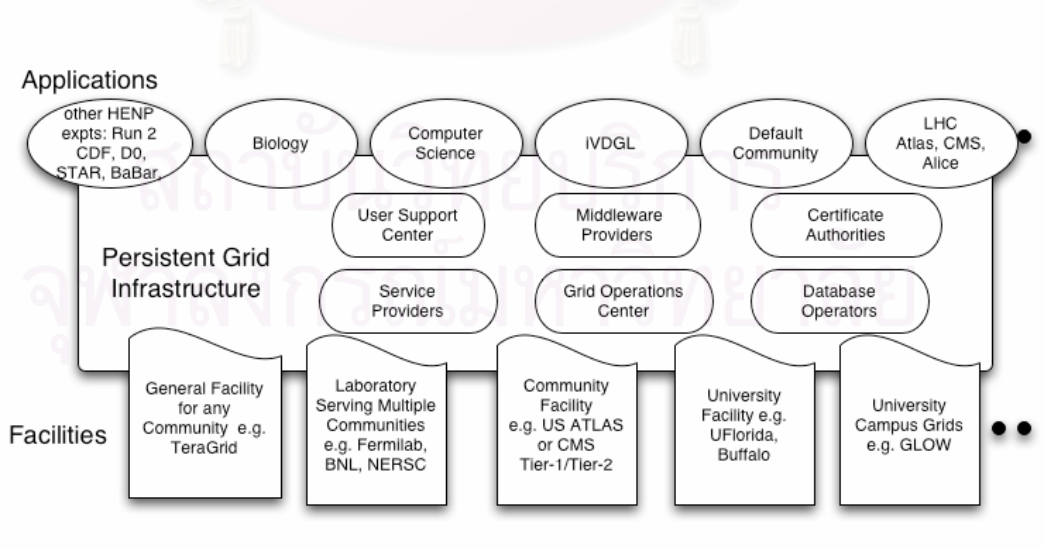
2.2.2 **ระบบจัดการสิทธิสำหรับสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือน**

องค์กรเสมือนต่างๆเมื่อตอนเริ่มต้นจะเกิดจากความร่วมมือไม่กี่องค์กร แต่เมื่อเวลาผ่านไปซักระยะหนึ่งแล้วองค์กรเสมือนต่างๆมีความต้องการที่จะเชื่อมต่อเข้าด้วยกัน เพื่อสร้างสภาพแวดล้อมสำหรับผู้ใช้ที่ดีขึ้นเนื่องจากมีหน่วยประมวลผลที่มากขึ้น แต่การที่จะรวมกันของ

องค์กรเสมือนย่อมทำให้จำนวนผู้ใช้ และทรัพยากรซึ่งมีมากอยู่แล้วยิ่งมีจำนวนมากขึ้นไป ทำให้เกิดปัญหาการขยายตัวของระบบขึ้นมาเช่นเดียวกับการขยายตัวขององค์กรเสมือน เมื่อเราแก้ไขปัญหาโดยการใช้เซอร์ฟเวอร์ตัวกลางที่ดูแลสิทธิ เช่น ซีเอเอสหรือวีโอเอ็มเอส จะก่อให้เกิดปัญหาต่างๆ ได้แก่ ปัญหาการหาเครื่องเซอร์ฟเวอร์ตัวกลางที่แต่ละองค์กรในองค์กรเสมือนเชื่อถือร่วมกันเป็นเรื่องที่ทำได้ยาก ปัญหาการจัดทำสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ของแต่ละองค์กรเสมือนใหม่ให้สอดคล้องกับทรัพยากรที่เพิ่มเข้ามา ปัญหาเมื่อซีเอเอสล่มจะทำให้ผู้ใช้งานในองค์กรเสมือนอื่นจะไม่สามารถทำงานได้แม้จะต้องการทำงานภายในองค์กรเสมือนของตนเอง ดังนั้นจึงจำเป็นที่จะต้องมีการออกแบบระบบจัดการสิทธิขึ้นใหม่ให้สอดคล้องกับลักษณะการเชื่อมต่อขององค์กรเสมือน ซึ่งในปัจจุบันได้เริ่มมีผู้สนใจคือโปรเจค โอเพ่นไซน์กริด (Open Science Grid) ซึ่งมีรายละเอียดดังหัวข้อ 2.2.2.1

2.2.2.1 **โอเพ่นไซน์กริด** (OSG – Open Science Grid) [12]

โอเพ่นไซน์กริดรับผิดชอบโดยหน่วยงานของกระทวงพลังงาน (DOE - Department of Energy) และ หน่วยงานทางวิทยาศาสตร์แห่งชาติ (NSF - National Science Foundation) เพื่อที่จะสร้าง โครงสร้างของกริดระดับชาติสำหรับประเทศสหรัฐอเมริกา ซึ่งจะทำการเชื่อมต่อกับประเทศอื่นๆที่มีโครงสร้างของกริดเพื่อนักวิทยาศาสตร์เช่น LHC Computing Grid เพื่อให้ได้โครงสร้างสำหรับการวิจัยทางวิทยาศาสตร์ระดับนานาชาติ (International scientific) ดังรูปที่ 2.10



รูปที่ 2.10 ภาพรวมของโอเพ่นไซน์กริด

งานวิจัยโอเพ่นไซน์กริดได้ออกแบบระบบจัดการสิทธิของผู้ใช้ในองค์กรเสมือนโดยปรับปรุงระบบจัดการสิทธิที่ได้ใช้ในองค์กรเสมือนกริด2003 (Grid2003 VOs) และมีการเพิ่มเติมส่วนประกอบเพื่อความสมบูรณ์ของระบบยิ่งขึ้น ซึ่งส่วนประกอบที่จะพัฒนาเพิ่มเติมส่วนใหญ่ยังอยู่ในระหว่างการออกแบบและทวนสอบอยู่

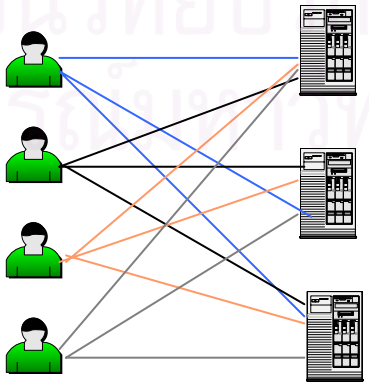
งานวิจัยโอเพ่นไซน์กริดต่างจากงานวิจัยนี้ตรงที่ งานวิจัยโอเพ่นไซน์กริดมีการพัฒนาส่วนประกอบอื่นๆนอกจากระบบจัดการสิทธิสำหรับสภาพแวดล้อมของการเชื่อมต่อขององค์กรเสมือน หรือสามารถกล่าวได้ว่างานวิจัยนี้เป็นเซตย่อย (Subset) ของงานวิจัยโอเพ่นไซน์กริด

บทที่ 3

การออกแบบและพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรภายในองค์กรเสมือนเดียวกัน

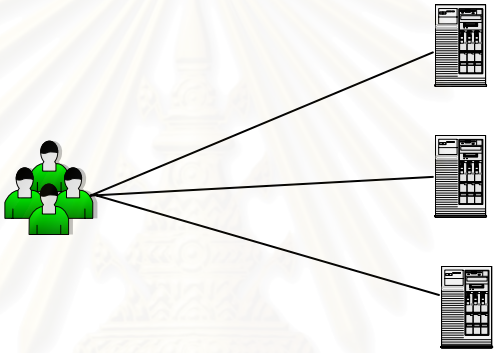
ในระบบกริดปัจจุบันจะเน้นไปด้านการทดลองทางวิทยาศาสตร์ซึ่งจะต้องใช้เครื่องทรัพยากรในการประมวลผลและเก็บข้อมูลและมีผู้ใช้จำนวนมาก ทำให้การดูแลจัดการภายในองค์กรเสมือนเป็นภาระสำหรับผู้ดูแลระบบกริดภายในองค์กรเสมือนที่จะต้องเพิ่มผู้ใช้และสิทธิการเข้าใช้ของผู้ใช้บนแต่ละเครื่องทรัพยากรหรือ สามารถกล่าวได้ว่า

- ถ้าในองค์กรเสมือนใดๆมีผู้ใช้จำนวน u และมีเครื่องทรัพยากรจำนวน r ผู้ดูแลระบบนั้นจะต้องเพิ่มผู้ใช้และสิทธิการเข้าใช้ทรัพยากรของผู้ใช้แต่ละคนจำนวน u x r ครั้งสำหรับการเริ่มสร้างองค์กรเสมือนใดๆ
- ถ้าปรากฏว่ามีผู้ใช้เพิ่มเข้ามาในองค์กรเสมือน ผู้ดูแลระบบนั้นจะต้องเพิ่มผู้ใช้และสิทธิการเข้าใช้ทรัพยากรของผู้ใช้บนเครื่องทรัพยากรจำนวน r เครื่อง
- ถ้ามีองค์กรอื่นต้องการที่จะเข้าร่วมเป็นองค์กรเสมือนเดียวกัน ผู้ดูแลระบบจะต้องเพิ่มผู้ใช้และสิทธิของผู้ใช้จากองค์กรอื่นให้กับเครื่องทรัพยากรขององค์กรเสมือนเดิม และเพิ่มจำนวนผู้ใช้และสิทธิการเข้าใช้ขนาดเท่ากับจำนวนผู้ใช้ของทั้งสององค์กรเสมือนให้กับจำนวนเครื่องทรัพยากรขององค์กรที่ต้องการจะเข้าร่วมเป็นองค์กรเสมือนเดียวกัน ดังนั้นงานที่ผู้ดูแลระบบจะต้องรับผิดชอบเพิ่มขึ้นเท่ากับ (จำนวนผู้ใช้ขององค์กรเสมือนอื่น x จำนวนทรัพยากรในองค์กรเสมือนเดียวกับผู้ดูแลระบบ)+ (จำนวนผู้ใช้ของทั้งสององค์กรเสมือน x จำนวนทรัพยากรขององค์กรเสมือนอื่น)
- ถ้ามีผู้ใช้ในองค์กรเสมือนต้องการเปลี่ยนสิทธิการเข้าใช้ของตนเอง ผู้ดูแลระบบนั้นจะต้องเปลี่ยนแปลงสิทธิของผู้ใช้บนเครื่องทรัพยากรจำนวน r เครื่อง



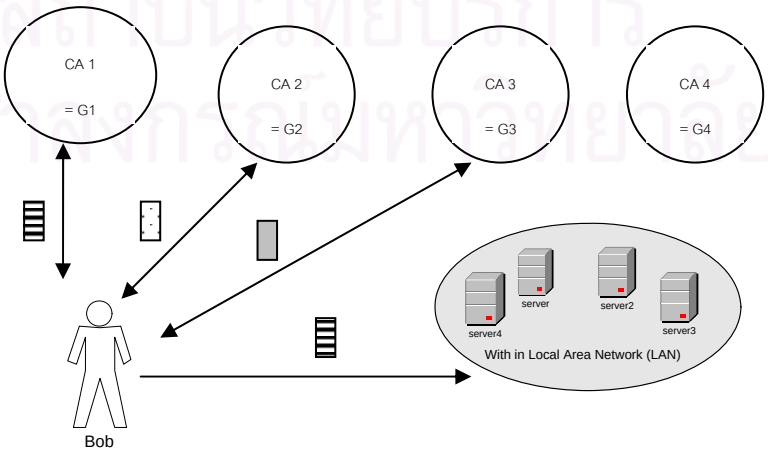
รูปที่ 3.1 รูปแสดงความสัมพันธ์ของสิทธิการเข้าใช้ของผู้ใช้กับทรัพยากร

เนื่องจากในองค์กรเสมือนผู้ใช้จะต้องเปลี่ยนไปใช้ชื่อผู้ใช้เฉพาะที่บนแต่ละทรัพยากร ซึ่งอยู่กระจัดกระจายกันทำให้สร้างความลำบากในการดูแลจัดการของผู้ดูแลระบบในองค์กรเสมือน ประกอบกับการที่ทรัพยากรในองค์กรเดียวกันมักจะดูแลโดยกลุ่มผู้ดูแลกลุ่มเดียวกัน จึงเกิดแนวคิดที่จะนำผู้ใช้จำนวนหนึ่งมามัดรวมกันเป็นกลุ่มของผู้ใช้ (User community) เพื่อลดภาระสำหรับผู้ดูแลระบบ โดยกำหนดให้จำนวนกลุ่มของผู้ใช้มีจำนวนน้อยกว่ามากๆเมื่อเทียบกับจำนวนผู้ใช้ในระบบ ซึ่งกลุ่มของผู้ใช้จะอยู่ในรูปแบบหน้าที่ของผู้ใช้เช่น กลุ่มผู้ใช้งานเพื่อคิดค้นยา กลุ่มผู้ใช้งานทางด้านฟิสิกส์ เป็นต้น หรือ กลุ่มผู้ใช้อาจจะหมายถึงองค์กรของผู้ใช้จริงๆเช่นกลุ่มผู้ใช้งานจากคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เป็นต้น ซึ่งแนวคิดการรวมกลุ่มของผู้ใช้จะช่วยลดความซับซ้อนได้ ดังรูปที่ 3.2



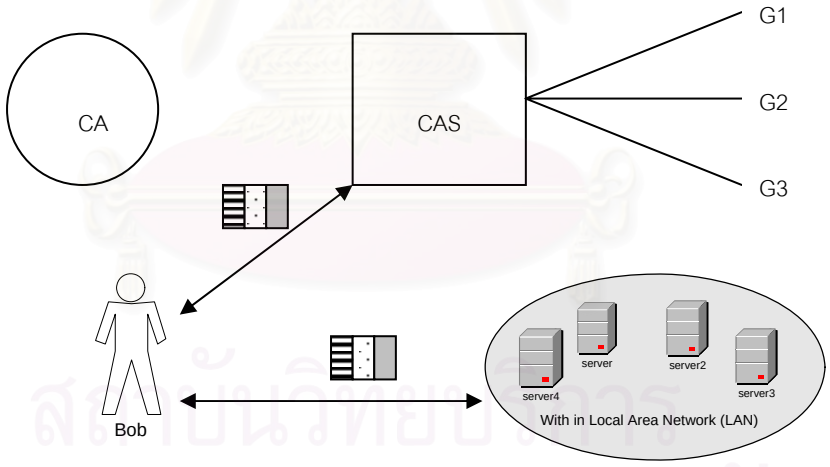
รูปที่ 3.2 รูปแสดงความสัมพันธ์ของสิทธิการเข้าใช้เมื่อใช้แนวคิดการรวมกลุ่มผู้ใช้กับทรัพยากร

การที่จะจัดแบ่งกลุ่มผู้ใช้สำหรับระบบกริดนั้นสามารถทำได้สองวิธีด้วยกันคือ การจัดแบ่งกลุ่มผู้ใช้โดยจำแนกตามผู้ออกหลักฐานอ้างอิงผู้ใช้ และการทำกลุ่มผู้ใช้โดยสร้างเซอร์ฟเวอร์ตัวกลางเพื่อระบุสิทธิของผู้ใช้เช่น ซีเอเอส ตามรูปที่ 3.3 และรูปที่ 3.4 ตามลำดับ



รูปที่ 3.3 แสดงการทำกลุ่มผู้ใช้ซึ่งจำแนกตามผู้ออกหลักฐานอ้างอิงผู้ใช้

จากรูปที่ 3.3 แสดงการทำกลุ่มผู้ใช้โดยจำแนกตามผู้ออกหลักฐานอ้างอิงผู้ใช้ โดยมีแนวคิดดังนี้ คือ ในระบบจะมีผู้ออกหลักฐานอ้างอิงผู้ใช้จำนวนเท่ากับจำนวนของกลุ่มผู้ใช้ในองค์กรเสมือน โดยที่แต่ละผู้ออกหลักฐานอ้างอิงผู้ใช้จะรับผิดชอบในการทำกลุ่มผู้ใช้แต่ละกลุ่มเช่น ผู้ออกหลักฐานอ้างอิงผู้ใช้ของกลุ่มผู้ใช้ซึ่งเป็นอาจารย์ของจุฬา เป็นต้น และทรัพยากรก็จะทำกริดแมปไฟล์สำหรับแต่ละกลุ่มผู้ใช้เพื่อที่จะเปลี่ยนเป็นชื่อผู้ใช้เฉพาะที่บนแต่ละเครื่องทรัพยากร ซึ่งจะมีความสามารถในการขยายตัวของระบบที่ดีเช่นเดียวกันกับการทำกลุ่มผู้ใช้โดยสร้างซีเอเอสเพียงแต่ว่า ถ้าผู้ใช้ในองค์กรเสมือนคนใดมีกลุ่มผู้ใช้อยู่หลายกลุ่มด้วยกัน ผู้ใช้คนนั้นจำเป็นที่จะต้องมีหลักฐานอ้างอิงผู้ใช้อยู่เป็นจำนวนเท่ากับกลุ่มผู้ใช้ที่ตนเองอยู่ แต่วิธีนี้จะก่อให้เกิดปัญหาขึ้นตอนใช้งาน เนื่องจากผู้ใช้จำเป็นที่จะต้องจำให้ได้ว่าหลักฐานอ้างอิงผู้ใช้อันไหนสำหรับกลุ่มผู้ใช้กลุ่มไหน และแนวคิดนี้ไม่รองรับการรวมสิทธิ(union)ระหว่างกลุ่มของผู้ใช้หลายกลุ่มเข้าด้วยกัน กล่าวคือ แนวคิดนี้จะไม่สามารถรองรับการทำงานลักษณะที่ผู้ใช้ต้องการใช้กลุ่มทรัพยากรซึ่งในกลุ่มนั้นต้องการสิทธิการเข้าใช้ซึ่งอยู่ในสองกลุ่มของผู้ใช้ ส่วนข้อดีของแนวคิดนี้ก็คือไม่จำเป็นที่จะต้องสร้างตัวบังคับใช้นโยบายและไม่ต้องแก้ไขซอร์สโคดของแกรม



รูปที่ 3.4 แสดงการทำกลุ่มผู้ใช้โดยการสร้างซีเอเอส

จากรูปที่ 3.4 แสดงการทำกลุ่มผู้ใช้โดยการสร้างซีเอเอส ซึ่งในแนวคิดนี้จะให้ซีเอเอสเป็นผู้ดูแลกลุ่มผู้ใช้ทั้งหมด เมื่อผู้ใช้ต้องการเข้าใช้ทรัพยากรก็จะติดต่อไปยังซีเอเอสเพื่อขอสิทธิทั้งหมดที่ผู้ใช้นั้นมี ซึ่งถ้าผู้ใช้อยู่ในกลุ่มผู้ใช้สามกลุ่มด้วยกัน ซีเอเอสก็จะทำบัตรซึ่งแนบสิทธิของผู้ใช้ในสามกลุ่มทำให้ผู้ใช้สะดวกต่อการใช้งานและการมีซีเอเอสยังสามารถรวมสิทธิ(union)ระหว่างกลุ่มของผู้ใช้หลายกลุ่มเข้าด้วยกันได้ แต่การที่มีซีเอเอสจำเป็นที่จะต้องแก้ไขซอร์สโคดของแกรมเพิ่มเติม

ในปัจจุบันระบบจัดการสิทธิการเข้าใช้ทรัพยากรบนโกลบัสทูลคิดนั้นมีอยู่หลายระบบด้วยกันเช่น วีโอเอ็มเอส ดับบลิวเอเอส พริม่า และ ซีเอเอส เป็นต้น แต่ที่ผู้วิจัยเลือกที่จะพัฒนาต่อจากซีเอเอสเพราะงานวิจัยอื่นนั้นสนับสนุนการทำงานของโกลบัสทูลคิดรุ่น2.x และยังไม่สนับสนุนโกลบัสทูลคิดรุ่น3.x ซึ่งโครงสร้างของโกลบัสทูลคิดรุ่น2.x และ รุ่น3.x นั้นมีความแตกต่างกันค่อนข้างมากเช่นเรื่องภาษาที่ใช้โกลบัสทูลคิดรุ่น 2.x จะใช้ภาษาซี แต่โกลบัสทูลคิดรุ่น3.x จะใช้ภาษาจาวา

3.1 โครงสร้างพื้นฐานขององค์กรเสมือน

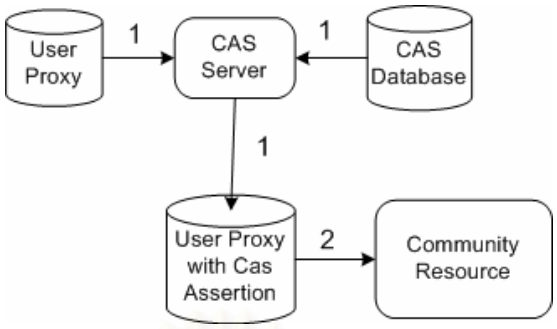
โครงสร้างพื้นฐานขององค์กรเสมือนประกอบด้วย ผู้ใช้ ผู้ให้บริการทรัพยากร ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้ ซึ่งแต่ละองค์ประกอบมีรายละเอียดดังนี้

- ผู้ใช้ (Client) เป็นสมาชิกของผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้ และสามารถเข้าใช้งานผู้ให้บริการทรัพยากรได้ตามสิทธิของผู้ใช้
- ผู้ให้บริการทรัพยากร (Service Provider) จะให้บริการแก่ผู้ใช้ตามที่ผู้ใช้ขอร้อง โดยที่ผู้ใช้และผู้ให้บริการทรัพยากรจะต้องพิสูจน์ตัวจริงซึ่งกันละกันเสียก่อน และผู้ให้บริการทรัพยากรจะทำการพิสูจน์สิทธิของผู้ใช้ว่าสามารถเข้าใช้บริการที่ร้องขอได้หรือไม่
- ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้ (Authorization Service) จะเป็นผู้กำหนดนโยบายการใช้งานต่างๆของผู้ใช้ในองค์กรเสมือน และมีหน้าที่สร้างข้อความอ้างสิทธิการใช้ (Authorization Assertion) ให้แก่ผู้ใช้ตามคำขอ

3.2 วิเคราะห์ระบบจัดการสิทธิซีเอเอส

3.2.1 ภาพรวมการใช้งานของระบบจัดการสิทธิซีเอเอส

แนวคิดของซีเอเอสจะเน้นการสร้างกลุ่มของผู้ใช้ซึ่งสอดคล้องกับแนวทางของงานวิจัยนี้ คือ สร้างเซอร์ฟเวอร์สำหรับดูแลสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ในกลุ่มของผู้ใช้เองและให้ผู้ครอบครองทรัพยากรกำหนดสิทธิการเข้าใช้ของกลุ่มคนแทนการกำหนดสิทธิการเข้าใช้เป็นรายบุคคล



รูปที่ 3.5 แสดงหลักการทำงานของซีเอเอส

จากรูปที่ 3.5 เราสามารถมองการทำงานของซีเอเอสออกได้เป็นสองขั้นตอนคือ

1. ผู้ใช้จะต้องติดต่อไปยังเซอร์ฟเวอร์ที่เก็บสิทธิการใช้งานทรัพยากรและทำการพิสูจน์ตัวจริง หลังจากนั้นเซอร์ฟเวอร์จะค้นหาสิทธิการเข้าใช้ทรัพยากรจากฐานข้อมูล พร้อมทั้งสร้างสิ่งที่อ้างสิทธิการใช้ (Authorization Assertion) พร้อมทั้งสร้างลายเซ็นดิจิตอลกำกับไว้
2. เมื่อผู้ใช้งานต้องการใช้งานทรัพยากรใดๆก็จะนำสิ่งที่อ้างสิทธิไปให้ทรัพยากร พร้อมทั้งยืนยันตัวบุคคลว่าเป็นบุคคลในสิ่งที่อ้างสิทธิจริง เพื่อที่จะสามารถใช้งานทรัพยากรนี้ได้ และทางทรัพยากรเองก็จะนำชื่อเฉพาะของผู้ใช้และชื่อเฉพาะของผู้ออกสิ่งที่อ้างสิทธิไปเปรียบเทียบกับสิทธิที่มีต่อทรัพยากรเอง พร้อมทำการอินเทอเซกชันเพื่อให้ได้สิทธิที่ใช้ได้จริงต่อไป

3.2.2 ข้อจำกัดของระบบจัดการสิทธิซีเอเอส

จากการศึกษาของผู้วิจัยพบว่าระบบจัดการสิทธิซีเอเอสพี่มาพร้อมกับโกลบัสทูลคิดรุ่น 3.2.1 มีข้อจำกัดดังนี้

- ระบบจัดการสิทธิซีเอเอสสนับสนุนการทำงานของโกลบัสทูลคิดรุ่น3.2.1 ในส่วนของกริดเอฟทีพีเท่านั้นและยังไม่สนับสนุนส่วนอื่นๆของโกลบัสทูลคิดเช่นแกรม
- ระบบจัดการสิทธิซีเอเอสเหมาะกับสภาพแวดล้อมที่มีผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้เพียงตัวเดียวภายในองค์กรเสมือน กล่าวคือไม่สามารถติดต่อกับผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้ขององค์กรเสมือนอื่นได้

3.3 การออกแบบระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับโกลบัสทูลคิดรุ่น 3.2 สำหรับองค์กรเสมือนที่มีซีเอเอสเพียงเครื่องเดียว

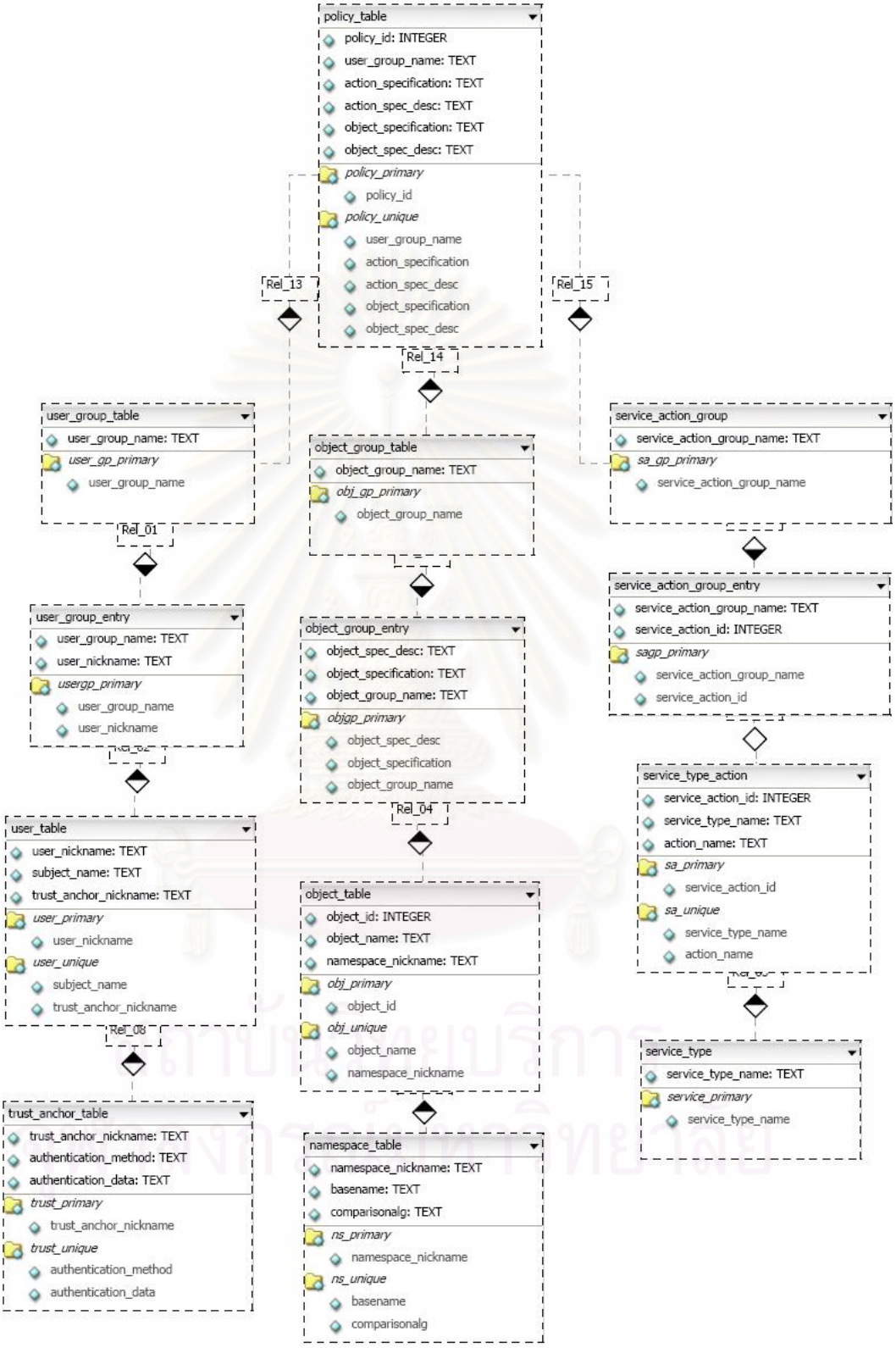
จากการศึกษาระบบจัดการสิทธิซีเอเอส ได้พบสาเหตุที่ทำให้ซีเอเอสไม่สนับสนุนการทำงานร่วมกันกับบริการอื่นๆในโกลบัสทูลคิดรุ่น 3.2.1 นอกเหนือจากกริดเอฟทีพี ดังนี้

- ฐานข้อมูลนโยบายการเข้าใช้ของซีเอเอสจะพบว่า มีตารางอยู่หลายตารางที่ยังขาดเขตข้อมูล (fields) ที่จะนำมาสร้างนโยบายการเข้าใช้บริการอื่น
- ส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิที่ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้เป็นผู้ออกมาให้และพิจารณาสิทธิของผู้ใช้บนทรัพยากรใดๆ
- ส่วนบังคับใช้นโยบายที่อยู่ในสิ่งที่อ้างสิทธิของผู้ใช้

ผู้วิจัยจึงได้ออกแบบองค์ประกอบต่างๆขึ้นมาเพิ่มเติมเพื่อให้ซีเอเอสสามารถทำงานร่วมกับบริการแกรมของโกลบัสทูลคิดได้ดังนี้

