การพัฒนาโปรแกรมระบบดูแลและบริหาร เครือข่ายเสมือนส่วนตัวผ่านเว็บ

THE DEVELOPMENT OF VIRTUAL PRIVATE NETWORK MANAGEMENT SYSTEM VIA WEB

โดย

เอกรัฐ ไพศาลเวชกรรม

EAKARAT PAISALVEJAKAM

อาจารย์ที่ปรึกษา

รศ. ดร. โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 1 ปีการศึกษา 2550

THE DEVELOPMENT OF VIRTUAL PRIVATE NETWORK MANAGEMENT SYSTEM VIA WEB

EAKARAT PAISALVEJAKAM

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/ 2007

ชื่อหัวข้อ	การพัฒนาโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ
นักศึกษา	นายเอกรัฐ ไพศาลเวชกรรม
รหัสนักศึกษา	48066510
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2550
อาจารย์ที่ปรึกษา	รศ.ดร.โชติพัชร์ ภรณวลัย

บทคัดย่อ

ในปัจจุบัน การใช้งานเครือข่ายเสมือนส่วนตัวผ่านเครือข่ายสาธารณะ (Virtual Private Network: VPN) ได้ถูกนำมาใช้งานอย่างแพร่หลาย เพื่อสร้างความปลอดภัยในการรับส่งข้อมูลจากเครื่องผู้ใช้ซึ่งอยู่ภายนอกองค์กรเชื่อมต่อไปยังเครือข่ายขององค์กรนั้นๆ ซึ่งในโครงงานนี้จะกล่าวถึงแอพลิเคชั่นที่ทำหน้าที่สร้างเครือข่ายเสมือนส่วนตัว คือ OpenVPN เนื่องจากซอฟต์แวร์ OpenVPN มีความยุ่งยากในการบริหารจัดการเพราะต้องแก้ไขค่าในไฟล์คอนฟิกหรือใช้ Command line และมีความยุ่งยากในการบริหารจัดการ key ที่ใช้เข้ารหัส รวมถึงการตรวจสอบสถานะของผู้เข้ามาใช้งาน ดังนั้นในโครงงานจึงได้ทำการศึกษาและวิเคราะห์ออกแบบเพื่อพัฒนาโปรแกรมโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านทางเว็บบราวเซอร์โดยในส่วนของการวิเคราะห์ออกแบบนั้นจะนำเสนอในรูปแบบของยูสเคสไดอะแกรม คลาสไดอะแกรม แอคทิวิตี้ไดอะแกรมและซีเควนซ์ไดอะแกรม เป็นหลักในการแสดงขั้นตอนการทำงานของตัวโปรแกรม พร้อมทั้งได้แสดงรูปแบบของข้อมูลที่เกี่ยวข้อง (Data format) ในโครงงานนี้เช่นกัน ส่วนหลักการทำงานของโปรแกรมนั้นจะเข้าไปจัดการควบคุม OpenVPN ซึ่งโปรแกรมที่พัฒนาขึ้นจะทำงานบนเว็บเซิร์ฟเวอร์พร้อมกับทำหน้าที่เป็น VPN เซิร์ฟเวอร์ด้วย โดยผู้ใช้จะสามารถใช้โปรแกรมที่พัฒนาขึ้นนี้ผ่านทางเว็บบราวเซอร์จากฝั่งไคลเอ็นท์โดยผ่านการพิสูจน์ตัวตนจาก Microsoft Active Directory ซึ่งสามารถร้องขอใบรับรอง ดาวน์โหลดซอฟต์แวร์และใบรับรองรวมถึงไฟล์คอนฟิกได้ นอกจากนี้ในส่วนของผู้ดูแลระบบยังสามารถจัดการเรื่องใบรับรอง จัดการเรื่องการสร้างไฟล์คอนฟิกของผู้ใช้และเซิร์ฟเวอร์ การดูสถานะการเชื่อมต่อและล็อก ซึ่งผลจากการพัฒนาโครงงานนี้จะทำให้ลดความยุ่งยากในการจัดการเครือข่ายแบบเดิมและยังได้เข้าใจหลักการการทำงานรวมถึงการพัฒนาโปรแกรมที่ใช้ในการจัดการเครือข่ายเสมือนส่วนตัวได้อีกด้วย

Title	The Development of Virtual Private Network Management System via Web
Student	Mr. Eakarat Paisalvejakam
Student ID.	48066510
Degree	Master of Science
Programme	Information Science
Academic Year	2007
Advisor	Assoc. Prof. Dr. Chotipat Pornnawalai

ABSTRACT

In recent years, Virtual Private Networks have become the de facto standard for secure remote access. They enable teleworkers, day extenders and business partners access to corporate network resources across un-trusted networks. So in this project will present the application that has functionality create Virtual Private Network that is "OpenVPN", a freeware SSL VPN based. This application has only been configured by using configuration file of Command Line Interface, it is very difficult to configure and manage the system. And the process of key distribution is insecure and hardly deploy. So this project will develop the web-based for manage OpenVPN called "Virtual Private Network Management System". In the analysis and design part, the representation of the program being introduced is the OpenVPN which VPN Server is working on the web server. The management will be controlled through the web browser on a client side. Users from the client side that authenticated via Microsoft Active Directory are able to request their certificate, download VPN Client Software and their certificate/ configuration files. Administrators are able to manage users and server certificate/configuration files, view OpenVPN status and log. The benefits of this project is not merely to reduce the difficulty in system management but it is also to gain the understanding of the OpenVPN principle and the development of VPN management too.

กิตติกรรมประกาศ

โครงการพัฒนาระบบงาน เรื่อง การพัฒนาโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ (The Development of Virtual Private Management System via Web) สำเร็จลงได้ด้วยความอนุเคราะห์จากบุคคลหลายฝ่าย ผู้เขียนใคร่ขอแสดงความระลึกถึงบุคคลสำคัญผู้ให้ความกรุณาดังต่อไปนี้

ขอกราบขอบพระคุณ รศ.ดร.โชติพัชร์ ภรณวลัย อาจารย์ที่ปรึกษาโครงงานและอาจารย์ประจำภาควิชาเทคโนโลยีสารสนเทศเป็นอย่างยิ่ง ที่กรุณาให้โอกาสในการทำโครงงานนี้ ตลอดจนการให้ความอนุเคราะห์ ให้คำแนะนำต่าง ๆ ทำให้การทำโครงการนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณบัณฑิตศึกษาและบัณฑิตวิทยาลัย คณะเทคโนโลยีสารสนเทศที่ให้ความช่วยเหลือในเรื่องต่าง ๆ

ขอขอบคุณเพื่อน ๆ หลักสูตรวิทยาศาสตรมาบัณฑิต สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกคนที่ให้คำแนะนำและให้ความช่วยเหลือต่าง ๆ เป็นอย่างดี รวมทั้งคอยให้กำลังใจเสมอมา

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา ครอบครัวและเพื่อน ๆ ของข้าพเจ้าที่เป็นกำลังใจ และให้การสนับสนุนในทุกเรื่อง ๆ ทำให้ข้าพเจ้าสามารถทำโครงงานนี้สำเร็จลุล่วงไปได้ด้วยดี

คุณค่าและประโยชน์อันพึงมาจากโครงงานนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

เอกรัฐ ไพศาลเวชกรรม

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในปัจจุบัน การทำงานของแต่ละองค์กรได้มีการเปลี่ยนแปลงไปจากเดิมมาก เนื่องจากองค์กรต่างๆต้องการให้พนักงานมีความคล่องตัวในการทำงานมากยิ่งขึ้น นั่นคือ สามารถทำงานได้ทุกที่ ทุกเวลา แม้อยู่ภายนอกองค์กร ดังนั้นจึงมีความจำเป็นต้องให้พนักงานเข้าถึงแอพลิเคชั่นที่ต้องการใช้งานได้ในทุกๆที่ การเชื่อมต่อเข้าไปยังบริษัทโดยวิธีหมุนโมเดมเป็นวิธีที่สามารถทำได้ แต่ถ้าเป็นการโทรทางไกลจะมีค่าใช้จ่ายที่สูงมาก อีกวิธีการหนึ่งคือการหมุนโมเดมไปยังผู้ให้บริการท้องถิ่นแล้วจึงเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตเข้าไปยังองค์กร ซึ่งวิธีการนี้ไม่จำเป็นต้องเสียค่าโทรทางไกล แต่สิ่งที่ต้องคำนึงอยู่เสมอสำหรับการใช้อินเทอร์เน็ตเป็นตัวกลางในการเชื่อมต่อก็คือ การดักจับข้อมูลจากผู้ไม่หวังดี ดังนั้นจึงได้มีเทคโนโลยีที่ออกมาเพื่อแก้ปัญหานี้ก็คือ การใช้งานโดยผ่านเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network: VPN) ซึ่งจะเป็นการจำลองเครือข่ายโดยเสมือนมีอุโมงค์ (Tunnel) มาหุ้มการเชื่อมต่อนั้นๆ ซึ่งก็คือ การเข้ารหัสและถอดรหัสข้อมูลนั่นเอง ทำให้ผู้ดักจับข้อมูลในเครือข่ายอินเทอร์เน็ตไม่สามารถนำข้อมูลไปใช้ได้

ระบบเครือข่ายเสมือนส่วนตัวได้ถูกพัฒนาเรื่อยมาทั้งที่อยู่ในรูปของฮาร์ดแวร์และซอฟต์แวร์ เช่น Poptop, Tinc Openswan VPN และ OpenVPN โดยเฉพาะ OpenVPN นั้นเป็นซอฟต์แวร์ที่รองรับการทำงานหลายแพล็ตฟอร์ม และเป็นฟรีแวร์คือไม่เสียค่าใช้จ่ายใดๆทั้งสิ้น จึงเป็นที่นิยมนำไปติดตั้งใช้งาน โดยผู้ดูแลระบบสามารถจะจัดการในส่วนของการเพิ่มหรือติดตั้งอินเทอร์เฟสเพื่อติดต่อระหว่างเครื่องไคลเอนต์กับ วีพีเอ็นเซิร์ฟเวอร์ อีกทั้งยังมีการเปิดเผยโค้ด (Open source code) เพื่อสามารถนำไปศึกษาการทำงานและพัฒนาต่อไปได้ ดังนั้นในโครงงานนี้จึงเลือกเอาซอฟต์แวร์ OpenVPN นี้มาพัฒนาต่อ

ในโครงงานพัฒนาระบบงานนี้จะมุ่งเน้นพัฒนาโปรแกรมเพื่อใช้ในการจัดการระบบการทำงานของเครือข่ายเสมือนส่วนตัว (VPN) โดยใช้แอพลิเคชั่น OpenVPN บนระบบปฏิบัติการ Red Hat Enterprise Linux ซึ่งโครงงานที่พัฒนาขึ้นนี้จะทำงานเป็นส่วนติดต่อกับผู้ใช้ผ่านเว็บบราวเซอร์ ซึ่งตัวโปรแกรมจะเข้าไปสร้างไฟล์คอนฟิกพร้อมกับการส่ง Command line ให้แทนการที่ผู้ใช้จะสร้างไฟล์คอนฟิกโดยตรงซึ่งจะต้องทำที่เครื่องเซิร์ฟเวอร์ แต่ด้วยความสามารถของโปรแกรมที่พัฒนาขึ้นนั้นจะสามารถทำการเพิ่มและลบผู้ดูแลระบบระบบ สร้างและยกเลิกการใช้ใบรับรองดิจิตอลของผู้ใช้งาน สร้างและดาวน์โหลดไฟล์คอนฟิกและใบรับรองดิจิตอล ตลอดจนตรวจสอบ

การใช้งานของผู้ใช้งานระบบได้ โดยผ่านการเชื่อมต่อแบบกราฟิก ทำให้ง่ายต่อการจัดการ และการใช้งาน

1.2 วัตถุประสงค์ของโครงการ

ในการพัฒนาระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ มีวัตถุประสงค์หลักดังต่อไปนี้

1. เพื่อช่วยลดความยุ่งยากและซับซ้อนของผู้ใช้และผู้ดูแลระบบในการบริหารจัดการการใช้งาน OpenVPN โดยผู้ใช้และผู้ดูแลสามารถใช้งานระบบได้โดยผ่านเว็บบราวเซอร์ โดยไม่จำเป็นต้องอยู่ที่เครื่องเซิร์ฟเวอร์ที่ให้บริการโดยตรง
2. เพื่อศึกษาการพัฒนาเครื่องมือที่ช่วยในการจัดการเครือข่ายเสมือนส่วนตัว OpenVPN บนระบบปฏิบัติการ Red Hat Enterprise Linux
3. โปรแกรมที่พัฒนาขึ้นจะสามารถเพิ่มประสิทธิภาพในการใช้งานโดยการจัดรูปแบบให้เข้าใจง่ายในการใช้งาน
4. ในการพัฒนาโปรแกรมจะพยายามให้ใช้ทรัพยากรของระบบให้น้อยที่สุด

1.3 ขอบเขตของโครงการ

ระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ถูกออกแบบมาให้มีหน้าที่การทำงานหลักๆ ดังนี้

1. ระบบการจัดการการใช้งานของผู้ดูแลระบบ (Account Management)
   - มีส่วนของการเพิ่มรายชื่อผู้ดูแลระบบ
   - มีส่วนของการลบรายชื่อผู้ดูแลระบบ
   - มีส่วนของการเปลี่ยนรหัสผ่านของผู้ดูแลระบบ
   - มีส่วนของการดูรายละเอียดของผู้ดูแลระบบทั้งหมด
2. ระบบการตรวจสอบสถานะในการใช้งาน (Status and log)
   - ผู้ดูแลระบบสามารถตรวจสอบการใช้งานของผู้ใช้งานระบบได้
   - ผู้ดูแลระบบสามารถดูของ log ของโปรแกรม OpenVPN ได้
3. ระบบการจัดการใบรับรอง (Certificate Management)
   - ผู้ใช้งานสามารถร้องขอใบรับรองจากผู้ดูแลได้
   - ผู้ดูแลระบบสามารถรับรองและอนุญาตหรือปฏิเสธให้ผู้ใช้งานมีใบรับรองได้
   - ผู้ดูแลระบบสามารถสร้างใบรับรองของผู้ใช้งานแต่ละคนได้ และสามารถกำหนดวันหมดอายุของใบรับรองได้ด้วย

- ผู้ดูแลระบบสามารถยกเลิกการใช้งานใบรับรองของผู้ใช้งานแต่ละรายได้
- ผู้ใช้งานระบบสามารถดาวน์โหลดใบรับรองของตนเองเพื่อนำไปใช้งานได้
- ผู้ดูแลระบบสามารถสร้างใบรับรองของเซิร์ฟเวอร์ได้

4. ระบบการจัดการคุณสมบัติต่างๆ (Configuration Management)
   - ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกของผู้ใช้งานระบบแต่ละรายได้
   - ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกของเซิร์ฟเวอร์ได้
   - ผู้ใช้งานระบบสามารถดาวน์โหลดไฟล์คอนฟิกของตนเองเพื่อนำไปใช้งานได้
5. ระบบควบคุมการเข้าใช้งานและพิสูจน์ตัวตน
   - ผู้ใช้สามารถ logon เข้าใช้งานระบบได้โดยสามารถพิสูจน์ตัวตนได้จาก Active Directory
6. ระบบให้บริการดาวน์โหลดซอฟต์แวร์
   - ผู้ใช้งานสามารถดาวน์โหลดซอฟต์แวร์ OpenVPN มาติดตั้งที่เครื่องตนเองได้
   - ผู้ดูแลระบบสามารถอัพโหลดและลบซอฟต์แวร์ OpenVPN ได้

1.4 ขั้นตอนการดำเนินงาน

แนวทางในการดำเนินการพัฒนาระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บจะมีขั้นตอนในการวิเคราะห์และออกแบบระบบงานตามทฤษฎีของ SDLC ซึ่งมีขั้นตอนหลักๆ ดังนี้

1. กำหนดความต้องการ เป็นขั้นตอนในการรวบรวมรายละเอียดต่างๆ ที่เกี่ยวข้องกับระบบงาน เพื่อหาข้อสรุปที่ชัดเจนในการที่จะนำเอารายละเอียดเหล่านี้ไปใช้ในขั้นตอนของการวิเคราะห์และออกแบบระบบต่อไป
2. วิเคราะห์ เป็นขั้นตอนในการวิเคราะห์การดำเนินงานของระบบปัจจุบันว่ามีขั้นตอนการทำงานเป็นอย่างไร
3. ออกแบบ เป็นการนำเอาผลลัพธ์ที่ได้ จากการวิเคราะห์มาออกแบบระบบใหม่ โดยจะนำเสนอออกมาในรูปของ
   - แผนภาพยูสเคสไดอะแกรม (Use Case Diagram) จะเป็นส่วนที่ใช้ในการแสดงความสัมพันธ์ระหว่างผู้ใช้ระบบกับกิจกรรมต่างๆ
   - แผนภาพแอคทิวิตีไดอะแกรม (Activity Diagram) จะเป็นส่วนที่ใช้แสดงกิจกรรมของผู้ใช้ระบบว่ามีขั้นตอนการทำงานเป็นอย่างไร
   - แผนภาพซีเควนซ์ไดอะแกรม (Sequence Diagram) จะเป็นส่วนที่ใช้แสดงการรับส่งข้อมูลในแต่ละฟังก์ชัน

- แผนภาพความสัมพันธ์ระหว่างเอนทิตี (Entity Relationship Diagram หรือ ER-Diagram) จะเป็นส่วนที่ใช้ในการแสดงให้เห็นถึงข้อมูลและความสัมพันธ์ของข้อมูลต่างๆ ที่มีต่อกันภายในระบบงาน

4. พัฒนา เป็นขั้นตอนในการเลือกเครื่องมือและภาษาที่จะใช้ในการพัฒนาระบบและพัฒนาระบบตามที่ได้ทำการวิเคราะห์และออกแบบไว้
5. ทดสอบ เป็นขั้นตอนในการทดสอบระบบก่อนที่จะนำไปใช้งานจริง โดยจะมีการทดสอบดังนี้
    - การทดสอบทำงานของฟังก์ชันภายในโปรแกรม ว่าสามารถทำงานได้ถูกต้องหรือไม่
    - การทดสอบการทำงานของทั้งระบบว่าถูกต้องตรงกับรายละเอียดของระบบที่ได้วิเคราะห์ไว้ และสามารถทำงานได้ถูกต้องตรงกับความต้องการของผู้ใช้งานหรือไม่
6. ติดตั้ง นำระบบที่ผ่านการทดสอบแล้วมาติดตั้งเพื่อใช้งาน โดยจะมีขั้นตอนดังนี้
    - เตรียมอุปกรณ์ฮาร์ดแวร์และอุปกรณ์ที่เกี่ยวกับระบบเครือข่ายที่จำเป็นต่อการติดตั้งระบบ
    - ลงระบบปฏิบัติการและแอพลิเคชั่นโปรแกรมทั้งหมดที่เกี่ยวข้อง
    - ใช้งานระบบ
    - จัดทำคู่มือระบบ
7. บำรุงรักษา ทำการปรับปรุงและแก้ไขระบบ หลังจากที่ได้มีการติดตั้งและใช้งานแล้ว