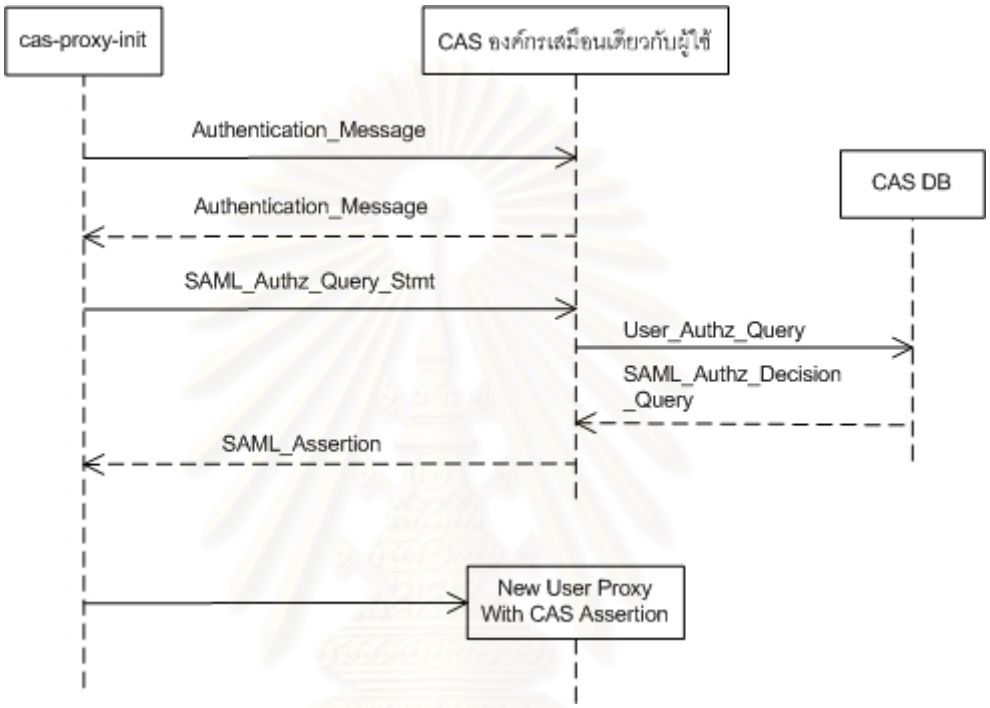
3.3.1 ข้อมูลเพิ่มเติมของฐานข้อมูลนโยบายเพื่อสร้างนโยบายการเข้าใช้บริการแกรม

ฐานข้อมูลนโยบายของระบบจัดการสิทธิซีเอเอสประกอบไปด้วยตารางทั้งหมด 13 ตาราง ได้แก่ NameSpace table, Trust Archer table, user table, user group table, user group entry table, object table, object group table, object group entry table, service type table, service type action table, service action group table และ service action group entry table ซึ่งมีความสัมพันธ์กันดังรูปที่3.6



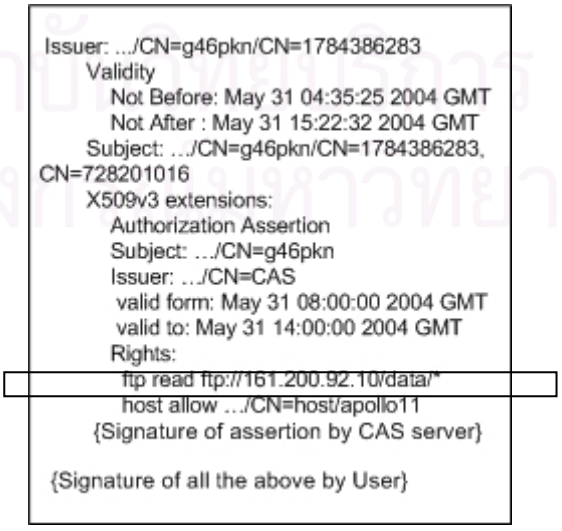
รูปที่ 3.6 แผนภาพฐานข้อมูลเชิงสัมพันธ์ของระบบจัดการสิทธิซีเอเอส

เมื่อสำรวจดูฐานข้อมูลเดิมของซีเอเอสพบว่า ฐานข้อมูลซีเอเอสมีเขตข้อมูลไม่เพียงพอต่อการสร้างนโยบายการเข้าใช้บริการแกรมซึ่งสามารถอ่านได้จากภาคผนวก ก หลังจากทำการเพิ่มเติมนโยบายการเข้าใช้บริการแกรมแล้วผู้ใช้สามารถส่งข้อความขอเข้าใช้ทรัพยากรในองค์กรเสมือนได้โดยใช้คำสั่ง cas-proxy-init ซึ่งมีแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 3.7



รูปที่ 3.7 แสดงแผนภาพลำดับการขอสิทธิการใช้งานจากซีเอเอสเซอร์ฟเวอร์

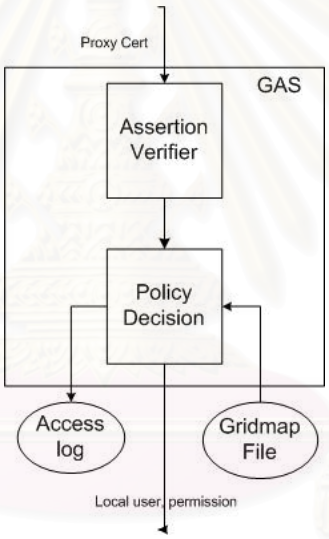
สำหรับสิ่งอ้างสิทธิการเข้าใช้ทรัพยากรซึ่งแนบไว้ในส่วนขยายของสิ่งอ้างอิงผู้ใช้หลังทำการเพิ่มนโยบายการใช้บริการแกรมในฐานข้อมูลซีเอเอสจะมีลักษณะดังรูปที่ 3.8



รูปที่ 3.8 แสดงหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนหลังทำการเพิ่มเติมเพื่อให้ทำงานร่วมกับแกรมได้

3.3.2 ทำการสร้างส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิที่ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้เป็นผู้ออกมาให้และพิจารณาสิทธิของผู้ใช้บนทรัพยากรใดๆ

จาก 3.3.1 เมื่อผู้ใช้ขอสิทธิการเข้าใช้ทรัพยากรกับผู้ให้บริการข้อมูลสำหรับระบุสิทธิแล้วจะได้สิ่งที่อ้างสิทธิแนบไว้ในหลักฐานอ้างอิงตัวผู้ใช้ตัวแทน เมื่อผู้ใช้ต้องการใช้งานทรัพยากรใดจะต้องยื่นหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนแก่ทรัพยากรนั้น แต่เนื่องด้วยว่าทรัพยากรในกริดยังไม่สามารถพิจารณาและบังคับใช้นโยบายที่อยู่ในสิ่งที่อ้างสิทธิที่ผู้ใช้ยื่นมาได้ จึงจำเป็นที่จะต้องออกแบบส่วนประกอบสำหรับตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิและพิจารณาสิทธิของผู้ใช้ขึ้นมาเป็นบริการ (จีเอเอส , GAS – Grid Authorization Service) โดยแบ่งออกเป็นส่วนประกอบย่อย 2 ส่วนด้วยกัน คือ ส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิ (Assertion Verifier) และส่วนพิจารณาสิทธิของผู้ใช้จากสิ่งที่อ้างสิทธิ (Policy Decision) ดังรูปที่ 3.9



รูปที่ 3.9 แสดงหลักการทำงานของจีเอเอส

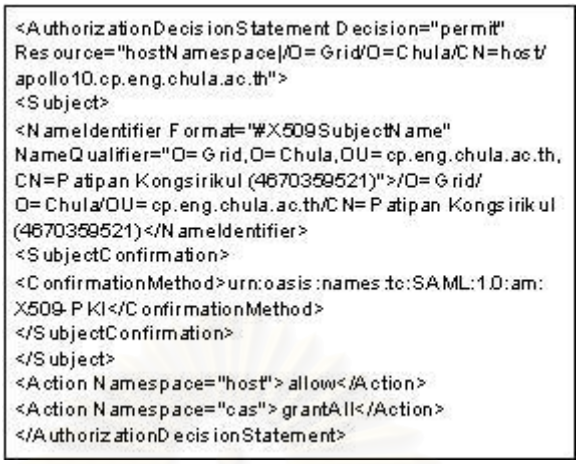
จากรูปที่ 3.9 อธิบายการทำงานของบริการสำหรับตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิและพิจารณาสิทธิของผู้ใช้โดยแบ่งเป็น 2 ขั้นตอนดังนี้

- ส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิจะรับหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนที่แนบสิ่งอ้างสิทธิ มาทำการพิสูจน์ความถูกต้องของสิ่งหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนและสิ่งที่อ้างสิทธิโดยจะต้องพิจารณา 4 อย่างด้วยกันได้แก่
  - ความน่าเชื่อถือของหลักฐานอ้างอิงผู้ใช้ โดยจะตรวจสอบว่าทรัพยากรมีความเชื่อถือกับผู้ออกหลักฐานอ้างอิงผู้ใช้ตัวแทนหรือไม่ ถ้าทรัพยากรไม่มีความเชื่อถือผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ ก็จะพิจารณาผู้ที่ออกหลักฐานอ้างอิงของผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ และทำไปเรื่อยจนกว่าผู้ที่ออกหลักฐานอ้างอิงผู้ใช้นั้นมีความ

เชื่อถือกันทำให้เกิดลูกโซ่ของความเชื่อถือ(Trust chain) การตรวจสอบว่าทรัพยากรมีความเชื่อถือกับผู้ออกหลังฐานอ้างอิงผู้ใช้สามารถทำได้ โดยพิจารณาว่าผู้ออกหลักฐานอ้างอิงผู้ใช้นั้นมีหลักฐานอ้างอิงตนเองอยู่ใน /etc/grid-security/certificates/ หรือไม่ ในกรณีที่ทรัพยากรไม่มีความเชื่อถือผู้ออกหลักฐานอ้างอิงผู้ใช้ ก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้ไปยังผู้เรียกส่วนตรวจสอบนี้

- หลักฐานอ้างอิงผู้ใช้ตัวแทนไม่ได้ถูกแก้ไข ซึ่งสามารถตรวจสอบได้โดยนำหลักฐานอ้างอิงผู้ใช้ตัวแทนไปทำเมสเซจไดเจส แล้วนำไปเทียบกับลายเซ็นดิจิตอลที่ถอดรหัสโดยกุญแจสาธารณะของผู้ออกหลักฐานอ้างอิงผู้ใช้ตัวแทน ถ้าผลการเปรียบเทียบพบว่าข้อความทั้งสองมีลักษณะตรงกันแสดงว่าหลักฐานอ้างอิงผู้ใช้ตัวแทนอันนี้ไม่ได้ถูกแก้ไขสามารถนำมาพิสูจน์ตัวจริงของผู้ใช้ได้ แต่ถ้าพบว่าข้อความทั้งสองไม่ตรงกันก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้ไปยังผู้เรียกส่วนตรวจสอบนี้
- ความน่าเชื่อถือของผู้ออกสิ่งอ้างสิทธิ โดยจะตรวจสอบหาลูกโซ่ของความเชื่อถือของผู้ออกสิ่งอ้างสิทธิ ซึ่งจะคล้ายการตรวจสอบความเชื่อถือของหลักฐานอ้างอิงผู้ใช้ ถ้าพบว่าลูกโซ่ของความเชื่อถือของผู้ออกสิ่งอ้างสิทธิไม่มีความเชื่อถือกับทรัพยากรก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว
- สิ่งอ้างสิทธิไม่ได้ถูกแก้ไข ซึ่งสามารถตรวจสอบได้โดยนำสิ่งอ้างสิทธิไปทำเมสเซจไดเจส แล้วนำไปเทียบกับลายเซ็นดิจิตอลที่ถอดรหัสโดยกุญแจสาธารณะของผู้ออกสิ่งที่อ้างสิทธิถ้าผลการเปรียบเทียบพบว่าข้อความทั้งสองมีลักษณะตรงกันแสดงว่าสิ่งอ้างสิทธิไม่ได้ถูกแก้ไขสามารถนำมาพิจารณาสิทธิการเข้าใช้ได้ แต่ถ้าพบว่าข้อความทั้งสองไม่ตรงกันก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว

หลังจากตรวจสอบแล้วจึงส่งสิ่งอ้างสิทธิไปยังส่วนพิจารณาสิทธิของผู้ใช้ ซึ่งสิ่งอ้างสิทธิแสดงอยู่ในรูปที่ 3.10 แต่ถ้าพิจารณาแล้วพบว่าหลักฐานอ้างอิงผู้ใช้ไม่มีสิ่งอ้างสิทธิแนบก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว

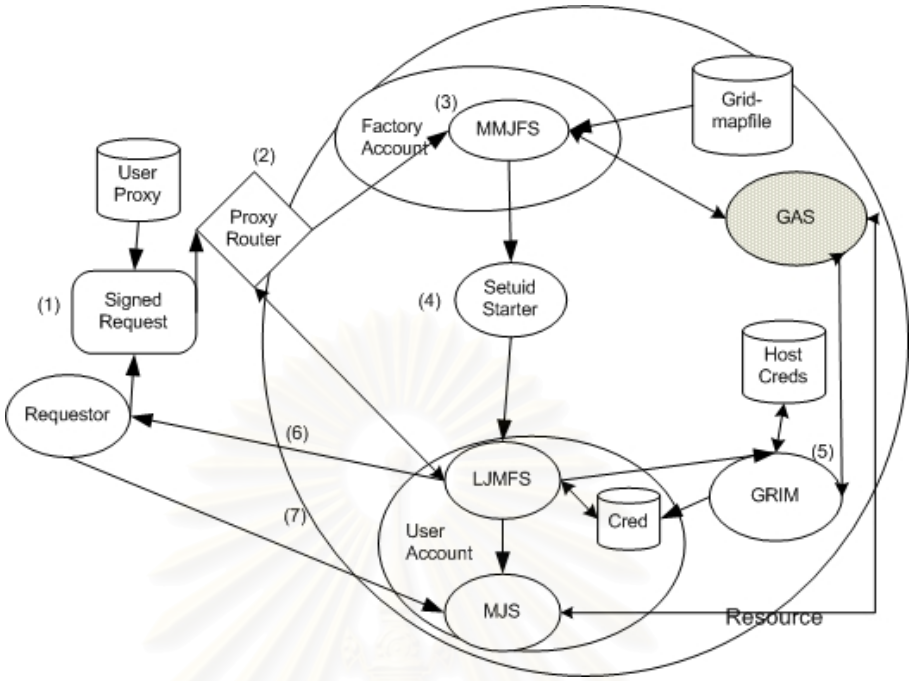


รูปที่ 3.10 แสดงเนื้อหาส่วนหนึ่งของสิ่งที่อ้างสิทธิการใช้ทรัพยากรโดยเขียนอยู่ในรูปแบบของเอสเอเอ็มแอล

- ส่วนจัดการนโยบายจะทำการอ่านสิ่งอ้างสิทธิแบบเอสเอเอ็มแอล โดยพิจารณาจาก AuthorizationDecisionStatement ในส่วนที่ตรงกับทรัพยากร ที่ผู้ใช้ต้องการเข้าใช้เพื่อดูสิทธิการเข้าใช้ ถ้าเป็น deny จะส่งข้อความไม่อนุญาตเข้าใช้ไปยังส่วนที่เรียกบริการนี้เพื่อที่จะทำงานต่อโดยไม่สนใจสิ่งที่อ้างสิทธิเหมือนทำงานปกติ แต่ถ้าเป็น allow จะต้องทำการหาชื่อผู้ใช้เฉพาะที่โดยทำการจับคู่ระหว่างชื่อเฉพาะของผู้ออกสิ่งอ้างอิงสิทธิกับชื่อผู้ใช้เฉพาะที่ที่ทำการเก็บไว้ใน กริดแมปไฟล์หลังจากได้ชื่อผู้ใช้เฉพาะที่แล้วจะทำการเก็บข้อมูลการเข้าใช้ซึ่งประกอบไปด้วย ชื่อเฉพาะของผู้ใช้ ชื่อเฉพาะของผู้ออกสิ่งอ้างอิงสิทธิ ชื่อผู้ใช้เฉพาะที่บนทรัพยากร และเวลาในการเข้าใช้ทรัพยากรไว้ในบันทึกการเข้าใช้ทรัพยากรพร้อมทั้งทำการคืนชื่อผู้ใช้เฉพาะที่ไปยังผู้เรียกบริการนี้

3.3.3 ทำการแก้ไขแกรมของโกลบัสทูลคิดรุ่น3.2.1 ให้เข้าใจรูปแบบสิ่งที่อ้างสิทธิการใช้ทรัพยากรจากซีเอเอสซึ่งแนบมากับหลักฐานอ้างอิงผู้ใช้

ในส่วนนี้จะเป็นการแก้ไขให้ทรัพยากรหรือแกรมสามารถตรวจสอบและพิจารณาสิ่งอ้างสิทธิจากซีเอเอสได้โดยการเรียกบริการสำหรับตรวจสอบและพิจารณาสิทธิหรือจีเอเอสใน 3.3.2 ดังนี้



รูปที่ 3.11 แสดงการทำงานของจีเอเอสร่วมกับส่วนประกอบอื่นๆของแกรมโกลบัสทูลคิด 3.x

จากรูปที่ 3.11 สามารถอธิบายการทำงานได้ดังนี้

1. เมื่อผู้ใช้ต้องการใช้แกรมจะส่งข้อความขอใช้แกรมโดยข้อความจะเข้ารหัสโดยกุญแจส่วนบุคคลของผู้ใช้ไปยังบริการจัดเส้นทางแทน (Proxy Router)
2. บริการจัดเส้นทางแทนจะทำการตรวจสอบว่าผู้ใช้ได้เคยทำการขอใช้มาก่อนหน้านี้หรือไม่ ถ้าพบว่ามีการขอใช้มาก่อนจะส่งข้อความขอใช้ทรัพยากรไปยังแอลเอ็มเจเอฟเอส (LMJFS – Local Managed Job Factory Service) เลยเพราะผู้ใช้ได้ทำการพิสูจน์ตัวจริงกับทรัพยากรและบนทรัพยากรก็ได้มีการสร้างสภาพแวดล้อมของผู้ใช้บนเครื่องทรัพยากร (UHE - User Host Environment) แล้ว แต่ถ้าไม่พบการขอใช้มาก่อนจะส่งข้อความขอใช้ไปยังเอ็มเอ็มเจเอฟเอส (MMJFS – Master Managed Job Factory Service)
3. เอ็มเอ็มเจเอฟเอสทำการค้นหาชื่อผู้ใช้เฉพาะที่จากกริดแมปไฟล์ซึ่งส่วนนี้เอ็มเอ็มเจเอฟเอสจะทำการเรียกใช้จีเอเอสเพื่ออ่านสิ่งอ้างสิทธิซึ่งซีเอเอสเป็นผู้ออกให้ซึ่งจะได้ผลลัพธ์เป็นชื่อเฉพาะที่ของผู้ใช้บนทรัพยากรนั้นและสิทธิการเข้าใช้ถ้าสิทธิถ้าสิทธิเป็น allow ก็จะเรียกสร้างแอลเอ็มเจเอฟเอสแต่ถ้าใน หลักฐานอ้างอิงผู้ใช้ตัวแทนไม่มีสิ่งอ้างอิงสิทธิหรือในสิทธิในสิ่งอ้างอิงสิทธิเป็น deny เอ็มเอ็มเจเอฟเอสจะพิจารณาจากหลักฐานอ้างอิงผู้ใช้ตัวแทนโดยตรงโดยจะไม่สนใจสิ่งอ้างอิงสิทธิของซีเอเอสและการทำงานของจีเอเอสอีกต่อไปจนกว่าจะสิ้นสุดการทำงาน

4. แอลเอ็มเจเอฟเอสจะถูกสร้างผ่านส่วน setuid เพื่อทำให้แอลเอ็มเจเอฟเอสถูกสร้างโดยผู้ใช้เฉพาะที่ ที่แมปจากชื่อเฉพาะของผู้ใช้ หรือชื่อเฉพาะของผู้ออกสิ่งอ้างสิทธิ ไม่ใช่เป็นการสร้างโดยผู้ใช้เฉพาะที่ที่เป็นคนรันโกลบัสคอนเทนเนอร์ (globus container)
5. แอลเอ็มเจเอฟเอสจะส่งข้อความไปลงทะเบียนกับบริการจัดเส้นทางแทนเพื่อว่าครั้งต่อไปผู้ใช้สามารถมายังแอลเอ็มเจเอฟเอสของตนเองได้เลยไม่ต้องผ่านเอ็มเอ็มเจเอฟเอส หลังจากนั้นแอลเอ็มเจเอฟเอสจะเรียกกริม (GRIM – Grid Resource Identity Mapper) เพื่อทำการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทนของแอลเอ็มเจเอฟเอส ซึ่งจะประกอบไปด้วยชื่อเฉพาะ และชื่อผู้ใช้เฉพาะที่ ซึ่งตรงจุดนี้กริมจะทำการเรียกจีเอเอสเพื่อรับชื่อเฉพาะของซีเอเอสผู้ที่ออกสิ่งอ้างอิงสิทธิให้ในกรณีที่มีสิ่งอ้างอิงสิทธิในสิ่งอ้างอิงผู้ใช้ตัวแทนเพื่อดูว่าผู้ใช้มีสิทธิเข้าใช้ทรัพยากรนี้หรือไม่ (สิทธินี้คือสิทธิที่เจ้าของทรัพยากรมีต่อผู้ใช้ หรือซีเอเอสผู้ออกสิ่งอ้างอิงสิทธิของผู้ใช้)
6. หลังจากนั้น แอลเอ็มเจเอฟเอสจึงทำการสร้างเอ็มเจเอฟ และ แอลเอ็มเจเอฟเอส แล้วได้ส่งข้อความไปยังผู้ใช้ ว่าผู้ใช้จึงสามารถรันงานได้โดยเอ็มเจเอฟ (MJS – Managed Job Service) จะเป็นผู้ดูแลงานให้
7. ผู้ใช้รันงานผ่านเอ็มเจเอฟ

บทที่ 4

การออกแบบและพัฒนาระบบจัดการสิทธิการเข้าใช้ทรัพยากรบนสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือน

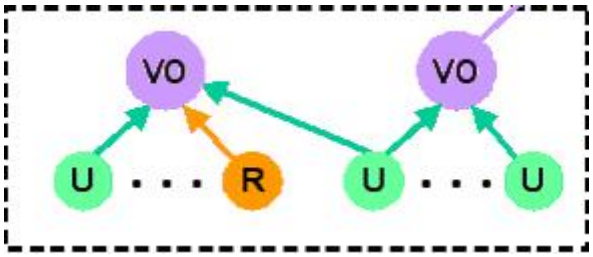
เมื่อมีความเชื่อมต่อองค์กรเสมือนตั้งแต่ 2 องค์กรเสมือนขึ้นไปเข้าด้วยกันแล้ว ระบบจัดการสิทธิการเข้าใช้แบบกลุ่มที่ได้ออกแบบและพัฒนาในบทที่ 3 ซึ่งใช้ซีเอเอสเซอร์ฟเวอร์เพียงเครื่องเดียวในการดูแลนโยบายการเข้าใช้งาน จะพบข้อจำกัดของระบบดังนี้

- ปัญหาการหาเครื่องเซอร์ฟเวอร์ตัวกลางที่แต่ละองค์กรในองค์กรเสมือนเชื่อถือร่วมกันเป็นเรื่องที่ทำได้ยาก
- ปัญหาการจัดทำสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ของแต่ละองค์กรเสมือนใหม่ให้สอดคล้องกับ ทรัพยากรที่เพิ่มเข้ามา
- ปัญหาเมื่อซีเอเอสเซอร์ฟเวอร์ล่มจะทำให้ผู้ใช้งานในองค์กรเสมือนอื่นจะไม่สามารถทำงานได้แม้จะต้องการทำงานภายในองค์กรเสมือนของตนเอง

ซึ่งปัญหาที่ได้กล่าวมาข้างต้นผู้วิจัยพบว่าสามารถแก้ไขได้ โดยให้แต่ละองค์กรเสมือนมีซีเอเอสเซอร์ฟเวอร์ของตนเองและผู้ใช้แต่ละองค์กรเสมือนสามารถใช้งานทรัพยากรในอีกองค์กรเสมือนได้ โดยติดต่อผ่านซีเอเอสเซอร์ฟเวอร์ขององค์กร์เสมือนนั้นคือ เมื่อซีเอเอสของอีกองค์กรเสมือนล่มผู้ใช้ก็ยังสามารถทำงานภายในองค์กรเสมือนตนเองได้ และตัดปัญหาเรื่องหาตัวแทนที่เชื่อถือทั้งสองฝ่าย

การเชื่อมต่อหรือรวมองค์กรเสมือนนั้นผู้วิจัยเห็นตรงกับโอเพ่นไซน์กริดที่ว่าโครงสร้างขององค์กรเสมือนมักจะต้องเป็นลำดับขั้น (Hierarchy VOs) โดยองค์กรเสมือนที่เป็นบัพลูก (Child node) จะต้องมีนโยบายที่สอดคล้องกับบัพแม่ (Parent node) แต่ถ้าองค์กรเสมือนใดมีนโยบายไม่สอดคล้องกับ องค์กรเสมือนใดเลยก้อจะแยกออกไปเป็นบัพอิสระ (Independent node)

โดยในงานวิจัยนี้จะมองการเชื่อมต่อและโครงสร้างขององค์กรเสมือนเป็นแบบไม่มีลำดับขั้น (non hierarchy VOs) เพื่อเป็นจุดเริ่มต้นของโครงสร้างการทำงานข้ามองค์กรเสมือนดังรูปที่ 4.1

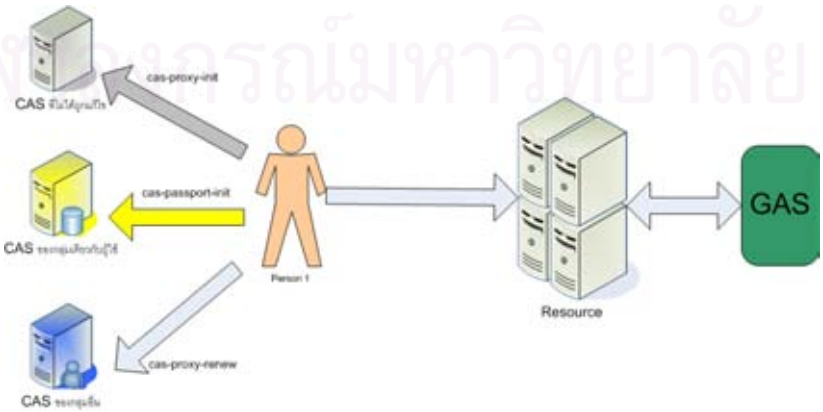


รูปที่ 4.1 แสดงโครงความสัมพันธ์ขององค์กรเสมือน 2 องค์กรเสมือน ที่ใช้เป็นต้นแบบในการพัฒนาระบบจัดการสิทธิในงานวิจัยนี้

4.1 ภาพรวมของระบบ

ภาพรวมการใช้ระบบของผู้ใช้ระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับโกลบัสทูลคิด รุ่น 3.2 บนสภาพแวดล้อมที่มีองค์กรเสมือนมากกว่า 1 องค์กรเสมือนแบ่งได้เป็นสองส่วน คล้ายคลึงกับระบบจัดการสิทธิซีเอเอส ได้แก่

1. ส่วนที่ทำหน้าที่สร้างหลักฐานอ้างอิงผู้ใช้ตัวแทน สำหรับพิสูจน์ตัวจริงในองค์กรเสมือนหรือระหว่างองค์กรเสมือน ซึ่งในส่วนแรกนี้ผู้วิจัยได้ออกแบบในสองแนวทางคือ แนวคิดการทำหลักฐานอ้างอิงผู้ใช้ตัวแทนและสิ่งอ้างสิทธิแบบหนังสือเดินทาง (Passport concept) ผู้ใช้สามารถเรียกใช้โดยคำสั่ง cas-passport-init และแนวคิดการทำหลักฐานอ้างอิงผู้ใช้ตัวแทนและสิ่งอ้างสิทธิแบบเปลี่ยนบัตร ผู้ใช้สามารถเรียกใช้โดยคำสั่ง cas-proxy-renew
2. ส่วนตรวจสอบพิจารณาสิทธิและบังคับใช้นโยบายที่แนบมากับสิ่งอ้างอิงผู้ใช้ตัวแทน โดยแก้ไขจากส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิที่ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้เป็นผู้ออกมาให้และพิจารณาสิทธิของผู้ใช้บนทรัพยากรใดๆในบทที่ 3 ซึ่งจะได้ภาพรวมการใช้งานของระบบดังรูปที่ 4.2

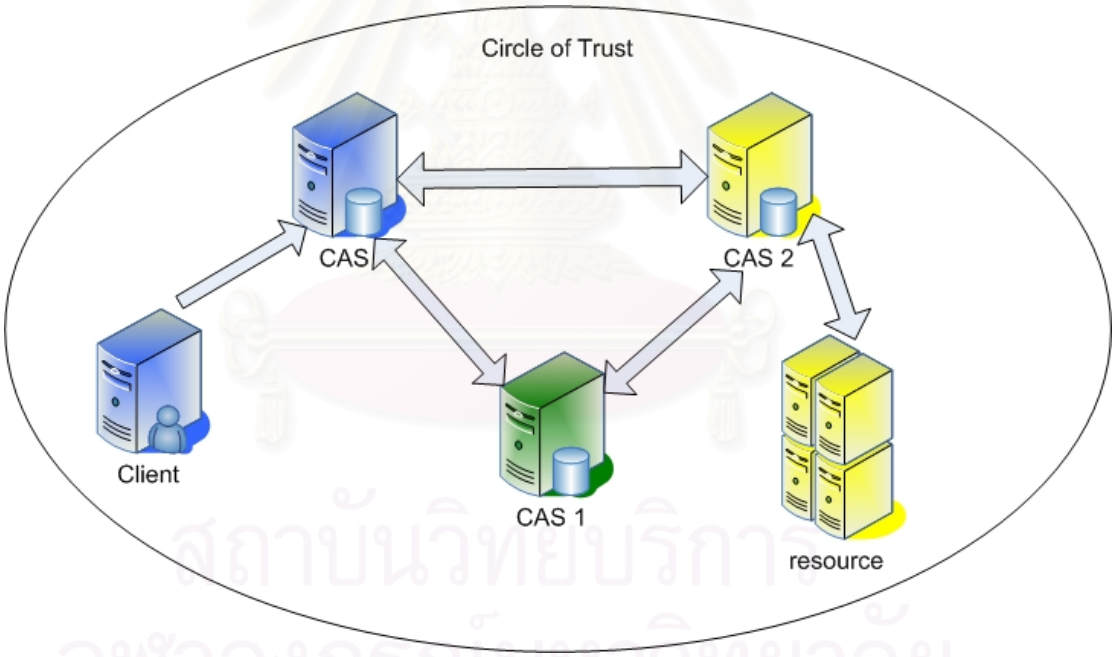


รูปที่ 4.2 แสดงภาพรวมการทำงานของผู้ใช้

ผู้วิจัยมองการเชื่อมต่อขององค์กรเสมือน 2 องค์กรเสมือนเข้าด้วยกันใน 2 ลักษณะได้แก่ ลักษณะที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง และลักษณะที่องค์กรเสมือนทั้งสองไม่ได้เชื่อถือกันโดยตรงแต่เชื่อตัวแทนตัวเดียวกัน ซึ่งจะกล่าวรายละเอียดใน 4.2 และ 4.3 ตามลำดับ

4.2 การออกแบบระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับโกลบัสทูลคิดรุ่น 3.2 บนสภาพแวดล้อมของการเชื่อมต่อกันขององค์กรเสมือนที่เชื่อถือกันโดยตรง

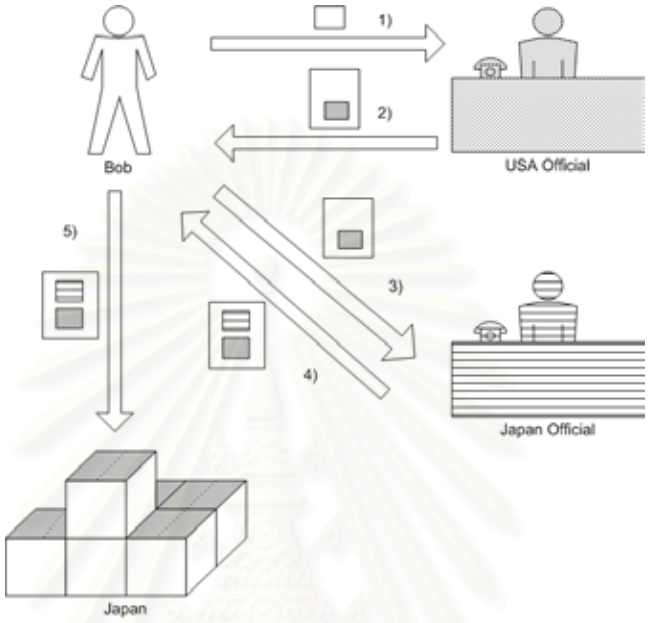
ในองค์กรเสมือนโดยทั่วไป เอนทิตีต่างๆจะต้องมีหลักฐานอ้างอิงของตนเองเพื่อนำมาใช้พิสูจน์ตัวจริงซึ่งกันและกัน สำหรับการเชื่อมต่อองค์กรเสมือนใดๆเข้าด้วยกันโดยให้มีความเชื่อถือกันโดยตรงนั้น สามารถทำได้โดยทำให้ทุกๆทรัพยากรในอีกองค์กรเสมือน B เชื่อถือกับผู้ออกหลักฐานอ้างอิงตนเองของทุกเอนทิตีในองค์กรเสมือน A และทำให้ทุกๆทรัพยากรในอีกองค์กรเสมือน A เชื่อถือกับผู้ออกหลักฐานอ้างอิงตนเองของทุกเอนทิตีในองค์กรเสมือน B ซึ่งจะได้สภาพแวดล้อมดังรูปที่ 4.3



รูปที่ 4.3 แสดงสภาพแวดล้อมหลังเชื่อมต่อองค์กรเสมือนให้เชื่อถือกันโดยตรง

ในสภาพแวดล้อมที่องค์กรเสมือนทั้งสองต่างเชื่อถือผู้ออกหลักฐานอ้างอิงตนเองของทุกเอนทิตีในทั้ง 2 องค์กรเสมือน ระบบสามารถนำหลักฐานอ้างอิงผู้ใช้ตัวแทนของในองค์กรเสมือนหนึ่งไปพิสูจน์ตัวบุคคลในอีกองค์กรเสมือนหนึ่งได้โดยไม่ต้องแก้ไข แต่ในขณะที่อีกองค์กรเสมือนยังไม่มีสิทธิการเข้าใช้ของผู้ใช้ในอีกองค์กรเสมือนหนึ่ง ดังนั้นผู้วิจัยจำเป็นที่จะต้องออกแบบระบบจัดการสิทธิสำหรับการเชื่อมต่อองค์กรเสมือนเข้าด้วยกัน โดยมีแนวคิดที่ให้แต่ละองค์กรเสมือน

จัดการสิทธิการเข้าใช้ทรัพยากรของตนเองและจัดการสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ในอีกองค์กรเสมือนโดยมองว่าผู้ใช้ในอีกองค์กรเสมือนนั้นมีสิทธิเท่ากันทุกคน ซึ่งการใช้งานของผู้ใช้ในอีกองค์กรเสมือนสามารถอธิบายได้รูปที่ 4.4



รูปที่ 4.4 แสดงภาพรวมการใช้งานของทรัพยากรในองค์กรเสมือนอื่นตามแนวคิดการทำหนังสือเดินทาง

☐ คือหลักฐานอ้างอิงผู้ใช้ตัวแทนของผู้ใช้ Bob ซึ่งอยู่ภายในองค์กรเสมือน USA

▒ คือสิ่งอ้างสิทธิที่สร้างโดยเจ้าหน้าที่ขององค์กรเสมือน USA ซึ่งในสิ่งอ้างสิทธิจะมีสิทธิที่ผู้ใช้ได้รับจากเจ้าหน้าที่ขององค์กรเสมือน USAให้สามารถติดต่อเพื่อขอสิทธิในองค์กรเสมือน Japan ได้

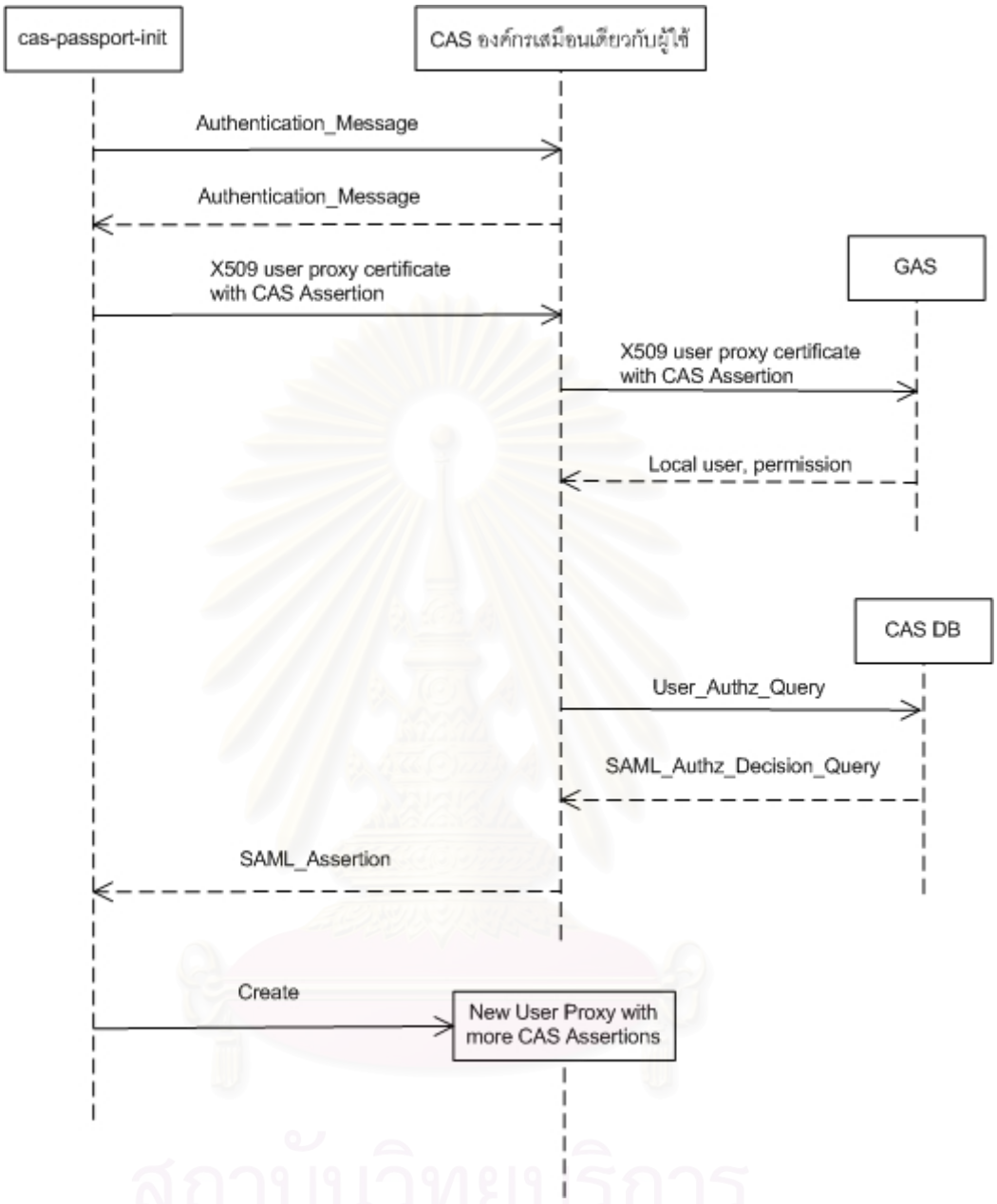
☐ คือสิ่งอ้างสิทธิที่สร้างโดยเจ้าหน้าที่ขององค์กรเสมือน Japan เพื่ออนุญาตให้ผู้ใช้สามารถเข้าไปใช้ทรัพยากรในองค์กรเสมือน Japan ได้เท่าที่สิทธิในสิ่งอ้างสิทธิกำหนดไว้

จากภาพที่ 4.4 แสดงภาพการใช้งานของทรัพยากรในองค์กรเสมือนอื่นตามแนวคิดการทำหนังสือเดินทาง โดยสมมติเหตุการณ์ว่า Bob เป็นผู้ใช้ในองค์กรเสมือน USA โดยที่ทุกเอนทิตีในองค์กรเสมือนUSA และองค์กรเสมือน Japan มีความเชื่อถือกันทั้งหมด และ Bob มีความต้องการไปใช้ทรัพยากรในองค์กรเสมือน Japan ซึ่งผู้ใช้ Bob จะต้องทำตามขั้นตอน 5 ขั้นดังนี้

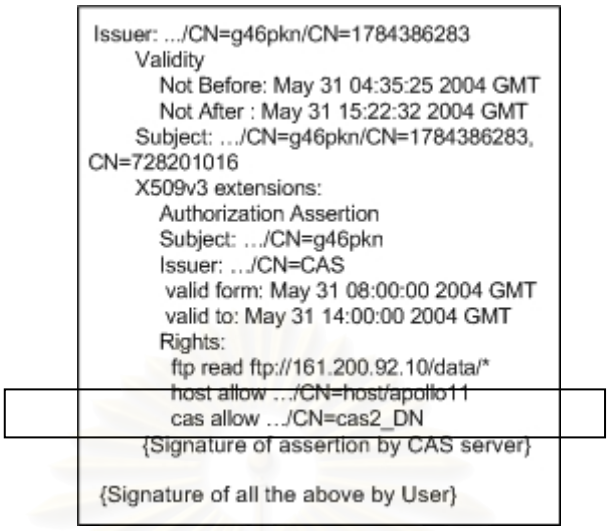
1. Bob ซึ่งเป็นผู้ใช้ในองค์กรเสมือน USA จะต้องติดต่อไปยังเจ้าหน้าที่ผู้ดูแลขององค์กรเสมือนของตนเองโดยนำหลักฐานอ้างอิงผู้ใช้ไปพิสูจน์ว่าตนเองชื่อ Bob จริงและเป็นผู้ใช้ในองค์กรเสมือน USA จริง

2. เมื่อเจ้าหน้าที่ผู้ดูแลขององค์กรเสมือน USA ตรวจสอบหลักฐานอ้างอิงผู้ใช้ของ Bob และพิสูจน์ได้ว่าเป็นสมาชิกขององค์กรเสมือน USA จริง จึงออกสิ่งอ้างอิงสิทธิที่มีสิทธิยินยอมให้ Bob สามารถไปติดต่อกับเจ้าหน้าที่ขององค์กรเสมือน Japan ได้
3. Bob นำหลักฐานอ้างอิงของตนเองที่แนบสิ่งอ้างสิทธิที่เจ้าหน้าที่ขององค์กรเสมือน USA ออกให้ไปยื่นต่อเจ้าหน้าที่ขององค์กรเสมือน Japan
4. เจ้าหน้าที่ขององค์กรเสมือน Japan จะตรวจสอบหลักฐานอ้างอิงผู้ใช้ Bob และสิ่งอ้างสิทธิที่แนบมาด้วยว่า Bob เป็นผู้ใช้ในองค์กรเสมือนของ USA จริงและเจ้าหน้าที่ขององค์กรเสมือน USA ยินยอมให้ Bob มาติดต่อกับเจ้าหน้าที่ขององค์กรเสมือน Japan ได้ และพิจารณาด้วยว่าทางองค์กรเสมือนของ Japan ยินยอมให้ผู้ใช้จากองค์กรเสมือน USA เข้ามาใช้ทรัพยากรหรือไม่ และจะได้สิทธิการเข้าใช้ทรัพยากรขององค์กรเสมือน Japan แค่ไหนบ้าง พร้อมทั้งออกสิ่งอ้างสิทธิอันใหม่ที่มีรายละเอียดสิทธิการเข้าใช้ทรัพยากรของนาย Bob ซึ่งเป็นสมาชิกขององค์กรเสมือน USA ที่มีต่อทรัพยากรในองค์กรเสมือนของ Japan พร้อมทั้งทำลายเซ็นดิจิตอลกำกับไว้
5. Bob นำสิ่งอ้างสิทธิที่ได้รับจากเจ้าหน้าที่ขององค์กรเสมือน Japan มาแนบกับหลักฐานอ้างอิงตัวผู้ใช้ของ Bob เอง แล้วนำไปยื่นต่อทรัพยากรในองค์กรเสมือน Japan ทรัพยากรนั้นจะพิจารณาลายเซ็นที่กำกับว่าเป็นของเจ้าหน้าที่ขององค์กรเสมือน Japan จริง และพิจารณาสิทธิการเข้าใช้ตามที่เจ้าหน้าที่ขององค์กรเสมือน Japan ได้ให้แก่ Bob

ขั้นตอนที่ 1 และขั้นตอนที่ 2 ซึ่งเป็นขั้นตอนที่ผู้ใช้จะต้องติดต่อกับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนตนเองเพื่อขอสิทธิในการติดต่อกับซีเอเอสเซอร์ฟเวอร์ของต่างองค์กรเสมือนสามารถอธิบายขั้นตอนการทำงานได้โดยแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 4.5 และหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่จากขั้นตอนนี้มีรายละเอียดดังรูปที่ 4.6

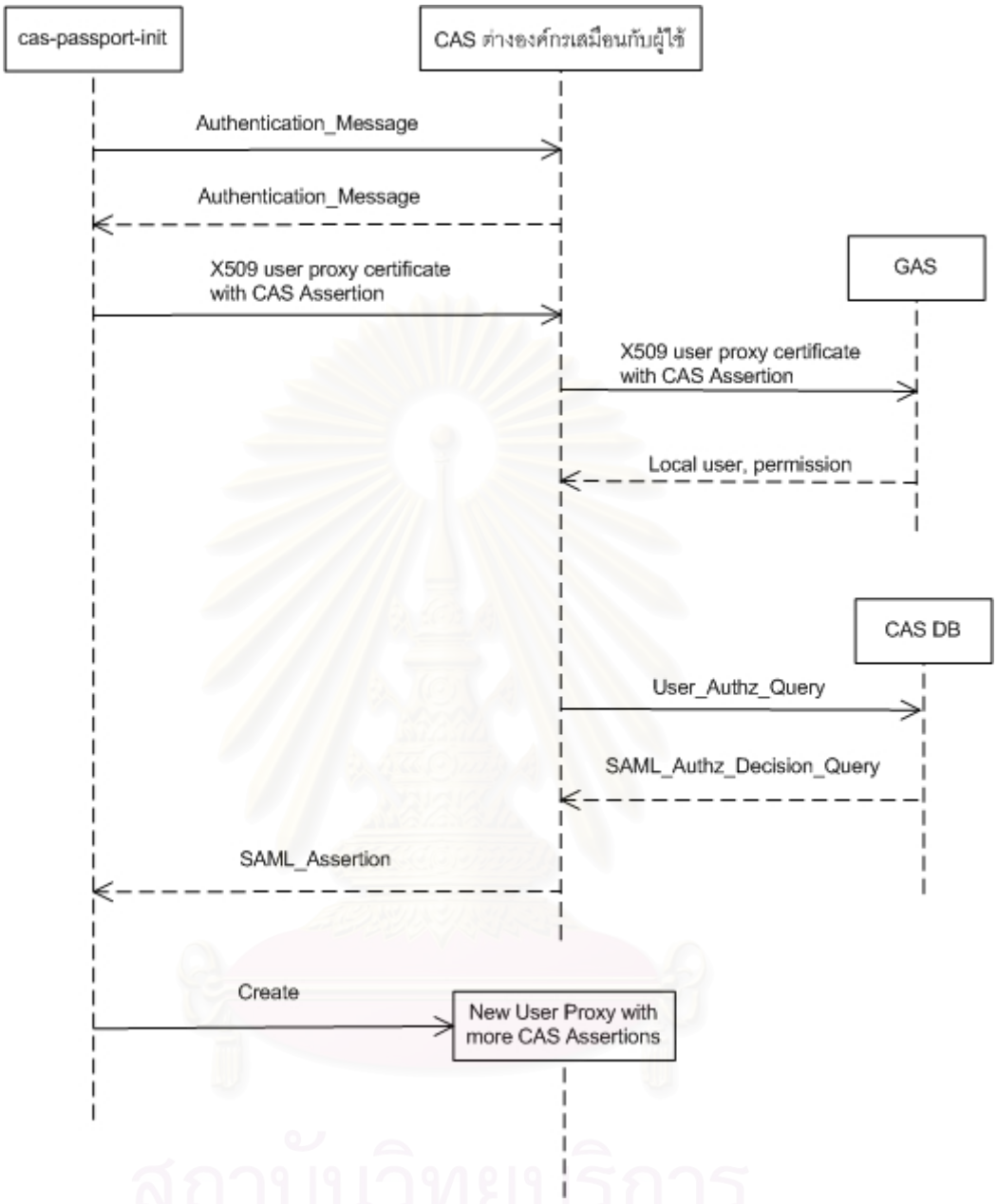


รูปที่ 4.5 แสดงแผนภาพลำดับของการร้องขอสิทธิการติดต่อกับซีเอเอสขององค์กรเสมือนอื่นจากซีเอเอสขององค์กรเสมือนเดียวกับผู้ใช้

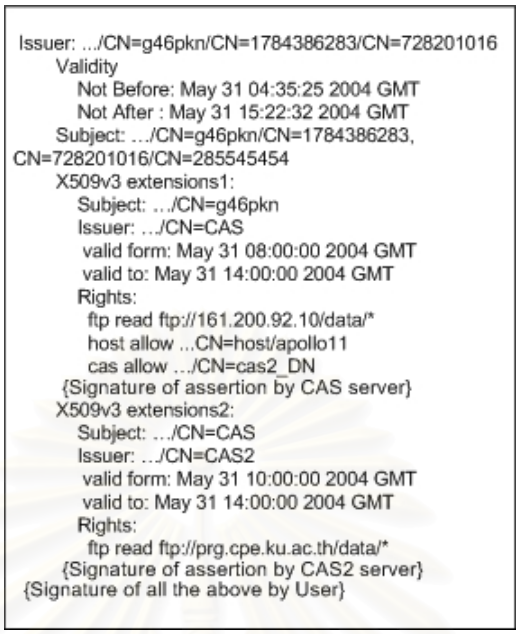


รูปที่ 4.6 แสดงหลักฐานอ้างอิงผู้ใช้อันใหม่ที่ได้เพิ่มสิทธิการติดต่อกับซีเอเอสขององค์กรเสมือนอื่น

ขั้นตอนที่ 3 และขั้นตอนที่ 4 ซึ่งเป็นขั้นตอนที่ผู้ใช้นำหลักฐานอ้างอิงผู้ใช้ที่แนบสิ่งอ้างสิทธิจากซีเอเอสเซอร์ฟเวอร์องค์กรเสมือนเดียวกับผู้ใช้ไปยื่นต่อซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่นเพื่อขอสิทธิการเข้าใช้ทรัพยากรในองค์กรเสมือนนั้นๆสามารถอธิบายขั้นตอนการทำงานได้โดยแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 4.7 และหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่จากขั้นตอนนี้มีรายละเอียดดังรูปที่ 4.8

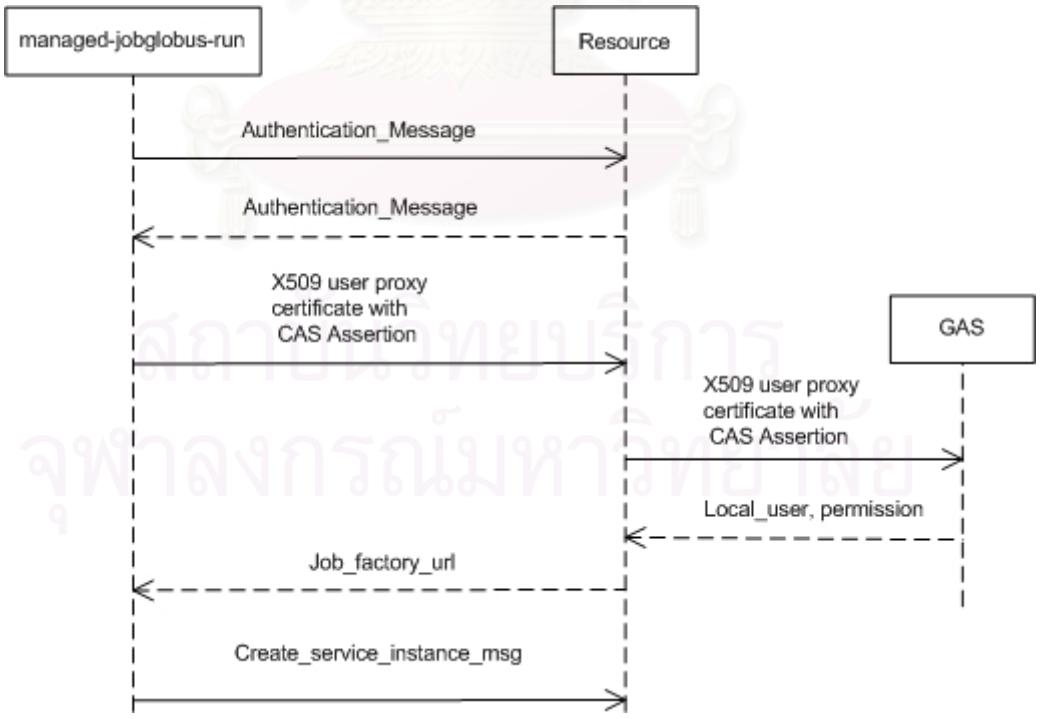


รูปที่ 4.7 แสดงแผนภาพลำดับของการร้องขอสิทธิการเข้าใช้ทรัพยากรในอีกองค์กรเสมือนตามแนวคิดของการทำหนังสือเดินทาง



รูปที่ 4.8 แสดงหลักฐานอ้างอิงผู้ใช้อันใหม่ที่ได้เพิ่มสิทธิการใช้ในองค์กรเสมือนอื่น

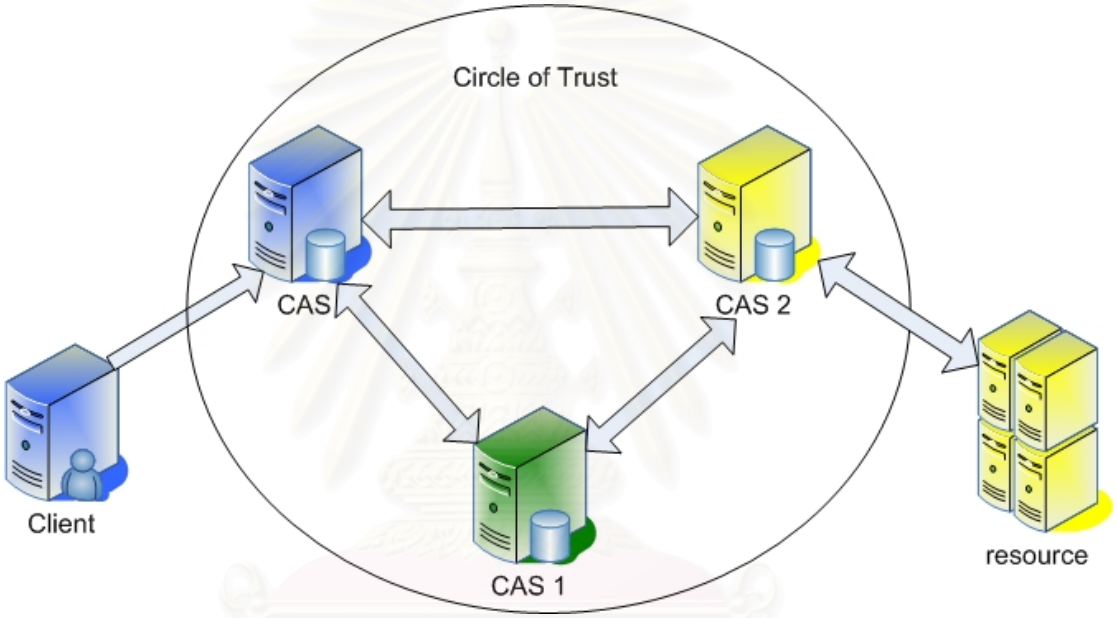
ขั้นตอนที่ 5 ผู้ใช้นำหลักฐานอ้างอิงผู้ใช้ซึ่งแนบสิ่งอ้างสิทธิที่ออกโดยซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนเดียวกับทรัพยากรที่ผู้ใช้ต้องการไปยื่นต่อทรัพยากรนั้น สามารถอธิบายขั้นตอนการทำงานได้โดยแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 4.9



รูปที่ 4.9 แสดงแผนภาพลำดับของการใช้งานทรัพยากรในอีกองค์กรเสมือนของผู้ใช้

4.3 การออกแบบระบบจัดการสิทธิการเข้าใช้ทรัพยากรสำหรับโกลบัสทูลคิดรุ่น 3.2 บนสภาพแวดล้อมของการเชื่อมต่อกันขององค์กรเสมือนที่ไม่ได้เชื่อถือกันโดยตรงแต่เชื่อถือกันผ่านตัวแทน

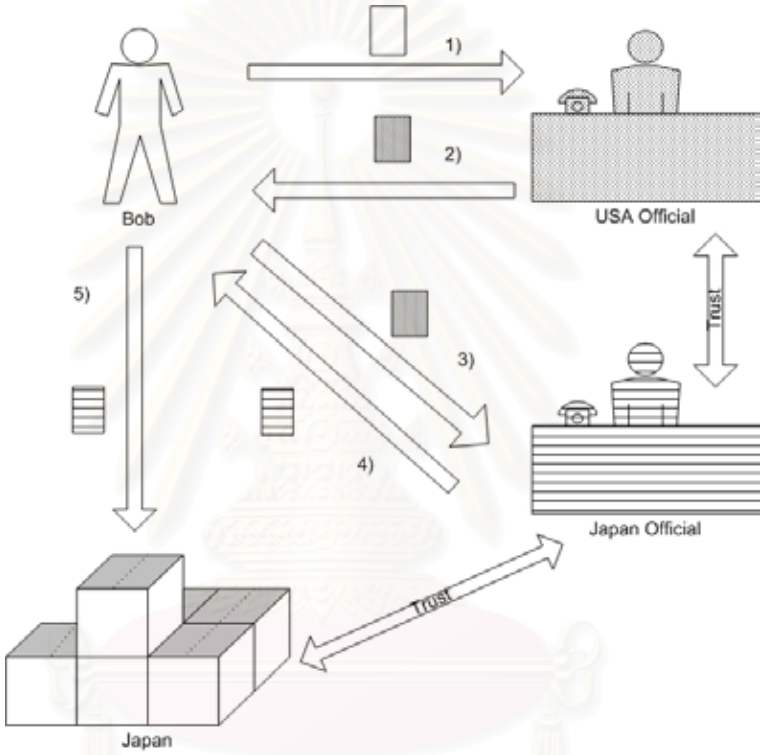
สำหรับการเชื่อมต่อองค์กรเสมือนใดๆเข้าด้วยกันโดยที่องค์กรเสมือนนั้นไม่ได้เชื่อถือกันโดยตรงแต่เชื่อถือกันผ่านตัวแทนคือเชื่อถือกันผ่านซีเอเอสของแต่ละองค์กรเสมือน สามารถทำได้โดยให้เครื่องซีเอเอสขององค์กรเสมือน B เชื่อถือผู้ออกหลักฐานอ้างอิงตนเองของซีเอเอสขององค์กรเสมือน A ซึ่งจะได้สภาพแวดล้อมดังรูปที่ 4.10



รูปที่ 4.10 แสดงสภาพแวดล้อมหลังเชื่อมต่อองค์กรเสมือนโดยที่องค์กรเสมือนไม่ได้มีความเชื่อถือกันโดยตรงแต่เชื่อถือผ่านตัวแทน