1.5 ประโยชน์ที่คาดว่าจะได้รับ

- ได้เครื่องมือที่ช่วยในการบริหารจัดการเครือข่ายเสมือนส่วนตัวโดยทำงานร่วมกับ OpenVPN ซึ่งเครื่องมือนี้สามารถใช้งานได้อย่างง่ายดายและสะดวกเพราะเป็นการใช้งานผ่านเว็บบราวเซอร์
- ได้ศึกษาหลักการทำงานของเครือข่ายเสมือนส่วนตัว
- ได้เรียนรู้การพัฒนาระบบด้วยภาษา PHP และ Java Script
- สามารถนำความรู้ที่ได้ไปประยุกต์ใช้กับการพัฒนาโปรแกรมเพื่อควบคุมแอพลิเคชั่นอื่นผ่านทางเว็บ

1.6 ขั้นตอนในการพัฒนาระบบ

ตารางที่ 1.1 ขั้นตอนการพัฒนาระบบ

ลำดับ	รายละเอียด	ปี 2550					
		พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.
1	รวบรวมรายละเอียดและศึกษาความเป็นไปได้ของโครงการ						
2	กำหนดขอบเขตและรวบรวมความต้องการของระบบ (Requirement)						
3	ศึกษาทฤษฎีที่เกี่ยวข้องกับการพัฒนาระบบ						
4	วิเคราะห์และออกแบบระบบ (Analysis & Design)						
4.1	ออกแบบแอพพลิเคชั่น (Application Design)						
4.2	ออกแบบฐานข้อมูล (Database Design)						
4.3	ออกแบบหน้าจอส่วนต่อประสานกับผู้ใช้ (User Interface Design)						
5	พัฒนาระบบ (Implementation)						
5.1	พัฒนา Module การจัดการการพิสูจน์ตัวตนจาก Microsoft Active Directory						
5.2	พัฒนา Module การสร้างไฟล์คอนฟิกของผู้ใช้งานและของเซิร์ฟเวอร์						
5.3	พัฒนา Module การจัดการใบรับรองดิจิตอลของผู้ใช้งาน						
5.4	พัฒนา Module การจัดการใบรับรองดิจิตอลของเซิร์ฟเวอร์						
6	ทดสอบระบบและทำการแก้ไข (Test and Debug)						
7	จัดทำเอกสารโครงการ						

บทที่ 2
เครือข่ายเสมือนส่วนตัวและโอเพ่นวีพีเอ็น

2.1 เครือข่ายเสมือนส่วนตัว (Virtual Private Network: VPN)

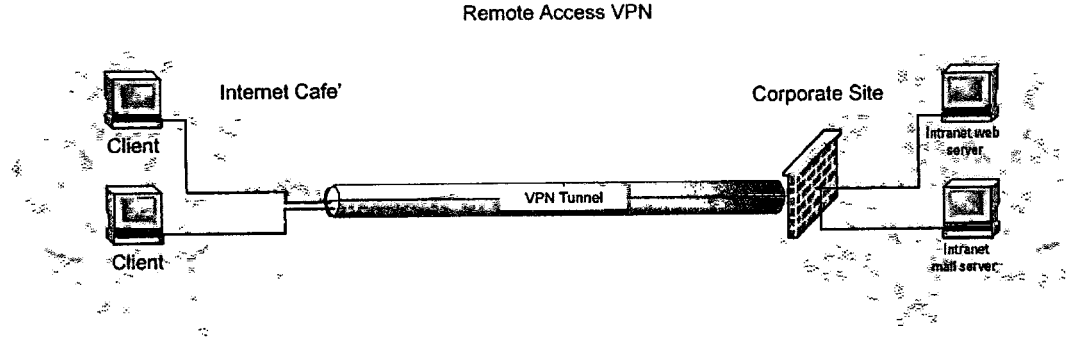
Virtual Private Network (VPN) หมายถึง เครือข่ายเสมือนส่วนตัวที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะ แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสแพ็คเก็ตก่อนส่งเพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น การเข้ารหัสนั้นมีหลายกลไกด้วยกัน ถ้าเป็นการเข้ารหัสที่เลเยอร์ 2 ส่วนมากจะใช้ Layer Two Tunneling Protocol (L2TP) หรือ Point-to-Point Tunneling Protocol (PPTP) และที่เลเยอร์ 3 จะใช้ Internet Protocol Security (IPSec) โดยปกติแล้ว VPN จะถูกนำมาใช้กับองค์กรขนาดใหญ่ที่มีสาขาอยู่ตามที่ต่างๆและต้องการเชื่อมต่อเข้าหากัน โดยยังคงสามารถรักษาเครือข่ายให้สามารถใช้ได้เฉพาะคนภายในองค์กรหรือบุคคลที่เกี่ยวข้องด้วยเช่น ลูกค้า และซัพพลายเออร์ เป็นต้น

2.2 รูปแบบการให้บริการของเครือข่ายเสมือนส่วนตัว

รูปแบบการให้บริการของ VPN แบ่งเป็น 2 รูปแบบหลักๆ คือ

2.2.1 Remote Access VPN

เป็นรูปแบบในการเข้าถึงเครือข่าย VPN จากอุปกรณ์เคลื่อนที่ต่างๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ โดยลักษณะแรกเป็นการเข้าถึงจากไคลเอนท์ใดๆ ก็ได้ โดยอาศัยผู้ให้บริการอินเทอร์เน็ตเป็นตัวกลางในการติดต่อ ซึ่งจะมีการเข้ารหัสในการรับส่งข้อมูลจากเครื่องไคลเอนท์ไปยังผู้ให้บริการอินเทอร์เน็ต และลักษณะที่สอง เป็นการเข้าถึงจากเครื่องแอ็กเซสเซิร์ฟเวอร์ (Network Access Server – NAS) โดยเริ่มต้นจากผู้ใช้หมุนโมเดม ติดต่อมายังผู้ให้บริการอินเทอร์เน็ตจากนั้นจะมีการเข้ารหัสข้อมูลและส่งต่อไปยังปลายทาง รูปที่ 2.1 แสดงการทำงานแบบ Remote Access VPN



รูปที่ 2.1 การใช้งาน VPN แบบ Remote Access

2.2.2 Site to Site VPN

รูปแบบบริการแบบนี้สามารถแบ่งย่อยได้อีก 2 ประเภทได้แก่

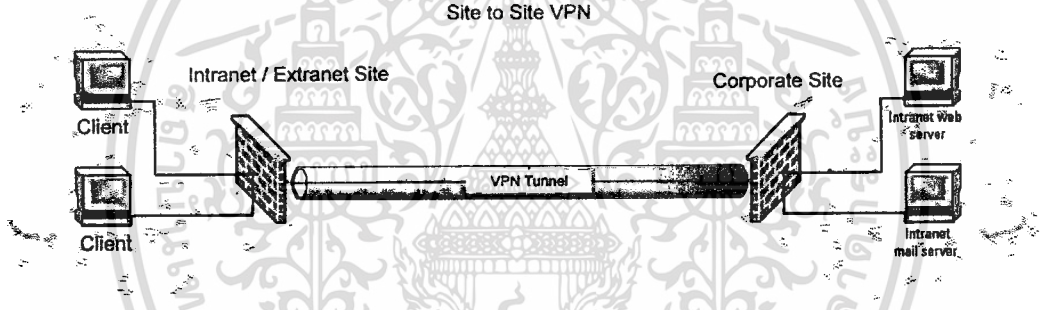
- Intranet VPN

เป็นรูปแบบในการเข้าถึงเครือข่าย VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น เช่น การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่ในกรุงเทพมหานคร กับสาขาย่อยในต่างจังหวัด เสมือนกับการทดแทนการเช่าวงจร leased line ระหว่างกรุงเทพฯกับต่างจังหวัด โดยที่แต่ละสาขาสามารถต่อเชื่อมกับผู้ให้บริการอินเทอร์เน็ตในท้องถิ่นของตนเพื่อเชื่อมเข้ากับเครือข่าย VPN ขององค์กรอีกทีหนึ่ง

- Extranet VPN

เป็นรูปแบบในการเข้าถึงเครือข่ายที่คล้ายกับ Intranet VPN แต่มีการขยายวงออกไป ได้แก่ กลุ่มลูกค้า ซัพพลายเออร์และพาร์ตเนอร์ เป็นต้น

รูปที่ 2.2 แสดงการทำงานแบบ Site to Site VPN



รูปที่ 2.2 การใช้งาน VPN แบบ Site to Site

2.3 หลักการทำงานของเครือข่ายเสมือนส่วนตัว

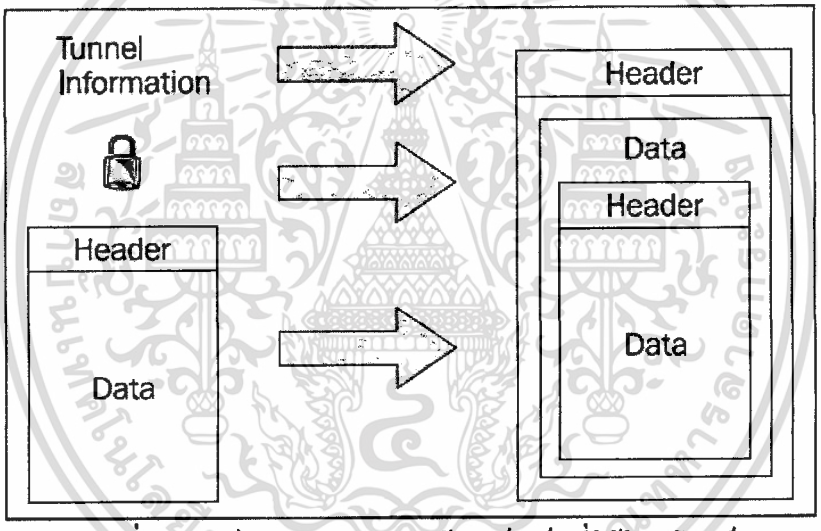
การทำงานของเครือข่ายเสมือนส่วนตัวจะเริ่มจากต้นทางและปลายทางซึ่งมีความสามารถในการเชื่อมต่อเครือข่ายเสมือนส่วนตัวอาจเป็นฮาร์ดแวร์หรือซอฟต์แวร์ มีการสร้างการเชื่อมต่อเป็นอุโมงค์หรือเรียกว่า Tunnel ซึ่งอุโมงค์นี้อาศัยหลักการของการเข้ารหัสและถอดรหัสนั่นเอง คือ ผู้ที่ไม่มีกุญแจในการถอดรหัสจะไม่สามารถนำข้อมูลไปใช้ประมวลผลต่อได้ ซึ่งเปรียบเสมือนเป็นการสร้างอุโมงค์ส่วนตัวในเครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะให้มีความปลอดภัยในการส่งข้อมูลเพิ่มมากขึ้นด้วย ในปัจจุบันอุปกรณ์ที่ทำหน้าที่เป็นวีพีเอ็นเกตเวย์จะอยู่รวมกับไฟร์วอลล์ขององค์กรนั้นๆโดยอาจเป็นฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้

ในการทำอุโมงค์ (Tunnel) นั้น จะประกอบด้วยส่วนต่างๆ 3 ส่วน ดังนี้

- Tunnel information เป็นส่วนของเฮดเดอร์ของอุโมงค์ซึ่งได้แก่ ข้อมูลของผู้รับและผู้ส่ง รวมถึงส่วนอธิบายข้อมูล (Metadata) ซึ่งจะใช้ในการทำงานของซอฟต์แวร์วีพีเอ็น

- Encryption data and method เป็นวิธีการและกลไกในการเข้ารหัสข้อมูลและถอดรหัสข้อมูล
- The original IP Packet (or network frame) เป็นส่วนของแพ็คเก็ตของข้อมูลที่ถูกเข้ารหัสหรือเฟรมข้อมูล แล้วแต่ว่าจะเข้ารหัสที่เลเยอร์ไหน

ซึ่ง 3 ส่วนนี้จะประกอบกันขึ้นเป็นแพ็คเก็ตใหม่เพื่อใช้ส่งผ่านอุโมงค์ไปยังปลายทางโดยมีการนำแพ็คเก็ตต้นฉบับมาเข้ารหัสด้วยวิธีการต่างๆและเพิ่มส่วนของเฮดเดอร์ซึ่งประกอบด้วยข้อมูลของผู้ส่งและผู้รับและข้อมูลต่างๆที่จำเป็นต้องใช้ซึ่งในส่วนนี้ตัวซอฟต์แวร์วีพีเอ็นจะเป็นตัวจัดการให้ ในการสร้างแพ็คเก็ตใหม่นี้จะทำให้เกิด overhead ในการส่งข้อมูลขึ้น ซึ่งจะมากหรือน้อยขึ้นกับความสามารถของซอฟต์แวร์วีพีเอ็นนั้นๆ รูปที่ 2.3 แสดงองค์ประกอบในการสร้างแพ็คเก็ตใหม่ที่ใช้ในการส่งข้อมูลไปในอุโมงค์ (Tunnel)



รูปที่ 2.3 องค์ประกอบในการสร้างแพ็คเก็ตที่ใช้ในอุโมงค์

2.4 มาตรฐานโปรโตคอลที่ใช้ในการอิมพลีเมนต์

General Routing Encapsulation หรือ GRE ได้กำหนดมาตรฐานสำหรับการทำอุโมงค์ข้อมูลขึ้นมาเมื่อปี 1994 ใน RFCs 1701 และ 1702 แม้ว่าจะไม่ได้กำหนดขึ้นมาเป็นนิยามของข้อตกลงแต่มาตรฐานนี้เป็นที่รู้จักและถูกนำไปใช้อย่างแพร่หลายในการสร้างอุโมงค์ข้อมูลในอุปกรณ์ต่างๆ จนกลายมาเป็นพื้นฐานของข้อตกลงอื่นๆ

แนวความคิดของ GRE คือ กำหนดให้เพิ่มส่วนหัวของโปรโตคอล (protocol header) และส่วนหัวของการส่งข้อมูล (delivery header) ลงไปในชุดข้อมูลต้นฉบับด้วย สำหรับส่วน payload ให้แยกออกมาเก็บไว้ในแพ็คเก็ตใหม่โดยไม่มีการเข้ารหัสข้อมูล แนวคิดอย่างง่ายนี้มีทางเป็นไปได้สูงและผู้ดูแลระบบ (administrator) รวมถึงเราท์เตอร์สามารถดูเนื้อแพ็คเก็ตได้เพื่อตัดสินใจให้แพ็คเก็ตนั้นๆควรไปทางใดตามชนิดของ payload

สำหรับโปรโตคอลที่ใช้ในการอิมพลีเมนต์เครือข่ายเสมือนส่วนตัวนั้น สามารถแบ่งได้ดังนี้

2.4.1 โปรโตคอลที่อิมพลีเมนต์ในเลเยอร์ 2 ของ OSI

- The Point to Point Tunneling Protocol (PPTP) เป็นส่วนขยายมาจาก PPP และรวมอยู่ในระบบปฏิบัติการไมโครซอฟต์ในปัจจุบัน PPTPใช้ GRE ในการห่อหุ้มและสร้างอุโมงค์ส่งข้อมูลที่ใช้โปรโตคอล IP , IPX และชนิดอื่นๆที่ใช้บน Internet ข้อจำกัดของเทคนิคนี้คือจะสร้างได้แค่ 1 อุโมงค์ต่อ 1 การเชื่อมต่อระหว่างกัน 1 คู่เท่านั้น
- The Layer 2 Forwarding (L2F) ช่วยขยายความสามารถของเทคนิค PPTP ในเรื่องการสร้างอุโมงค์ส่งข้อมูลเป็น network frame และเพิ่มช่องทางอุโมงค์ให้มากขึ้นและใช้งานพร้อมๆกัน(multiple simultaneous tunnels)
- The Layer 2 Tunneling Protocol (L2TP) เป็นเทคนิคที่ยอมรับให้เป็นมาตรฐานอุตสาหกรรมและใช้อย่างแพร่หลายในการผลิตอุปกรณ์เครือข่ายของโรงงานต่างๆ เช่น CISCO เทคนิคนี้รวมเอาประโยชน์ที่ได้จาก PPTP และ L2F มารวมกัน และแม้ว่าจะไม่มีกระบวนการรักษาความปลอดภัยข้อมูล แต่ว่าสามารถนำเทคนิคเช่น IPSec มาใช้ร่วมในระดับชั้นที่สูงกว่าได้ (Layer 3)
- The Layer 2 Security Protocol (L2Sec) ถูกพัฒนาเพื่อแก้ปัญหาเกี่ยวกับการรักษาความปลอดภัยของการไหลของข้อมูลประเภท IPSec แม้ว่าการเข้ารหัสจะทำให้ส่วนหัวของแพ็คเก็ตมีขนาดใหญ่ขึ้น แต่รับรองความปลอดภัยสูงเนื่องจากนำหลักการ SSL/TLS มาใช้

2.4.2 โปรโตคอลที่อิมพลีเมนต์ในเลเยอร์ 3 ของ OSI

IPSec เป็นเทคนิคที่นิยมใช้กันแพร่หลายในการสร้างอุโมงค์ส่งข้อมูล IPSec ถูกพัฒนาขึ้นให้เป็นมาตรฐานระบบรักษาความปลอดภัยในอินเทอร์เน็ต (an Internet Security Standard) ในระดับชั้นที่ 3 ของมาตรฐาน OSI ซึ่งประกาศโดยองค์กร IETF ตั้งแต่ปี 1995 IPsec สามารถใช้ห่อหุ้มการส่งข้อมูลในระดับชั้นแอพลิเคชั่น (Application Layer) แต่ไม่สามารถใช้ในระดับชั้นที่ต่ำกว่าเน็ตเวิร์คได้ IPSec แบ่งเป็น 2 แบบ คือ

- Tunnel Mode หรือแบบอุโมงค์ ทำงานโดย IP packet ทั้งหมดถูกห่อหุ้มเป็นแพ็คเก็ตใหม่และส่งไปในอีกอุโมงค์หนึ่งที่ไปยังปลายทางเดียวกัน และจะถูกเปิดออกโดยซอฟต์แวร์วีพีเอ็นแล้วส่งไปยังผู้รับ ด้วยวิธีการนี้ทั้งหมายเลขไอพีของผู้ส่งและผู้รับก็จะถูกป้องกันด้วยเช่นกัน