สำหรับสภาพแวดล้อมที่องค์กรเสมือนทั้งสองไม่ได้เชื่อถือกันโดยตรงแต่เชื่อถือกันผ่านซีเอเอสนั้น หลักฐานอ้างอิงผู้ใช้ตัวแทนของในองค์กรเสมือนหนึ่งไม่สามารถนำไปพิสูจน์ตัวบุคคลในอีกองค์กรเสมือนหนึ่งได้โดยตรง เนื่องจากในอีกองค์กรเสมือนนั้นไม่ได้เชื่อถือผู้ออกหลักฐานอ้างอิงผู้ใช้โดยตรง ดังนั้นผู้วิจัยจำเป็นที่จะต้องออกแบบระบบสำหรับสร้างหลักฐานอ้างอิงผู้ใช้ขึ้นใหม่โดยให้หลักฐานอ้างอิงอันใหม่มีความเชื่อถือกับซีเอเอสในอีกองค์กรเสมือนที่จะเข้าไปใช้ ซึ่งหลักฐานอ้างอิงผู้ใช้อันใหม่จะสร้างโดยซีเอเอสขององค์กรเสมือนเดียวกะผู้ใช้และมีความเชื่อถือกับซีเอเอสในอีกองค์กรเสมือน โดยหลักฐานอ้างอิงผู้ใช้อันใหม่จะสร้างขึ้นโดยใช้หลักการมอบอำนาจจากหลักฐานอ้างอิงผู้ใช้อันเดิม คล้ายกับการที่ผู้ใช้เมื่อไปติดต่องานที่ตึกใดๆที่มีระบบรักษาความปลอดภัยจำเป็นที่จะต้องติดต่อผู้ที่มีอำนาจตรวจสอบและอนุญาตให้สามารถเข้าไปในตึกได้โดยจำเป็นจะต้องพิสูจน์ตัวบุคคล โดยใช้บัตรประชาชนและนำบัตรประชาชนไปแลกเป็นบัตร

ที่มีสิทธิเข้าไปในตึกได้และเมื่อต้องการออกจากตึกผู้ใช้ก็จะแลกบัตรที่มีสิทธิเข้าไปในตึกกับบัตรประชาชนของผู้ใช้เองคืน โดยที่ตึกเปรียบได้กับทรัพยากรในอีกองค์กรเสมือน ผู้ที่มีอำนาจตรวจสอบและอนุญาตให้สามารถเข้าไปในตึกหรือยามเปรียบได้กับ ซีเอเอสของอีกองค์กรเสมือน บัตรประชาชนเปรียบได้กับหลักฐานอ้างอิงผู้ใช้ตัวแทนที่สร้างโดยซีเอเอสขององค์กรเสมือนของผู้ใช้เอง และ บัตรที่มีสิทธิเข้าไปในตึกเปรียบได้กับหลักฐานอ้างอิงอันใหม่ที่ออกโดยซีเอเอสของอีกองค์กรเสมือน ซึ่งการใช้งานของผู้ใช้ในอีกองค์กรเสมือนสามารถอธิบายได้ดังรูปที่ 4.11



รูปที่ 4.11 แสดงภาพรวมการใช้งานของทรัพยากรในองค์กรเสมือนอื่นตามแนวคิดการเปลี่ยนบัตร

คือหลักฐานอ้างอิงผู้ใช้ตัวแทนของผู้ใช้ Bob ซึ่งอยู่ภายในองค์กรเสมือน USA

คือหลักฐานอ้างอิงผู้ใช้ที่สร้างโดยเจ้าหน้าที่ขององค์กรเสมือน USA ซึ่งในหลักฐานอ้างอิงผู้ใช้จะมีสิ่งอ้างสิทธิที่ผู้ใช้ได้รับจากเจ้าหน้าที่ขององค์กรเสมือน USAให้สามารถติดต่อเพื่อขอสิทธิในองค์กรเสมือน Japan ได้

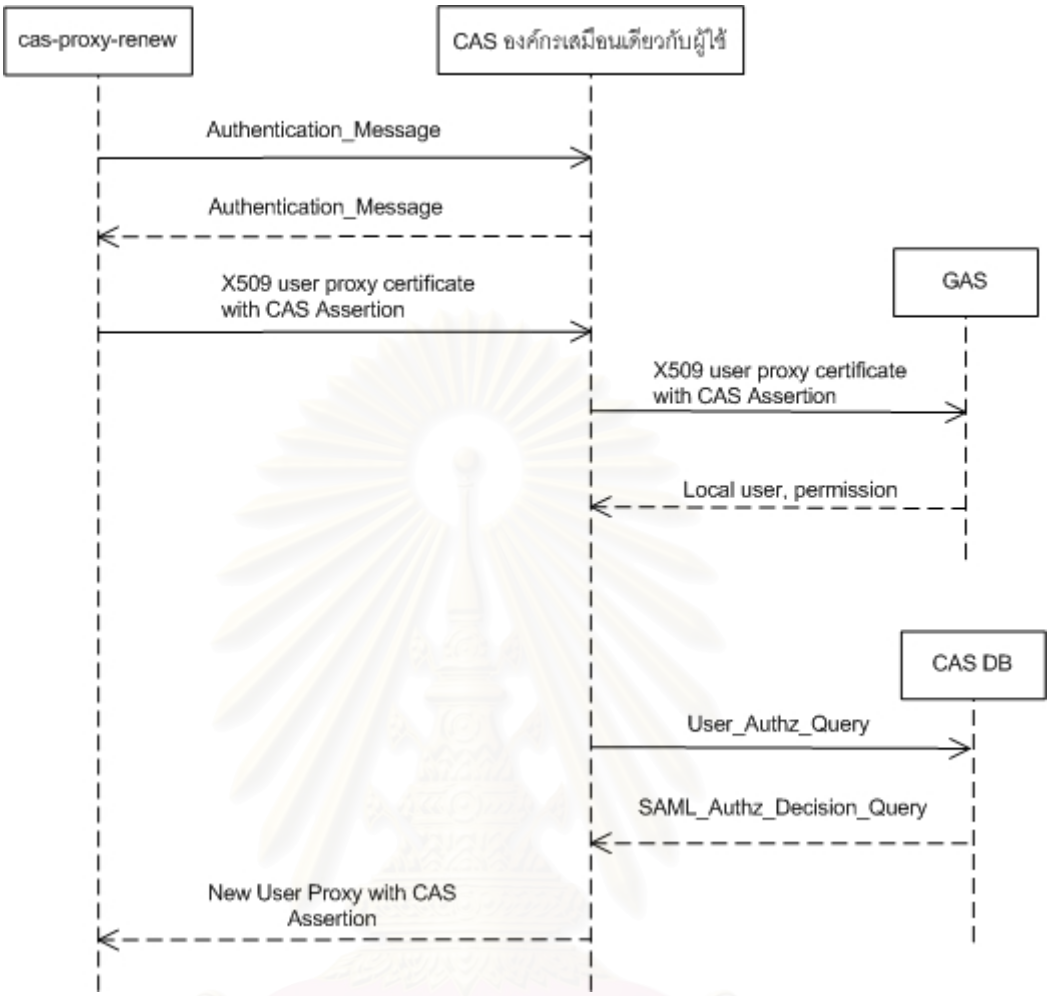
คือหลักฐานอ้างอิงผู้ใช้ที่สร้างโดยเจ้าหน้าที่ขององค์กรเสมือน Japan เพื่ออนุญาตให้ผู้ใช้สามารถเข้าไปใช้ทรัพยากรในองค์กรเสมือน Japan ได้เท่าที่สิทธิในสิ่งอ้างสิทธิกำหนดไว้

จากภาพที่ 4.11 แสดงภาพการใช้งานของทรัพยากรในองค์กรเสมือนอื่นตามแนวคิดการเปลี่ยนบัตร โดยสมมติเหตุการณ์ว่า Bob เป็นผู้ใช้ในองค์กรเสมือน USA โดยที่เจ้าหน้าที่ขององค์กรเสมือน Japan จะไม่เชื่อถือเอนทิตีอื่นใดเลยในองค์กรเสมือน USA นอกจากเจ้าหน้าที่ขององค์กรเสมือน USA เพื่อให้สอดคล้องกับสภาพแวดล้อมที่องค์กรเสมือนนั้นไม่ได้เชื่อถือกันโดยตรง

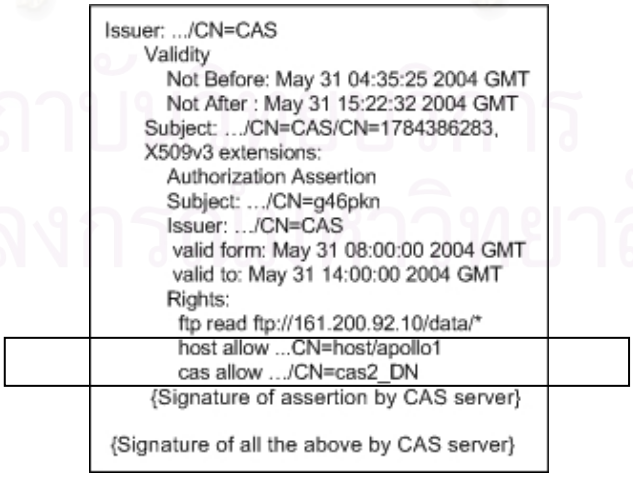
แต่เชื่อถือกันผ่านตัวแทน และ Bob มีความต้องการไปใช้ทรัพยากรในองค์กรเสมือน Japan ซึ่งผู้ใช้ Bob จะต้องทำตามขั้นตอน 5 ขั้นดังนี้

1. Bob ซึ่งเป็นผู้ใช้ในองค์กรเสมือน USA จะต้องติดต่อไปยังเจ้าหน้าที่ผู้ดูแลขององค์กรเสมือนของตนเองโดยนำหลักฐานอ้างอิงผู้ใช้ไปพิสูจน์ว่าตนเองชื่อ Bob จริงและเป็นผู้ใช้ในองค์กรเสมือน USA จริง
2. เมื่อเจ้าหน้าที่ผู้ดูแลขององค์กรเสมือน USA ตรวจสอบหลักฐานอ้างอิงผู้ใช้ของ Bob และพิสูจน์ได้ว่าเป็นสมาชิกขององค์กรเสมือน USA จริง จึงสร้างหลักฐานอ้างอิงผู้ใช้ที่แนบสิทธิยินยอมให้ Bob สามารถไปติดต่อกับเจ้าหน้าที่ขององค์กรเสมือน Japan ได้โดยหลักฐานอ้างอิงผู้ใช้อันใหม่นี้จะมีชื่อเฉพาะเป็นชื่อเฉพาะของเจ้าหน้าที่ขององค์กรเสมือนตัวแทน แล้วทำการส่งหลักฐานอ้างอิงผู้ใช้นั้นกลับไปยัง Bob
3. Bob นำหลักฐานอ้างอิงของผู้ใช้ที่แนบสิ่งอ้างสิทธิที่เจ้าหน้าที่ขององค์กรเสมือน USA ออกให้ไปยื่นต่อเจ้าหน้าที่ขององค์กรเสมือน Japan
4. เจ้าหน้าที่ขององค์กรเสมือน Japan จะตรวจสอบหลักฐานอ้างอิงผู้ใช้ และสิ่งอ้างสิทธิที่แนบมาด้วยว่า เป็นตัวแทนเจ้าหน้าที่ขององค์กรเสมือน USA จริง และพิจารณาว่าทางองค์กรเสมือนของ Japan ยินยอมให้ผู้ใช้จากองค์กรเสมือน USA เข้ามาใช้ทรัพยากรหรือไม่ และจะได้สิทธิการเข้าใช้ทรัพยากรขององค์กรเสมือน Japan แค่ไหนบ้าง พร้อมทั้งออกหลักฐานอ้างอิงผู้ใช้อันใหม่ที่มีรายละเอียดสิทธิการเข้าใช้ทรัพยากรของผู้ใช้ในองค์กรเสมือน USA ที่มีต่อทรัพยากรในองค์กรเสมือนของ Japan พร้อมทั้งทำลายเซ็นดิจิตอลกำกับไว้
5. Bob นำหลักฐานอ้างอิงผู้ใช้ที่ได้รับจากเจ้าหน้าที่ขององค์กรเสมือน Japan ไปยื่นต่อทรัพยากรในองค์กรเสมือน Japan ทรัพยากรนั้นจะพิจารณาลายเซ็นที่กำกับว่าเป็นของเจ้าหน้าที่ขององค์กรเสมือน Japan จริง และพิจารณาสิทธิการเข้าใช้ตามที่เจ้าหน้าที่ขององค์กรเสมือน Japan ได้ให้แก่ Bob

ขั้นตอนที่ 1 และขั้นตอนที่ 2 ซึ่งเป็นขั้นตอนที่ผู้ใช้จะต้องติดต่อกับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนตนเองเพื่อขอสิทธิในการติดต่อกับซีเอเอสเซอร์ฟเวอร์ของต่างองค์กรเสมือนสามารถอธิบายขั้นตอนการทำงานได้โดยแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 4.12 และหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่จากขั้นตอนนี้มีรายละเอียดดังรูปที่ 4.13

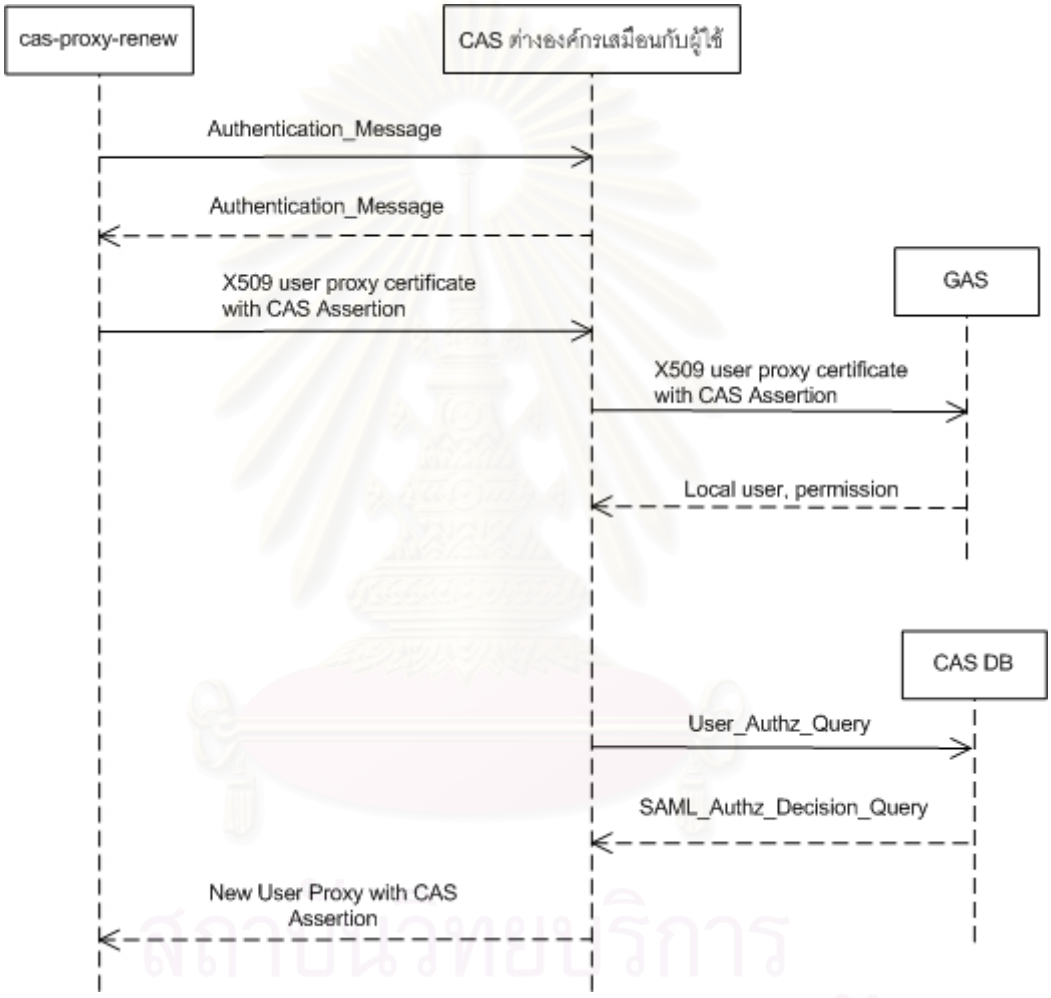


รูปที่ 4.12 แสดงแผนภาพลำดับของการร้องขอสิทธิการติดต่อกับซีเอเอสขององค์กรเสมือนอื่นจากซีเอเอสขององค์กรเสมือนเดียวกับผู้ใช้ตามแนวคิดของการเปลี่ยนบัตร

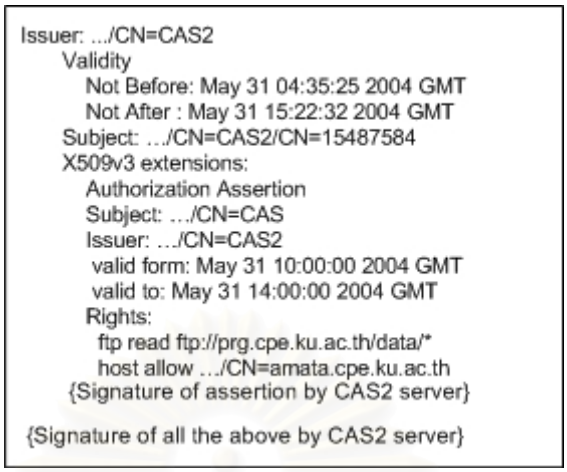


รูปที่ 4.13 แสดงหลักฐานอ้างอิงผู้ใช้อันใหม่ที่ได้เพิ่มสิทธิการติดต่อกับซีเอเอสขององค์กรเสมือนอื่นในแนวคิดเปลี่ยนบัตร

ขั้นตอนที่ 3 และขั้นตอนที่ 4 ซึ่งเป็นขั้นตอนที่ผู้ใช้นำหลักฐานอ้างอิงผู้ใช้ที่แนบสิ่งอ้างสิทธิจากซีเอเอสเซอร์ฟเวอร์องค์กรเสมือนเดียวกับผู้ใช้ไปยื่นต่อซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่นเพื่อขอสิทธิการเข้าใช้ทรัพยากรในองค์กรเสมือนนั้นๆสามารถอธิบายขั้นตอนการทำงานได้โดยแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 4.14 และหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่จากขั้นตอนนี้มีรายละเอียดดังรูปที่ 4.15

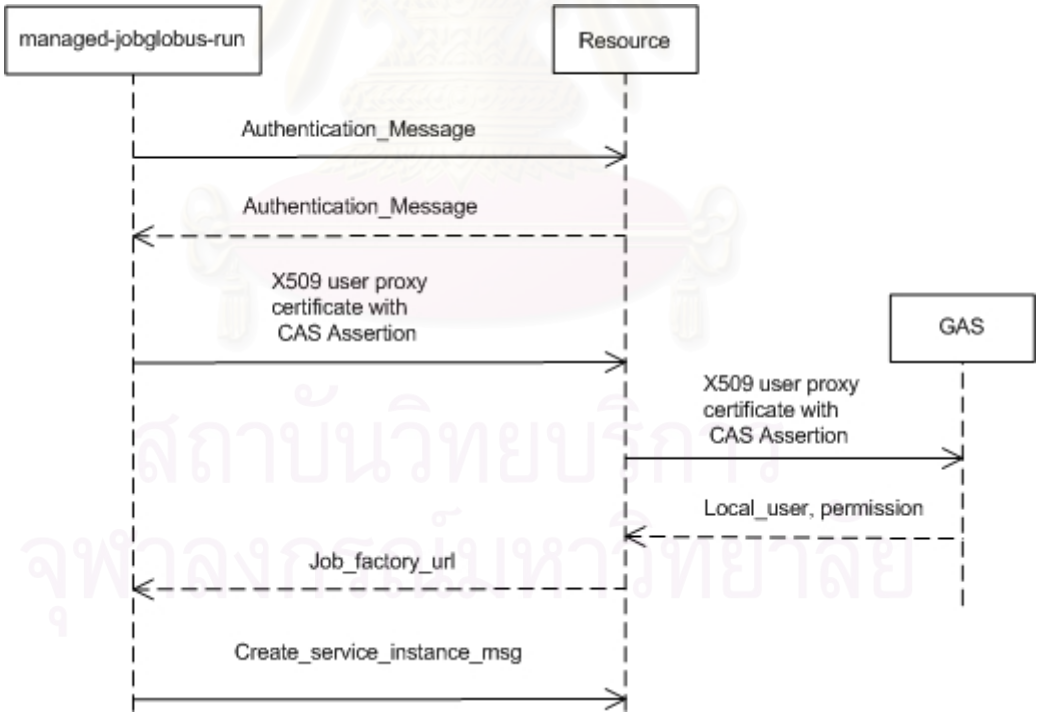


รูปที่ 4.14 แสดงแผนภาพลำดับของการร้องขอสิทธิการเข้าใช้ทรัพยากรในอีกองค์กรเสมือนตามแนวคิดของการเปลี่ยนบัตร



รูปที่ 4.15 แสดงหลักฐานอ้างอิงผู้ใช้อันใหม่ที่ได้เพิ่มสิทธิการติดต่อกับซีเอเอสขององค์กรเสมือนอื่นในแนวคิดแบบเปลี่ยนบัตร

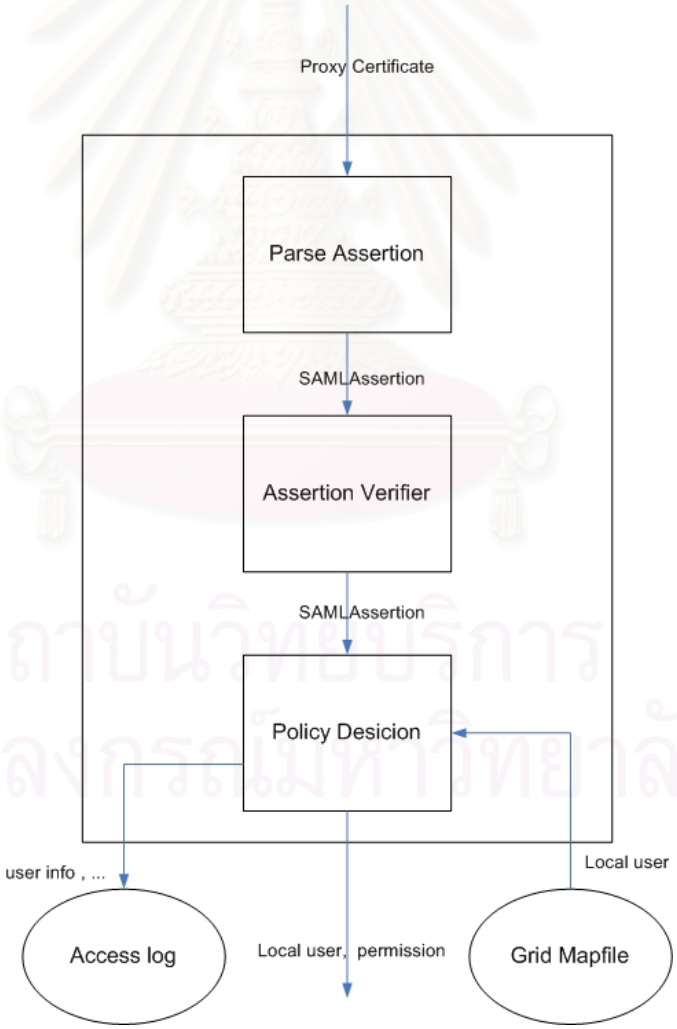
ขั้นตอนที่ 5 ผู้ใช้นำหลักฐานอ้างอิงผู้ใช้ซึ่งแนบสิ่งอ้างสิทธิที่ออกโดยซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนเดียวกับทรัพยากรที่ผู้ใช้ต้องการไปยื่นต่อทรัพยากรนั้น สามารถอธิบายขั้นตอนการทำงานได้โดยแผนภาพลำดับ (Sequence Diagram) ดังรูปที่ 4.16



รูปที่ 4.16 แสดงแผนภาพลำดับของการใช้งานทรัพยากรในอีกองค์กรเสมือนของผู้ใช้

4.4 การออกแบบส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิที่ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้เป็นผู้ออกมาให้และพิจารณาสิทธิของผู้ใช้บนทรัพยากรใดๆให้สามารถทำงานข้ามองค์กรเสมือนได้

การออกแบบระบบจัดการสิทธิการเข้าใช้ทรัพยากรระหว่างองค์กรเสมือนที่เชื่อมต่อกันตั้งแต่ 2 องค์กรเสมือนขึ้นไปบน 2 สภาพแวดล้อมที่ได้กล่าวในหัวข้อ 4.2 และหัวข้อ 4.3 นั้น ซีเอเอสและทรัพยากรจะมีการเรียกใช้ส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิที่ผู้ให้บริการข้อมูลสำหรับระบุสิทธิของผู้ใช้เป็นผู้ออกมาให้และพิจารณาสิทธิของผู้ใช้บนทรัพยากรใดๆหรือจีเอเอสเพื่อทำการตรวจสอบสิ่งอ้างสิทธิที่แนบมากับหลักฐานอ้างอิงผู้ใช้ ซึ่งสิ่งอ้างอิงสิทธินั้นอาจจะมีมากกว่า 1 อันจึงจำเป็นต้องเปลี่ยนแปลงจีเอเอสที่ได้ออกแบบในหัวข้อ 3.3.2 ซึ่งได้จีเอเอสตัวใหม่มีลักษณะดังรูปที่ 4.17



รูปที่ 4.17 แสดงส่วนประกอบของจีเอเอสหลังจากเปลี่ยนแปลงจากจีเอเอสเดิมในหัวข้อ 3.3.2

จากรูปที่ 4.17 สามารถอธิบายการทำงานของจีเอเอสหลังจากเปลี่ยนแปลงจากจีเอเอสเดิมในหัวข้อ 3.3.2 โดยแบ่งเป็น 3 ขั้นตอนดังนี้

- ส่วนพิจารณาและคัดกรองสิ่งอ้างสิทธิจากส่วนขยายของหลักฐานอ้างอิงผู้ใช้ (Parse Assertion) เนื่องจากแนวคิดแบบการทำหนังสือเดินทางจะประกอบไปด้วยสิ่งอ้างสิทธิมากกว่า 1 อัน จึงจำเป็นที่จะต้องมีส่วนพิจารณาและคัดกรองสิ่งอ้างสิทธิที่เกี่ยวข้องกับซีเอเอสเซอร์ฟเวอร์หรือทรัพยากรที่ผู้ใช้กำลังติดต่ออยู่ โดยในส่วนนี้จะตรวจสอบความถูกต้องของหลักฐานอ้างอิงผู้ใช้เสียก่อนถ้าพบว่าหลักฐานอ้างอิงผู้ใช้ถูกต้องจะทำการส่งต่อสิ่งอ้างสิทธิทั้งหมดที่เกี่ยวข้องไปยังส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิ แต่ถ้าพิจารณาแล้วพบว่าหลักฐานอ้างอิงผู้ใช้ไม่มีสิ่งอ้างสิทธิแนบก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว
- ส่วนตรวจสอบความถูกต้องของสิ่งที่อ้างสิทธิ (Assertion Verifier) จะรับหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนที่แนบสิ่งอ้างสิทธิ มาทำการพิสูจน์ความถูกต้องของสิ่งหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนและสิ่งที่อ้างสิทธิโดยจะต้องพิจารณา 4 อย่างด้วยกันได้แก่
  - ความน่าเชื่อถือของหลักฐานอ้างอิงผู้ใช้ โดยจะตรวจสอบว่าทรัพยากรมีความเชื่อถือกับผู้ออกหลักฐานอ้างอิงผู้ใช้ตัวแทนหรือไม่ ถ้าทรัพยากรไม่มีความเชื่อถือผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ ก็จะพิจารณาผู้ที่ออกหลักฐานอ้างอิงของผู้ที่ออกหลักฐานอ้างอิงผู้ใช้ และทำไปเรื่อยจนกว่าผู้ที่ออกหลักฐานอ้างอิงผู้ใช้นั้นมีความเชื่อถือกันทำให้เกิดลูกโซ่ของความเชื่อถือ(Trust chain) การตรวจสอบว่าทรัพยากรมีความเชื่อถือกับผู้ออกหลังฐานอ้างอิงผู้ใช้สามารถทำได้โดยพิจารณาว่าผู้ออกหลักฐานอ้างอิงผู้ใช้นั้นมีหลักฐานอ้างอิงตนเองอยู่ใน /etc/grid-security/certificates/ หรือไม่ ในกรณีที่ทรัพยากรไม่มีความเชื่อถือผู้ออกหลักฐานอ้างอิงผู้ใช้ ก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้ไปยังผู้เรียกส่วนตรวจสอบนี้
  - หลักฐานอ้างอิงผู้ใช้ตัวแทนไม่ได้ถูกแก้ไข ซึ่งสามารถตรวจสอบได้ โดยนำหลักฐานอ้างอิงผู้ใช้ตัวแทนไปทำเมสเซจไดเจส แล้วนำไปเทียบกับลายเซ็นดิจิตอลที่ถอดรหัสโดยกุญแจสาธารณะของผู้ออกหลักฐานอ้างอิงผู้ใช้ตัวแทน ถ้าผลการเปรียบเทียบพบว่าข้อความทั้งสองมีลักษณะตรงกันแสดงว่าหลักฐานอ้างอิงผู้ใช้ตัวแทนอันนี้ไม่ได้ถูกแก้ไขสามารถนำมาพิสูจน์ตัวจริงของผู้ใช้ได้ แต่ถ้า

พบว่าข้อความทั้งสองไม่ตรงกันก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้ไปยังผู้เรียกส่วนตรวจสอบนี้