- Transport Mode หรือแบบขนส่ง จะทำการเข้ารหัสและห่อหุ้มเฉพาะส่วนของ payload เท่านั้น ด้วยกระบวนการนี้ทำเห็นว่า overhead จะมีขนาดเล็กกว่าการทำแบบอุโมงค์ (Tunnel Mode) แต่หากมีผู้ดักจับข้อมูล ก็จะสามารถทราบได้ว่ามีข้อมูลถูกส่งจากใครไปหาใคร อย่างไรก็ตามจะไม่สามารถอ่านข้อมูลได้เนื่องจากถูกเข้ารหัสไว้ ทำให้ IPSec จึงเหมือนกับเป็นเครือข่ายเสมือนส่วนตัวจริงๆ

2.4.3 โปรโตคอลที่อิมพลีเมนต์ในเลเยอร์ 4 ของ OSI

ผู้ใช้งานสามารถเชื่อมต่อเข้ากับระบบเครือข่ายส่วนตัวเสมือนผ่านทาง HTTPS จากเว็บบราวเซอร์เชื่อมต่อไปยังระบบในองค์กรของตนเองได้โดยอาศัยระบบรักษาความปลอดภัยที่ชื่อว่า Secure Sockets Layer (SSL) และ Transport Layer Security (TLS) ในปัจจุบัน มีซอฟต์แวร์หลายยี่ห้อที่รองรับการทำงานผ่านระบบรักษาความปลอดภัย SSL จากเว็บบราวเซอร์เพิ่มมากขึ้น การเข้ารหัสข้อมูลด้วยกระบวนการของ SSL/TLS ทำให้สามารถรับรองได้ว่าข้อมูลในขณะทำการส่งนั้นมีความปลอดภัยจากผู้โจรกรรมข้อมูลทางเครือข่ายได้

2.5 กลไกในการรักษาความปลอดภัยของเครือข่ายเสมือนส่วนตัว

เป้าหมายหลักในการรักษาความปลอดภัยของเครือข่ายเสมือนส่วนตัวนั้นประกอบด้วย 3 หัวข้อหลัก ดังนี้

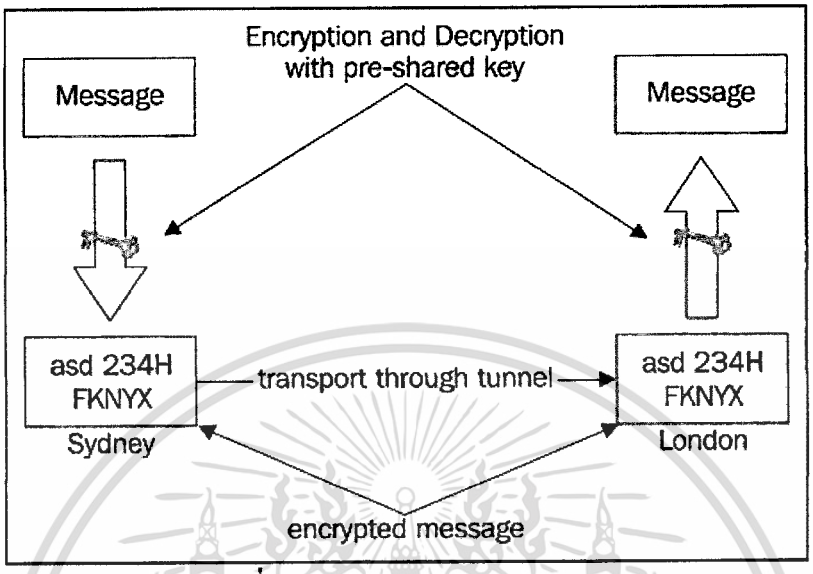
- Privacy (Confidentiality) หมายถึงข้อมูลที่ส่งออกไปต้องไม่ถูกเปิดเผยโดยผู้ที่ไม่ได้รับอนุญาต
- Reliability (Integrity) หมายถึง ข้อมูลที่ส่งออกไปจะต้องไม่ถูกเปลี่ยนแปลงแก้ไขก่อนถึงผู้รับ
- Authentication/ Non-Repudiation หมายถึง ข้อมูลที่ส่งออกไปจะต้องสามารถตรวจสอบได้ว่าใครเป็นผู้ส่งข้อมูลและในทางกลับกันก็ไม่สามารถปฏิเสธการกระทำของตนเองได้

สำหรับการสร้างความปลอดภัยของเครือข่ายเสมือนส่วนตัวนั้นจะอาศัยหลักการของการเข้ารหัสและถอดรหัสนั่นเอง เราสามารถแบ่งประเภทการเข้ารหัสได้เป็น 2 แบบ ดังนี้

2.5.1 การเข้ารหัสแบบสมมาตร (Symmetric key Encryption)

การเข้ารหัสแบบสมมาตรบางครั้งอาจเรียกว่า การเข้ารหัสแบบกุญแจส่วนตัว (Private/secret key or Pre-shared key encryption) อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) หรือ Pre-shared key ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้าและถอดรหัสข้อความที่ส่งไป อัลกอริทึมยังสามารถแบ่งย่อยออกเป็น 2 ประเภท ได้แก่ แบบบล็อค (Block Algorithms) ซึ่งจะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์ เช่น 64 ไบต์ เป็นต้น) และแบบ

สตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์ ตัวอย่างอัลกอริทึมการเข้ารหัสแบบสมมาตรได้แก่ DES, 3DES, IDEA, Blowfish และ AES เป็นต้น การเข้ารหัสแบบสมมาตรแสดงดังรูปที่ 2.4



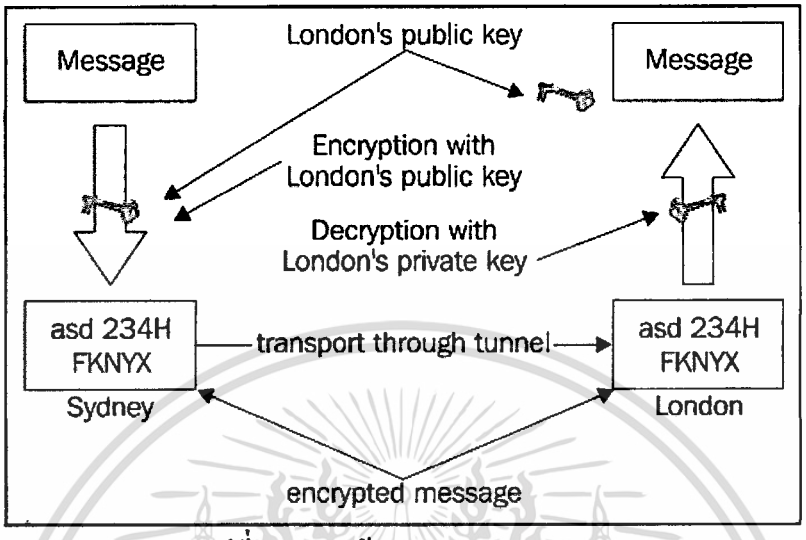
รูปที่ 2.4 การเข้ารหัสแบบสมมาตร

ข้อดีของการใช้วิธีนี้ในการทำงานของวีพีเอ็นคือ ทำงานได้รวดเร็วและมีความง่ายและสะดวกสบายมากกว่า แต่มีข้อเสียคือ เนื่องจากมีการใช้ Secret key เดียวในการเข้ารหัสและถอดรหัสข้อมูล ทำให้สามารถโดนการโจมตีแบบสุ่ม (Brute-force attack) เพื่อหาค่า secret key จากผู้ไม่หวังดีได้ ปัญหานี้อาจแก้ได้โดยมีการเปลี่ยนค่า secret key บ่อยๆ อีกปัญหาหนึ่งคือ การแลกเปลี่ยน secret key ระหว่างผู้ส่งและผู้รับ ต้องมีความปลอดภัยมากพอ ซอฟต์แวร์วีพีเอ็น เช่น IP Sec จะใช้วิธีการของ IKE ในการแลกเปลี่ยนกุญแจ

2.5.2 การเข้ารหัสแบบอสมมาตร (Asymmetric key Encryption)

การเข้ารหัสแบบอสมมาตรบางครั้งอาจเรียกว่า การเข้ารหัสแบบกุญแจสาธารณะ (Public key encryption) อัลกอริทึมนี้จะใช้กุญแจสองตัวเพื่อทำงาน ตัวหนึ่งใช้ในการเข้ารหัสและอีกตัวหนึ่งใช้ในการถอดรหัสข้อมูลที่เข้ารหัสมาโดยกุญแจตัวแรก อัลกอริทึมกลุ่มสำคัญในแบบอสมมาตรนี้คือ อัลกอริทึมแบบกุญแจสาธารณะ (Public keys Algorithms) ซึ่งใช้กุญแจที่เรียกกันว่า กุญแจสาธารณะ (Public keys) ในการเข้ารหัสและใช้กุญแจที่เรียกกันว่า กุญแจส่วนตัว (Private keys) ในการถอดรหัสข้อมูลนั้น กุญแจสาธารณะนี้สามารถส่งมอบให้กับผู้อื่นได้ เช่น เพื่อนร่วมงานที่เราต้องการติดต่อด้วย หรือแม้กระทั่งวางไว้บนเว็บไซต์เพื่อให้ผู้อื่นสามารถดาวน์โหลดไปใช้งานได้ สำหรับกุญแจส่วนตัวนั้นต้องเก็บไว้กับผู้เป็นเจ้าของกุญแจส่วนตัวเท่านั้นและห้าม

เปิดเผยให้ผู้อื่นทราบโดยเด็ดขาด ตัวอย่างอัลกอริทึมการเข้ารหัสแบบอสมมาตรได้แก่ RSA, DSS เป็นต้น การเข้ารหัสแบบสมมาตรแสดงดังรูปที่ 2.5



รูปที่ 2.5 การเข้ารหัสแบบอสมมาตร

ข้อดีของการใช้วิธีนี้ในการทำงานของวีพีเอ็นคือ มีความปลอดภัยมากกว่าเพราะเป็นการใช้กุญแจคู่ ผู้รับจะสามารถถอดรหัสได้ต้องมี Private key ของผู้รับเท่านั้นและข้อความที่จะถอดรหัสได้ต้องถูกเข้ารหัสด้วย public key ของผู้รับโดยผู้ส่งเท่านั้น ข้อดีอีกข้อคือสามารถยืนยันตัวตนของผู้ส่งได้ โดยผู้ส่งจะเข้ารหัสข้อมูลด้วย private key ของตนเองแล้วผู้รับก็ถอดรหัสด้วย public key ของผู้ส่ง วิธีการเช่นนี้เรียกว่าลายเซ็นดิจิตอล (Digital Signature)

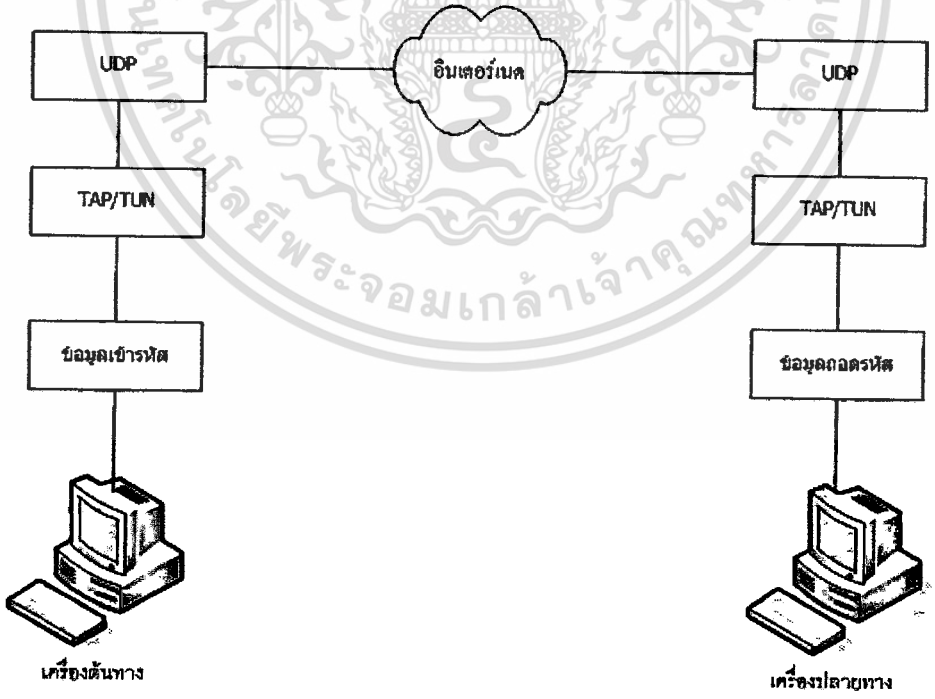
ข้อเสียของวิธีการนี้คือ ต้องใช้เวลาในการคำนวณการเข้าและถอดรหัส เมื่อเทียบกับระบบกุญแจสมมาตร และอาจใช้เวลาเป็นพันเท่าของเวลาที่ใช้โดยระบบกุญแจสมมาตร

อย่างไรก็ตามการเข้ารหัสทั้งแบบสมมาตรและอสมมาตรยังมีข้อเสียคือในเรื่องของการขยายขนาดของการใช้งาน (Scalability) สมมติว่ามีการเชื่อมต่อกัน N คู่โดยแบบสมมาตรจะต้องใช้กุญแจในการเข้ารหัสถึง N(N-1)/2 ตัว แต่แบบอสมมาตรจะลดลงได้เยอะคือจะใช้กุญแจสาธารณะของเซิร์ฟเวอร์ที่ติดต่อด้วยเท่านั้น แต่ก็ยังมากอยู่ดีถ้าเซิร์ฟเวอร์มีจำนวนมาก ดังนั้นจึงเกิดการประยุกต์ใช้ขึ้นใหม่เป็น Public Key Infrastructure (PKI) โดยมีเซิร์ฟเวอร์ตัวหนึ่งทำหน้าที่เป็นผู้ให้บริการเรื่อง Certificate ซึ่งเรียกว่า Certificate Authority (CA) เพื่อใช้ในการออก Digital Certificate โดยอาศัยหลักการคือ CA จะ sign กุญแจสาธารณะของเซิร์ฟเวอร์ด้วยกุญแจส่วนตัวของ CA จากนั้นไคลเอนต์จะต้อง trust ตัว CA โดยอาศัยหลักการที่ว่า ถ้า CA Trust กับใครแล้ว เราจะถือว่า Certificate ของเซิร์ฟเวอร์นั้นมีความน่าเชื่อถือไปด้วย การทำงานจะเริ่มจากการที่ไคลเอนต์ได้รับกุญแจสาธารณะของ CA เก็บไว้ก่อน แล้วเมื่อมีการติดต่อกับเซิร์ฟเวอร์ที่ต้องการติดต่อด้วยก็จะส่ง certificate มาให้ซึ่งจะมี signature ที่ sign โดยกุญแจส่วนตัวของ CA ด้วย จากนั้นไคลเอนต์ก็

สามารถใช้กุญแจสาธารณะของ CA ถอดรหัสต่อไป ในการใช้งานจริง ไคลเอนต์จะเก็บแค่กุญแจสาธารณะของ CA เท่านั้น และเมื่อมีการติดต่อกับเซิร์ฟเวอร์ก็เพียงแค่ตรวจสอบว่า Certificate นั้นมีการ sign โดย CA ที่เรา trust หรือไม่

2.6 OpenVPN

OpenVPN ถูกพัฒนาโดย James Yonan โดยจัดเป็นซอฟต์แวร์ที่ใช้ในการสร้างระบบเครือข่ายเสมือนส่วนตัวประเภทซอฟต์แวร์เบส และเป็นฟรีแวร์ด้วย ซึ่งสามารถนำไปใช้ได้โดยไม่เสียค่าใช้จ่ายใดๆ รวมถึงมีการเปิดเผยโค้ดเพื่อให้สามารถนำไปพัฒนาต่อได้ด้วย OpenVPN นั้นถูกออกแบบมาให้ทำงานได้ในเลเยอร์ 2 และ 3 ของ OSI model และใช้หลักการของ SSL/TLS ด้วย จากแนวคิดของ James Yonan ซึ่งเน้นการออกแบบให้สามารถใช้งานได้หลากหลายแพล็ตฟอร์ม การติดตั้งต้องสามารถทำได้ง่าย ปลอดภัย รวมถึงความรวดเร็วทำงาน ดังนั้น OpenVPN จึงนำแนวคิดเหล่านี้ถ่ายทอดออกมาเป็นในรูปแบบการส่งข้อมูลที่เข้ารหัสแล้วผ่านโปรโตคอล UDP (User Datagram Protocol) ซึ่ง James Yonan ได้บอกว่าการนำข้อมูลที่เข้ารหัส ห่อหุ้มด้วยไอพีแพ็คเก็ต และวิ่งไปบนโปรโตคอล UDP เป็นทางเลือกที่ดีที่สุด (ในกรณีที่ต้องการให้ไอพีแพ็คเก็ต วิ่งบน TCP ก็สามารถทำได้แต่ค่าปกติที่กำหนดไว้คือ UDP) ดังรูปที่ 2.6



รูปที่ 2.6 การส่งข้อมูลของ OpenVPN ผ่าน UDP

2.6.1 คุณสมบัติของ OpenVPN

- สามารถทำอุโมงค์แบบ IP Packet และ Ethernet frame ได้
- มีความปลอดภัยในระดับป้องกัน (Preventive) ทั้งการโจมตีแบบ active และ passive
- ทำ chroot environment และสามารถวิ่งในสิทธิ์ของผู้ใช้ธรรมดาได้ หลังจาก Initialize สำเร็จแล้ว
- ทำ Load Balance กรณีที่มี VPN เซิร์ฟเวอร์หลายตัว
- สนับสนุนการเข้ารหัสในรูปแบบ Pre-shared Keys และ Certificated Keys
- สนับสนุนการทำงานในรูปแบบ HMAC Authentication
- สนับสนุนการบีบอัดข้อมูลเพื่อลดปริมาณการจราจรบนเครือข่าย
- ทำ DHCP เพื่อแจกจ่ายไปยัง VPC ไคลเอนต์ ไม่ว่าจะเป็นการกำหนด route, DNS, WINS ซึ่งเหมาะกับการใช้งานแบบ road-warrior
- ทำอุโมงค์ผ่าน Network Address Translation (NAT) ได้
- ใช้ได้หลากหลายแพล็ตฟอร์ม เช่น Linux, FreeBSD, Windows เป็นต้น

2.6.2 หลักการทำงานของ OpenVPN

OpenVPN ทำงานในระดับ Application Layer (ใน TCP/IP Model) โดยการใช้ SSL (Secure Socket Layer) ซึ่งต่อมาถูกพัฒนาเป็น TLS (Transport Layer Security) และสร้างอุโมงค์ (Tunneling) โดยใช้อุปกรณ์ TUN/TAP Adapter และโปรโตคอล TCP/UDP ในการส่งข้อมูล OpenVPN ประกอบด้วย

- การเข้ารหัสข้อมูลที่ส่งจากไคลเอนต์ไปเซิร์ฟเวอร์โดยใช้ SSL/TLS
- โปรโตคอลที่ใช้ในการรับส่งข้อมูลโดยใช้ TCP หรือ UDP
- การสร้างช่องทางในการส่งข้อมูลโดยใช้ TUN/TAP Adapter

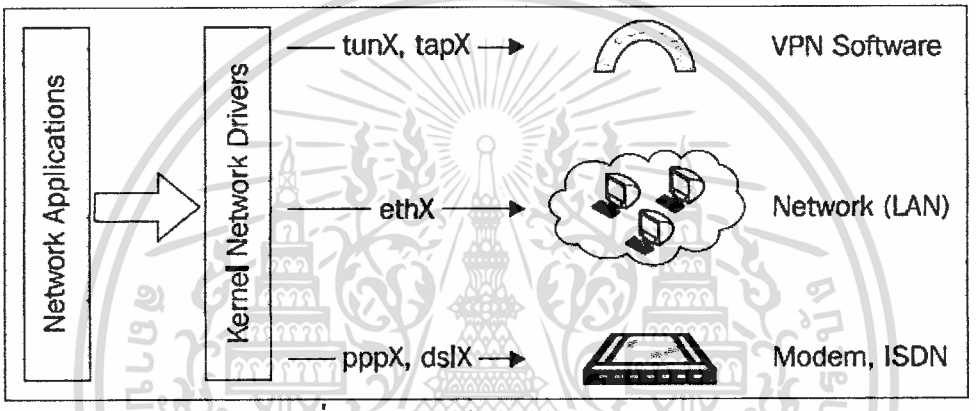
สำหรับขั้นตอนการสร้างอุโมงค์และส่งข้อมูลมีดังนี้

- เริ่มจากแอพลิเคชั่นส่งข้อมูลไปที่ Private network โดยใช้ไอพีต้นทางเป็น Private และปลายทางเป็นไอพีของเครื่องที่อยู่ใน Private network
- หลังจากรันแอพลิเคชั่นนั้น OpenVPN จะสร้างกุญแจที่ใช้ในการเข้ารหัสข้อมูลมา 2 ชุด โดยอันแรกอยู่ที่ไคลเอนต์ ส่วนอันที่สองอยู่ที่วีพีเอ็นเซิร์ฟเวอร์ กุญแจที่ได้มานั้นมาจากฟังก์ชั่นของ OpenSSL Library
- ในการส่งข้อมูลจากไคลเอนต์ไปยังเซิร์ฟเวอร์นั้นจะเข้ารหัสข้อมูลแบบ RSA
- เมื่อข้อมูลถูกเข้ารหัสเสร็จก็จะถูกส่งผ่าน adapter ที่ใช้ในการสร้างอุโมงค์ โดย adapter นั้นมี 2 แบบ คือ TUN และ TAP

TUN เป็น Virtual Point-to-Point network adapter มีหน้าที่สร้างอุโมงค์ไอพี (IP Tunneling) โดยแอพลิเคชั่นอ่านและเขียนไอพีแพ็คเก็ตผ่าน TUN ข้อดีสำหรับการทำงานผ่าน TUN คือทำงานได้รวดเร็ว แต่มีข้อเสียคือ สนับสนุนการทำงานผ่านไอพีแพ็คเก็ตเท่านั้น

TAP เป็น Virtual Ethernet network adapter ทำหน้าที่คล้ายกับ TUN เพียงแต่แอพลิเคชั่นจะทำหน้าที่อ่านและเขียนอีเทอร์เน็ตเฟรมผ่าน TAP ข้อดีสำหรับการทำงานผ่าน TAP คือสนับสนุนการใช้งานโปรโตคอลอื่นๆที่ไม่ใช่ไอพี เช่น ไอพีเอ็กซ์ (IPX) ของ Novell เป็นต้น แต่มีข้อเสียคือทำงานช้ากว่า TUN

การส่งข้อมูลโดยใช้ OpenVPN นั้น สามารถใช้ adapter ได้ทั้ง 2 แบบ แสดงดังรูปที่ 2.7



รูปที่ 2.7 การส่งข้อมูลผ่าน TUN/TAP

2.6.3 การจัดการและการแก้ไขค่าคอนฟิกของ OpenVPN

รูปแบบการจัดการการใช้งาน OpenVPN ในปัจจุบันนั้นสามารถทำได้ 2 วิธี วิธีแรกคือการเข้าไปแก้ไขค่าในไฟล์คอนฟิก (File Configure) วิธีที่สองคือการใช้ Command line ในการแก้ไขค่าคอนฟิก

- การจัดการระบบเครือข่ายเสมือนส่วนตัวโดยใช้วิธีแก้ไขไฟล์คอนฟิก นั้นมักเป็นที่นิยม เนื่องจากง่ายและสามารถตรวจสอบได้ก่อนที่จะรันไฟล์คอนฟิก ดังนั้นในกรณีที่ผู้ดูแลระบบยังไม่คุ้นเคยกับ OpenVPN จึงมักใช้วิธีนี้ ซึ่งการสร้างที่วีพีเอ็นเซิร์ฟเวอร์นั้นจะสร้างไฟล์ server.ovpn (Windows) หรือ server.conf (Linux) ขึ้นมา ดังตัวอย่างรูปที่ 2.8 เมื่อแก้ไขไฟล์คอนฟิกตามที่ต้องการแล้วจากนั้นก็ทำการเซฟแล้วรีสตาร์ทเซอร์วิส เพื่อให้ระบบรันค่าคอนฟิกขึ้นมา ส่วนที่ไคลเอนต์ก็จะต้องสร้างไฟล์คอนฟิกชื่อ client.ovpn ขึ้นมาดังตัวอย่างรูปที่ 2.9 เช่นเดียวกับเซิร์ฟเวอร์ เมื่อมีการแก้ไขไฟล์คอนฟิกของไคลเอนต์ก็ต้องเซฟและรีสตาร์ทเซอร์วิสเหมือนกัน

```
##############################################
# Sample OpenVPN 2.0 config file for         #
# multi-client server.                       #
#                                            #
# This file is for the server side           #
# of a many-clients <-> one-server           #
# OpenVPN configuration.                     #
#                                            #
# OpenVPN also supports                      #
# single-machine <-> single-machine          #
# configurations (See the Examples page      #
# on the web site for more info).            #
#                                            #
# This config should work on Windows         #
# or Linux/BSD systems.  Remember on         #
# Windows to quote pathnames and use         #
# double backslashes, e.g.:                  #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                            #
# Comments are preceded with '#' or ';'      #
##############################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp
```

รูปที่ 2.8 ตัวอย่างไฟล์คอนฟิกบนเซิร์ฟเวอร์ของ OpenVPN

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
```

รูปที่ 2.9 ตัวอย่างไฟล์คอนฟิกบนไคลเอนท์ของ OpenVPN

- การจัดการระบบเครือข่ายเสมือนส่วนตัวโดยใช้ Command line วิธีนี้เป็นการส่ง Command line เพื่อจัดการระบบเครือข่ายเสมือนส่วนตัวโดยตรง ซึ่ง OpenVPN จะจัดเตรียมค่าพารามิเตอร์ต่างๆเตรียมไว้ให้ การใช้วิธีนี้นั้นมักใช้ในกรณีที่จะแก้ไขหรือเพิ่มออปชั่น เป็นส่วนใหญ่ ส่วนกรณีติดตั้งระบบเครือข่ายนั้นมักใช้วิธีการแก้ไขไฟล์คอนฟิกในการติดตั้ง เมื่อผู้ดูแลระบบต้องการแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ในระบบเครือข่ายก็จะส่ง Command Line ผ่านโปรแกรม OpenVPN ใน Kernel จากนั้นระบบก็จะอัพเดท ไฟล์คอนฟิกในหน่วยความจำสำรอง ส่วนรูปแบบของการใช้คำสั่งของ OpenVPN มีตัวอย่างดังนี้

  openvpn [**--help**]

  openvpn [**--genkey**] [**--secret** *file*]

2.6.4 การเข้ารหัสของ OpenVPN

สำหรับการเข้ารหัสของ OpenVPN นั้นสามารถทำได้ทั้งสองแบบคือ แบบสมมาตร (Symmetric or Shared/ Secret key) และแบบอสมมาตร (Asymmetric) โดยใช้ X.509 Certificate

- แบบ Shared/ Secret Key การเข้ารหัสแบบนี้เป็นแบบที่ง่ายที่สุด โดยที่เซิร์ฟเวอร์สร้าง Secret key ซึ่งเป็น static key ขึ้นมา จากนั้นก็นำไปวางไว้ที่ฝั่งไคลเอนต์ จากนั้นก็แก้ไขในไฟล์คอนฟิกให้ระบุค่ามาที่ secret key นี้ ก็จะสามารถใช้งานได้ แบบนี้มีข้อดีคือง่าย แต่มีข้อเสียคือความปลอดภัยต่ำเพราะถ้ามีใครเอา key ไปก็สามารถใช้งานได้เลย และข้อเสียอีกอย่างคือ ไม่สามารถพิสูจน์ตัวตนของผู้ใช้ได้
- แบบ X.509 Certificate การเข้ารหัสแบบนี้เป็นแบบที่มีความปลอดภัยสูง สามารถพิสูจน์ตัวตนของผู้ใช้งานได้ โดยอาศัยหลักการทำงานของ Public Key Infrastructure (PKI) ซึ่งในการทำงานแบบนี้จะประกอบด้วย
  - ใบรับรอง (Certificate) หรือ public key ของเซิร์ฟเวอร์และไคลเอนต์แต่ละราย
  - Private key ของเซิร์ฟเวอร์และไคลเอนต์แต่ละราย
  - ใบรับรอง (Certificate) และ key ของ Master Certificate Authority (CA) เพื่อใช้ sign ใบรับรองของเซิร์ฟเวอร์และไคลเอนต์แต่ละราย

ในการทำงานแบบ X.509 Certificate ที่เซิร์ฟเวอร์ต้องสร้าง CA และ key ขึ้นมาก่อนหลังจากนั้นก็สร้างใบรับรอง (Certificate) ของเซิร์ฟเวอร์และไคลเอนต์ แล้ว sign (Self-sign Certificate) ให้กับใบรับรองของทั้งเซิร์ฟเวอร์และไคล์เอนต์ จากนั้นก็นำไฟล์ที่จำเป็นคือค่า key และ certificate

ของไคลเอนต์ไปเก็บไว้ที่เครื่องไคลเอนต์ จากนั้นก็แก้ไขค่าไฟล์คอนฟิกให้ถูกต้องจึงจะสามารถใช้งานได้ ตัวอย่างไฟล์คอนฟิกในการใช้งาน Certificate แสดงดังรูปที่ 2.10

```
# If you have set up more than one TAP-Win32 adapter
# on your system, you must refer to it by name.
;dev-node my-tap

# You can generate a static OpenVPN key
# by selecting the Generate Key option
# in the start menu.
#
# You can also generate key.txt manually
# with the following command:
#   openvpn --genkey --secret key.txt
#
# key must match on both ends of the connection,
# so you should generate it on one machine and
# copy it to the other over a secure medium.
# Place key.txt in the same directory as this
# config file.
# secret key.txt