- ความน่าเชื่อถือของผู้ออกสิ่งอ้างสิทธิ โดยจะตรวจสอบหาลูกโซ่ของความเชื่อถือของผู้ออกสิ่งอ้างสิทธิ ซึ่งจะคล้ายการตรวจสอบความเชื่อถือของหลักฐานอ้างอิงผู้ใช้ ถ้าพบว่าลูกโซ่ของความเชื่อถือของผู้ออกสิ่งอ้างสิทธิไม่มีความเชื่อถือกับทรัพยากรก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว
- สิ่งอ้างสิทธิไม่ได้ถูกแก้ไข ซึ่งสามารถตรวจสอบได้โดยนำสิ่งอ้างสิทธิไปทำเมสเซจไดเจส แล้วนำไปเทียบกับลายเซ็นดิจิตอลที่ถอดรหัสโดยกุญแจสาธารณะของผู้ออกสิ่งที่อ้างสิทธิถ้าผลการเปรียบเทียบพบว่าข้อความทั้งสองมีลักษณะตรงกันแสดงว่าสิ่งอ้างสิทธิไม่ได้ถูกแก้ไขสามารถนำมาพิจารณาสิทธิการเข้าใช้ได้ แต่ถ้าพบว่าข้อความทั้งสองไม่ตรงกันก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว

โดนส่วนนี้จะทำการตรวจสอบกับสิ่งอ้างอิงสิทธิทุกอันที่ส่งมาจากส่วนพิจารณาและคัดกรอง แล้วจึงส่งสิ่งอ้างสิทธิที่ถูกต้องไปยังส่วนพิจารณาสิทธิของผู้ใช้ ถ้าพบว่าสิ่งอ้างอิงสิทธิทั้งหมดไม่มีอันไหนที่ถูกต้องเลยก็จะส่งข้อความปฏิเสธการขอเข้าใช้ทรัพยากรของผู้ใช้โดยใช้สิ่งอ้างสิทธิไปยังผู้เรียกส่วนตรวจสอบนี้ ให้กลับไปทำงานโดยใช้จีเอสไอเพียงอย่างเดียว

- ส่วนจัดการนโยบาย (Policy Desicion) จะทำการอ่านสิ่งอ้างสิทธิแบบเอสเอเอ็มแอลโดยทำการอ่านสิ่งอ้างสิทธิตั้งแต่อันแรก โดยจะพิจารณาจาก Authorization Decision Statement ในส่วนที่ตรงกับทรัพยากร ที่ผู้ใช้ต้องการเข้าใช้เพื่อดูสิทธิการเข้าใช้ ถ้าเป็น deny ก็จะพิจารณาสิ่งอ้างสิทธิอันต่อไป ถ้าพิจารณาทั้งหมดแล้วพบว่าไม่มีสิ่งอ้างสิทธิอันใหม่เป็น allow ก็จะส่งข้อความไม่อนุญาตเข้าใช้ไปยังส่วนที่เรียกบริการนี้เพื่อที่จะทำงานต่อโดยไม่สนใจสิ่งที่อ้างสิทธิเหมือนทำงานปกติ แต่ถ้าเป็น allow จะต้องทำการหาชื่อผู้ใช้เฉพาะที่โดยทำการจับคู่ระหว่างชื่อเฉพาะของผู้ออกสิ่งอ้างอิงสิทธิกับชื่อผู้ใช้เฉพาะที่ที่ทำการเก็บไว้ใน กริดแมปไฟล์หลังจากได้ชื่อผู้ใช้เฉพาะที่แล้วจะทำการเก็บข้อมูลการเข้าใช้ซึ่งประกอบไปด้วย ชื่อเฉพาะของผู้ใช้ ชื่อเฉพาะของผู้ออกสิ่งอ้างอิงสิทธิ ชื่อผู้ใช้เฉพาะที่บนทรัพยากร และเวลาในการเข้าใช้

ทรัพยากรไว้ในบันทึกการเข้าใช้ทรัพยากรพร้อมทั้งทำการคืนชื่อผู้ใช้เฉพาะที่ไปยังผู้เรียกบริการนี้

บทที่ 5

การทดสอบระบบ

ผู้วิจัยได้แบ่งประเภทของการทดสอบระบบตามสภาพแวดล้อมของการใช้งาน 3 สภาพแวดล้อมด้วยกันได้แก่ การทดสอบระบบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้ การทดสอบระบบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองเชื่อถือกันโดยตรง และการทดสอบระบบบนสภาพแวดล้อมที่องค์กรเสมือนไม่มีความเชื่อถือกันโดยตรงแต่จะเชื่อถือกันผ่านตัวแทนหรือซีเอเอส นอกจากการทดสอบระบบตามสภาพแวดล้อมการใช้งานที่กล่าวมาข้างต้นทั้ง 3 สภาพแวดล้อมแล้ว ยังมีการทดสอบความสามารถในการทำงานร่วมกันกับสภาพแวดล้อมของโกลบัสทูลคิดรุ่น 3.2.1 ที่ไม่ได้ถูกแก้ไข ภายในองค์กรเสมือนของตนเอง (Backward Compatible)

5.1 การทดสอบระบบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกันกับผู้ใช้

5.1.1 วิธีการทดลอง

1. เลือกเครื่องที่จะมาทำการทดสอบดังนี้
    a. เครื่อง apollo11.cp.eng.chula.ac.th สำหรับทำเป็นไคลเอนท์
    b. เครื่อง apollo1.cp.eng.chula.ac.th สำหรับเป็นซีเอเอสเซอร์ฟเวอร์
    c. เครื่อง apollo10.cp.eng.chula.ac.th สำหรับเป็นเครื่องทรัพยากร
2. ติดตั้งโกลบัสทูลคิดรุ่น 3.2.1 บนเครื่องทั้งสามเครื่องพร้อมทั้งทำ grid-cert-request เพื่อขอคำร้องขอหลักฐานอ้างอิงโฮสท์(hostcert_request.pem) และนำคำร้องขอหลักฐานอ้างอิงโฮสท์ของทั้งสามเครื่องไปขอหลักฐานอ้างอิงตัวโฮสท์(hostcert.pem) จากผู้ออกหลักฐานอ้างอิงเดียวกับผู้ออกหลักฐานอ้างอิงให้ผู้ใช้(usercert.pem) ของผู้ที่จะทำการทดสอบ
3. ติดตั้งจีเอเอสบนเครื่องทั้งสามเครื่อง
4. ทำการแก้ไขระบบให้สามารถใช้งานซีเอเอสได้ตามปกติ (ทำตามขั้นตอนในเวปไซต์ http://www-unix.globus.org/toolkit/docs/3.2/installation/install_config_cas.html) บนเครื่องที่เป็นซีเอเอสเซอร์ฟเวอร์
5. ทำการเพิ่มข้อมูลเข้าไปในฐานข้อมูลของซีเอเอสเซอร์ฟเวอร์ดังรูปที่ 5.1

```
# เนื่องจากการติดตั้ง cas โดยตามweb page ในข้อ 4 มีส่วนผิดพลาด (cas-server-bootstrap จะอ่าน $GLOBUS_LOCATION/etc/casDBProperties ผิด) จึงต้องแก้ไขให้ถูกต้อง ดังนี้

UPDATE trust_anchor_table SET authentication_method='x509' , authentication_data =
'/O=Grid/O=Chula/CN=Apollo CA' WHERE trust_anchor_nickname = 'defaultTrustAnchor';

#เพิ่ม namespace ที่จะนำมาใช้กับ resource (GRAM)
```

```
INSERT INTO namespace_table VALUES ('hostNamespace', '.',
'databaseAccess.accessors.ExactComparison');

#เพิ่มกลุ่มของผู้ใช้

INSERT into user_group_table (user_group_name) VALUES ('grad');

#เพิ่มชื่อผู้ใช้โดยค่าที่ต้องใส่คือ local user, user DN และ CA ผู้ sign usercert.pem

INSERT into user_table VALUES ('g46pkn', '/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan
Kongsirikul (4670359521)', 'defaultTrustAnchor');

#เพิ่มผู้ใช้เข้าไปในกลุ่ม

INSERT into user_group_entry VALUES ('grad','g46pkn');

#เพิ่ม service แบบ host

INSERT INTO service_type VALUES ('host');

#เพิ่ม action แบบ allow และ deny ให้กับ service แบบ host (เมื่อนำ Assertion ไปยื่นต่อ #resource GAS จะ
check สิทธิของ user โดยถ้าเป็น allow ผู้ใช้จะสามารถใช้งาน #resource ได้)

INSERT INTO service_type_action VALUES (24,'host','allow');

INSERT INTO service_type_action VALUES (25,'host','deny');

#เพิ่ม action แบบ allow และ deny ให้กับ service แบบ cas (เมื่อนำ Assertion ไปยื่นต่อ cas ขององค์กรเสมือน
อื่นหรือกลุ่มอื่น cas จะเรียก GAS เพื่อ check สิทธิของ user ถ้าเป็น allow จะอนุญาตให้ทำงานในองค์กรเสมือน
ของตนโดยสร้าง assertion ขึ้นมาให้ใหม่)

INSERT INTO service_type_action VALUES (26,'cas','allow');

INSERT INTO service_type_action VALUES (27,'cas','deny');

#เพิ่ม object เป็นเครื่องresource ที่เราจะทดสอบคือ apollo10 โดยใช้ host DN ใน hostcert.pem ของเครื่อง
apollo10

INSERT INTO object_table VALUES (2, '/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th',
'hostNamespace');

#เพิ่ม policy ให้ผู้ใช้กลุ่ม grad (กลุ่มที่ผู้ทดสอบอยู่) ให้มีสิทธิใช้ apollo10

INSERT into policy_table VALUES (2,'grad', 24,'host allow to used',2,'object');
```

รูปที่ 5.1 แสดงรายละเอียดการเพิ่มข้อมูลเข้าไปในฐานข้อมูลซีเอเอสสำหรับไว้ทดสอบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

6. ผู้ใช้ทำการทดสอบโดยเข้าไปยังเครื่องไคลเอนท์ผ่านทางเทลเนต (telnet)
7. ทำการเปิดคอนเทนเนอร์โดยใช้คำสั่ง globus-start-container ที่เครื่อง apollo1 และ apollo10

8. ผู้ใช้ทำคำสั่ง grid-proxy-init เพื่อเป็นการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทน
9. ผู้ใช้ทำคำสั่ง cas-proxy-init เพื่อขอสิ่งอ้างสิทธิ ดังนี้

```
cas-proxy-init

–c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService

-s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas
```

10. เมื่อได้สิ่งอ้างสิทธิที่แนบมากับหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่ ซึ่งปกติจะเป็น /tmp/x509up_u{uid}.cas เช่น /tmp/x509up_u5561.cas จึงทำการทดสอบการเข้าใช้ทรัพยากรบนเครื่อง apollo10 ดังนี้

```
managed-job-globusrun -factory
http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService

-file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas
```

11. ทำการแก้ไขฐานข้อมูลซีเอเอสโดยแก้ให้ผู้ใช้ไม่มีสิทธิบน apollo10 ดังนี้

```
UPDATE policy_table SET action_specification = 25 where policy_id=2;
```

12. ทำตามข้อ9 อีกครั้งเพื่อสร้างสิ่งอ้างสิทธิอันใหม่โดยเปลี่ยน –t cas เป็น –t cas-notallow
13. ทดสอบสิทธิการเข้าใช้แกรมใหม่ดังนี้

```
managed-job-globusrun -factory
http://161.200.92.10:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file
$GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas-notallow
```

5.1.2 ผลการทดลอง

5.1.2.1 ผลของการทำคำสั่ง grid-proxy-init

เมื่อทำคำสั่ง grid-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนขึ้นมาใหม่คือแฟ้ม /tmp/x509up_u5561 ซึ่งเราสามารถดูรายละเอียดในแฟ้มได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561 –noout -text ซึ่งได้ผลดังรูปที่ 5.2

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 131801859 (0x7db2303)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521)
    Validity
      Not Before: Jan 18 04:38:46 2005 GMT
      Not After : Jan 18 16:43:46 2005 GMT
```

```
        Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:e1:08:29:be:ba:5f:99:47:af:03:7d:03:26:29:
                    97:ca:08:44:4d:48:f2:f1:92:09:f8:85:05:87:59:
                    5b:f4:89:2d:32:34:83:d1:d9:9b:18:bf:91:60:35:
                    db:5f:22:2e:7a:ab:e8:3a:ba:29:71:67:e6:c0:12:
                    5b:42:01:95:47
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.3536.1.222: critical
                0.0
..+.....
    Signature Algorithm: md5WithRSAEncryption
        9b:e4:8c:ee:c6:df:68:5b:56:ac:56:88:53:7e:f2:37:35:47:
        62:e5:03:62:28:96:1f:05:42:19:79:de:f9:bd:8f:c2:b6:13:
        ee:5a:2b:a5:cb:6f:6c:bd:b2:6d:f2:e1:76:8e:30:86:67:6c:
        87:38:1d:4a:cf:c8:96:c8:dd:9f:a3:49:8c:d7:90:bf:18:48:
        5b:20:47:b0:88:9e:40:4c:ed:5e:1b:f1:69:3a:ac:a7:d8:12:
        e6:60:03:2b:92:5d:2b:b7:6e:2c:c3:44:42:66:c2:82:7f:68:
        1d:43:ce:e4:c1:24:14:f9:90:cb:52:31:14:40:aa:40:cc:37:
        32:09
```

รูปที่ 5.2 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังทำคำสั่ง grid-proxy-init บนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

5.1.2.2 **ผลของการทำคำสั่ง** cas-proxy-init –c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas

เมื่อทำคำสั่ง cas-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนขึ้นมาใหม่คือ /tmp/x509up_u5561.cas ซึ่งเราสามารถดูรายละเอียดได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas –noout -text ซึ่งได้ผลดังรูปที่ 5.3

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 198649 (0x307f9)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859
        Validity
```

Not Before: Jan 18 05:28:10 2005 GMT

Not After : Jan 18 16:43:45 2005 GMT

Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859, CN=1374791765

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:a1:24:dc:f9:1b:35:5a:a1:ba:67:35:cd:c6:86:

e4:d5:f3:fd:7f:09:32:2d:3c:f4:5d:d8:7d:fe:0a:

94:94:6e:a8:2c:6f:f7:55:3d:51:dd:d6:2e:40:b3:

bd:c1:8c:39:c3:be:f1:3d:c9:8b:06:98:64:ec:95:

f3:37:8c:c8:67

Exponent: 65537 (0x10001)

X509v3 extensions:

1.3.6.1.4.1.3536.1.222: critical

0.0

..+.....

1.3.6.1.4.1.3536.1.1.1.99:

1

1.3.6.1.4.1.3536.1.1.1.9.1:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="e0ccf105-9878-4c1b-9168-ae30c08efdc4" IssueInstant="2005-01-18T07:34:07Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T07:34:07Z" NotOnOrAfter="2005-01-19T07:34:07Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

```
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>4Wiu3vcEbUVhsZDrfOO6GDP0lok=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
HuPswDw1eW4NRniedFcmbDU6EipIYkcD2rbZ9UiCF0/TlhYVDzqow4GxGocAKFBRQ5oBljzOWz5w
nIEw3QhEPqy6umS0IuuistFg9Wgn3oBKjLOzJQ4ULGCAMZaVxIljRjgaxH728SZbAIh4/Rpl7iy/
LTUv/fxLI1rUEDgVK6s=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIB6zCCAVQCAQQwDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1
bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDIwNDA4MTBaFw0xNDExMzAwNDA4MTBaMEkx
DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMSgwJgYDVQQDEx9jYXMvYXBvbGxvMTAuY3Au
ZW5nLmNodWxhLmFjLnRoMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKbvxw2FhR1awR+tmJ
li90IUIwK/YaTN4pCof6149RmcETYslrmHs+umWT26g8faF3ZHWTIoggX1J5RkbrrC9/097z8yaZ
NMhZnb1JQRS89T0E12IcAvnlmSB+LVHWS7h+8WT+gZlYJSMhq6Xzl9HdGYimNfNmBxR6/fojPtYQ
7wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHJtaMwxFJ4ZMuq5KOa4qmh0N+/z2E4z8FBqfKCVG/9f
tS5wgbPf3ja4ST7Zq/NLmIEiM2docXw6z95hi6kUmB6Q8DzzewrBNTijGt2SgIrc8SbM75tJ87xQ
WpquzY/ytj6vaL0hUiMN/lemSBSfpRkZul4R1bDCJg5y1zceFBlG
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></ds:Signature></Assertion>
   Signature Algorithm: md5WithRSAEncryption
      9d:f4:3c:89:02:99:8e:44:67:aa:99:11:8b:4d:52:7d:0f:43:
      53:52:1c:b4:e1:b3:07:8d:77:60:76:b4:52:30:82:a1:36:62:
      4c:64:76:dc:7a:91:fb:73:00:ae:e8:7e:d8:2c:83:24:26:83:
      7c:59:6b:dc:1b:f2:cc:83:70:f7
```


รูปที่ 5.3 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง cas-proxy-init บนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

5.1.2.3 **ผลของการทำคำสั่ง** managed-job-globusrun -factory http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง managed-job-globusrun งานของผู้ใช้ที่ระบุไว้ในแฟ้ม test.xml จะถูกทำงาน ซึ่งรายละเอียดของการทำงานเป็นไปดังรูปที่ 5.4 เมื่อทำงานเสร็จจะได้แฟ้มผลลัพธ์ที่ /home/casuser/stdout ซึ่งมีรายละเอียดดังรูปที่ 5.5 และเครื่องทรัพยากรจะพบแฟ้มลงบันทึกเข้าออก(log file) ชื่อ CasAssertionLog.txt ซึ่งมีรายละเอียดดังรูปที่ 5.6

```
WAITING FOR JOB TO FINISH
========== Status Notification ==========
Job Status: Active
=========================================
========== Status Notification ==========
Job Status: Done
=========================================
DESTROYING SERVICE
SERVICE DESTROYED
```

รูปที่ 5.4 แสดงรายละเอียดของการทำงานหลังจากเข้าไปใช้แกรมที่ทำการทดสอบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

```
12 abc 34 pdscaex_instr_GrADS_grads23_28919.cfg pgwynnel was here
```

รูปที่ 5.5 แสดงรายละเอียดของแฟ้มผลลัพธ์ที่ทำการทดสอบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

```
Assertion Validation : true
Used Date : Tue Jan 18 14:34:07 ICT 2005
user DN: /O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan Kongsirikul (4670359521)/CN=131801859/CN=1374791765
Issuer: /O=Grid/O=Chula/CN=Apollo CA
Assertion Issuer: /O=Grid/O=Chula/CN=Apollo CA
Local user: casuser
Decision : Permit
Resouce : /O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th
Namespace : host
Action : allow
```

รูปที่ 5.6 แสดงรายละเอียดของแฟ้มลงบันทึกเข้าออกที่ทำการทดสอบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

5.1.2.4 **ผลของการทำคำสั่ง** cas-proxy-init –c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas-notallow

เมื่อทำคำสั่ง cas-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนขึ้นมาใหม่คือ /tmp/x509up_u5561.cas-notallow ซึ่งเราสามารถดูรายละเอียดได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas-notallow –noout -text ซึ่งได้ผลลัพธ์ดังรูปที่ 5.7

```
Certificate:
```

Data:

Version: 3 (0x2)

Serial Number: 198649 (0x307f9)

Signature Algorithm: md5WithRSAEncryption

Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859

Validity

Not Before: Jan 18 7:30:07 2005 GMT

Not After : Jan 18 16:43:45 2005 GMT

Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859, CN=1374791765

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:a1:24:dc:f9:1b:35:5a:a1:ba:67:35:cd:c6:86:

e4:d5:f3:fd:7f:09:32:2d:3c:f4:5d:d8:7d:fe:0a:

94:94:6e:a8:2c:6f:f7:55:3d:51:dd:d6:2e:40:b3:

bd:c1:8c:39:c3:be:f1:3d:c9:8b:06:98:64:ec:95:

f3:37:8c:c8:67

Exponent: 65537 (0x10001)

X509v3 extensions:

1.3.6.1.4.1.3536.1.222: critical

0.0

..+.....

1.3.6.1.4.1.3536.1.1.1.99: 1

1.3.6.1.4.1.3536.1.1.1.9.1:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="e0ccf105-9878-4c1b-9168-ae30c08efdc4" IssueInstant="2005-01-18T07:34:07Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T07:34:07Z" NotOnOrAfter="2005-01-19T07:34:07Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">deny</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

```
</xfilter2b:XPath>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd
xsi"></ec:InclusiveNamespaces></ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>4Wiu3vcEbUVhsZDrfOO6GDP0lok=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
HuPswDw1eW4NRniedFcmbDU6EipIYkcD2rbZ9UiCF0/TlhYVDzqow4GxGocAKFBRQ5oBljzOWz5w
nIEw3QhEPqy6umS0IuuistFg9Wgn3oBKjLOzJQ4ULGCAMZaVxIljRjgaxH728SZbAIh4/Rpl7iy/
LTUv/fxLI1rUEDgVK6s=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIB6zCCAVQCAQQwDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1
bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDIwNDA4MTBaFw0xNDExMzAwNDA4MTBaMEkx
DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMSgwJgYDVQQDEx9jYXMvYXBvbGxvMTAuY3Au
li90IUIwK/YaTN4pCof6149RmcETYslrmHs+umWT26g8faF3ZHWTIoggX1J5RkbrrC9/097z8yaZ
NMhZnb1JQRS89T0E12IcAvnlmSB+LVHWS7h+8WT+gZlYJSMhq6Xzl9HdGYimNfNmBxR6/fojPtYQ
7wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHJtaMwxFJ4ZMuq5KOa4qmh0N+/z2E4z8FBqfKCVG/9f
tS5wgbPf3ja4ST7Zq/NLmIEiM2docXw6z95hi6kUmB6Q8DzzewrBNTijGt2SgIrc8SbM75tJ87xQ
WpquzY/ytj6vaL0hUiMN/lemSBSfpRkZul4R1bDCJg5y1zceFBlG
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></ds:Signature></Assertion>
   Signature Algorithm: md5WithRSAEncryption
      9d:f4:3c:89:02:99:8e:44:67:aa:99:11:8b:4d:52:7d:0f:43:
      53:52:1c:b4:e1:b3:07:8d:77:60:76:b4:52:30:82:a1:36:62:
      4c:64:76:dc:7a:91:fb:73:00:ae:e8:7e:d8:2c:83:24:26:83:
      7c:59:6b:dc:1b:f2:cc:83:70:f7
```


รูปที่ 5.7 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้หลังทำการแก้ไขฐานข้อมูลให้สิทธิเป็น deny แล้วทำการทดสอบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

5.1.2.5 **ผลของการทำคำสั่ง** managed-job-globusrun -factory http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas-notallow

เมื่อทำคำสั่ง managed-job-globusrun แล้วจีเอเอสพบว่าผู้ใช้ไม่มีสิทธิในการเข้าใช้แกรมตามสิ่งอ้างสิทธิ ก็จะส่งรายละเอียดของข้อผิดพลาดพร้อมทั้งปฏิเสธการใช้สิ่งอ้างสิทธิดังรูปที่5.8 โดยจะเปลี่ยนกลับไปพิจารณาสิทธิจากกริดแมปไฟล์เพียงอย่างเดียว ถ้าผู้ใช้สามารถเปลี่ยนเป็นชื่อเฉพาะที่ได้ก็จะสามารถทำงานได้ตามปกติดังรูปที่ 5.9

```
Permission deny in cas assertion ! Ignore cas assertion , use normal mode instead.
```

รูปที่ 5.8 แสดงรายละเอียดของข้อผิดพลาดที่ระบบแจ้งเตือนหลังเมื่อถูกปฏิเสธการใช้สิ่งอ้างสิทธิที่ทำการทดสอบบนสภาพแวดล้อมภายในองค์กรเสมือนเดียวกับผู้ใช้

```
WAITING FOR JOB TO FINISH
========== Status Notification ==========
Job Status: Active
=========================================
========== Status Notification ==========
Job Status: Done
=========================================
DESTROYING SERVICE
SERVICE DESTROYED
```

รูปที่ 5.9 แสดงรายละเอียดของการทำงานหลังจากเข้าไปใช้แกรมแล้วถูกปฏิเสธการใช้สิ่งอ้างสิทธิและพิจารณาสิทธิจากกริดแมปไฟล์เพียงอย่างเดียว

5.1.3 **วิเคราะห์ผลการทดลอง**

จากการทดลองดังกล่าวจะเห็นได้ว่าหลักฐานอ้างอิงตัวผู้ใช้ตัวแทนที่แนบสิ่งอ้างสิทธิที่ขอจากซีเอเอสภายในองค์กรเสมือนเดียวกันจะสามารถใช้กับทรัพยากรในองค์กรเสมือนเดียวกับผู้ใช้ได้ เมื่อเราติดตั้งจีเอเอสแล้วโดยจีเอเอสของทรัพยากรจะเป็นตัวตรวจสอบสิ่งอ้างสิทธิและหาสิทธิที่ตรงกับทรัพยากรนั้นๆ ถ้าเป็น allow จะสามารถทำงานได้ในนามของผู้ใช้เฉพาะที่ที่ตรงกับชื่อเฉพาะของผู้ออกสิ่งอ้างสิทธิแต่ถ้าเป็น deny จะไม่สนใจสิ่งอ้างสิทธิแล้วทำงานตามปกติต่อไป ซึ่งแสดงให้เห็นว่านอกจากจะทำงานภายในองค์กรเสมือนเดียวกันโดยพิจารณาการใช้งานจากสิ่งอ้างสิทธิได้แล้ว ยังสามารถนำหลักฐานอ้างอิงผู้ใช้ตัวแทนที่ไม่มีสิ่งอ้างสิทธิมาใช้งานกับทรัพยากรที่มีจีเอเอสได้ด้วย

5.2 การทดสอบระบบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองเชื่อถือกันโดยตรง

5.2.1 วิธีการทดลอง

1. เลือกเครื่องที่จะมาทำการทดสอบดังนี้
    a. เครื่อง apollo11.cp.eng.chula.ac.th สำหรับทำเป็นไคลเอนท์ที่จะใช้ทดสอบอยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้
    b. เครื่อง apollo1.cp.eng.chula.ac.th สำหรับเป็นซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้
    c. เครื่อง apollo10.cp.eng.chula.ac.th สำหรับเป็นเครื่องทรัพยากรที่อยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้
    d. เครื่อง test1.cp.eng.chula.ac.th สำหรับเป็นซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในอีกองค์กรเสมือน
    e. เครื่อง test2.cp.eng.chula.ac.th สำหรับเป็นเครื่องทรัพยากรที่อยู่ภายในอีกองค์กรเสมือน
2. ติดตั้งโกลบัสทูลคิดรุ่น 3.2.1 บนเครื่องทั้งห้าเครื่องพร้อมทั้งทำ grid-cert-request เพื่อขอ คำร้องขอหลักฐานอ้างอิงโฮสท์และ นำคำร้องขอหลักฐานอ้างอิงโฮสท์ของทั้งสามเครื่องไปขอหลักฐานอ้างอิงโฮสท์จากผู้ออกหลักฐานอ้างอิงเดียวกับผู้ออกหลักฐานอ้างอิงให้ผู้ใช้ของผู้ที่จะทำการทดสอบ และนำคำร้องขอหลักฐานอ้างอิงโฮสท์ของอีกสองเครื่องที่อยู่คนละองค์กรเสมือนกับผู้ใช้ไปขอหลักฐานอ้างอิงโฮสท์จากผู้ออกหลักฐานอ้างอิงอื่น แล้วนำหลักฐานอ้างอิงกับนโยบายการออกหลักฐานอ้างอิง(signing policy) ของทุกผู้ออกหลักฐานอ้างอิงไว้ใน /etd/grid-security/certificates/ ของทั้ง 5 เครื่องเพื่อสร้างสภาพแวดล้อมที่สององค์กรเสมือนเชื่อถือกันกันโดยตรง
3. ติดตั้งจีเอเอสบนเครื่องทั้งห้าเครื่อง
4. ทำการแก้ไขระบบให้สามารถใช้งานซีเอเอสได้ตามปกติ (ทำตามขั้นตอนในเวปไซต์ http://www-unix.globus.org/toolkit/docs/3.2/installation/install_config_cas.html) บนเครื่องซีเอเอสเซอร์ฟเวอร์ของทั้งสององค์กรเสมือน
5. ทำการเพิ่มข้อมูลเข้าไปในฐานข้อมูลของซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้ และฐานข้อมูลของซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในองค์กรเสมือนอื่น
6. ผู้ใช้ทำการทดสอบโดยเข้าไปยังเครื่องไคลเอนท์ผ่านทางเทลเนต

7. ทำการเปิดคอนเทนเนอร์โดยใช้คำสั่ง globus-start-container ที่เครื่อง apollo1, apollo10, test1 และ test2
8. ผู้ใช้ทำคำสั่ง grid-proxy-init เพื่อเป็นการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทน
9. ผู้ใช้ทำคำสั่ง cas-proxy-init เพื่อขอสิ่งอ้างสิทธิดังนี้

```
cas-proxy-init
–c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService
-s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas
```

10. เมื่อได้สิ่งอ้างสิทธิที่แนบมากับหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่ ซึ่งปกติจะเป็น /tmp/x509up_u{uid}.cas เช่น /tmp/x509up_u5561.cas จะนำไปขอสิ่งอ้างสิทธิจาก test1 ซึ่งเป็นซีเอเอสเซอร์ฟเวอร์ของอีกองค์กรเสมือน เพื่อทำการทดสอบการใช้งานในอีกองค์กรเสมือนดังนี้

```
cas-passport-init –c http://test1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService
-s /O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th
–p /tmp/x509up_u5561.cas
```

11. หลังจากนั้นจึงทำการทดสอบการเข้าใช้ทรัพยากรบนเครื่อง test2 ดังนี้

```
managed-job-globusrun -factory
http://test2.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService
-file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas
```

12. หลังจากนั้นจึงทำการทดสอบการเข้าใช้ทรัพยากรบนเครื่อง apollo10 เพื่อทดสอบหลักฐานอ้างอิงผู้ใช้ตัวแทนใบใหม่ที่มีสิ่งอ้างสิทธิขององค์กรเสมือนอื่นรวมอยู่ด้วยดังนี้

```
managed-job-globusrun -factory
http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService
-file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas
```

13. ทำการแก้ไขฐานข้อมูลซีเอเอสโดยแก้ให้ผู้ใช้ไม่มีสิทธิขอสิ่งอ้างสิทธิกับ test1 ดังนี้

```
UPDATE policy_table SET action_specification = 27 where policy_id=3;
```

14. ทำตามข้อ9 อีกครั้งเพื่อสร้างสิ่งอ้างสิทธิอันใหม่โดยเปลี่ยน –t cas เป็น –t cas-assertion-notallow
15. ทำตามข้อ 11 อีกครั้งเพื่อขอสิ่งอ้างสิทธิกับ test1 โดยเปลี่ยน x509up_u5561.cas เป็น x509up_u5561.cas-assertion-notallow

5.2.2 ผลการทดลอง

5.2.2.1 ผลของการทำ grid-proxy-init

เมื่อรันคำสั่ง grid-proxy-init จะได้แฟ้ม proxy certificate ขึ้นมาใหม่คือ /tmp/x509up_u5561 ซึ่งมีรายละเอียดดังรูปที่ 5.10

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 131801859 (0x7db2303)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521)
        Validity
            Not Before: Jan 18 04:38:46 2005 GMT
            Not After : Jan 18 16:43:46 2005 GMT
        Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:e1:08:29:be:ba:5f:99:47:af:03:7d:03:26:29:
                    97:ca:08:44:4d:48:f2:f1:92:09:f8:85:05:87:59:
                    5b:f4:89:2d:32:34:83:d1:d9:9b:18:bf:91:60:35:
                    db:5f:22:2e:7a:ab:e8:3a:ba:29:71:67:e6:c0:12:
                    5b:42:01:95:47
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.3536.1.222: critical
                0.0
..+.....
    Signature Algorithm: md5WithRSAEncryption
        9b:e4:8c:ee:c6:df:68:5b:56:ac:56:88:53:7e:f2:37:35:47:
        62:e5:03:62:28:96:1f:05:42:19:79:de:f9:bd:8f:c2:b6:13:
        ee:5a:2b:a5:cb:6f:6c:bd:b2:6d:f2:e1:76:8e:30:86:67:6c:
        87:38:1d:4a:cf:c8:96:c8:dd:9f:a3:49:8c:d7:90:bf:18:48:
        5b:20:47:b0:88:9e:40:4c:ed:5e:1b:f1:69:3a:ac:a7:d8:12:
        e6:60:03:2b:92:5d:2b:b7:6e:2c:c3:44:42:66:c2:82:7f:68:
        1d:43:ce:e4:c1:24:14:f9:90:cb:52:31:14:40:aa:40:cc:37:
        32:09
```

รูปที่ 5.10 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง grid-proxy-init

สำหรับการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง

5.2.2.2 **ผลของการทำคำสั่ง** cas-proxy-init –c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas

เมื่อทำคำสั่ง cas-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนขึ้นมาใหม่คือ /tmp/x509up_u5561.cas ซึ่งเราสามารถดูรายละเอียดได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas –noout -text ซึ่งได้ผลดังรูปที่ 5.11

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 198649 (0x307f9)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859
      Validity
         Not Before: Jan 18 7:28:10 2005 GMT
         Not After : Jan 18 16:43:45 2005 GMT
      Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859,
CN=1374791765
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (512 bit)
            Modulus (512 bit):
               00:a1:24:dc:f9:1b:35:5a:a1:ba:67:35:cd:c6:86:
               e4:d5:f3:fd:7f:09:32:2d:3c:f4:5d:d8:7d:fe:0a:
               94:94:6e:a8:2c:6f:f7:55:3d:51:dd:d6:2e:40:b3:
               bd:c1:8c:39:c3:be:f1:3d:c9:8b:06:98:64:ec:95:
               f3:37:8c:c8:67
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         1.3.6.1.4.1.3536.1.222: critical
            0.0
..+.....
         1.3.6.1.4.1.3536.1.1.1.99:
            1
         1.3.6.1.4.1.3536.1.1.1.9.1:
            <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="ac5c196a-dbc0-4f6e-8a6a-
5c123911333d" IssueInstant="2005-01-18T07:33:09Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1"
MinorVersion="0"><Conditions NotBefore="2005-01-18T07:33:09Z" NotOnOrAfter="2005-01-
19T07:33:09Z"></Conditions><AuthorizationDecisionStatement Decision="Permit"
Resource="/O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th"><Subject><NameIdentifier
Format="#X509SubjectName" NameQualifier="O=Grid,O=Chula,OU=cp.eng.chula.ac.th,CN=Patipan Kongsirikul
(4670359521)">/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan Kongsirikul
(4670359521)</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509
-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action
```

Namespace="cas">allow</Action></AuthorizationDecisionStatement><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>jyWfi0Ccucsu0/UnjxnPPIMcN6M=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

swxKmqYIDfgC4oQv36VAEYd9FefLrFX1sOXxPtL0phpWn8jyS1W2Befcbs09p59fx3L4iZXWa8Ra

LiLmpaBa2gCi3nb6DEEagdJTD8AlwDs5C77jzU8TMe0kmFe1DXl3dNz3jm1FaIIK+irtXBvMmih6

oB/YZg/+sjYR/hjtL6A=

</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>

MIIB6jCCAVMCAQ8wDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1

bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDcwNzQzNDFaFw0xNDEyMDUwNzQzNDFaMEgx

DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMScwJQYDVQQDEx5jYXMvYXBvbGxvMS5jcC5l

bmcuY2h1bGEuYWMudGgwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMk/Tn+Pip6IsmfgVTI3

e7B2neXVMpe/LtjO/JN1+2PNurWpi7O0O89To8yDPnEllodfO5qXAZGLiXubXq20Dv7qJXEbFQJs

2oR038m3OvroLGZ/3PftY6khDmlLO02J0nvtvjfbecSVSxkAcPcPTTBQtzc2pbMHBisUDt+q71Gz

AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAFacTxqa2LZSNnnq6DvoK+w9dYteJqFaV+kg/zKAr2v7z

sJT6ysttun58HM1XCBEmwmWCRenUWykhJ75ugCnLqJeQ6uG8P2acNB0pN4i3TLjQ5r3Kflt8FF6z

ipc6IeQjlRjqfolX01o73MldEZrWNusslWrTTZMN945I5A+KzSk=

</ds:X509Certificate>

</ds:X509Data>

```
</ds:KeyInfo></ds:Signature></Assertion>
   Signature Algorithm: md5WithRSAEncryption
      9d:f4:3c:89:02:99:8e:44:67:aa:99:11:8b:4d:52:7d:0f:43:
      53:52:1c:b4:e1:b3:07:8d:77:60:76:b4:52:30:82:a1:36:62:
      4c:64:76:dc:7a:91:fb:73:00:ae:e8:7e:d8:2c:83:24:26:83:
      7c:59:6b:dc:1b:f2:cc:83:70:f7
```

รูปที่ 5.11 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง cas-proxy-init ที่ทำการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง

5.2.2.3 **ผลของการทำคำสั่ง** cas-passport-init –c http://test1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th –p /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง cas-passport-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนที่มีสิ่งอ้างสิทธิของอีกองค์กรเสมือนขึ้นมาใหม่คือแฟ้มที่เราตามหลัง –p ซึ่งเราสามารถดูรายละเอียดได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas –noout -text ซึ่งได้ผลดังรูปที่ 5.12

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 385707 (0x5e2ab)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859,
CN=1374791765
      Validity
         Not Before: Jan 18 10:33:08 2005 GMT
         Not After : Jan 18 16:43:44 2005 GMT
      Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859,
CN=1374791765, CN=736618254
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (512 bit)
            Modulus (512 bit):
               00:ad:b6:94:54:5e:fe:4c:40:73:50:9c:33:b8:31:
               52:75:91:ce:2f:0c:e6:17:cf:3e:4d:27:30:23:60:
               5b:6b:90:0c:6f:a2:e2:1a:b3:98:40:d6:61:da:04:
               a4:90:6d:bd:7f:90:31:1b:f6:d7:1a:fb:dc:64:22:
               30:aa:7a:2b:5f
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         1.3.6.1.4.1.3536.1.222: critical
            0.0
..+.....
```

1.3.6.1.4.1.3536.1.1.1.99:

2

1.3.6.1.4.1.3536.1.1.1.9.2:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="e0ccf105-9878-4c1b-9168-ae30c08efdc4" IssueInstant="2005-01-18T07:34:07Z" Issuer="O=Grid,O=Chula,CN=Test CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T10:34:07Z" NotOnOrAfter="2005-01-19T10:34:07Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>4Wiu3vcEbUVhsZDrfOO6GDP0lok=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

HuPswDw1eW4NRniedFcmbDU6EipIYkcD2rbZ9UiCF0/TlhYVDzqow4GxGocAKFBRQ5oBljzOWz5w

nIEw3QhEPqy6umS0IuuistFg9Wgn3oBKjLOzJQ4ULGCAMZaVxIljRjgaxH728SZbAIh4/Rpl7iy/

LTUv/fxLI1rUEDgVK6s=

</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>

MIIB6zCCAVQCAQQwDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1

bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDIwNDA4MTBaFw0xNDExMzAwNDA4MTBaMEkx

DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMSgwJgYDVQQDEx9jYXMvYXBvbGxvMTAuY3Au

ZW5nLmNodWxhLmFjLnRoMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKbvxw2FhR1awR+tmJ

li90IUIwK/YaTN4pCof6149RmcETYslrmHs+umWT26g8faF3ZHWTIoggX1J5RkbrrC9/097z8yaZ

NMhZnb1JQRS89T0E12IcAvnlmSB+LVHWS7h+8WT+gZlYJSMhq6Xzl9HdGYimNfNmBxR6/fojPtYQ

7wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHJtaMwxFJ4ZMuq5KOa4qmh0N+/z2E4z8FBqfKCVG/9f

tS5wgbPf3ja4ST7Zq/NLmIEiM2docXw6z95hi6kUmB6Q8DzzewrBNTijGt2SgIrc8SbM75tJ87xQ

WpquzY/ytj6vaL0hUiMN/lemSBSfpRkZul4R1bDCJg5y1zceFBlG

</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo></ds:Signature></Assertion>

1.3.6.1.4.1.3536.1.1.1.9.1:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="ac5c196a-dbc0-4f6e-8a6a-5c123911333d" IssueInstant="2005-01-18T07:33:09Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T07:33:09Z" NotOnOrAfter="2005-01-19T07:33:09Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="O=Grid,O=Chula,OU=cp.eng.chula.ac.th,CN=Patipan Kongsirikul (4670359521)">/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan Kongsirikul (4670359521)</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="cas">allow</Action></AuthorizationDecisionStatement><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>jyWfi0Ccucsu0/UnjxnPPIMcN6M=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

swxKmqYIDfgC4oQv36VAEYd9FefLrFX1sOXxPtL0phpWn8jyS1W2Befcbs09p59fx3L4iZXWa8Ra

LiLmpaBa2gCi3nb6DEEagdJTD8AlwDs5C77jzU8TMe0kmFe1DXl3dNz3jm1FaIIK+irtXBvMmih6

oB/YZg/+sjYR/hjtL6A=

</ds:SignatureValue>

<ds:KeyInfo>

```
<ds:X509Data>
<ds:X509Certificate>
MIIB6jCCAVMCAQ8wDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1
bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDcwNzQzNDFaFw0xNDEyMDUwNzQzNDFaMEgx
DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMScwJQYDVQQDEx5jYXMvYXBvbGxvMS5jcC5l
bmcuY2h1bGEuYWMudGgwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMk/Tn+Pip6IsmfgVTI3
e7B2neXVMpe/LtjO/JN1+2PNurWpi7O0O89To8yDPnEIlodfO5qXAZGLiXubXq20Dv7qJXEbFQJs
2oR038m3OvroLGZ/3PftY6khDmlLO02J0nvtvjfbecSVSxkAcPcPTTBQtzc2pbMHBisUDt+q71Gz
AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAFacTxqa2LZSNnnq6DvoK+w9dYteJqFaV+kg/zKAr2v7z
sJT6ysttun58HM1XCBEmwmWCRenUWykhJ75ugCnLqJeQ6uG8P2acNB0pN4i3TLjQ5r3Kflt8FF6z
ipc6IeQjlRjqfolX01o73MldEZrWNusslWrTTZMN945I5A+KzSk=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></ds:Signature></Assertion>
   Signature Algorithm: md5WithRSAEncryption
      85:51:eb:57:51:d8:ee:4e:8f:aa:7d:51:e4:c0:b4:57:5f:b9:
      2d:df:d3:d4:72:c0:26:91:88:2d:26:b9:43:84:ab:74:31:af:
      ba:32:99:02:82:78:cd:ac:17:5b:97:8d:ce:7a:72:31:11:fa:
      e5:b4:d2:e9:c7:ce:10:6c:bf:1d
```

รูปที่ 5.12 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง cas-passport-init ที่ทำการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง

5.2.2.4 **ผลของการทำคำสั่ง** managed-job-globusrun -factory http://test2.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง managed-job-globusrun งานของผู้ใช้ที่ระบุไว้ในแฟ้ม test.xml จะถูกทำงานบนทรัพยากรขององค์กรเสมือนอื่น ซึ่งรายละเอียดของการทำงานเป็นไปดังรูปที่ 5.13

```
WAITING FOR JOB TO FINISH
========== Status Notification ==========
Job Status: Active
=========================================
========== Status Notification ==========
Job Status: Done
=========================================
DESTROYING SERVICE
SERVICE DESTROYED
```

รูปที่ 5.13 แสดงผลการทดลองหลังจากเข้าไปใช้แกรมขององค์กรเสมือนอื่นโดยทำการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง

5.2.2.5 **ผลของการทำคำสั่ง** managed-job-globusrun -factory http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง managed-job-globusrun งานของผู้ใช้ที่ระบุไว้ในแฟ้ม test.xml จะถูกทำงานบนทรัพยากรขององค์กรเสมือนเดียวกับผู้ใช้ ซึ่งรายละเอียดของการทำงานเป็นไปดังรูปที่ 5.14

```
WAITING FOR JOB TO FINISH
========== Status Notification ==========
Job Status: Active
=========================================
========== Status Notification ==========
Job Status: Done
=========================================
DESTROYING SERVICE
SERVICE DESTROYED
```

รูปที่ 5.14 แสดงผลการทดลองหลังจากเข้าไปใช้แกรมขององค์กรเสมือนเดียวกับผู้ใช้โดยทำการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง

5.2.2.6 **ผลของการทำคำสั่ง** cas-proxy-init –c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas-notallow

เมื่อทำคำสั่ง cas-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ขึ้นมาใหม่คือแฟ้ม /tmp/x509up_u5561.cas-notallow ซึ่งเราสามารถดูรายละเอียดได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas-notallow –noout -text ซึ่งได้ผลดังรูปที่ 5.15

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 198649 (0x307f9)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859
    Validity
      Not Before: Jan 18 11:28:10 2005 GMT
      Not After : Jan 18 16:43:45 2005 GMT
    Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859,
CN=1374791765
    Subject Public Key Info:
```

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:a1:24:dc:f9:1b:35:5a:a1:ba:67:35:cd:c6:86:

e4:d5:f3:fd:7f:09:32:2d:3c:f4:5d:d8:7d:fe:0a:

94:94:6e:a8:2c:6f:f7:55:3d:51:dd:d6:2e:40:b3:

bd:c1:8c:39:c3:be:f1:3d:c9:8b:06:98:64:ec:95:

f3:37:8c:c8:67

Exponent: 65537 (0x10001)

X509v3 extensions:

1.3.6.1.4.1.3536.1.222: critical

0.0

..+.....

1.3.6.1.4.1.3536.1.1.1.99:

1

1.3.6.1.4.1.3536.1.1.1.9.1:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="ac5c196a-dbc0-4f6e-8a6a-5c123911333d" IssueInstant="2005-01-18T11:33:09Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T11:33:09Z" NotOnOrAfter="2005-01-19T07:33:09Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="O=Grid,O=Chula,OU=cp.eng.chula.ac.th,CN=Patipan Kongsirikul (4670359521)">/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan Kongsirikul (4670359521)</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="cas">deny</Action></AuthorizationDecisionStatement><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

```
<ds:DigestValue>jyWfi0Ccucsu0/UnjxnPPIMcN6M=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
swxKmqYIDfgC4oQv36VAEYd9FefLrFX1sOXxPtL0phpWn8jyS1W2Befcbs09p59fx3L4iZXWa8Ra
LiLmpaBa2gCi3nb6DEEagdJTD8AlwDs5C77jzU8TMe0kmFe1DXl3dNz3jm1FaIIK+irtXBvMmih6
oB/YZg/+sjYR/hjtL6A=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIB6jCCAVMCAQ8wDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1
bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDcwNzQzNDFaFw0xNDEyMDUwNzQzNDFaMEgx
DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMScwJQYDVQQDEx5jYXMvYXBvbGxvMS5jcC5l
bmcuY2h1bGEuYWMudGgwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMk/Tn+Pip6IsmfgVTI3
e7B2neXVMpe/LtjO/JN1+2PNurWpi7O0O89To8yDPnEIIodfO5qXAZGLiXubXq20Dv7qJXEbFQJs
2oR038m3OvroLGZ/3PftY6khDmlLO02J0nvtvjfbecSVSxkAcPcPTTBQtzc2pbMHBisUDt+q71Gz
AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAFacTxqa2LZSNnnq6DvoK+w9dYteJqFaV+kg/zKAr2v7z
sJT6ysttun58HM1XCBEmwmWCRenUWykhJ75ugCnLqJeQ6uG8P2acNB0pN4i3TLjQ5r3Kflt8FF6z
ipc6IeQjlRjqfolX01o73MldEZrWNusslWrTTZMN945I5A+KzSk=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></ds:Signature></Assertion>
   Signature Algorithm: md5WithRSAEncryption
      9d:f4:3c:89:02:99:8e:44:67:aa:99:11:8b:4d:52:7d:0f:43:
      53:52:1c:b4:e1:b3:07:8d:77:60:76:b4:52:30:82:a1:36:62:
      4c:64:76:dc:7a:91:fb:73:00:ae:e8:7e:d8:2c:83:24:26:83:
      7c:59:6b:dc:1b:f2:cc:83:70:f7
```


รูปที่ 5.15 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้หลังทำการแก้ไขฐานข้อมูลให้สิทธิเป็น deny สำหรับติดต่อกับ test1

5.2.2.7 **ผลของการทำคำสั่ง** cas-passport-init –c http://test1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th –p /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง cas-passport-init จะพบรายงานความผิดพลาดเนื่องจากผู้ใช้ไม่มีสิทธิขอสิ่งอ้างสิทธิกับ test1 ซึ่งเป็นซีเอเอสเซอร์ฟเวอร์ของอีกองค์กรเสมือนดังรูปที่ 5.16

```
Error: Permission deny in cas assertion !: Can't delegated cas assertion embedded in proxy certificate
```

รูปที่ 5.16 แสดงรายงานความผิดพลาดเมื่อผู้ใช้ไม่มีสิทธิติดต่อกับซีเอเอสขององค์กรเสมือนอื่นหลังการทำคำสั่ง cas-passport-init

5.2.3 วิเคราะห์ผลการทดลอง

จากผลการทดลองนี้จะเห็นได้ว่าสิทธิของผู้ใช้ในแต่ละองค์กรเสมือนจะอยู่ในสิ่งอ้างสิทธิในส่วนขยายของหลักฐานอ้างอิงผู้ใช้ต่อไปเรื่อย โดยทรัพยากรจะพิจารณาเฉพาะสิ่งอ้างอิงสิทธิที่เกี่ยวกับทรัพยากรเอง และจากการนำหลักฐานอ้างอิงผู้ใช้ตัวแทนซึ่งได้จาก cas-passport-init ไปใช้ภายในองค์กรเสมือนเดียวกับผู้ใช้และต่างองค์กรเสมือน ปรากฏว่าสามารถใช้งานได้อย่างถูกต้องตามที่ได้ออกแบบไว้ กล่าวคือผู้ใช้ต้องการไปใช้ที่องค์กรเสมือนไหนก็ติดต่อไปยังซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนนั้นก่อน โดยจะได้สิ่งอ้างอิงสิทธิเพิ่มขึ้นมาเหมือนกับแนวคิดการทำหนังสือเดินทาง

5.3 การทดสอบระบบบนสภาพแวดล้อมที่องค์กรเสมือนไม่มีความเชื่อถือกันโดยตรงแต่จะเชื่อถือตัวกลางร่วมกัน

5.3.1 วิธีการทดลอง

1. เลือกเครื่องที่จะมาทำการทดสอบดังนี้
    a. เครื่อง apollo11.cp.eng.chula.ac.th สำหรับทำเป็นไคลเอนท์ที่จะใช้ทดสอบอยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้
    b. เครื่อง apollo1.cp.eng.chula.ac.th สำหรับเป็นซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้ และมีความเชื่อถือกับ test1.cp.eng.chula.ac.th
    c. เครื่อง apollo10.cp.eng.chula.ac.th สำหรับเป็นเครื่องทรัพยากรที่อยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้
    d. เครื่อง test1.cp.eng.chula.ac.th สำหรับเป็นซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในอีกองค์กรเสมือนและมีความเชื่อถือกับ apollo1.cp.eng.chula.ac.th
    e. เครื่อง test2.cp.eng.chula.ac.th สำหรับเป็นเครื่องทรัพยากรที่อยู่ภายในอีกองค์กรเสมือน
2. ติดตั้งโกลบัสทูลคิดรุ่น 3.2.1 บนเครื่องทั้งห้าเครื่องพร้อมทั้งทำคำสั่ง grid-cert-request เพื่อขอคำร้องขอหลักฐานอ้างอิงโฮสท์และสร้างหลักฐานอ้างอิงโฮสท์ของแต่ละเครื่องดังนี้
    a. เครื่อง apollo10 และ apollo11 นำคำร้องขอหลักฐานอ้างอิงโฮสท์ไปให้ผู้ออกหลักฐานอ้างอิงตัวที่ 1 (bf89f2c8.0) เป็นผู้ออกหลักฐานอ้างอิงโฮสท์ให้
    b. เครื่อง apollo1 นำคำร้องขอหลักฐานอ้างอิงโฮสท์ไปให้ผู้ออกหลักฐานอ้างอิงตัวที่ 2 (039b7acf.0) เป็นผู้ออกหลักฐานอ้างอิงโฮสท์ให้

c. เครื่อง test1 นำคำร้องขอหลักฐานอ้างอิงโฮสท์ไปให้ผู้ออกหลักฐานอ้างอิงตัวที่ 3 (8d37f301.0) เป็นผู้ออกหลักฐานอ้างอิงโฮสท์ให้
d. เครื่อง test2 นำคำร้องขอหลักฐานอ้างอิงโฮสท์ไปให้ผู้ออกหลักฐานอ้างอิงตัวที่ 4 (411204bc.0)เป็นผู้ออกหลักฐานอ้างอิงโฮสท์ให้
e. ทำสำเนาแฟ้ม bf89f2c8.0, bf89f2c8.signing_policy, 039b7acf.0 และ 039b7acf.signing_policy ไปยังเครื่อง apollo10 และ apollo11 ใน /etc/grid-security/certificates
f. ทำสำเนาแฟ้ม 411204bc.0, 411204bc.signing_policy, 8d37f301.0 และ 8d37f301.signing_policyไปยัง test2 ใน /etc/grid-security/certificates
g. ทำสำเนาแฟ้ม 039b7acf.0, 039b7acf.signing_policy, 8d37f301.0, 8d37f301.signing_policy, 411204bc.0 และ 411204bc.signing_policyไปยัง test1 ใน /etc/grid-security/certificates
h. ทำสำเนาแฟ้ม 039b7acf.0, 039b7acf.signing_policy, 8d37f301.0, 8d37f301.signing_policy, bf89f2c8.0 และ bf89f2c8.signing_policy ไปยัง apollo1 ใน /etc/grid-security/certificates

3. ติดตั้งจีเอเอสบนเครื่องทั้งห้าเครื่อง
4. ทำการแก้ไขระบบให้สามารถใช้งานซีเอเอสได้ตามปกติ (ทำตามขั้นตอนในเวปไซต์ http://www-unix.globus.org/toolkit/docs/3.2/installation/ install_config_cas.html) บนเครื่อง cas server ทั้งสององค์กรเสมือน
5. ทำการเพิ่มข้อมูลเข้าไปในฐานข้อมูลของซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในองค์กรเสมือนเดียวกับผู้ใช้ และฐานข้อมูลของซีเอเอสเซอร์ฟเวอร์ที่อยู่ภายในองค์กรเสมือนอื่น
6. ผู้ใช้ทำการทดสอบโดยเข้าไปยังเครื่องไคลเอนท์ผ่านทางเทลเนต
7. ทำการเปิดคอนเทนเนอร์โดยใช้คำสั่ง globus-start-container ที่เครื่อง apollo1, apollo10, test1 และ test2
8. ผู้ใช้ทำคำสั่ง grid-proxy-init เพื่อเป็นการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทน
9. ผู้ใช้ทำคำสั่ง cas-proxy-renew เพื่อขอสิ่งอ้างสิทธิดังนี้

```
cas-proxy-renew –c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService

-s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas
```

10. เมื่อได้สิ่งอ้างสิทธิที่แนบมากับหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่ ซึ่งปกติจะเป็นแฟ้ม /tmp/x509up_u{uid}.cas เช่น /tmp/x509up_u5561.cas จะนำไปขอสิ่งอ้างสิทธิ จาก test1

ซึ่งเป็นซีเอเอสเซอร์ฟเวอร์ของอีกองค์กรเสมือน เพื่อทำการทดสอบการใช้งานในอีกองค์กรเสมือน ดังนี้

```
cas-proxy-renew –c http://test1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService
-s /O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th –p /tmp/x509up_u5561.cas
```

11. หลังจากนั้นจึงทำการทดสอบการเข้าใช้ทรัพยากรบนเครื่อง test2 ดังนี้

```
managed-job-globusrun -factory
http://test2.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService
-file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas
```

12. หลังจากนั้นจึงทำการทดสอบการเข้าใช้ทรัพยากรบนเครื่อง apollo10 เพื่อทดสอบหลักฐานอ้างอิงผู้ใช้ใบใหม่ที่มีสิ่งอ้างสิทธิขององค์กรเสมือนอื่นรวมอยู่ด้วยดังนี้

```
managed-job-globusrun -factory
http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -
file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas
```

5.3.2 ผลการทดลอง

5.3.2.1 ผลของการทำคำสั่ง grid-proxy-init

เมื่อทำคำสั่ง grid-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนขึ้นมาใหม่คือ /tmp/x509up_u5561 ซึ่งเราสามารถดูรายละเอียดในแฟ้มได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561 –noout -text ซึ่งได้ผลดังรูปที่ 5.17

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 131801859 (0x7db2303)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521)
    Validity
      Not Before: Jan 18 04:38:46 2005 GMT
      Not After : Jan 18 16:43:46 2005 GMT
    Subject: O=Grid, O=Chula, OU=cp.eng.chula.ac.th, CN=Patipan Kongsirikul (4670359521), CN=131801859
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
        Modulus (512 bit):
          00:e1:08:29:be:ba:5f:99:47:af:03:7d:03:26:29:
          97:ca:08:44:4d:48:f2:f1:92:09:f8:85:05:87:59:
```

```
                5b:f4:89:2d:32:34:83:d1:d9:9b:18:bf:91:60:35:
                db:5f:22:2e:7a:ab:e8:3a:ba:29:71:67:e6:c0:12:
                5b:42:01:95:47
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.3536.1.222: critical
                0.0
..+.....
    Signature Algorithm: md5WithRSAEncryption
        9b:e4:8c:ee:c6:df:68:5b:56:ac:56:88:53:7e:f2:37:35:47:
        62:e5:03:62:28:96:1f:05:42:19:79:de:f9:bd:8f:c2:b6:13:
        ee:5a:2b:a5:cb:6f:6c:bd:b2:6d:f2:e1:76:8e:30:86:67:6c:
        87:38:1d:4a:cf:c8:96:c8:dd:9f:a3:49:8c:d7:90:bf:18:48:
        5b:20:47:b0:88:9e:40:4c:ed:5e:1b:f1:69:3a:ac:a7:d8:12:
        e6:60:03:2b:92:5d:2b:b7:6e:2c:c3:44:42:66:c2:82:7f:68:
        1d:43:ce:e4:c1:24:14:f9:90:cb:52:31:14:40:aa:40:cc:37:
        32:09
```

รูปที่ 5.17 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง grid-proxy-init ที่ทำการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนไม่เชื่อถือกันโดยตรงแต่เชื่อถือกันผ่านตัวแทน

5.3.2.2 **ผลของการทำคำสั่ง** cas-proxy-renew –c http://apollo1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/apollo1.cp.eng.chula.ac.th –t cas

เมื่อทำคำสั่ง cas-proxy-init จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ขึ้นมาใหม่คือ /tmp/x509up_u5561.cas ซึ่งเราสามารถดูรายละเอียดในแฟ้มได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas –noout -text ซึ่งได้ผลดังรูปที่ 5.18

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 395116 (0x6076c)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: O=Grid, O=Chula, CN=cas/apollo1.cp.eng.chula.ac.th
        Validity
            Not Before: Jan 18 06:59:22 2005 GMT
            Not After : Jan 18 17:04:22 2005 GMT
        Subject: O=Grid, O=Chula, CN=cas/apollo1.cp.eng.chula.ac.th, CN=1404201924
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
```

00:a1:de:17:7f:e5:a3:33:a3:1d:af:90:98:25:2b:

96:e9:09:db:db:ba:00:c1:89:34:27:9b:c9:a0:f9:

b7:a0:3d:c1:33:a2:31:0c:e3:1b:bb:4b:06:a2:22:

7f:81:f0:00:a9:f2:47:8c:ad:95:06:52:2a:43:8f:

d1:94:df:88:0f

Exponent: 65537 (0x10001)

X509v3 extensions:

1.3.6.1.4.1.3536.1.222: critical

0.0

..+.....