dh keys/dh2048.pem
ca keys/ca.crt
cert keys/VPN-Server.crt
key keys/VPN-Server.key
```

รูปที่ 2.10 ตัวอย่างไฟล์คอนฟิกในการใช้ใบรับรอง

2.6.5 ข้อเสียของ OpenVPN

- ในการจัดการระบบเครือข่ายในปัจจุบันนั้นค่อนข้างยากเพราะผู้ดูแลระบบจำเป็นต้องมีความคุ้นเคยกับ OpenVPN พอสมควร จึงจะสามารถจัดการระบบได้ ไม่ว่าจะเป็นการแก้ไขไฟล์คอนฟิกหรือการใช้ Command Line
- ไม่สนับสนุนการทำงานร่วมกับ IPSec VPN ซึ่งเป็นมาตรฐานที่นิยมใช้ในปัจจุบัน
- ไม่มีส่วนติดต่อกับผู้ใช้แบบกราฟฟิคในการบริหารจัดการ

บทที่ 3
การวิเคราะห์และออกแบบระบบ

3.1 การใช้งานของโอเพ่นวีพีเอ็นของระบบเดิม

รูปแบบการจัดการการใช้งานโอเพ่นวีพีเอ็น ในปัจจุบันนั้นสามารถทำได้ 2 วิธี วิธีแรกคือการเข้าไปแก้ไขค่าในไฟล์คอนฟิก (File Configure) วิธีที่สองคือการใช้คอมมานด์ไลน์ (Command Line) ในการแก้ไขค่าคอนฟิก

3.1.1 การจัดการระบบเครือข่ายเสมือนส่วนตัวโดยใช้วิธีแก้ไขไฟล์คอนฟิก นั้นมักเป็นที่นิยม เนื่องจากง่ายและสามารถตรวจสอบได้ก่อนที่จะรันไฟล์คอนฟิก ดังนั้นในกรณีที่ผู้ดูแลระบบยังไม่คุ้นเคยกับโอเพ่นวีพีเอ็น จึงมักใช้วิธีนี้ ซึ่งการสร้างที่วีพีเอ็นเซิร์ฟเวอร์นั้นจะสร้างไฟล์ server.ovpn (Windows) หรือ server.conf (Linux) ขึ้นมา เมื่อแก้ไขไฟล์คอนฟิกตามที่ต้องการแล้วจากนั้นก็ทำการเซฟแล้วรีสตาร์ทเซอร์วิส เพื่อให้ระบบรันค่าคอนฟิกขึ้นมา ส่วนที่ไคลเอนท์ก็จะต้องสร้างไฟล์คอนฟิกชื่อ client.ovpn ขึ้นมา เช่นเดียวกับเซิร์ฟเวอร์ เมื่อมีการแก้ไขไฟล์คอนฟิกของไคลเอนท์ก็ต้องเซฟและรีสตาร์ทเซอร์วิสเหมือนกัน

3.1.2 การจัดการระบบเครือข่ายเสมือนส่วนตัวโดยใช้ Command line วิธีนี้เป็นการส่ง Command line เพื่อจัดการระบบเครือข่ายเสมือนส่วนตัวโดยตรง ซึ่งโอเพ่นวีพีเอ็น จะจัดเตรียมค่าพารามิเตอร์ต่างๆเตรียมไว้ให้ การใช้วิธีนี้นั้นมักใช้ในกรณีที่จะแก้ไขหรือเพิ่มออปชั่นเป็นส่วนใหญ่ ส่วนกรณีติดตั้งระบบเครือข่ายนั้นมักใช้วิธีการแก้ไขไฟล์คอนฟิกในการติดตั้ง เมื่อผู้ดูแลระบบต้องการแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ในระบบเครือข่ายก็จะส่งคอมมานด์ไลน์ ผ่านโปรแกรมโอเพ่นวีพีเอ็น ในเคอร์แนล จากนั้นระบบก็จะอัพเดท ไฟล์คอนฟิกในหน่วยความจำสำรอง

3.2 ข้อเสียของโอเพ่นวีพีเอ็นของระบบเดิม

ข้อเสียของการใช้งานโอเพ่นวีพีเอ็น นั้นมีดังนี้

- ผู้ใช้ระบบหรือผู้ดูแลระบบต้องกำหนดค่าคอนฟิกต่างๆในไฟล์คอนฟิกเองทั้งหมด โดยผู้ดูแลระบบต้องรู้ค่าที่จะต้องใช้ในระบบทั้งหมดและต้องไปคอนฟิกให้ไคลเอนท์ในแต่ละเครื่องด้วย
- ในการใช้คีย์ในการเข้ารหัส หลังจากที่สร้างคีย์แล้ว ผู้ดูแลระบบต้องนำคีย์ไปยังเครื่องไคลเอนท์แต่ละเครื่องเอง ซึ่งไม่ค่อยสะดวกนัก

- ในการตรวจสอบสถานะของผู้ใช้งานทำได้ค่อนข้างลำบาก
- ในการแก้ไขค่าไฟล์คอนฟิกต้องทำจากที่เซิร์ฟเวอร์เท่านั้น ไม่สามารถทำจากที่อื่นได้

3.3 โครงงานพัฒนาระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

3.3.1 วัตถุประสงค์

- เพื่อให้เข้าใจการทำงานของระบบเครือข่ายเสมือนส่วนตัว
- เพื่อให้เข้าใจหลักการทำงานของการเข้ารหัสและถอดรหัสแบบมีใบรับรอง (Certificate)
- เพื่อเรียนรู้การวิเคราะห์และออกแบบตลอดจนพัฒนาโปรแกรมเพื่อจัดการแอพลิเคชั่นผ่านทางเว็บ

3.3.2 ความต้องการของระบบ

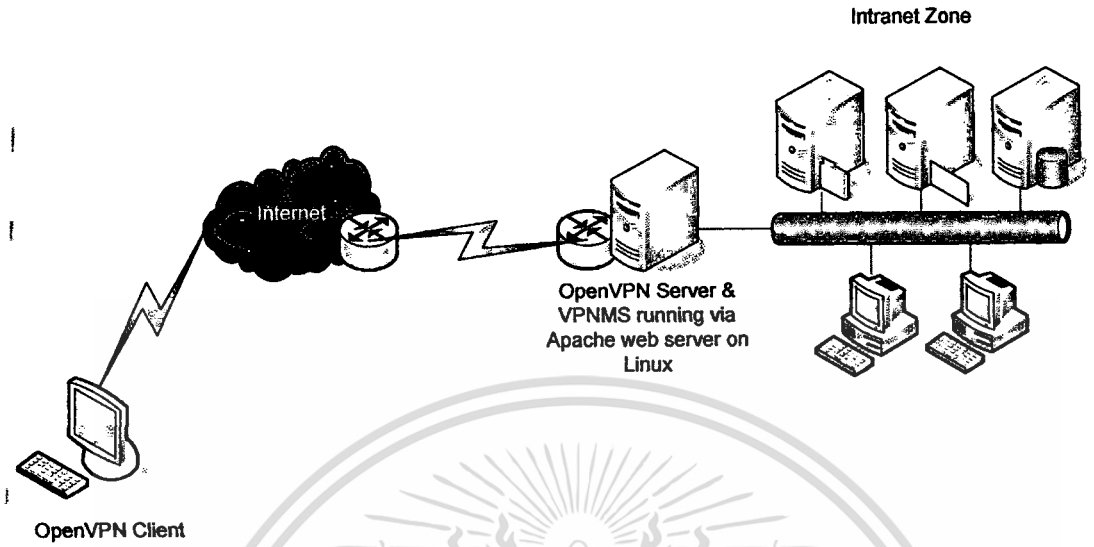
โครงงานนี้จะเป็นระบบที่ใช้เว็บบราวเซอร์ ในการที่จะเข้าไปบริหารจัดการหรือเรียกใช้งานระบบ ซึ่งจะมีส่วนของฟังก์ชันหรือความต้องการหลักๆดังนี้

- ทำงานบนเว็บบราวเซอร์ซึ่งจะเป็นเครื่องเดียวกับเซิร์ฟเวอร์ของโอเพ่นวีพีเอ็น และจะรันอยู่ภายใต้ระบบปฏิบัติการ Red Hat Enterprise Linux
- สามารถสร้าง ลบและเปลี่ยนรหัสผ่านของผู้ดูแลระบบผ่านเว็บบราวเซอร์ได้ รวมถึงการพิสูจน์ตัวตนของผู้ใช้งานระบบผ่าน Microsoft Active Directory ด้วย
- ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกของผู้ใช้งานแต่ละรายแล้วเก็บไว้เพื่อให้ผู้ใช้เข้ามาดาวน์โหลดไปใช้งานได้
- สามารถช่วยในการสร้าง Certificate key และ ช่วยในการกระจาย key ไปยังไคลเอนท์ได้ง่ายขึ้น รวมถึงการยกเลิก Certificate ด้วย
- สามารถตรวจสอบการใช้งานของผู้ใช้ได้

3.4 การวิเคราะห์และออกแบบระบบ

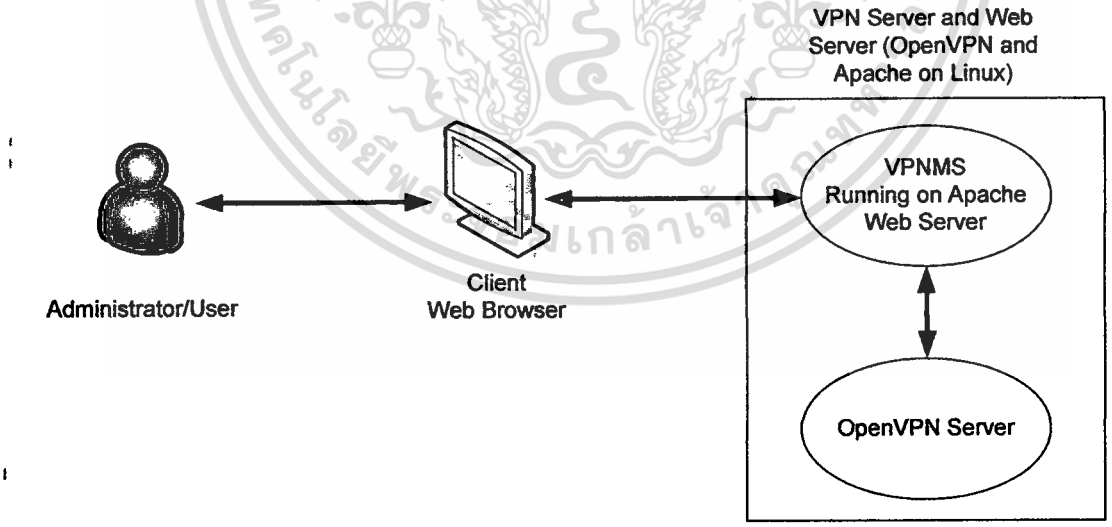
3.4.1 สถาปัตยกรรมของระบบ

สำหรับการเชื่อมต่อของระบบใหม่นั้นจะเป็นการใช้งานระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัว (VPNMS) ผ่านเว็บ ซึ่งจะรับอยู่บนระบบปฏิบัติการลินุกซ์ โดยใช้ Apache เป็นเว็บเซิร์ฟเวอร์ ซึ่งเครื่องนี้ก็ทำหน้าที่เป็นเซิร์ฟเวอร์ของโอเพ่นวีพีเอ็น ด้วย



รูปที่ 3.1 รูปแบบการเชื่อมต่อเพื่อใช้งานระบบ

จากรูปที่ 3.1 จะแสดงรูปแบบโดยรวมของระบบของโครงงานซึ่งจะประกอบด้วยเซิร์ฟเวอร์ที่เป็นเว็บและวีพีเอ็น เซิร์ฟเวอร์โดยที่ผู้ดูแลระบบสามารถเข้ามาจัดการเครือข่ายเสมือนส่วนตัวโดยใช้เว็บบราวเซอร์ได้

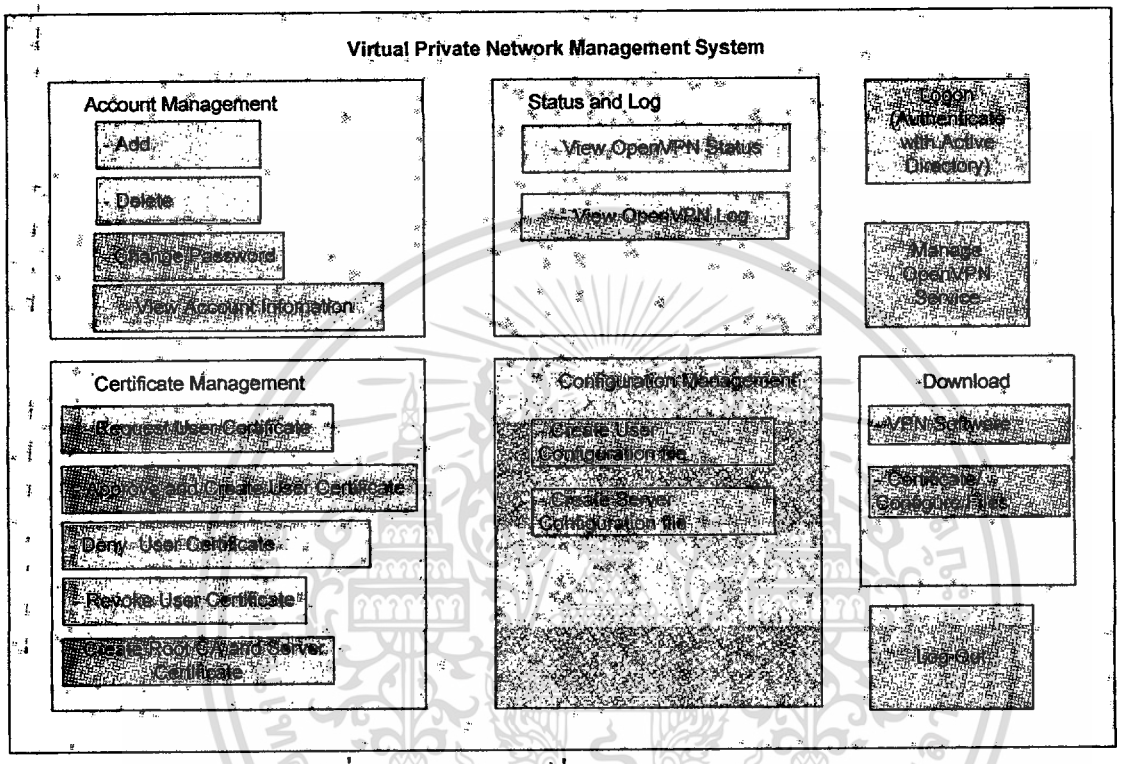


รูปที่ 3.2 องค์ประกอบการทำงานของระบบ

จากรูปที่ 3.2 จะแสดงองค์ประกอบการทำงานของระบบโดยตัวโครงงานนั้นจะอยู่บนฝั่งเซิร์ฟเวอร์ที่ทำงานเป็นเว็บและวีพีเอ็นเซิร์ฟเวอร์ด้วย โดยผู้ใช้และผู้ดูแลระบบสามารถจัดการเครือข่ายเสมือน

ส่วนตัวได้จากฝั่งไคลเอนท์โดยเรียกใช้งานผ่านเว็บบราวเซอร์เพื่อเรียกใช้ระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัว (VPNMS) ที่อยู่ฝั่งเซิร์ฟเวอร์ได้

จากการวิเคราะห์และออกแบบระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวนี้สามารถแบ่งย่อยเป็นโมดูลต่างๆได้ดังรูปที่ 3.3



รูปที่ 3.3 ภาพรวมฟังก์ชั่นการทำงานของระบบ

จากรูปที่ 3.3 จะมีฟังก์ชั่นการทำงานหลักๆ โดยแบ่งย่อยเป็นโมดูลต่างๆดังต่อไปนี้

1. ระบบการจัดการการใช้งานของผู้ดูแลระบบ (Account Management)
   - มีส่วนของการเพิ่มรายชื่อผู้ดูแลระบบ
   - มีส่วนของการลบรายชื่อผู้ดูแลระบบ
   - มีส่วนของการเปลี่ยนรหัสผ่านของผู้ดูแลระบบ
   - มีส่วนของการดูข้อมูลของผู้ดูแลระบบทั้งหมด
2. ระบบการตรวจสอบสถานะในการใช้งาน (Status and log)
   - ผู้ดูแลระบบสามารถตรวจสอบการใช้งานของผู้ใช้งานระบบได้
   - ผู้ดูแลระบบสามารถดูล็อกของโอเพ่นวีพีเอ็น ได้
3. ระบบการจัดการใบรับรอง (Certificate Management)
   - ผู้ใช้งานสามารถร้องขอใบรับรองจากผู้ดูแลได้โดยจะมีการส่งอีเมลล์แจ้งเตือนไปยังผู้ดูแลระบบได้

- ผู้ดูแลระบบสามารถรับรองหรือปฏิเสธให้ผู้ใช้งานมีใบรับรองได้
- ผู้ดูแลระบบสามารถสร้างใบรับรองของผู้ใช้งานแต่ละคนได้ และสามารถกำหนดวันหมดอายุของใบรับรองได้ด้วย
- ผู้ดูแลระบบสามารถยกเลิกการใช้งานใบรับรองของผู้ใช้งานแต่ละรายได้
- ผู้ดูแลระบบสามารถสร้างใบรับรองของเซิร์ฟเวอร์ และสามารถกำหนดวันหมดอายุของใบรับรองได้ด้วย

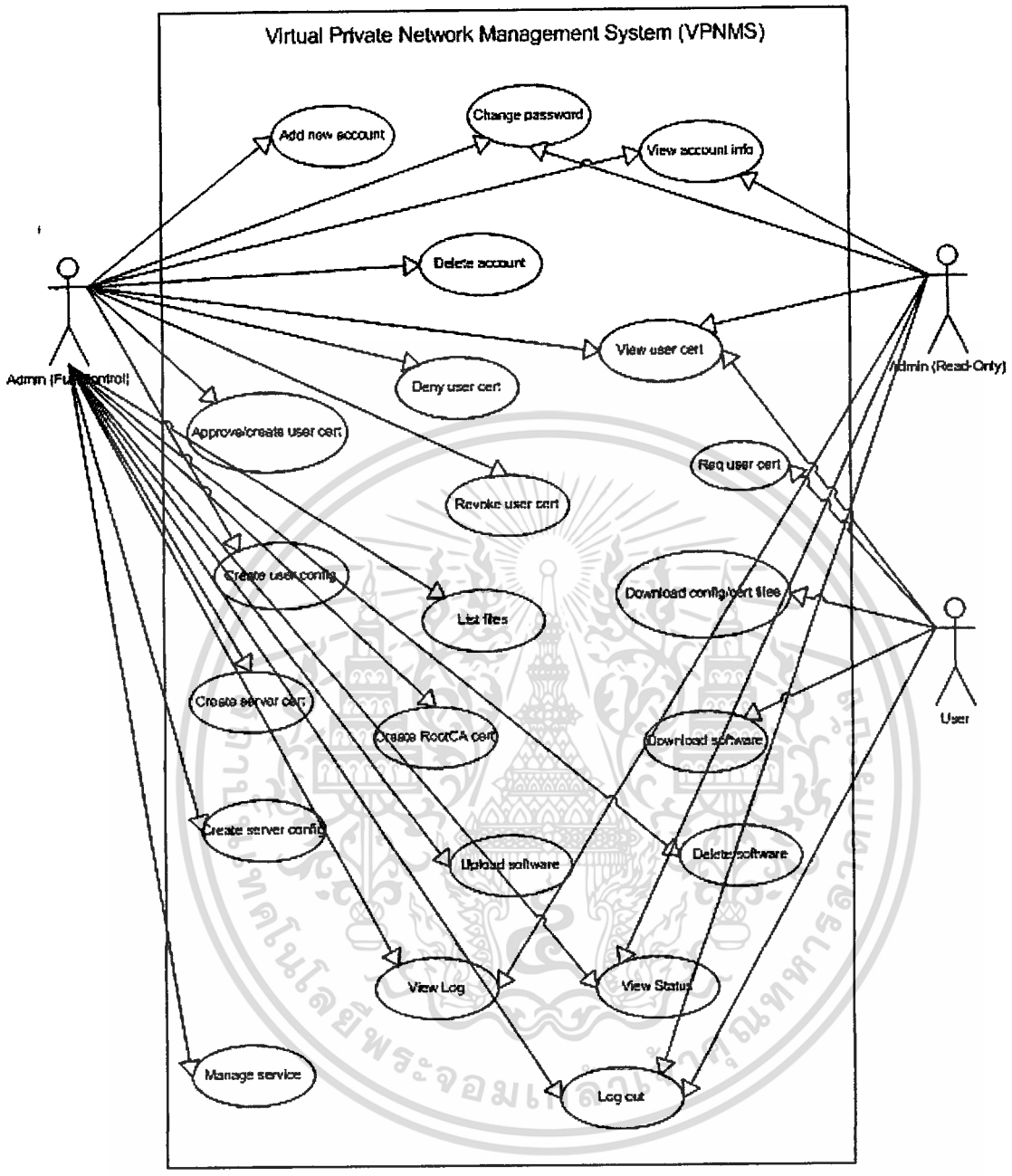
4. ระบบการจัดการคุณสมบัติต่างๆ (Configuration Management)
   - ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกของผู้ใช้งานระบบแต่ละรายได้
   - ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกของเซิร์ฟเวอร์ได้
5. ระบบควบคุมการดาวน์โหลด
   - ผู้ดูแลระบบสามารถจัดการเรื่องการดาวน์โหลดซอฟต์แวร์ได้เช่นการอัพโหลดและลบซอฟต์แวร์บนเซิร์ฟเวอร์
   - ผู้ใช้งานระบบสามารถดาวน์โหลดใบรับรองของตนเองเพื่อนำไปใช้งานได้
   - ผู้ใช้งานระบบสามารถดาวน์โหลดไฟล์คอนฟิกของตนเองเพื่อนำไปใช้งานได้
   - ผู้ใช้งานสามารถดาวน์โหลดซอฟต์แวร์โอเพ่นวีพีเอ็น มาติดตั้งที่เครื่องตนเองได้
6. ระบบควบคุมการเข้าใช้งานและพิสูจน์ตัวตน
   - ผู้ใช้สามารถ logon เข้าใช้งานระบบได้โดยสามารถพิสูจน์ตัวตนได้จาก Active Directory
7. ระบบการจัดการเซอร์วิสของโอเพ่นวีพีเอ็น
   - ผู้ดูแลระบบสามารถจัดการเซอร์วิสของโอเพ่นวีพีเอ็น ได้ เช่นการรีสตารท์ เซอร์วิส เป็นต้น
8. การออกจากระบบ
   - ผู้ใช้และผู้ดูแลระบบสามารถออกจากระบบได้จากเมนู Log out จะเป็นการทำลายเซสชันที่เกิดขึ้น

จากการศึกษาและวิเคราะห์ระบบการใช้งานต่างๆ ของโอเพ่นวีพีเอ็น ทำให้ทราบถึงปัญหาต่างๆ ที่เกิดขึ้น จึงทำให้เกิดการออกแบบระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัว ซึ่งจะถูกนำเสนอออกมาใน 3 รูปแบบคือ

- แผนภาพยูสเคสไดอะแกรม (Use Case Diagram) จะเป็นส่วนที่ใช้ในการแสดงความสัมพันธ์ระหว่างผู้ใช้ระบบกับกิจกรรมต่างๆ
- แผนภาพสวิมเลนไดอะแกรม (Swimlane Diagram) ซึ่งเป็นส่วนที่ใช้ในการแสดงให้เห็นกิจกรรมต่างๆเป็นลำดับโดยแบ่งตามผู้ใช้ระบบ
- แผนภาพซีเควนซ์ไดอะแกรม (Sequence Diagram) จะเป็นส่วนที่ใช้แสดงการรับส่งข้อมูลในแต่ละฟังก์ชัน

3.4,2 การออกแบบยูสเคสไดอะแกรม (Use Case Diagram)

ระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ สามารถเขียนเป็นยูสเคสเพื่อแสดงแอกเตอร์และรายละเอียดโมดูลหลัก ๆ ของระบบได้ดังรูปที่ 3.4



รูปที่ 3.4 ยูสเคสไดอะแกรมของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

ยูสเคสไดอะแกรม จะมีแอกเตอร์ที่เป็นการแสดงถึงบุคคลที่เกี่ยวข้องกับระบบจำหน่ายดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ซึ่งจากยูสเคสไดอะแกรมข้างต้น ประกอบด้วยแอกเตอร์ 3 แอกเตอร์ ดังต่อไปนี้

- **Admin (Full-Control)** คือ ผู้ดูแลระบบซึ่งมีสิทธิ์สูงสุดในการใช้งาน
- **Admin (Read-Only)** คือ ผู้ดูแลระบบซึ่งมีสิทธิ์ดูข้อมูลได้อย่างเดียว
- **User** คือ ผู้ใช้งานระบบที่มีสิทธิ์ต่ำที่สุด

สำหรับหน้าที่และการทำงานหลักของระบบ จากยูสเคสไดอะแกรมข้างต้นจะเห็นว่าประกอบด้วย ยูสเคส 22 ยูสเคส ดังต่อไปนี้

- **Add new account** คือการเพิ่มรายชื่อและกำหนดสิทธิ์ผู้ดูแลระบบ
- **Change password** คือการเปลี่ยนรหัสผ่าน