1.3.6.1.4.1.3536.1.1.1.99:

1

1.3.6.1.4.1.3536.1.1.1.9.1:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="ac5c196a-dbc0-4f6e-8a6a-5c123911333d" IssueInstant="2005-01-18T07:33:09Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T07:33:09Z" NotOnOrAfter="2005-01-19T07:33:09Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="O=Grid,O=Chula,OU=cp.eng.chula.ac.th,CN=Patipan Kongsirikul (4670359521)">/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan Kongsirikul (4670359521)</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="cas">allow</Action></AuthorizationDecisionStatement><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>jyWfi0Ccucsu0/UnjxnPPIMcN6M=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

```
<ds:SignatureValue>
swxKmqYIDfgC4oQv36VAEYd9FefLrFX1sOXxPtL0phpWn8jyS1W2Befcbs09p59fx3L4iZXWa8Ra
LiLmpaBa2gCi3nb6DEEagdJTD8AlwDs5C77jzU8TMe0kmFe1DXl3dNz3jm1FaIIK+irtXBvMmih6
oB/YZg/+sjYR/hjtL6A=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIB6jCCAVMCAQ8wDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1
bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDcwNzQzNDFaFw0xNDEyMDUwNzQzNDFaMEgx
DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMScwJQYDVQQDEx5jYXMvYXBvbGxvMS5jcC5l
bmcuY2h1bGEuYWMudGgwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMk/Tn+Pip6IsmfgVTI3
e7B2neXVMpe/LtjO/JN1+2PNurWpi7O0O89To8yDPnEIIodfO5qXAZGLiXubXq20Dv7qJXEbFQJs
2oR038m3OvroLGZ/3PftY6khDmlLO02J0nvtvjfbecSVSxkAcPcPTTBQtzc2pbMHBisUDt+q71Gz
AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAFacTxqa2LZSNnnq6DvoK+w9dYteJqFaV+kg/zKAr2v7z
sJT6ysttun58HM1XCBEmwmWCRenUWykhJ75ugCnLqJeQ6uG8P2acNB0pN4i3TLjQ5r3Kflt8FF6z
ipc6IeQjlRjqfolX01o73MldEZrWNusslWrTTZMN945I5A+KzSk=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></ds:Signature></Assertion>
   Signature Algorithm: md5WithRSAEncryption
      b7:dd:05:81:a6:c6:7b:54:75:6e:93:1e:e2:3c:31:cb:5a:d6:
      be:d3:2f:b1:ff:1c:62:25:34:1e:1e:94:49:4c:91:0c:65:f7:
      8d:d4:cc:54:7e:27:28:d9:b0:8a:30:ae:2c:a2:1c:46:e7:53:
      22:fd:e0:a5:bd:d9:d3:03:90:2f:de:64:64:81:8b:e1:73:8b:
      50:90:64:0f:85:e5:fa:68:13:4d:07:22:c6:e7:63:12:74:82:
      0c:88:00:a8:39:e1:3d:d5:f1:95:90:ae:54:6a:17:9d:e9:74:
      8d:d1:7b:7b:b6:a3:42:c4:7c:cd:d9:e8:b9:3d:c5:87:0e:97:
      23:dd
```


รูปที่ 5.18 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง cas-proxy-renew กับซีเอเอสองค์กรเสมือนเดียวกับผู้ใช้

5.3.2.3 **ผลของการทำคำสั่ง** cas-proxy-renew –c http://test1.cp.eng.chula.ac.th:8080/ogsa/services/base/cas/CASService -s /O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th –p /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง cas-proxy-renew จะได้แฟ้มของหลักฐานอ้างอิงผู้ใช้ตัวแทนที่มีสิ่งอ้างสิทธิของอีกองค์กรเสมือนขึ้นมาใหม่คือแฟ้มที่เราตามหลัง –p ซึ่งเราสามารถดูรายละเอียดในแฟ้มได้โดยใช้คำสั่ง openssl x509 –in /tmp/x509up_u5561.cas –noout -text ซึ่งได้ผลดังรูปที่ 5.19

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 385707 (0x5e2ab)

Signature Algorithm: md5WithRSAEncryption

Issuer: O=Grid, O=Chula, CN=cas/test1.cp.eng.chula.ac.th

Validity

Not Before: Jan 18 10:33:08 2005 GMT

Not After : Jan 18 16:43:44 2005 GMT

Subject: O=Grid, O=Chula, CN=cas/test1.cp.eng.chula.ac.th, CN=736618254

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:ad:b6:94:54:5e:fe:4c:40:73:50:9c:33:b8:31:

52:75:91:ce:2f:0c:e6:17:cf:3e:4d:27:30:23:60:

5b:6b:90:0c:6f:a2:e2:1a:b3:98:40:d6:61:da:04:

a4:90:6d:bd:7f:90:31:1b:f6:d7:1a:fb:dc:64:22:

30:aa:7a:2b:5f

Exponent: 65537 (0x10001)

X509v3 extensions:

1.3.6.1.4.1.3536.1.222: critical

0.0

..+.....

1.3.6.1.4.1.3536.1.1.1.99:

2

1.3.6.1.4.1.3536.1.1.1.9.2:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="e0ccf105-9878-4c1b-9168-ae30c08efdc4" IssueInstant="2005-01-18T07:34:07Z" Issuer="O=Grid,O=Chula,CN=Test CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T10:34:07Z" NotOnOrAfter="2005-01-19T10:34:07Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/test2.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>4Wiu3vcEbUVhsZDrfOO6GDP0lok=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

HuPswDw1eW4NRniedFcmbDU6EipIYkcD2rbZ9UiCF0/TlhYVDzqow4GxGocAKFBRQ5oBljzOWz5w

nIEw3QhEPqy6umS0IuuistFg9Wgn3oBKjLOzJQ4ULGCAMZaVxIljRjgaxH728SZbAIh4/Rpl7iy/

LTUv/fxLI1rUEDgVK6s=

</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>

MIIB6zCCAVQCAQQwDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1

bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDIwNDA4MTBaFw0xNDExMzAwNDA4MTBaMEkx

DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMSgwJgYDVQQDEx9jYXMvYXBvbGxvMTAuY3Au

ZW5nLmNodWxhLmFjLnRoMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKbvxw2FhR1awR+tmJ

li90IUIwK/YaTN4pCof6149RmcETYslrmHs+umWT26g8faF3ZHWTIoggX1J5RkbrrC9/097z8yaZ

NMhZnb1JQRS89T0E12IcAvnlmSB+LVHWS7h+8WT+gZlYJSMhq6Xzl9HdGYimNfNmBxR6/fojPtYQ

7wIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAHJtaMwxFJ4ZMuq5KOa4qmh0N+/z2E4z8FBqfKCVG/9f

tS5wgbPf3ja4ST7Zq/NLmIEiM2docXw6z95hi6kUmB6Q8DzzewrBNTijGt2SgIrc8SbM75tJ87xQ

WpquzY/ytj6vaL0hUiMN/lemSBSfpRkZul4R1bDCJg5y1zceFBlG

</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo></ds:Signature></Assertion>

1.3.6.1.4.1.3536.1.1.1.9.1:

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="ac5c196a-dbc0-4f6e-8a6a-5c123911333d" IssueInstant="2005-01-18T07:33:09Z" Issuer="O=Grid,O=Chula,CN=Apollo CA" MajorVersion="1" MinorVersion="0"><Conditions NotBefore="2005-01-18T07:33:09Z" NotOnOrAfter="2005-01-19T07:33:09Z"></Conditions><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=cas/test1.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="O=Grid,O=Chula,OU=cp.eng.chula.ac.th,CN=Patipan Kongsirikul (4670359521)">/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=Patipan Kongsirikul (4670359521)</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="cas">allow</Action></AuthorizationDecisionStatement><AuthorizationDecisionStatement Decision="Permit" Resource="/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th"><Subject><NameIdentifier Format="#X509SubjectName" NameQualifier="/O=Grid/O=Chula/CN=Apollo CA">/O=Grid/O=Chula/CN=Apollo CA</NameIdentifier><SubjectConfirmation><ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:am:X509-PKI</ConfirmationMethod></SubjectConfirmation></Subject><Action Namespace="host">allow</Action></AuthorizationDecisionStatement><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms xmlns:signs="urn:oasis:names:tc:SAML:1.0:assertion">

<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">

here()/ancestor::signs:Assertion[1]

</xfilter2b:XPath>

<xfilter2b:XPath xmlns:xfilter2b="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">

here()/ancestor::ds:Signature[1]

</xfilter2b:XPath>

</ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="#default code ds kind rw saml samlp signs xsd xsi"></ec:InclusiveNamespaces></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>jyWfi0Ccucsu0/UnjxnPPIMcN6M=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

swxKmqYIDfgC4oQv36VAEYd9FefLrFX1sOXxPtL0phpWn8jyS1W2Befcbs09p59fx3L4iZXWa8Ra

LiLmpaBa2gCi3nb6DEEagdJTD8AlwDs5C77jzU8TMe0kmFe1DXl3dNz3jm1FaIIK+irtXBvMmih6

oB/YZg/+sjYR/hjtL6A=

</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>

MIIB6jCCAVMCAQ8wDQYJKoZIhvcNAQEEBQAwMzENMAsGA1UEChMER3JpZDEOMAwGA1UEChMFQ2h1

bGExEjAQBgNVBAMTCUFwb2xsbyBDQTAeFw0wNDEyMDcwNzQzNDFaFw0xNDEyMDUwNzQzNDFaMEgx

DTALBgNVBAoTBEdyaWQxDjAMBgNVBAoTBUNodWxhMScwJQYDVQQDEx5jYXMvYXBvbGxvMS5jcC5l

bmcuY2h1bGEuYWMudGgwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMk/Tn+Pip6IsmfgVTI3

e7B2neXVMpe/LtjO/JN1+2PNurWpi7O0O89To8yDPnEIlodfO5qXAZGLiXubXq20Dv7qJXEbFQJs

2oR038m3OvroLGZ/3PftY6khDmlLO02J0nvtvjfbecSVSxkAcPcPTTBQtzc2pbMHBisUDt+q71Gz

AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAFacTxqa2LZSNnnq6DvoK+w9dYteJqFaV+kg/zKAr2v7z

sJT6ysttun58HM1XCBEmwmWCRenUWykhJ75ugCnLqJeQ6uG8P2acNB0pN4i3TLjQ5r3Kflt8FF6z

ipc6IeQjlRjqfolX01o73MldEZrWNusslWrTTZMN945I5A+KzSk=

</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo></ds:Signature></Assertion>

Signature Algorithm: md5WithRSAEncryption

85:51:eb:57:51:d8:ee:4e:8f:aa:7d:51:e4:c0:b4:57:5f:b9:

2d:df:d3:d4:72:c0:26:91:88:2d:26:b9:43:84:ab:74:31:af:

```
ba:32:99:02:82:78:cd:ac:17:5b:97:8d:ce:7a:72:31:11:fa:
e5:b4:d2:e9:c7:ce:10:6c:bf:1d
```

รูปที่ 5.19 แสดงรายละเอียดของหลักฐานอ้างอิงผู้ใช้ตัวแทนหลังการทำคำสั่ง cas-proxy-renew กับซีเอเอสขององค์กรเสมือนอื่น

5.3.2.4 **ผลของการทำคำสั่ง** managed-job-globusrun -factory http://test2.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง managed-job-globusrun งานของผู้ใช้ที่ระบุไว้ในแฟ้ม test.xml จะถูกทำงานบนทรัพยากรขององค์กรเสมือนอื่นที่ไม่เชื่อถือกับผู้ใช้โดยตรง แต่เชื่อถือกันผ่านซีเอเอสเซอร์ฟเวอร์ของทั้งสององค์กรเสมือน ซึ่งรายละเอียดของการทำงานเป็นไปดังรูปที่ 5.20

```
WAITING FOR JOB TO FINISH
========== Status Notification ==========
Job Status: Active
=========================================
========== Status Notification ==========
Job Status: Done
=========================================
DESTROYING SERVICE
SERVICE DESTROYED
```

รูปที่ 5.20 แสดงผลการทดลองหลังจากเข้าไปใช้แกรมขององค์กรเสมือนอื่นโดยทำการทดสอบบนสภาพแวดล้อมที่องค์กรเสมือนไม่เชื่อถือกันโดยตรงแต่เชื่อถือกันผ่านตัวแทน

5.3.2.5 **ผลของการทำคำสั่ง** managed-job-globusrun -factory http://apollo10.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy /tmp/x509up_u5561.cas

เมื่อทำคำสั่ง managed-job-globusrun จะพบรายงานความผิดพลาดเนื่องจากแกรมขององค์กรเสมือนเดียวกับผู้ใช้ไม่มีความเชื่อถือกับผู้ออกหลักฐานอ้างอิงผู้ใช้ตัวแทนดังรูปที่ 5.21

```
Error: error submitting job request: Could not connect to job manager [Root error message: Unknown CA]
```

รูปที่ 5.21 แสดงรายงานความผิดพลาดหลังจากเข้าไปใช้แกรมในองค์กรเสมือนเดียวกับผู้ใช้โดยใช้หลักฐานอ้างอิงตัวผู้ใช้ที่ได้จากคำสั่ง cas-proxy-renew

5.3.3 วิเคราะห์ผลการทดลอง

จากการทดลองหลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-renew ตามแนวคิดของการเปลี่ยนบัตร พบว่าผู้ใช้สามารถใช้หลักฐานอ้างอิงผู้ใช้ตัวแทนแบบนี้กับสภาพแวดล้อมที่สององค์กรเสมือนไม่เชื่อถือกันโดยตรงแต่เชื่อผ่านตัวกลางร่วมกันนั้นสามารถทำงานได้อย่างถูกต้อง แต่เมื่อนำหลักฐานอ้างอิงผู้ใช้ที่ได้หลังจากการยื่นไปยังซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนกลับมาใช้งานที่องค์กรเสมือนของตนเองพบว่าไม่สามารถใช้งานได้เพราะองค์กรเสมือนเดียวกับผู้ใช้ไม่ได้เชื่อถือผู้ออกหลักอ้างอิงผู้ใช้นั้น

ตามแนวคิดของการเปลี่ยนบัตรถ้าผู้ใช้ต้องการเข้าใช้ทรัพยากรที่องค์กรเสมือนของตนเองจึงต้องทำ grid-proxy-init ใหม่ ดังนั้นแนวคิดของการเปลี่ยนบัตรจึงไม่เหมาะกับงานที่ใช้ทรัพยากรที่มากกว่าองค์กรเสมือนพร้อมๆกัน

5.4 การทดสอบระบบบนสภาพแวดล้อมของเครื่องทรัพยากรของโกลบัสทูลคิดรุ่น 3.2.1 ที่ไม่ได้ถูกแก้ไขโดยงานวิจัยนี้

5.4.1 วิธีการทดลอง

1. ในการทดลองนี้เป็นการทดสอบคุณสมบัติหลักฐานอ้างอิงผู้ใช้ตัวแทนแบบต่างๆ เมื่อนำมาใช้กับทรัพยากรที่มีสภาพแวดล้อมของโกลบัสทูลคิดรุ่น3.2.1 ที่ไม่ได้ลงจีเอเอส ซึ่งประกอบไปด้วยหลักฐานอ้างอิงผู้ใช้ตัวแทนดังนี้
    a. หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง grid-proxy-init ภายในองค์กรเสมือนเดียวกับผู้ทดสอบ
    b. หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-init ภายในองค์กรเสมือนเดียวกับผู้ทดสอบ
    c. หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-passport-init กับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่น
    d. หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-renew ภายในองค์กรเสมือนเดียวกับผู้ใช้
    e. หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-renew กับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่น

2. นำหลักฐานอ้างอิงผู้ใช้ตัวแทนที่เตรียมจากข้อ 1 มาทดสอบโดยใช้คำสั่ง

managed-job-globusrun -factory http://apollo9.cp.eng.chula.ac.th:8080/ogsa/services/base/gram/MasterForkManagedJobFactoryService -file $GLOBUS_LOCATION/schema/base/gram/examples/test.xml –proxy (ชื่อแฟ้ม ของหลักฐานอ้างอิงผู้ใช้ตัวแทนแบบต่างๆ)

5.4.2 ผลการทดลอง

เมื่อทดสอบหลักฐานอ้างอิงผู้ใช้ตัวแทนทั้ง 5 แล้วได้ผลดังตารางที่ 5.1

ตารางที่ 5.1 แสดงผลการทดสอบหลักฐานอ้างอิงผู้ใช้ตัวแทนกับทรัพยากรที่ติดตั้ง GT3.2.1 แต่ไม่ได้ติดตั้งจีเอเอส

รูปแบบหลักฐานอ้างอิงผู้ใช้ตัวแทน	ผลการทดสอบ
หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง grid-proxy-init ภายในองค์กรเสมือนเดียวกับผู้ทดสอบ	WAITING FOR JOB TO FINISH ========== Status Notification ========== Job Status: Active ========== ========== Status Notification ========== Job Status: Done ========== DESTROYING SERVICE SERVICE DESTROYED

หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-init ภายในองค์กรเสมือนเดียวกับผู้ทดสอบ	WAITING FOR JOB TO FINISH ========== Status Notification ========== Job Status: Active ========== ========== Status Notification ========== Job Status: Done ========== DESTROYING SERVICE SERVICE DESTROYED
หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-passport-init กับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่น	WAITING FOR JOB TO FINISH ========== Status Notification ========== Job Status: Active ========== ========== Status Notification ========== Job Status: Done ========== DESTROYING SERVICE SERVICE DESTROYED

หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-renew ภายในองค์กรเสมือนเดียวกับผู้ใช้	WAITING FOR JOB TO FINISH ========== Status Notification ========== Job Status: Active ========== ========== Status Notification ========== Job Status: Done ========== DESTROYING SERVICE SERVICE DESTROYED
หลักฐานอ้างอิงผู้ใช้ตัวแทนที่ได้จากคำสั่ง cas-proxy-renew กับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่น	Error: error submitting job request: Could not connect to job manager [Root error message: Unknown CA]

5.4.3 วิเคราะห์ผลการทดลอง

จากผลการทดลองตารางที่ 5.1 สามารถสรุปได้ว่าหลักฐานอ้างอิงผู้ใช้ตัวแทนที่ใช้ในงานวิจัยนี้สามารถนำมาใช้กับโกลบัสทูลคิดรุ่น 3.2.1 ที่ไม่ได้ติดตั้งจีเอเอสได้ยกเว้นรูปแบบที่ไปขอแลกบัตรกับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่นซึ่งจะทำให้ไม่สามารถมาใช้ภายในองค์กรเสมือนของตนเองได้

5.5 การทดสอบเพื่อวัดประสิทธิภาพของระบบจัดการสิทธิแบบกลุ่มคนในกริด

5.5.1วิธีการทดลอง

1. ทำการเปรียบเทียบโดยจับเวลาการทำงานของขั้นตอนการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทนอันใหม่ตามแนวคิดการทำหนังสือเดินทางและแนวคิดเปลี่ยนบัตร
2. ทำการเปรียบเทียบโดยจับเวลาการทำงานของแกรมเมื่อใช้หลักฐานอ้างอิงผู้ใช้ในแบบต่างๆสำหรับระบบจัดการสิทธิแบบกลุ่มคนกับหลักฐานอ้างอิงผู้ใช้ตามปกติของโกลบัสทูลคิด

3. บันทึกผลการทดลอง

4. วิเคราห์ผลการทดลอง

5.5.2 สภาวะที่ใช้ในการทดลอง

1. ตัวประมวลผลกลาง Intel Pentium 4 1.8 เมกกะเฮิร์ทซ์

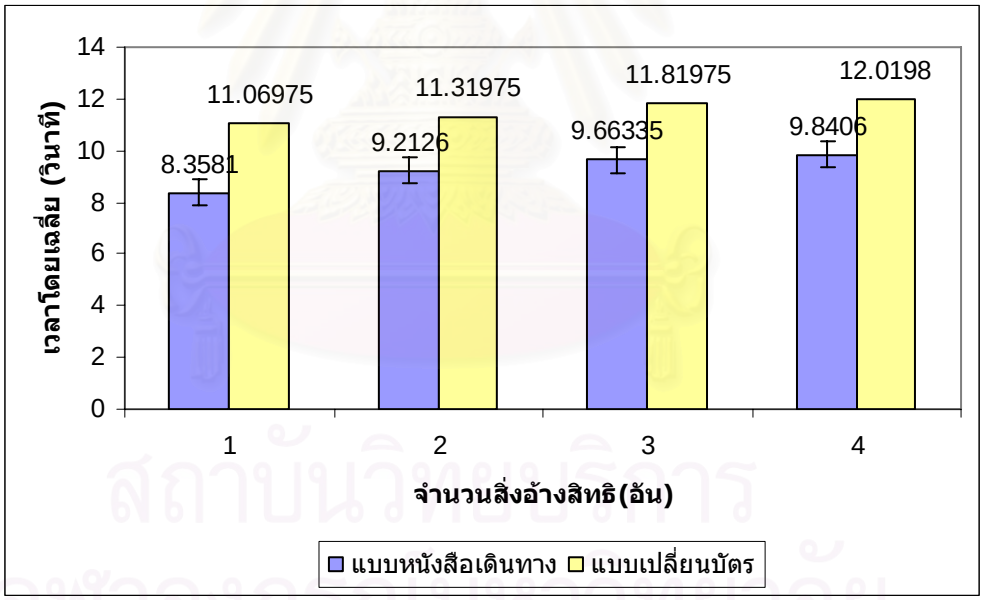
2. หน่วยความจำขนาด 512 เมกกะไบต์

3.ระบบปฏิบัติการลินิกซ์ เรดแฮท รุ่น 9.0

4. ทำการทดลองเพื่อจับเวลาเป็นจำนวน 20 ครั้ง

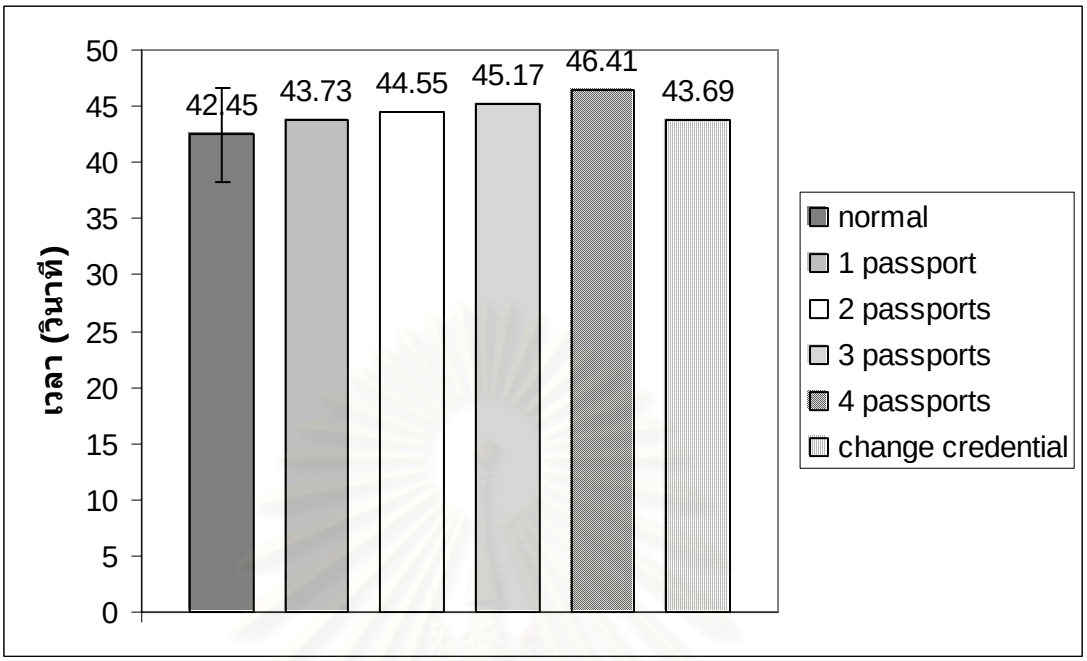
5.5.3 ผลการทดลอง

ผลการทดสอบประสิทธิภาพของขั้นตอนการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทนตามแนวคิดการทำหนังสือเดินทางและแนวคิดเปลี่ยนบัตรได้ดังรูปที่ 5.22



รูปที่ 5.22 ผลการวัดประสิทธิภาพของขั้นตอนการสร้างหลักฐานอ้างอิงผู้ใช้ตัวแทนตามแนวคิดการทำหนังสือเดินทางและแนวคิดเปลี่ยนบัตร

ผลการทดสอบประสิทธิภาพการทำงานของแกรมเมื่อใช้หลักฐานอ้างอิงผู้ใช้ในแบบต่างๆ สำหรับระบบจัดการสิทธิแบบกลุ่มคนได้ดังรูปที่ 5.23



รูปที่ 5.23 ผลการวัดประสิทธิภาพการทำงานของแกรมเมื่อใช้หลักฐานอ้างอิงผู้ใช้ในแบบต่างๆ

5.5.4 วิเคราะห์ผลการทดลอง

จากรูปที่ 5.22 ที่ทำการวัดประสิทธิภาพของขั้นตอนการสร้างหลักฐานอ้างอิงผู้ใช้ตามแนวคิดหนังสือเดินทางและแนวคิดการเปลี่ยนบัตร พบว่าเวลาที่ใช้ในการสร้างหลักฐานอ้างอิงผู้ใช้แบบเปลี่ยนบัตรจะมากกว่าการสร้างหลักฐานอ้างอิงผู้ใช้แบบหนังสือเดินทาง เนื่องจากเวลาที่ใช้ในการเคลื่อนย้ายแฟ้มข้อมูลหลักฐานอ้างอิงผู้ใช้จากเครื่องซีเอเอสเซอร์ฟเวอร์มายังเครื่องไคลเอนท์ซึ่งใช้เวลาประมาณ 2-3 วินาที โดยการเคลื่อนย้ายแฟ้มข้อมูลนั้นทำโดยใช้กริดเอฟทีพี (grid FTP) ซึ่งเป็นบริการเคลื่อนย้ายไฟล์ที่ใช้ระบบรักษาความปลอดภัยของโกลบัสทูลคิด และในรูปที่ 5.22 ยังมีการเปรียบเทียบเวลาของการสร้างหลักฐานอ้างอิงผู้ใช้ที่มีจำนวนสิ่งอ้างสิทธิต่างกันไปตั้งแต่ 1 อันจนถึง 4 อัน ซึ่งพบว่าเวลาที่เพิ่มขึ้นสำหรับการทำสิ่งอ้างสิทธิ 1 อันนั้นจะมีค่าน้อยกว่า 1 วินาทีซึ่งมีค่าน้อยมากเมื่อเทียบกับเวลาการทำงานของผู้ใช้ในระบบกริดที่ใช้เวลารันงานมากกว่า 1 วัน

จากรูปที่ 5.23 ที่ทำการวัดประสิทธิภาพการทำงานของแกรมเมื่อใช้หลักฐานอ้างอิงผู้ใช้ในแบบต่างๆได้แก่ หลักฐานอ้างอิงผู้ใช้แบบปกติที่ไม่มีสิ่งอ้างสิทธิ หลักฐานอ้างอิงผู้ใช้แบบหนังสือเดินทาง และหลักฐานอ้างอิงผู้ใช้แบบเปลี่ยนบัตร พบว่าเวลาในการรันงานของแกรมที่ใช้หลักฐานอ้างอิงผู้ใช้แบบปกติจะน้อยที่สุดคือ 42.45 วินาที เวลาในการรันงานของแกรมที่ใช้หลักฐานอ้างอิงผู้ใช้แบบหนังสือเดินทางที่มีสิ่งอ้างสิทธิเพียงอันเดียวคือ 43.73 วินาที และเวลาในการรันงานของ

แกรมที่ใช้หลักฐานอ้างอิงผู้ใช้แบบเปลี่ยนบัตรคือ 43.69 วินาที ซึ่งเวลาที่ใช้ของหลักฐานอ้างอิงแบบหนังสือเดินทางและแบบเปลี่ยนบัตรจะมากกว่าแบบธรรมดาประมาณ 1 วินาทีเนื่องจากจีเอเอสต้องพิจารณาสิ่งอ้างสิทธิที่อยู่ในหลักฐานอ้างอิงผู้ใช้ที่นำมาทดสอบ และเมื่อพิจารณาถึงจำนวนของสิ่งอ้างสิทธิที่อยู่ถายในหลักฐานอ้างอิงผู้ใช้แบบหนังสือเดินทางพบว่าเวลาที่ใช้จะเพิ่มขึ้นตามจำนวนสิ่งอ้างสิทธิมีค่าเพิ่มขึ้นประมาณ 0.5 วินาทีต่อสิ่งอ้างสิทธิ 1 อัน โดยที่ในการทดลองนี้จะใช้เวลารันงานประมาณ 3 วินาที และเวลาส่วนใหญ่ประมาณ 40 วินาทีจะถูกใช้ในการพิสูจน์ตัวจริง การจัดการสิทธิของผู้ใช้ และการสร้างสภาพแวดล้อมในการทำงานบนแกรมของผู้ใช้ และการทำงานส่วนมากในกริดจะใช้เวลานานในระดับวัน ทำให้เวลาที่ผู้ใช้ต้องสร้างหลักฐานอ้างอิงผู้ใช้แบบหนังสือเดินทางหรือหลักฐานอ้างอิงผู้ใช้แบบเปลี่ยนบัตรซึ่งอยู่ในระดับวินาที มีค่าน้อยมาก ส่งผลให้ผู้ใช้ไม่รู้สึกถึงความแตกต่างในการรันงานแกรมเมื่อเทียบกับการรันงานโดยใช้หลักฐานอ้างอิงผู้ใช้ของจีเอสไอ

บทที่ 6

สรุปผลการวิจัยและข้อเสนอแนะ

6.1 สรุปผลการวิจัย

วิทยานิพนธ์นี้นำเสนอวิธีการแก้ปัญหาการขยายตัวที่ไม่ดีเนื่องจากมีผู้ใช้หรือทรัพยากรเพิ่มเข้ามาในองค์กรเสมือนและการขยายตัวที่ไม่ดีเมื่อมีการเชื่อมต่อองค์กรเสมือนมากกว่า 1 องค์กรเสมือนเข้าด้วยกัน เพราะเมื่อระบบกริดมีการขยายตัวที่ดีขึ้นส่งผลดีแก่ผู้ใช้ของแต่ละองค์กรเสมือนที่จะได้มีทรัพยากรมากขึ้นในระบบ การทำงานของผู้ใช้มีประสิทธิภาพดีขึ้นด้วย