- **View account info** คือการเรียกดู รายชื่อและข้อมูลของผู้ดูแลระบบทุกคน
- **Delete account** คือการลบรายชื่อผู้ดูแลระบบ
- **View user cert** คือการเรียกดูใบรับรองของผู้ใช้งานระบบ
- **Deny user cert** คือการปฏิเสธคำขอร้องอนุมัติใบรับรองจากผู้ใช้งานระบบ
- **Approve user cert** คือการอนุมัติการสร้างใบรับรองให้ผู้ใช้ระบบ
- **Revoke user cert** คือการเพิกถอนสิทธิ์ในการยืนยันการเข้าใช้งานระบบโอเพ่นวีพีเอ็นของผู้ใช้งานระบบ
- **Req user cert** คือการทำใบคำร้องขออนุมัติการสร้างใบรับรองให้ผู้ใช้ระบบ
- **Create user configure** คือการสร้างไฟล์คอนฟิกเพื่อให้โปรแกรมโอเพ่นวีพีเอ็นท์ไคล์เอนท์ได้เรียกใช้
- **List file** คือการขอดูรายชื่อไฟล์ต่างๆ แบ่งเก็บเป็นโฟล์เดอร์ตามชื่อของผู้ใช้งานเพื่อตรวจสอบว่าผู้ใช้งานคนไหนไม่ได้สร้างไฟล์อะไรให้บ้าง
- **Download Config/Cert file** ผู้ใช้งานสามารถดาวน์โหลดไฟล์คอนฟิกและใบรับรองได้หากมีการร้องขอและถูกอนุมัติแล้ว
- **Download software** ผู้ใช้งานระบบทำการดาวน์โหลดโปรแกรมโอเพ่นวีพีเอ็นเพื่อติดตั้งลงบนเครื่อง PC
- **Create server cert** คือการสร้างใบรับรองใหม่ให้กับเซิร์ฟเวอร์
- **Create RootCA cert** คือการสร้างใบรับรองส่วนกลางให้กับเซิร์ฟเวอร์เพื่อใช้เป็นกุญแจตั้งต้นในการสร้างใบรับรองให้กับผู้ใช้งาน
- **Create server config** คือการสร้างไฟล์คอนฟิกให้กับเซิร์ฟเวอร์เพื่อนำเป็นใช้งาน
- **Upload software** คือการนำโปรแกรมโอเพ่นวีพีเอ็นไคล์เอ็นท์เวอร์ชั่นใหม่ๆขึ้นไปเก็บไว้ในเซิร์ฟเวอร์
- **Delete software** คือการลบโปรแกรมโอเพ่นวีพีเอ็นไคล์เอ็นท์เวอร์ชั่นเก่าออกจากเซิร์ฟเวอร์
- **Manage service** คือการจัดการเกี่ยวกับเซอร์วิสการให้บริการของระบบโอเพ่นวีพีเอ็น

- **View log** คือการเรียกดูบันทึกการทำงานของเซิร์ฟเวอร์เพื่อตรวจสอบและแก้ไขข้อผิดพลาดของระบบ
- **View status** คือการเรียกดูบันทึกการเข้าใช้งานระบบโอเพ่นวีพีเอ็น
- **Log out** คือการออกจากระบบ

ตารางที่ 3.1 รายละเอียดยูสเคส Add new account

ชื่อยูสเคส	Add new account
คำอธิบายยูสเคส	เพิ่มรายชื่อและกำหนดสิทธิ์ผู้ดูแลระบบ
เหตุการณ์ที่กระตุ้นการทำงาน	เมื่อผู้ดูแลระบบระดับสิทธิ์สูงสุดต้องการเพิ่มรายชื่อและกำหนดสิทธิ์ให้ผู้ดูแลระบบคนอื่นๆ
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. ต้องมีผู้ดูแลระบบระดับสิทธิ์สูงสุดอยู่ในระบบแล้ว 2. รายชื่อผู้ดูแลระบบที่เพิ่มต้องไม่ซ้ำกับชื่อผู้ดูแลระบบเดิมที่มีอยู่ในระบบ
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุดป้อนชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าระบบ 2. ผู้ดูแลระบบทำการเพิ่มรายชื่อผู้ดูแลระบบคนอื่นๆ และกำหนดสิทธิ์ให้กับผู้ดูแลระบบคนนั้นๆ 3. ระบบทำการตรวจสอบรายชื่อผู้ดูแลระบบที่กำลังถูกเพิ่ม หากตรวจสอบและพบว่ามีรายชื่อซ้ำ ระบบจะแจ้งเตือนในหน้าจอให้ทราบ และไม่สามารถเพิ่มรายชื่อผู้ดูแลระบบคนใหม่ที่ชื่อซ้ำได้ 4. เมื่อผู้ดูแลระบบระดับสิทธิ์สูงสุดระบุข้อมูลเรียบร้อยแล้ว ระบบจะตรวจสอบข้อผิดพลาดก่อนการบันทึกข้อมูลเข้าสู่ระบบ
เงื่อนไขการทำงาน	1. หากชื่อผู้ใช้ระบบคนใหม่ซ้ำกับชื่อผู้ดูแลระบบที่มีอยู่แล้วในระบบ ระบบจะแสดงข้อความเตือนในหน้าจอเพื่อให้ผู้ดูแลระบบระดับสิทธิ์สูงสุดแก้ไขชื่อใหม่ 2. หากผู้ดูแลระบบระดับสิทธิ์สูงสุดป้อนข้อมูลผิด หรือป้อนข้อมูลไม่ครบถ้วน ระบบจะแสดงข้อความเตือนในหน้าจอเพื่อให้ผู้ใช้ระบบป้อนข้อมูลใหม่ก่อนการบันทึกข้อมูลเข้าสู่ระบบ
เงื่อนไขเมื่อสำเร็จ	มีชื่อผู้ดูแลระบบคนใหม่ในระบบ

ตารางที่ 3.2 รายละเอียดยูสเคส Change Password

ชื่อยูสเคส	Change Password
คำอธิบายยูสเคส	เปลี่ยนรหัสผ่านของผู้ดูแลระบบทุกระดับสิทธิ์การใช้งาน
เหตุการณ์ที่กระตุ้นการทำงาน	เมื่อผู้ดูแลระบบทุกระดับต้องการเปลี่ยนรหัสผ่านของตนเองในการเข้าถึงระบบ
แอกเตอร์	1. Admin (Full-Control) 2. Admin (Read-Only)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	มีรายชื่อผู้ดูแลระบบที่ต้องการเปลี่ยนรหัสผ่านอยู่ในระบบแล้ว
การทำงาน	1. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งาน ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ดูแลระบบเลือกเมนู Change Password 4. ผู้ดูแลระบบป้อนรหัสผ่านเดิมที่ใช้งานอยู่ 5. ผู้ดูแลระบบป้อนรหัสผ่านใหม่ที่ต้องการ 6. ผู้ดูแลระบบป้อนรหัสผ่านใหม่ที่ต้องการอีกครั้ง 7. ผู้ดูแลระบบกดปุ่ม Ok 8. ระบบทำการตรวจสอบรหัสผ่านเดิม และรหัสผ่านใหม่ หากถูกต้องระบบทำการบันทึกข้อมูลและแสดงข้อความให้ทราบว่าการเปลี่ยนรหัสผ่านเสร็จสมบูรณ์แล้ว
เงื่อนไขการทำงาน	1. หากผู้ดูแลระบบป้อนรหัสผ่านเก่าไม่ถูกต้อง ระบบแสดงข้อความไม่สามารถเปลี่ยนรหัสผ่านได้ พร้อมให้แก้ไขข้อมูลอีกครั้ง 2. หากผู้ดูแลระบบป้อนรหัสผ่านใหม่ที่ต้องการเปลี่ยนไม่ตรงกันทั้งสองช่อง ระบบแสดงข้อความไม่สามารถเปลี่ยนรหัสผ่านได้พร้อมให้แก้ไขข้อมูลอีกครั้ง
เงื่อนไขเมื่อสำเร็จ	ผู้ดูแลระบบสามารถใช้รหัสผ่านใหม่ในการเข้าใช้งานระบบในครั้งต่อไปได้

ตารางที่ 3.3 รายละเอียดยูสเคส View account info

ชื่อยูสเคส	View account info

คำอธิบายยูสเคส	ผู้ดูแลระบบขอดูชื่อและข้อมูลของผู้ดูแลระบบทุกระดับสิทธิ์การใช้งาน
เหตุการณ์ที่กระตุ้นการทำงาน	เมื่อผู้ดูแลระบบทุกระดับต้องการดูรายชื่อและข้อมูลของผู้ดูแลระบบคนอื่นๆ
แอกเตอร์	1. Admin (Full-Control) 2. Admin (Read-Only)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีรายชื่อผู้ดูแลระบบอยู่ในระบบแล้ว
การทำงาน	1. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งาน ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ดูแลระบบเลือกเมนู View account info 4. ระบบแสดงรายชื่อและข้อมูลของผู้ดูแลระบบทุกคนที่มีในระบบ
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	-

ตารางที่ 3.4 รายละเอียดยูสเคส Delete account

ชื่อยูสเคส	Delete account
คำอธิบายยูสเคส	ผู้ดูแลระบบถูกลบรายชื่อออกจากระบบ
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบระดับสิทธิ์สูงสุดต้องการลบรายชื่อผู้ดูแลระบบคนอื่นๆออกจากระบบ
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	View account info
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	มีรายชื่อผู้ดูแลระบบที่ต้องการลบอยู่ในระบบแล้ว
การทำงาน	1. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งาน ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู View account information

	4. ระบบแสดงรายชื่อและข้อมูลของผู้ดูแลระบบทุกคนที่มีในระบบ 5. ผู้ดูแลระบบระดับสิทธิ์สูงสุดกดปุ่ม delete หลังชื่อของผู้ดูแลระบบที่ต้องการลบ 6. ระบบแสดงข้อความยืนยัน 7. ชื่อและข้อมูลของผู้ดูแลระบบที่เลือกถูกลบออกจากระบบ
เงื่อนไขการทำงาน	ผู้ดูแลระบบระดับสิทธิ์สูงสุดเท่านั้นที่สามารถเห็นปุ่ม delete เมื่อทำการเลือกเมนู View account information แต่ผู้ดูแลระบบระดับสิทธิ์อ่านอย่างเดียวไม่สามรถเห็นปุ่ม delete
เงื่อนไขเมื่อสำเร็จ	ผู้ดูแลระบบที่ถูกลบไม่สามารถใช้งานระบบได้

ตารางที่ 3.5 รายละเอียดยูสเคส View user cert

ชื่อยูสเคส	View user cert
คำอธิบายยูสเคส	ผู้ดูแลระบบและผู้ใช้งานระบบต้องการขอดูรายละเอียดและข้อมูลสถานะของใบรับรอง
เหตุการณ์ที่กระตุ้นการทำงาน	1. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งานต้องการดูใบรับรองของผู้ใช้งานระบบทุกคน 2. ผู้ใช้งานระบบต้องการดูรายละเอียดใบรับรองของตนเอง
แอกเตอร์	1. Admin (Full-Control) 2. Admin (Read-Only) 3. User
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	มีรายชื่อผู้ใช้งานระบบอยู่ในระบบแล้ว
การทำงาน	1. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งานและผู้ใช้งานระบบ ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งานเลือกเมนู View User Certificate 4. ระบบแสดงข้อมูลใบรับรองของผู้ใช้งานในระบบทุกคน 5. ผู้ใช้งานระบบเลือกเมนู View User Certificate 6. ระบบแสดงข้อมูลใบรับรองเฉพาะของผู้ใช้งานคนนั้น

เงื่อนไขการทำงาน	1. ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งานสามารถเห็นข้อมูลใบรับรองของผู้ใช้งานทุกคนได้ 2. ผู้ดูแลระบบเฉพาะระดับสิทธิ์สูงสุดเท่านั้นสามารถจัดการกับใบรับรองของผู้ใช้งานได้ 3. ผู้ใช้งานระบบสามารถดูข้อมูลใบรับรองของตนเองได้เท่านั้น
เงื่อนไขเมื่อสำเร็จ	-

ตารางที่ 3.6 รายละเอียดยูสเคส Deny user cert

ชื่อยูสเคส	Deny user cert
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดปฏิเสธการร้องขอใบรับรองจากผู้ใช้งาน
เหตุการณ์ที่กระตุ้นการทำงาน	1. ผู้ใช้งานทำการร้องขอใบรับรองเพื่อใช้ยืนยันสิทธิ์ในการเข้าใช้งานระบบโอเพ่นวีพีเอ็น 2. มีใบรับรองจากผู้ใช้งานรอการอนุมัติอยู่ในระบบ 3. ผู้ดูแลระบบปฏิเสธการร้องขอใบรับรองจากผู้ใช้งาน
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีรายชื่อผู้ใช้งานระบบอยู่ในระบบแล้ว 2. มีใบรับรองจากผู้ใช้งานรอการอนุมัติอยู่ในระบบ
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Create User Certificate 4. ระบบแสดงข้อมูลใบรับรองที่รอการอนุมัติจากผู้ใช้งาน 5. ผู้ดูแลระบบระดับสิทธิ์สูงสุดกดปุ่ม Deny หลังใบรับรองที่ขออนุมัติ 6. ระบบแสดงข้อความยืนยันการปฏิเสธคำร้องขอใบรับรองเสร็จสมบูรณ์
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	1. คำร้องขออนุมัติใบรับรองถูกลบออกจากระบบ 2. สถานะของใบรับรองของผู้ใช้งานในหน้า View User Certificate จะแสดงสถานะปฏิเสธ (Deny)

ตารางที่ 3.7 รายละเอียดยูสเคส Approve user cert