การเพิ่มความสามารถในการขยายตัวของระบบภายในองค์กรเสมือนใช้แนวคิดการจัดการสิทธิแบบรวมศูนย์กลางโดยการสร้างเซอร์ฟเวอร์สำหรับจัดการสิทธิที่กระจายอยู่ตามทรัพยากรต่างๆมาไว้ในฐานข้อมูลและกำหนดสิทธิของผู้ใช้แต่ละคนในการเข้าใช้ทรัพยากรในองค์กรเสมือน โดยในการกำหนดสิทธิของผู้ใช้จะกำหนดสิทธิตามบทบาท (Role) หรือ กลุ่ม (Group) ของผู้ใช้ในองค์กรเสมือน และให้แต่ละทรัพยากรในองค์กรเสมือนกำหนดสิทธิให้กับบทบาทหรือกลุ่มต่างๆแทนที่การกำหนดสิทธิให้กับผู้ใช้โดยตรงซึ่งเป็นแนวคิดของระบบจัดการสิทธิภายในองค์กรเสมือนสำหรับกริดทั่วไปคือ งานซีเอเอส และ งานวิจัยวีโอเอ็มเอส เพียงแต่งานวิจัยที่กล่าวมาข้างต้นนั้นยังไม่สนับสนุนการทำงานร่วมกับบริการแกรมซึ่งเป็นบริการพื้นฐานของโกลบัสทูลคิดรุ่น 3.x

ในงานวิจัยนี้จึงนำแนวคิดการสร้างเซอร์ฟเวอร์จัดการสิทธิมาประยุกต์ใช้ โดยเริ่มพัฒนาจากการเพิ่มเติมนโยบายที่จำเป็นสำหรับการเข้าใช้บริการแกรมเข้าไปในฐานข้อมูลสิทธิ และส่วนสำหรับให้บริการแกรมเรียกใช้เพื่อตรวจสอบความถูกต้องของสิทธิ

ในส่วนของการเพิ่มความสามารถในการขยายตัวของระบบเมื่อมีการเชื่อมต่อขององค์กรเสมือนเข้าด้วยกันได้เสนอแนวทางในการแก้ปัญหาตามสภาพแวดล้อมขององค์กรเสมือนหลังเชื่อมต่อกันแล้วซึ่งมีอยู่ 2 สภาพแวดล้อมด้วยกันได้แก่ สภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง และสภาพแวดล้อมที่องค์กรเสมือนทั้งสองไม่ได้เชื่อถือกันโดยตรงแต่เชื่อตัวแทนตัวเดียวกัน

สำหรับสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรงนั้นผู้วิจัยได้เสนอแนวคิดการทำหลักฐานอ้างอิงผู้ใช้ตัวแทนและสิ่งอ้างสิทธิแบบหนังสือเดินทาง คือเมื่อผู้ใช้ต้องการใช้งานทรัพยากรในองค์กรเสมือนอื่นจะต้องไปขออนุญาตจากซีเอเอสเซอร์ฟเวอร์ผู้ดูแลสิทธิในองค์กรเสมือนของผู้ใช้เสียก่อน เมื่อซีเอเอสเซอร์ฟเวอร์ผู้ดูแลสิทธิในองค์กรเสมือนอนุญาตจะสร้าง

สิ่งอ้างสิทธิแนบไปกับหลักฐานอ้างอิงผู้ใช้สำหรับให้ผู้ใช้ไปติดต่อกับซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนอื่นได้ จากนั้นผู้ใช้จึงนำหลักฐานอ้างอิงผู้ใช้ที่แนบสิ่งอ้างสิทธิไปยื่นต่อซีเอเอสเซอร์ฟเวอร์ขององค์กรเสมือนนั้นเพื่อขออนุญาตเข้าใช้ทรัพยากรในองค์กรเสมือนดังกล่าว เมื่อซีเอเอสขององค์กรเสมือนเดียวกับทรัพยากรพิจารณาและอนุญาตจึงสร้างสิ่งอ้างสิทธิสำหรับการเข้าไปใช้ทรัพยากรในองค์กรเสมือนแนบต่อท้ายในหลักฐานอ้างอิงตัวผู้ใช้ หลังจากนั้นผู้ใช้จึงสามารถเข้าไปใช้ทรัพยากรได้โดยยื่นหลักฐานอ้างอิงผู้ใช้ที่มีสิ่งอ้างสิทธิอันล่าสุด เปรียบได้กับการตรวจลงตราหนังสือเดินทางก่อนออกนอกประเทศ เมื่อไปถึงประเทศอื่นแล้วจึงยื่นหนังสือเดินทางเพื่อให้เจ้าหน้าที่ของประเทศนั้นอนุญาตให้อีกครั้งถึงจะเข้าไปในประเทศนั้นๆได้

สำหรับสภาพแวดล้อมที่องค์กรเสมือนทั้งสองไม่ได้เชื่อถือกันโดยตรงแต่เชื่อตัวแทนตัวเดียวกัน ผู้วิจัยได้เสนอแนวคิดการทำหลักฐานอ้างอิงผู้ใช้ตัวแทนและสิ่งอ้างสิทธิแบบเปลี่ยนบัตร กล่าวคือเมื่อผู้ใช้ต้องการไปใช้งานทรัพยากรในองค์กรเสมือนอื่นจะต้องไปแลกหลักฐานอ้างอิงผู้ใช้กับซีเอเอสเซอร์ฟเวอร์ในองค์กรเสมือนของตนเองก่อนแล้วจึงนำหลักฐานอ้างอิงที่ได้รับมาไปแลกกับซีเอเอสเซอร์ฟเวอร์ในอีกองค์กรเสมือนเพราะในสภาพแวดล้อมนี้ซีเอเอสเซอร์ฟเวอร์จะไม่มีความเชื่อถือกับผู้ใช้โดยตรงแต่จะเชื่อซีเอเอสขององค์กรเราเท่านั้น หลังจากนั้นจึงทำการแลกหลักฐานอ้างอิงผู้ใช้ที่ได้รับจากซีเอเอสขององค์กรเสมือนเรากับหลักฐานอ้างอิงผู้ใช้ที่ซีเอเอสขององค์กรเสมือนเดียวกับทรัพยากรเป็นผู้ออกมาให้ แล้วนำหลักฐานอ้างอิงผู้ใช้นั้นไปยื่นต่อทรัพยากรก็จะสามารถเข้าใช้งานได้

สำหรับการทดสอบระบบที่ได้ออกแบบมาบนโกลบัสทูลคิดรุ่น 3.2.1 ได้แบ่งออกเป็น 4 กรณีด้วยกันได้แก่ การทดสอบการทำงานของระบบจัดการสิทธิร่วมกับบริการแกรมภายในองค์กรเสมือนเดียวกัน การทดสอบการทำงานของระบบจัดการสิทธิบนสภาพแวดล้อมที่องค์กรเสมือนทั้งสองมีความเชื่อถือกันโดยตรง การทดสอบการทำงานของระบบสภาพแวดล้อมที่องค์กรเสมือนทั้งสองไม่ได้เชื่อถือกันโดยตรงแต่เชื่อตัวแทนตัวเดียวกัน และการทดสอบการทำงานของระบบกับสภาพแวดล้อมของโกลบัสทูลคิดรุ่น 3.2.1 ที่ไม่ได้ถูกแก้ไข พบว่าระบบจัดการสิทธิที่ได้ออกแบบมาสามารถทำงานได้อย่างถูกต้อง ทำให้ได้ระบบการจัดการสิทธิที่มีความสามารถในการขยายตัวที่ดีขึ้นสำหรับภายในองค์กรเสมือนเองและสภาพแวดล้อมการเชื่อมต่อขององค์กรเสมือนตรงตามวัตถุประสงค์ของงานวิจัยนี้

6.2 ข้อเสนอแนะ

1. เนื่องจากในงานวิจัยนี้สนับสนุนการทำงานข้ามองค์กรเสมือนโดยที่แต่ละองค์กรเสมือนนั้นไม่มีโครงสร้างแบบลำดับขั้น แต่ในความเป็นจริงแล้วยิ่งองค์กรมีขนาดใหญ่จะมีโครงสร้างขององค์กรเป็นลำดับขั้น เพราะลำดับขั้นเป็นส่วนหนึ่งที่สำคัญที่ช่วยลดความซับซ้อนขององค์กร โดยผู้พัฒนาระบบจะต้องใช้ข้อดีของการมีลำดับขั้นมาช่วยเพิ่มความสามารถในการขยายตัวขององค์กรเสมือน
2. ในโกลบัสทูลคิดรุ่น 3.x จะมีการสร้างกริดเซอร์วิสขึ้นมา 3 ประเภทได้แก่ บริการระบบ (System service) บริการพื้นฐาน (Based service) และบริการที่ผู้ใช้สร้างขึ้นมาภายหลัง (User defined service) ซึ่งผู้ใช้จะไม่สามารถทราบได้ว่าเครื่องทรัพยากรใดบ้างที่ให้บริการที่ผู้ใช้ต้องการแบบบริการที่ผู้ใช้สร้างขึ้นมาภายหลังได้ จึงควรมีการสร้างบริการสำหรับจดทะเบียนบริการต่างๆที่เป็นบริการที่สร้างขึ้นมาภายหลัง และบริการสำหรับค้นหาเครื่องทรัพยากรที่มีบริการที่ผู้ใช้ต้องการได้ ซึ่งบริการที่สร้างขึ้นมานี้จะมีประโยชน์สำหรับการนำไปประยุกต์ใช้กับนายหน้าจัดหาทรัพยากร (resource broker) เพื่อให้ได้นายหน้าจัดหาทรัพยากรที่มีความสามารถจัดหาทรัพยากรข้ามองค์กรเสมือนได้
3. การที่ระบบจัดการสิทธิสร้างซีเอเอสเซอร์ฟเวอร์ซึ่งมีรูปแบบรวมศูนย์กลาง (centralize) ย่อมเกิดปัญหาต่างๆ เช่น ปัญหาเมื่อซีเอเอสล่มทำให้ระบบไม่สามารถทำงานต่อได้ (single point of failure) ผู้วิจัยเห็นว่าควรมีการทำระบบทนต่อความผิดพลาดที่อาจเกิดขึ้นได้ (fault tolerance) กล่าวคือควรจะมีสำเนา (replica) ของแต่ละซีเอเอสเซอร์ฟเวอร์ เพื่อกรณีที่ซีเอเอสเซอร์ฟเวอร์ล่มตัวที่เป็นสำเนาจะได้เข้ามาทำงานแทนจะได้ระบบที่มีสภาพพร้อมใช้งาน (availability) ที่สูงขึ้น
4. นายหน้าจัดหาทรัพยากรส่วนใหญ่จะจัดหาทรัพยากรโดยดูจาก โหลดงานบนแต่ละทรัพยากรซึ่ง นายหน้าจัดหาทรัพยากรแบบดังกล่าวไม่เหมาะที่จะนำมาใช้จัดการกับงานที่รันโดยมี ซีเอเอสเซอร์ฟเวอร์เป็นตัวจัดการสิทธิการเข้าใช้เนื่องจากในระบบที่มีซีเอเอสเซอร์ฟเวอร์ ผู้ใช้จะต้องมาขอสิทธิจากซีเอเอสเซอร์ฟเวอร์ ซึ่งสิทธิของผู้ใช้ที่อยู่ในรูปแบบสิ่งอ้างสิทธิแบบเอสเอเอ็มแอล โดยที่ผู้ใช้อาจจะไม่มีสิทธิบนทรัพยากรที่นายหน้าจัดหาทรัพยากรจัดมาให้ ซึ่งวิธีแก้ไขก็คือให้นายหน้าจัดหาทรัพยากรส่งข้อความไปถามสิทธิของผู้ใช้บนทรัพยากรที่นายหน้าจัดหาทรัพยากรเห็นสมควรถ้าผู้ใช้มีสิทธิบนทุกทรัพยากรก็จะทำการแจกงานไปยังทรัพยากรนั้นๆแต่ถ้ามีทรัพยากรตัวไหนที่ผู้ใช้ไม่มีสิทธิ นายหน้าจัดหาทรัพยากรจะต้องหาทรัพยากรที่เหมาะสมกับผู้ใช้คนนั้นมาทดแทน และโดยเฉพาะ

อย่างยิ่งในขณะนี้ยังไม่มีนายหน้าจัดหาทรัพยากรตัวไหนที่รองรับการทำงานข้ามองค์กรเสมือนเลย

รายการอ้างอิง

[1] " Thailand e-Science project" available from http://www.thai-escience.net/ [25/3/2005]

[2] "Thai Grid Project" available from http://www.thaigrid.net/ [25/3/2005]

[3] "Globus Project" available from http://www.globus.org [25/3/2005]

[4] "The Grid Economic Project" available from http://www.buyya.com/ecogrid/ [25/3/2005]

[5] "Grid Datafarm" available from http://datafarm.apgrid.org/ [25/3/2005]

[6] R. Butler, V. Welch, D. Engert, I. Foster, S. Tuecke, J. Volmer, and C. Kesselman, "A national-scale authentication infrastructure," *Computer*, vol. 33, pp. 60-66, 2000.

[7] C. K. Ian Foster, Gene Tsudik, Steven Tuecke, "A security architecture for computational grids," presented at Conference on Computer and Communications Security Proceedings of the 5th ACM conference on Computer and communications security, San Francisco, California, United States, 1998.

[8] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, "A community authorization service for group collaboration," presented at Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on, 2002.

[9] C. K. L. Pearlman, V. Welch, I. Foster, S. Tuecke, "The Community Authorization Service: Status and Future," presented at Computing in High Energy and Nuclear Physics 2003, La Jolla, California, 2003.

[10] S. C. S. Cannon, D. Olson, C. Tull, V. Welch, L. Pearlman, "Using CAS to Manage Role-Based VO Sub-Groups," presented at Computing in High Energy and Nuclear Physics 2003, La Jolla, California, 2003.

[11] R. C. R. Alfieri, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. L orentey, and F. Spataro, "VOMS, an Authorization System for Virtual Organizations," 2002.

[12] "Open Science Grid Project" available from http://www.opensciencegrid.org/home/index.html [25/3/2005]

[13] I. Foster, "The anatomy of the grid: enabling scalable virtual organizations," presented at Cluster Computing and the Grid, 2001. Proceedings. First IEEE/ACM International Symposium on, 2001.

[14] "The Physiology of the Grid" available from www.globus.org/research/papers/ogsa.pdf [25/3/2005]

[15] "Open Grid Services Infrastructure (OGSI) Version 1.0" available from www-unix.globus.org/toolkit/ draft-ggf-ogsi-gridservice-33_2003-06-27.pdf [25/3/2005]

[16] J. J. Dongkyoo shin and a. D. Shin, "Design and Implementation of a Single Sign-On Library Supporting SAML (Security Assertion Markup Language) for Grid and Web Services Security," presented at GCC 2003, 2003.

[17] "OpenSAML Project" available from www.opensaml.org [25/3/2005]

[18] M. Lorch, D. B. Adams, D. Kafura, M. S. R. Koneni, A. Rathi, and S. Shah, "The PRIMA system for privilege management, authorization and enforcement in grid environments," presented at Grid Computing, 2003. Proceedings. Fourth International Workshop on, 2003.

[19] David W. Chadwick and A. Otenko, "The PERMIS X.509 role based privilege management infrastructure," *Future Gener. Comput. Syst.*, vol. 19, pp. 277-289, 2003.

[20] A. E. Mary R. Thompson, Srilekha Mudumbai, "Certificate-based authorization policy in a PKI environment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 6, pp. 566 - 588, 2003.

[21] S.-H. Kim, J. Kim, S.-J. Hong, and S. Kim, "Workflow-based authorization service in grid," presented at Grid Computing, 2003. Proceedings. Fourth International Workshop on, 2003.

ภาคผนวก

ภาคผนวก ก

รายละเอียดการเพิ่มเติมฐานข้อมูลซีเอเอส

1. ตาราง namespace_table เป็นตารางที่เกี่ยวกับรายละเอียดของเนมสเปซต่างๆซึ่งมีเขตข้อมูลดังนี้

    - namespace_nickname คือ ชื่อของเนมสเปซ
    - basename คือ ประเภทของเนมสเปซ
    - comparisonalg คือ ประเภทของการเปรียบเทียบมีสองแบบด้วยกันได้แก่ การเปรียบเทียบแบบตรงตัว (ExactComparison) และการเปรียบเทียบแบบอักขระตัวแทน (WildCardComparison)

ซึ่งค่าโดยปริยาย (default values) ของตาราง namespace_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.1 ข้อมูลในตาราง namespace_table ก่อนทำการเพิ่มเติม

namespace_nickname	basename	comparisonalg
casNamespace	baseName	org.globus.ogsa.impl.base.cas.server. databaseAccess.accessors.ExactComparison

เนื่องจากในงานวิจัยนี้จะมีการทำนโยบายเพื่อไปขอใช้ทรัพยากรกับซีเอเอสตัวอื่นๆและเครื่องที่เป็นซีเอเอสอาจจะเป็นเครื่องทรัพยากรด้วย ผู้วิจัยจึงได้ทำการเพิ่มข้อมูลเนมสเปซแบบ hostNamspace เข้าไปโดยให้มีวิธีการเปรียบเทียบเนมสเปซ แบบ host นี้คือการเปรียบเทียบแบบอักขระตัวแทน เพื่อแยกนโยบายที่มีต่อทรัพยากรโดยตรงและนโยบายที่มีต่อซีเอเอสอื่น โดยข้อมูลตาราง namespace_table เป็นดังนี้

ตารางที่ ก.2 ข้อมูลในตาราง namespace_table หลังทำการเพิ่มเติม

namespace_nickname	basename	comparisonalg
casNamespace	baseName	org.globus.ogsa.impl.base.cas.server .databaseAccess.accessors.ExactComparison
hostNamespace	.	org.globus.ogsa.impl.base.cas.server .databaseAccess.accessors.WildCardComparison

2. ตาราง trust_anchor_table เป็นตารางที่เกี่ยวกับรายละเอียดของผู้ออกหลักฐานอ้างอิงผู้ใช้ที่มีความเชื่อถือกับผู้ใช้ของซีเอเอส ซึ่งมีเขตข้อมูลดังนี้
    - trust_anchor_nickname คือ ชื่อของผู้ออกหลักฐานอ้างอิงผู้ใช้ที่มีความเชื่อถือ และมีการกำหนดเขตข้อมูลนี้ให้เป็น ไพมารีคีย์คือจะต้องไม่ซ้ำกัน
    - authentication_method คือ วิธีในการพิสูจน์ตัวจริง ซึ่งปกติจะเป็น x509
    - authentication_data คือ ชื่อเฉพาะ(DN) ของผู้ออกหลักฐานอ้างอิงผู้ใช้ที่มีความเชื่อถือ

ซึ่งค่าโดยปริยายของตาราง trust_anchor_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.3 ข้อมูลในตาราง trust_anchor_table

trust_anchor_nickname	authentication_method	authentication_data
defaultTrustAnchor	x509	/O=Grid/O=Chula/CN=Apollo CA

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆ นอกจากว่าจะเป็นการเพิ่มเนื่องจากมีชื่อผู้ออกหลักฐานอ้างอิงผู้ใช้เพิ่มเติม

3. ตาราง user_table เป็นตารางเกี่ยวกับรายละเอียดผู้ใช้ ซึ่งมีเขตข้อมูลดังนี้
    - user_nickname คือ ชื่อผู้ใช้ในองค์กร
    - subject_name คือ ชื่อเฉพาะของผู้ใช้
    - trust_anchor_nickname คือ ชื่อผู้ออกหลักฐานอ้างอิงของผู้ใช้ที่เชื่อถือกับซีเอเอสในตาราง trust_anchor_table

ซึ่งค่าโดยปริยายของตาราง user_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.4 ข้อมูลในตาราง user_table

user_nickname	subject_name	trust_anchor_nickname
globus	/O=Grid/O=Chula/OU=cp.eng.chula.ac.th/CN=GlobusonApollo9	defaultTrustAnchor

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆ นอกจากว่าจะเป็นการเพิ่มเนื่องจากมีผู้ใช้ในองค์กรเพิ่มเติม

4. ตาราง user group table เป็นตารางเกี่ยวกับรายละเอียดกลุ่มผู้ใช้ว่าในองค์กรมีกลุ่มใดบ้าง ซึ่งมีเขตข้อมูลดังนี้
    - user_group_name คือ ชื่อของกลุ่มในองค์กร

ซึ่งค่าโดยปริยายของตาราง user_group_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.5 ข้อมูลในตาราง user_group_table

user_group_name
superUserGroup

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆ นอกจากว่าจะเป็นการเพิ่มเนื่องจากมีการทำกลุ่มผู้ใช้เพิ่มเติม โดย superUserGroup เป็นกลุ่มที่ซีเอเอสสร้างมาสำหรับจัดการฐานข้อมูลโดยผ่านทางโปรแกรมไคลเอนท์ของทางซีเอเอส

5. ตาราง user_group_entry table เป็นตารางเกี่ยวกับรายละเอียดผู้ใช้ในองค์กรได้อยู่ในกลุ่มผู้ใช้ใดบ้าง ซึ่งมีเขตข้อมูลดังนี้
    - user_group_name คือ ชื่อกลุ่มผู้ใช้ในองค์กร
    - user_nickname คือ ชื่อผู้ใช้ที่อยู่ในกลุ่มดังกล่าว

ซึ่งค่าโดยปริยายของตาราง user_group_entry ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.6 ข้อมูลในตาราง user_group_entry

user_group_name	user_nickname
superUserGroup	globus

6. ตาราง object_table เป็นตารางเกี่ยวกับรายละเอียดทรัพยากรในองค์กรซึ่งมีเขตข้อมูลดังนี้
    - object_id คือ หมายเลขของทรัพยากร
    - object_name คือ ชื่อของทรัพยากร โดยปกติจะใช้ชื่อเฉพาะของทรัพยากรนั้นๆเพื่อตัดปัญหาชื่อทรัพยากรซ้ำกัน
    - namespace_nickname คือ ประเภทของเนมสเปซที่นำมาใช้กับทรัพยากรนี้

    ซึ่งค่าโดยปริยายของตาราง object_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.7 ข้อมูลในตาราง object_table ก่อนทำการเพิ่มเติม

object_id	object_name	namespace_nickname
1	casServer	casNamespace

ในตารางนี้ถ้าต้องการเพิ่มเติมทรัพยากรในองค์กรเสมือนให้ทำการเพิ่มโดยใช้ชื่อเฉพาะของทรัพยากรและใช้เนมสเปซ แบบ hostNamespace ตัวอย่างเช่น

ตารางที่ ก.8 ข้อมูลในตาราง object_table หลังทำการเพิ่มเติม

object_id	object_name	namespace_nickname
1	casServer	casNamespace
2	/O=Grid/O=Chula/CN=host/apollo10.cp.eng.chula.ac.th	hostNamespace

7. ตาราง object_group_table เป็นตารางเกี่ยวกับกลุ่มของทรัพยากรในองค์กรเสมือนซึ่งมีเขตข้อมูลดังนี้
    - object_group_name คือ กลุ่มของทรัพยากรในองค์กรเสมือน

ซึ่งค่าโดยปริยายของตาราง object_group_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.9 ข้อมูลในตาราง object_group_name

object_group_name

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆ นอกจากว่าจะเป็นการเพิ่มเนื่องจากมีการทำกลุ่มของทรัพยากรเพิ่มเติม

8. ตาราง object_group_entry เป็นตารางที่เกี่ยวกับทรัพยากรว่าอยู่ในกลุ่มทรัพยากรใดบ้างซึ่งมีเขตข้อมูลดังนี้
    - object_spec_desc คือ คำอธิบายเพิ่มเติมสำหรับทรัพยากรนี้
    - object_specification คือ หมายเลขทรัพยากรที่อยู่ในกลุ่มนี้
    - object_group_name คือ ชื่อกลุ่มของทรัพยากร

ซึ่งค่าโดยปริยายของตาราง object_group_entry ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.10 ข้อมูลในตาราง object_group_entry

object_spec_desc	object_specification	object_group_name

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆ นอกจากว่าจะเป็นการเพิ่มเนื่องจากเพิ่มทรัพยากรเข้าไปในกลุ่มทรัพยากรใดๆ

9. ตาราง service_type เป็นตารางที่เกี่ยวกับประเภทของบริการในองค์กรเสมือน ซึ่งมีเขตข้อมูลดังต่อไปนี้
    - service_type_name คือ ประเภทของบริการในองค์กรเสมือน

ซึ่งค่าโดยปริยายของตาราง service_type ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.11 ข้อมูลในตาราง service_type ก่อนทำการเพิ่มเติม

service_type_name
cas

ซึ่งในตารางนี้จะมีเพียงบริการ cas แต่ว่าในการทำงานร่วมกันกับแกรมที่ผู้วิจัยออกแบบให้เป็นบริการแบบ host ทำให้จำเป็นต้องเพิ่มบริการแบบ host เข้าไปเพื่อให้ได้ข้อมูลในตารางดังนี้

ตารางที่ ก.12 ข้อมูลในตาราง service_type หลังทำการเพิ่มเติม

service_type_name
cas
host

10. ตาราง service_type_action เป็นตารางที่เกี่ยวกับบริการและการกระทำ (action) บนบริการ ซึ่งมีเขตข้อมูลดังต่อไปนี้
    - service_action_id คือ หมายเลขของการกระทำบนบริการหนึ่งๆ
    - service_type_name คือ ชื่อของบริการ เช่น บริการ cas
    - action_name คือชื่อการกระทำบนบริการหนึ่งๆ

ซึ่งค่าโดยปริยายของตาราง service_type_action ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.13 ข้อมูลในตาราง service_type_action ก่อนทำการเพิ่มเติม

service_action_id	service_type_name	action_name
1	cas	enroll_trustAnchor
…	…	…
17	cas	query

ซึ่งในตารางนี้จะมีเพียงการกระทำต่างๆบนบริการ cas แต่ว่าในการทำงานร่วมกันกับแกรมที่ผู้วิจัยออกแบบให้เป็นบริการแบบ host ทำให้จำเป็นต้องเพิ่มการกระทำบนบริการแบบ host เข้าไปอีกสองการกระทำได้แก่ การกระทำ allow และ การกระทำ deny เพื่อให้ได้ข้อมูลในตารางดังนี้

ตารางที่ ก.14 ข้อมูลในตาราง service_type หลังทำการเพิ่มเติม

service_action_id	service_type_name	action_name
1	cas	enroll_trustAnchor
…	…	…
17	cas	query
18	host	allow
19	host	deny

11. ตาราง service_action_group เป็นตารางที่เกี่ยวกับ กลุ่มของการกระทำบนบริการใดๆ ซึ่งมีเขตข้อมูลดังต่อไปนี้

    - service_action_group_name คือ ชื่อของกลุ่มการกระทำบนบริการใดๆ

ซึ่งค่าโดยปริยายของตาราง service_action_group_name ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.15 ข้อมูลในตาราง service_action_group_name

service_action_group_name

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆนอกจากว่าจะเป็นการเพิ่มเนื่องจากเพิ่มกลุ่มการกระทำ

12. ตาราง service_action_group_entry เป็นตารางที่เกี่ยวกับกลุ่มการกระทำและการกระทำ ซึ่งมีเขตข้อมูลดังต่อไปนี้
    - service_action_group_name คือ ชื่อกลุ่มการกระทำ
    - service_action_id คือ หมายเลขการกระทำในตาราง service_type_action

ซึ่งค่าโดยปริยายของตาราง service_action_group_name ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.16 ข้อมูลในตาราง service_action_group_name

service_action_group_name	service_action_id

ในตารางนี้จะไม่เกี่ยวกับการทำนโยบายการใช้งานแกรมดังนั้นจึงไม่จำเป็นที่จะเพิ่มเติมข้อมูลใดๆ นอกจากว่าจะเป็นการเพิ่มเนื่องจากเพิ่มการกระทำเข้าไปในกลุ่มการกระทำ

13. ตาราง policy_table เป็นตารางเกี่ยวกับนโยบายการใช้งานบนแต่ละบริการของแต่ละทรัพยากรในองค์กรเสมือน ซึ่งมีเขตข้อมูลดังต่อไปนี้
    - policy_id คือ หมายเลขนโยบายการใช้งานบนแต่ละบริการของแต่ละทรัพยากรในองค์กรเสมือน
    - user_group_name คือ ชื่อกลุ่มผู้ใช้ในตาราง user_group_table
    - action_specification คือ หมายเลขการกระทำในตาราง service_type_action
    - action_spec_desc คือ คำอธิบายการกระทำ
    - object_specification คือ หมายเลขทรัพยากรในตาราง object_table
    - object_spec_desc คือคำอธิบายทรัพยากร

ซึ่งค่าโดยปริยายของตาราง policy_table ในงานวิจัยซีเอเอสเป็นดังนี้

ตารางที่ ก.17 ข้อมูลในตาราง policy_table ก่อนทำการเพิ่มเติม

policy_id	user_group_name	action specification	action_spec_desc	object_specification	object_spec_desc
1	superUserGroup	16	serviceAction	1	object

เมื่อจะทำนโยบายการใช้งานแกรมทำได้โดยเลือกหมายเลขการกระทำที่เกี่ยวข้องกับบริการ host และเลือกทรัพยากร ดังเช่นตัวอย่าง

ตารางที่ ก.18 ข้อมูลในตาราง policy_table หลังทำการเพิ่มเติม

policy _id	user_group_ name	action specification	action_spec_ desc	object_ specification	object_spec_ desc
1	superUserGroup	16	serviceAction	1	object
2	grad	18	serviceAction	2	object

ประวัติผู้เขียนวิทยานิพนธ์

นายปฏิภาณ คงสิริกุล เกิดเมื่อวันที่ 23 พฤศจิกายน พ.ศ. 2525 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ จากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2545 และเข้าศึกษาในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ปีการศึกษา 2546