ชื่อยูสเคส	Approve user cert
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดอนุมัติการร้องขอใบรับรองจากผู้ใช้งาน
เหตุการณ์ที่กระตุ้นการทำงาน	1. ผู้ใช้งานทำการร้องขอใบรับรองเพื่อยืนยันสิทธิ์ขอเข้าใช้ระบบโอเพ่นวีพีเอ็น 2. มีใบรับรองจากผู้ใช้งานรอการอนุมัติอยู่ในระบบ 3. ผู้ดูแลระบบอนุมัติการร้องขอใบรับรองจากผู้ใช้งาน
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีรายชื่อผู้ใช้งานระบบอยู่ในระบบแล้ว 2. มีใบรับรองจากผู้ใช้งานรอการอนุมัติอยู่ในระบบ
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Create User Certificate 4. ระบบแสดงข้อมูลใบรับรองที่รอการอนุมัติจากผู้ใช้งาน 5. ผู้ดูแลระบบระดับสิทธิ์สูงสุดกดปุ่ม Approve หลังใบรับรองที่ขออนุมัติ 6. ระบบแสดงข้อความยืนยันการอนุมัติคำร้องขอใบรับรองเสร็จสมบูรณ์ 7. ระบบทำการสร้างใบรับรองให้กับผู้ใช้งาน 8. ระบบแสดงหน้าจอเพื่อให้ผู้ใช้งานระบบสร้างไฟล์คอนฟิกของผู้ใช้งานที่ถูกอนุมัติใบรับรอง
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	1. ระบบสร้างใบรับรองให้ผู้ใช้งาน 2. ข้อมูลใบรับรองของผู้ใช้งานจะถูกบันทึกลงในตารางแสดงข้อมูลใบรับรอง 3. สถานะของใบรับรองของผู้ใช้งานในหน้า View User Certificate จะแสดงสถานะอนุมัติ (Approve) 4. ผู้ใช้งานสามารถนำใบรับรองเพื่อยืนยันสิทธิ์ในการเข้าใช้ระบบโอเพ่นวีพีเอ็นได้

ตารางที่ 3.8 รายละเอียดยูสเคส Revoke user cert

ชื่อยูสเคส	Revoke user cert
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดเพิกถอนใบรับรองจากผู้ใช้งาน
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบต้องการเพิกถอนใบรับรองของผู้ใช้งาน ไม่ให้ใช้งานระบบได้
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	View User Cert.
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	ใบรับรองของผู้ใช้งานถูกอนุมัติแล้วและมีข้อมูลอยู่ในระบบ
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู View User Certificate 4. ระบบแสดงข้อมูลใบรับรองของผู้ใช้งาน 5. ผู้ดูแลระบบระดับสิทธิ์สูงสุดกดปุ่ม Revoke หลังใบรับรองเพื่อเพิกถอนสิทธิ์ใบรับรอง ทำให้ผู้ใช้งานไม่สามารถใช้ระบบได้ 6. ระบบแสดงข้อความยืนยันการเพิกถอนใบรับรองเสร็จสมบูรณ์ 7. ระบบทำการแก้ไขรายละเอียดในใบรับรองของผู้ใช้งานว่าถูกเพิกถอน 8. ระบบทำการลบใบรับรองของผู้ใช้งานที่ถูกเพิกถอนออกจากระบบ
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	ผู้ใช้งานไม่สามารถใช้ใบรับรองเพื่อยืนยันสิทธิ์การเข้าใช้งานระบบโอเพ่นวีพีเอ็นได้

ตารางที่ 3.9 รายละเอียดยูสเคส Req user cert

ชื่อยูสเคส	Req user cert
คำอธิบายยูสเคส	ผู้ใช้งานระบบทำการร้องขอใบรับรองจากผู้ดูแลระบบ
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ใช้งานระบบต้องการใบรับรองเพื่อใช้ยืนยันสิทธิ์ในการเข้าใช้งานระบบโอเพ่นวีพีเอ็น
แอกเตอร์	User
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-

เงื่อนไขเริ่มต้น	มีรายชื่อผู้ใช้งานอยู่ในระบบแล้ว
การทำงาน	1. ผู้ใช้งานระบบ ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ใช้งานระบบเลือกเมนู Request User Certificate 4. ระบบแสดงหน้าจอให้ผู้ใช้งานป้อนอีเมล์ของผู้ใช้งานที่ร้องขอใบรับรอง 5. ผู้ใช้งานกดปุ่ม submit ระบบเพิ่มข้อมูลคำร้องขอใบรับรองให้กับตาราง Create User Certificate และส่งอีเมล์ไปหาผู้ดูแลระบบ 6. ระบบเพิ่มข้อมูลใบรับรองของผู้ใช้งานในหน้า View User Certificate โดยมีสถานะเป็น request
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	มีข้อมูลคำร้องขออนุมัติใบรับรองปรากฏอยู่ในหน้าจอของผู้ดูแลระบบระดับสิทธิ์สูงสุด

ตารางที่ 3.10 *รายละเอียดยูสเคส* Create user config

ชื่อยูสเคส	Create user config
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดสร้างไฟล์คอนฟิกให้ผู้ใช้งานแต่ละคน
เหตุการณ์ที่กระตุ้นการทำงาน	1. ใบรับรองจากผู้ใช้งานถูกอนุมัติแล้ว 2. ผู้ดูแลระบบระดับสิทธิ์สูงสุดต้องการสร้างไฟล์คอนฟิกให้กับผู้ใช้งานที่ยังไม่มีไฟล์คอนฟิก
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีรายชื่อผู้ใช้งานระบบและใบรับรองของผู้ใช้งานอยู่ในระบบแล้ว 2. ไม่มีไฟล์คอนฟิกของผู้ใช้งานอยู่ในระบบ
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู View Certificat และเลือกปุ่ม Create Config ที่สคมภ์ action 2 4. ระบบแสดงหน้าจอเพื่อให้ผู้ใช้งานระบบสร้างไฟล์คอนฟิกของผู้ใช้งาน

	ที่ถูกอนุมัติใบรับรอง 5. ผู้ดูแลระบบระดับสิทธิ์สูงสุดป้อนข้อมูลค่าคอนฟิกให้กับผู้ใช้งานและกดปุ่ม Ok 6. ระบบสร้างไฟล์คอนฟิกให้กับผู้ใช้งาน และเพิ่มรายชื่อไฟล์ให้กับหน้า list file ของผู้ดูแลระบบระดับสิทธิ์สูงสุด
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	ผู้ใช้งานสามารถนำไฟล์คอนฟิกไปใช้เพื่อปรับแต่งค่าให้เข้าใช้โปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์ได้

ตารางที่ 3.11 รายละเอียดยูสเคส List files

ชื่อยูสเคส	List files
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดต้องการดูชื่อไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้งานระบบทุกคน
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบระดับสิทธิ์สูงสุดต้องการตรวจสอบว่าได้สร้างไฟล์ใบรับรองและไฟล์คอนฟิกให้กับผู้ใช้งานแล้วหรือยัง
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีรายชื่อผู้ใช้งานระบบอยู่ในระบบแล้ว
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู List User Files 4. ระบบแสดงโฟล์เดอร์ตามชื่อของผู้ใช้งานระบบ ซึ่งภายในบรรจุไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้งานคนนั้นๆ
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	-

ตารางที่ 3.12 รายละเอียดยูสเคส Download config/cert file

ชื่อยูสเคส	Download config/cert file

คำอธิบายยูสเคส	ผู้ใช้งานระบบดาวน์โหลดไฟล์เพื่อใช้งานโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ใช้งานระบบต้องการใช้งานโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์
แอกเตอร์	User
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีใบรับรองของผู้ใช้งานอยู่ในระบบแล้ว 2. มีไฟล์คอนฟิกของผู้ใช้งานอยู่ในระบบแล้ว
การทำงาน	1. ผู้ใช้งานระบบ ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบ 3. ผู้ใช้งานระบบเลือกเมนู Download และ Download Configure file / Certificate 4. ระบบแสดงรายชื่อไฟล์ 5. ผู้ใช้งานระบบดาวน์โหลดไฟล์ลงเครื่องพีซีที่ต้องการใช้งานโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	ผู้ใช้งานสามารถนำไฟล์คอนฟิกไปใช้กับโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์และยืนยันสิทธิ์ในการเข้าระบบโอเพ่นวีพีเอ็นได้

ตารางที่ 3.13 รายละเอียดยูสเคส Download Software

ชื่อยูสเคส	Download Software
คำอธิบายยูสเคส	ผู้ใช้งานระบบดาวน์โหลดโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์ไปติดตั้งลงในเครื่องพีซี
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ใช้งานระบบต้องการใช้เข้าถึงระบบภายในองค์กรผ่านโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์
แอกเตอร์	User
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	1. มีใบรับรองของผู้ใช้งานอยู่ในระบบแล้ว 2. มีไฟล์คอนฟิกของผู้ใช้งานอยู่ในระบบแล้ว

	3. มีชื่อผู้ใช้งานในระบบอยู่แล้ว
การทำงาน	1. ผู้ใช้งานระบบ ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบ 3. ผู้ใช้งานระบบเลือกเมนู Download และ Download OpenVPN Software 4. ระบบแสดงรายชื่อไฟล์ 5. ผู้ใช้งานระบบดาวน์โหลดไฟล์ลงเครื่องพีซีที่ต้องการติดตั้งโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	ผู้ใช้งานสามารถติดตั้งและใช้งานโปรแกรมโอเพ่นวีพีเอ็นไคลเอนท์ได้

ตารางที่ 3.14 รายละเอียดยูสเคส Create Server Cert

ชื่อยูสเคส	Create Server Cert
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดทำการสร้างใบรับรองสำหรับเซิร์ฟเวอร์ใหม่
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบต้องการสร้างใบรับรองใหม่ให้กับเซิร์ฟเวอร์
แอคเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	มีเซิร์ฟเวอร์ที่ติดตั้งและให้บริการระบบโอเพ่นวีพีเอ็นอยู่แล้ว
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Create Server Certificate 4. ระบบแสดงหน้าจอเพื่อให้ผู้ดูแลระบบป้อนข้อมูลเพื่อสร้างใบรับรองของเซิร์ฟเวอร์ 5. ระบบสร้างใบรับรองของเซิร์ฟเวอร์ และเก็บไว้ในโฟล์เดอร์ที่ใช้เป็นค่าเริ่มต้นของระบบโอเพ่นวีพีเอ็นท์และถูกนำไปเรียกใช้งาน
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	เซิร์ฟเวอร์ได้ใบรับรองใหม่

ตารางที่ 3.15 รายละเอียดยูสเคส Create RootCA Cert

ชื่อยูสเคส	Create RootCA Cert
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดทำการสร้างใบรับรองส่วนกลางสำหรับเซิร์ฟเวอร์ใหม่
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบต้องการสร้างใบรับรองส่วนกลางใหม่ให้กับเซิร์ฟเวอร์
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	มีเซิร์ฟเวอร์ที่ติดตั้งและให้บริการระบบโอเพ่นวีพีเอ็นอยู่แล้ว
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Create RootCA Certificate 4. ระบบแสดงหน้าจอเพื่อให้ผู้ดูแลระบบป้อนข้อมูลเพื่อสร้างใบรับรองส่วนกลางของเซิร์ฟเวอร์ เพื่อเป็นกุญแจตั้งต้นที่ใช้ในการเข้ารหัสเมื่อสร้างใบรับรองให้กับผู้ใช้งาน 5. ระบบสร้างใบรับรองของเซิร์ฟเวอร์ และเก็บไว้ในโฟล์เดอร์ที่ใช้เป็นค่าเริ่มต้นของระบบโอเพ่นวีพีเอ็นท์และถูกนำไปเรียกใช้งาน
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	เซิร์ฟเวอร์ได้ใบรับรองส่วนกลางใหม่

ตารางที่ 3.16 รายละเอียดยูสเคส Create server config

ชื่อยูสเคส	Create server config
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดทำการสร้างไฟล์คอนฟิกสำหรับเซิร์ฟเวอร์
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบต้องการสร้างหรือปรับแต่งค่าฟังก์ชันการทำงานให้กับเซิร์ฟเวอร์
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-

เงื่อนไขเริ่มต้น	มีเซิร์ฟเวอร์ที่ติดตั้งและให้บริการระบบโอเพ่นวีพีเอ็นอยู่แล้ว
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Create Server Configuration 4. ระบบแสดงหน้าจอเพื่อให้ผู้ดูแลระบบป้อนข้อมูลเพื่อหรับแต่งค่าคอนฟิกให้กับเซิร์ฟเวอร์ 5. ระบบสร้างไฟล์คอนฟิกให้เซิร์ฟเวอร์ และเก็บไว้ในโฟล์เดอร์ที่ใช้เป็นค่าเริ่มต้นของระบบโอเพ่นวีพีเอ็นท์และถูกนำไปเรียกใช้งาน
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	เซิร์ฟเวอร์ได้รับการปรับเปลี่ยนค่าใหม่

ตารางที่ 3.17 รายละเอียดยูสเคส Upload software

ชื่อยูสเคส	Upload software
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดนำโปรแกรมโอเพ่นวีพีเอ็นท์เวอร์ชั่นล่าสุดอัพโหลดขึ้นเซิร์ฟเวอร์
เหตุการณ์ที่กระตุ้นการทำงาน	มีโปรแกรมโอเพ่นวีพีเอ็นท์เวอร์ชั่นใหม่ออกมา
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	-
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Download OpenVPN และเมนูระดับย่อย VPN Software 4. ระบบแสดงหน้าจอเพื่อให้ผู้ดูแลระบบทำการบราวซ์ไฟล์ที่ต้องการอัพโหลดขึ้นไปยังเซิร์ฟเวอร์ 5. ระบบจัดเก็บไฟล์ขึ้นไปยังเซิร์ฟเวอร์และเพิ่มบรรทัดแสดงชื่อไฟล์ใหม่ในหน้า List File

เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	มีโปรแกรมโอเพ่นวีพีเอ็นท์ไคล์เอ็นท์ใหม่มาให้เลือกดาวน์โหลด

ตารางที่ 3.18 รายละเอียดยูสเคส Delete software

ชื่อยูสเคส	Delete software
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดนำโปรแกรมโอเพ่นวีพีเอ็นท์เวอร์ชั่นเก่าออกจากเซิร์ฟเวอร์
เหตุการณ์ที่กระตุ้นการทำงาน	1. มีโปรแกรมโอเพ่นวีพีเอ็นท์เวอร์ชั่นใหม่ออกมา 2. ต้องการนำโปรแกรมเวอร์ชั่นเก่าออกจากระบบ
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	-
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Download OpenVPN และเมนูระดับย่อย VPN Software 4. ระบบแสดงหน้าจอรายชื่อโปรแกรมโอเพ่นวีพีเอ็นท์ไคล์เอ็นท์แต่ละเวอร์ชั่น 5. ผู้ดูแลระบบกดปุ่ม delete หลังบรรทัดของโปรแกรมที่ต้องการจะลบออกจากเซิร์ฟเวอร์ 6. ระบบทำการลบโปรแกรมออกจากเซิร์ฟเวอร์
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	ชื่อโปรแกรมโอเพ่นวีพีเอ็นท์ไคล์เอ็นท์เวอร์ชั่นเก่าถูกลบทิ้งออกจากระบบ

ตารางที่ 3.19 รายละเอียดยูสเคส Manage service

ชื่อยูสเคส	Manage service
คำอธิบายยูสเคส	ผู้ดูแลระบบระดับสิทธิ์สูงสุดต้องการจัดการเกี่ยวกับเซอร์วิสที่ให้บริการของระบบ
เหตุการณ์ที่กระตุ้น	ผู้ดูแลระบบต้องการปรับปรุงหรือแก้ไขการทำงานของระบบโอเพ่นวีพีเอ็นท์

การทำงาน	
แอกเตอร์	Admin (Full-Control)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	-
การทำงาน	1. ผู้ดูแลระบบระดับสิทธิ์สูงสุด ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์การทำงานสูงสุด 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Manage OpenVPN Service 4. ระบบแสดงหน้าจอเพื่อให้ผู้ดูแลระบบสามารถจัดการหยุดการทำงานเซอร์วิส เริ่มการทำงานเซอร์วิสหรือรีสตาร์ทเซอร์วิสของโอเพ่นวีพีเอ็น 5. ระบบรับคำสั่งจากปุ่มกดและทำการหยุดการให้บริการ เริ่มการให้บริการ หรือรีสตาร์ทการให้บริการของโอเพ่นวีพีเอ็น พร้อมแจ้งสถานะปัจจุบันสู่หน้าจอเดิม
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	-

ตารางที่ 3.20 รายละเอียดยูสเคส View log

ชื่อยูสเคส	View log
คำอธิบายยูสเคส	ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งานเรียกดูบันทึกการทำงานของระบบ
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบต้องการตรวจสอบการทำงานของระบบและดูบันทึกการทำงานของระบบ
แอกเตอร์	1. Admin (Full-Control) 2. Admin (Read-Only)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	-
การทำงาน	1. ผู้ดูแลระบบ ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Status and Log ที่ระดับเมนูย่อย

	OpenVPN Log 4. ระบบแสดงบันทึกการทำงานของระบบทั้งหมด
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	-

ตารางที่ 3.21 รายละเอียดยูสเคส View status

ชื่อยูสเคส	View status
คำอธิบายยูสเคส	ผู้ดูแลระบบทุกระดับสิทธิ์การใช้งานเรียกดูบันทึกรายชื่อผู้เข้าใช้งานโอเพ่นวีพีเอ็นในขณะนั้น
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบต้องการตรวจสอบการใช้งานของโอเพ่นวีพีเอ็นและดูสถานะการทำงานของระบบ
แอกเตอร์	1. Admin (Full-Control) 2. Admin (Read-Only)
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	-
การทำงาน	1. ผู้ดูแลระบบ ป้อนชื่อผู้ใช้งานและรหัสผ่านเข้าสู่ระบบ 2. ระบบทำการตรวจสอบผู้ใช้งาน รหัสผ่าน สิทธิ์การเข้าใช้งานและอนุญาติให้เข้าสู่ระบบตามสิทธิ์ที่ได้รับ 3. ผู้ดูแลระบบระดับสิทธิ์สูงสุดเลือกเมนู Status and Log ที่ระดับเมนูย่อย OpenVPN Status 4. ระบบแสดงรายชื่อผู้เข้าใช้งานโอเพ่นวีพีเอ็นในขณะนั้น
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	-

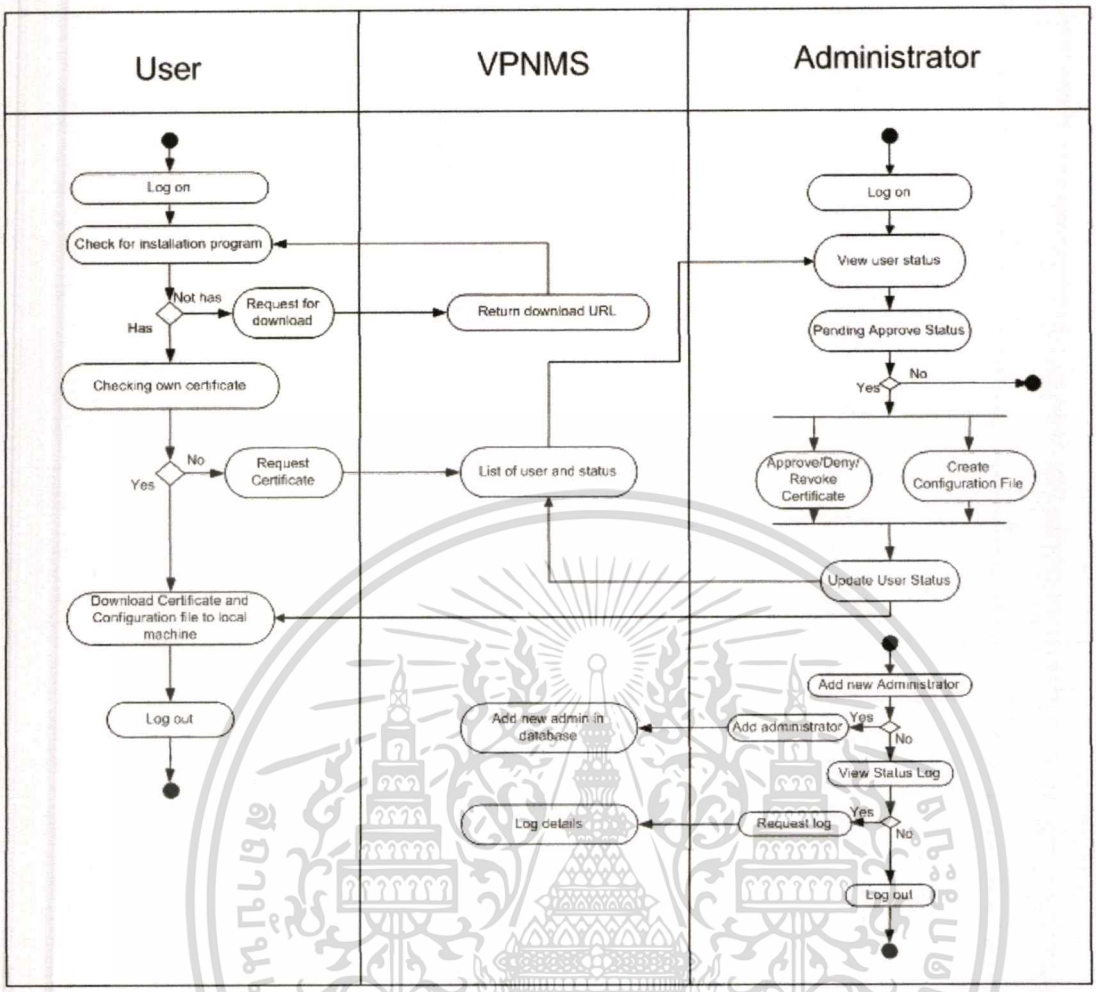
ตารางที่ 3.22 รายละเอียดยูสเคส Log out

ชื่อยูสเคส	Log out
คำอธิบายยูสเคส	ออกจากระบบ
เหตุการณ์ที่กระตุ้นการทำงาน	ผู้ดูแลระบบและผู้ใช้ระบบเสร็จสิ้นกระบวนการใช้ระบบและต้องการออกจากระบบ
แอกเตอร์	1. Admin (Full-Control)

	2. Admin (Read-Only) 3. User
ยูสเคสที่เกี่ยวข้อง	-
ผู้เกี่ยวข้องอื่น	-
เงื่อนไขเริ่มต้น	-
การทำงาน	1. ผู้ดูแลระบบและผู้ใช้ระบบเสร็จสิ้นกระบวนการใช้งานระบบ 2. ผู้ดูแลระบบและผู้ใช้งานระบบเลือกเมนู Log Out 3. ระบบคืนค่าสถานะในการเข้าใช้ระบบและลบค่าการเข้าใช้ ชื่อผู้ใช้และรหัสผ่านในหน่วยความจำของเครื่องพีซี 4. ระบบกลับไปยังหน้าแรกสำหรับการป้อนชื่อผู้ใช้งานและรหัสผ่าน
เงื่อนไขการทำงาน	-
เงื่อนไขเมื่อสำเร็จ	ผู้ดูแลระบบและผู้ใช้งานออกจากระบบ

3.4.3 การออกแบบแผนภาพสวิมเลนไดอะแกรม (Swim-lane Diagram)

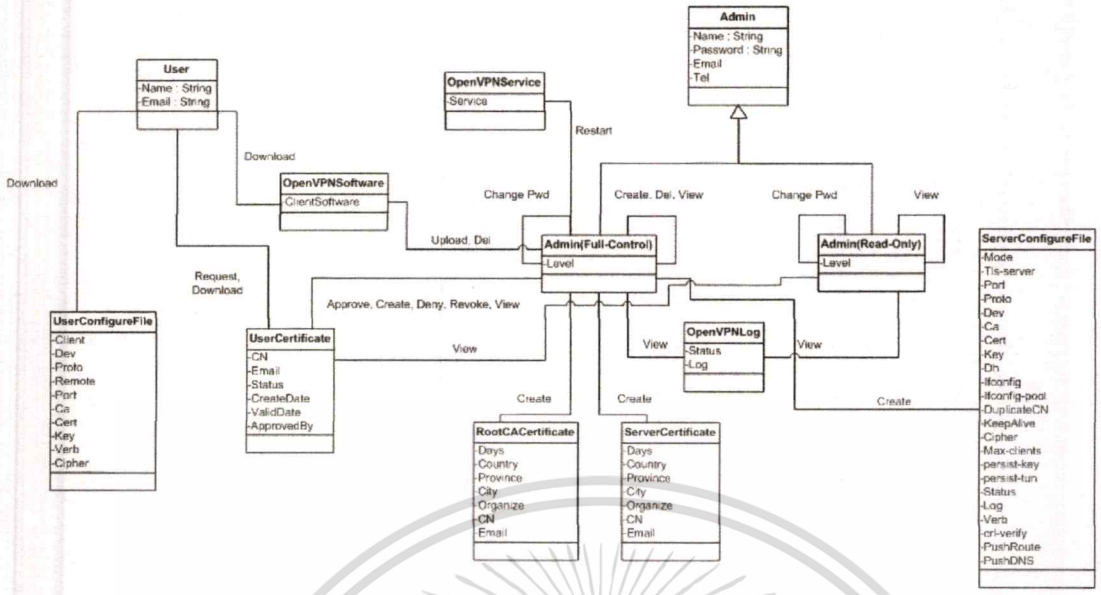
แผนภาพสวิมเลนไดอะแกรมแสดงการทำงานต่างๆของผู้ใช้งานในระบบ ว่าในแต่ละกิจกรรม กิจกรรมไหนเกิดขึ้นก่อนและมีความสัมพันธ์กับกิจกรรมไหนบ้าง ซึ่งแสดงดังรูปที่ 3.5



รูปที่ 3.5 สวิมเลนไดอะแกรมของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

3.4.4 การออกแบบแผนภาพคลาสไดอะแกรม (Class Diagram)

แผนภาพคลาสไดอะแกรมแสดงความสัมพันธ์ของส่วนต่างๆที่เกี่ยวข้องกันในระบบว่ามีส่วนใดเรียกใช้กันบ้าง ซึ่งแสดงดังรูปที่ 3.6



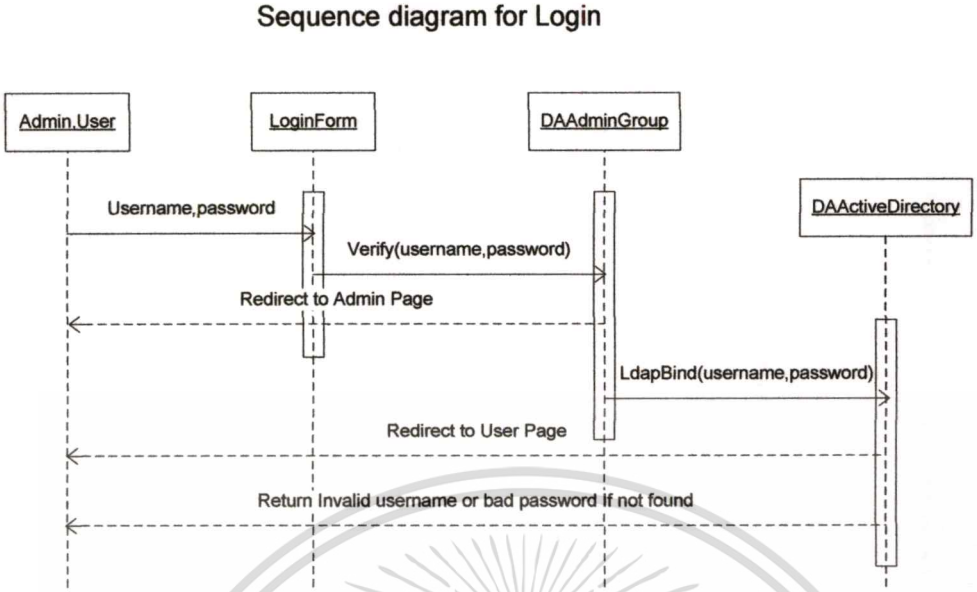
รูปที่ 3.6 คลาสไดอะแกรมของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

3.4.5 การออกแบบแผนภาพซีเควนซ์ไดอะแกรม (Sequence Diagram)

แผนภาพซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชันต่างๆว่ามีการเรียกใช้งานกันหรือมีการส่งค่าตัวแปรกันอย่างไร

- **ซีเควนซ์ไดอะแกรม Login**

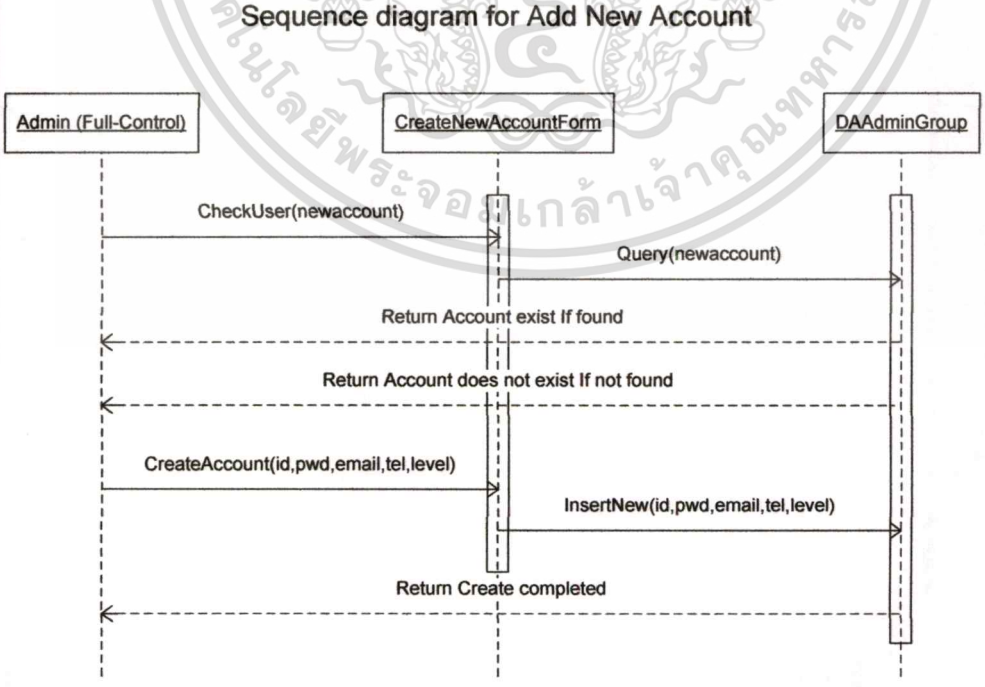
เมื่อผู้ดูแลระบบหรือผู้ใช้งานต้องการล็อกอินเข้าสู่ระบบ จะมีการตรวจสอบสิทธิ์การเข้าก่อนโดยตรวจจากฐานข้อมูลของ AdminGroup ก่อนถ้าพบก็จะคืนค่า URL ของหน้าผู้ดูแลระบบ ถ้าไม่พบก็จะไปตรวจสอบจาก Microsoft Active directory ต่อ ถ้าพบก็จะคืนค่า URL ของหน้าผู้ใช้งาน หรือถ้าไม่พบเลยก็จะแสดงหน้าจอข้อผิดพลาด ดังรูปที่ 3.7



รูปที่ 3.7 ซีเควนซ์ไดอะแกรม Login

- **ซีเควนซ์ไดอะแกรม Add new account**

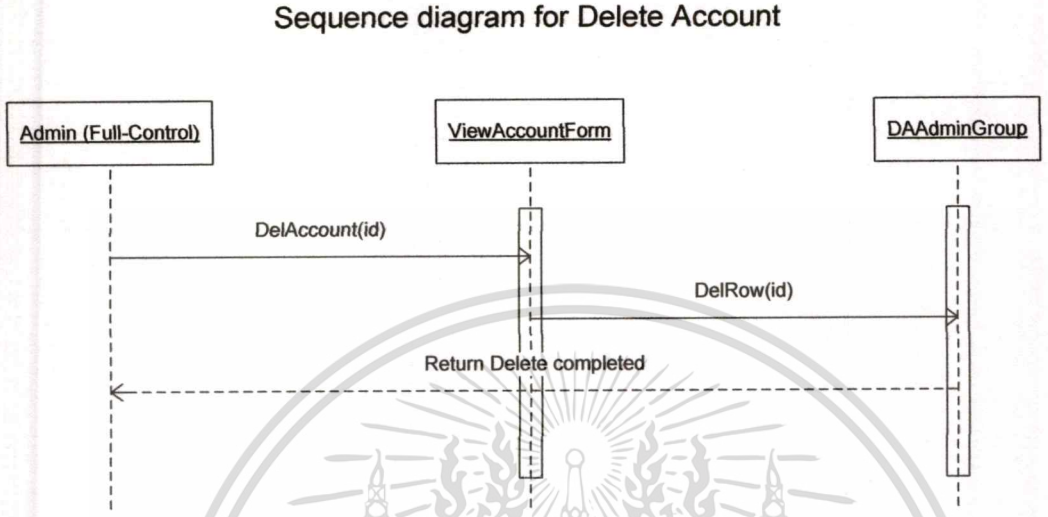
เมื่อผู้ดูแลระบบที่มีสิทธิ์สูงสุดต้องการเพิ่มผู้ดูแลระบบคนใหม่ จะมีการตรวจสอบจากฐานข้อมูลของ AdminGroup ก่อนถ้าพบก็จะคืนค่าข้อผิดพลาด ถ้าไม่พบก็จะไปสร้างผู้ดูแลระบบคนใหม่ ดังรูปที่ 3.8



รูปที่ 3.8 ซีเควนซ์ไดอะแกรม Create New Account

- **ซีเควนซ์ไดอะแกรม Delete account**

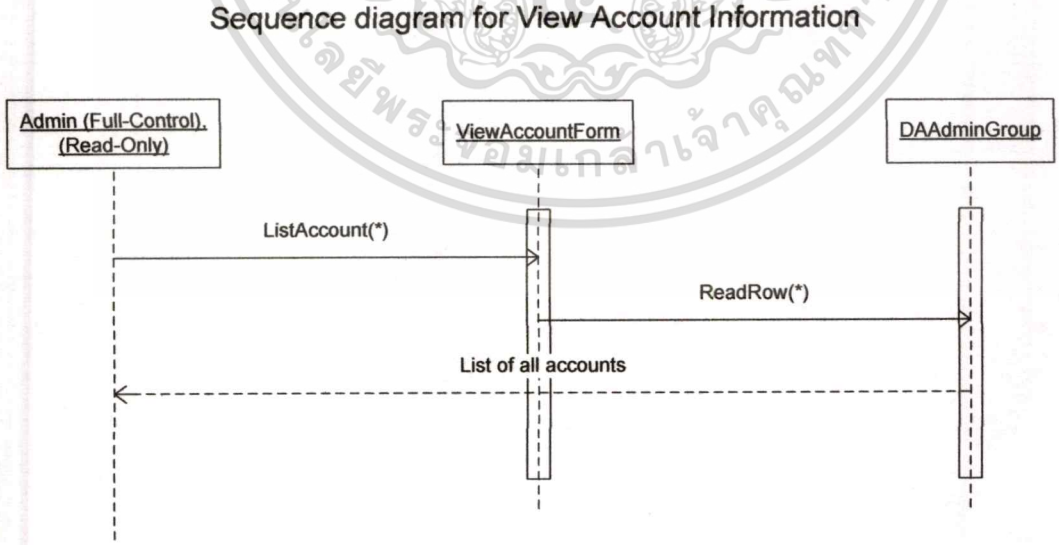
เมื่อผู้ดูแลระบบที่มีสิทธิ์สูงสุดต้องการลบผู้ดูแลระบบ จะมีการลบข้อมูลออกจากฐานข้อมูลของ AdminGroup ดังรูปที่ 3.9



รูปที่ 3.9 ซีเควนซ์ไดอะแกรม Delete Account

- **ซีเควนซ์ไดอะแกรม View Account Information**

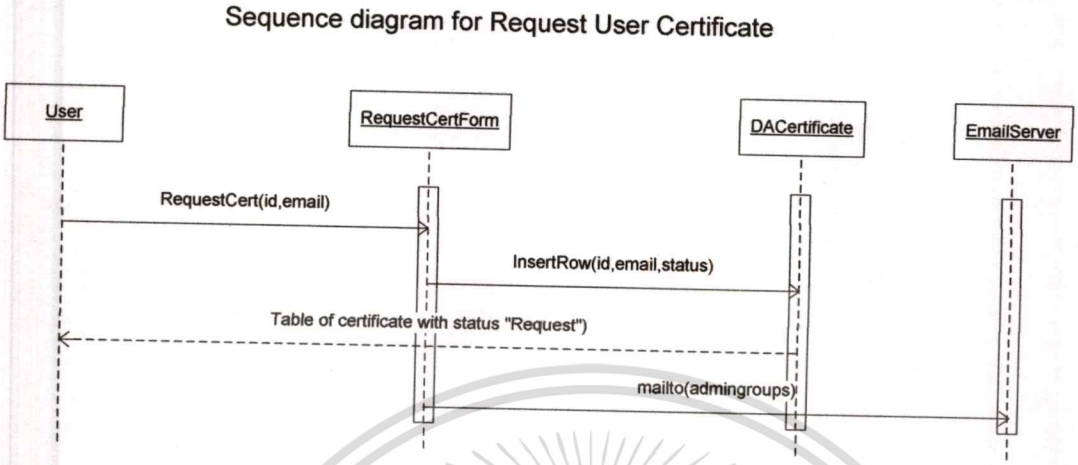
เมื่อผู้ดูแลระบบต้องการดูข้อมูลของผู้ดูแลระบบทั้งหมด จะมีการเรียกดูข้อมูลจากฐานข้อมูลของ AdminGroup ดังรูปที่ 3.10



รูปที่ 3.10 ซีเควนซ์ไดอะแกรม View Account Information

- **ซีเควนซ์ไดอะแกรม Request User Certificate**

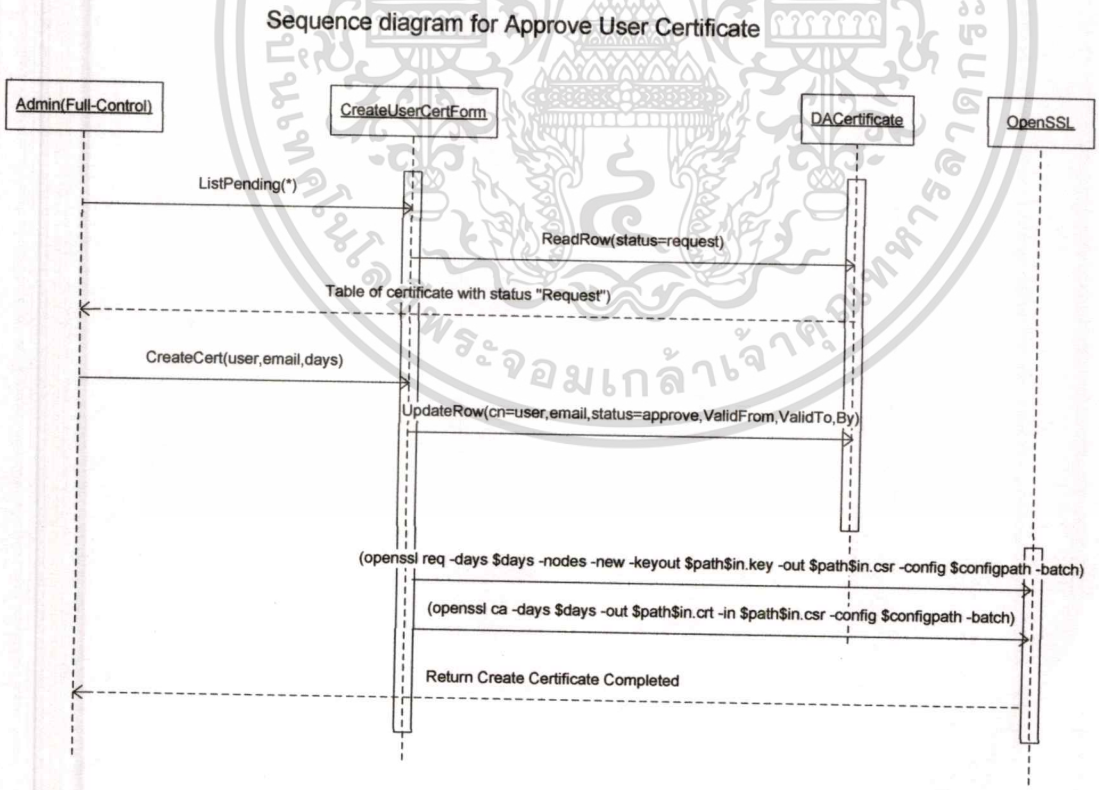
เมื่อผู้ใช้ต้องการร้องขอใบรับรองจะมีการทำงาน ดังรูปที่ 3.11



รูปที่ 3.11 ซีเควนซ์ไดอะแกรม Request User Certificate

- **ซีเควนซ์ไดอะแกรม Approve User Certificate**

เมื่อผู้ดูแลระบบสิทธิ์สูงสุดต้องการอนุมัติใบรับรองจะมีการทำงาน ดังรูปที่ 3.12

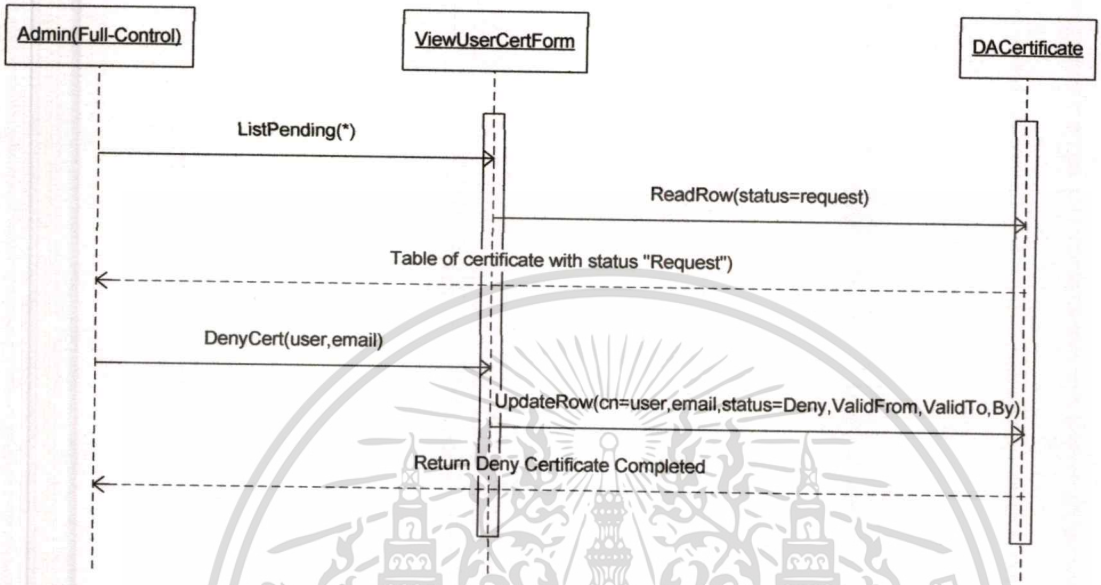


รูปที่ 3.12 ซีเควนซ์ไดอะแกรม Approve User Certificate

- **ซีเควนซ์ไดอะแกรม Deny User Certificate**

เมื่อผู้ดูแลระบบสิทธิ์สูงสุดต้องการปฏิเสธใบรับรองจะมีการทำงาน ดังรูปที่ 3.13

Sequence diagram for Deny User Certificate

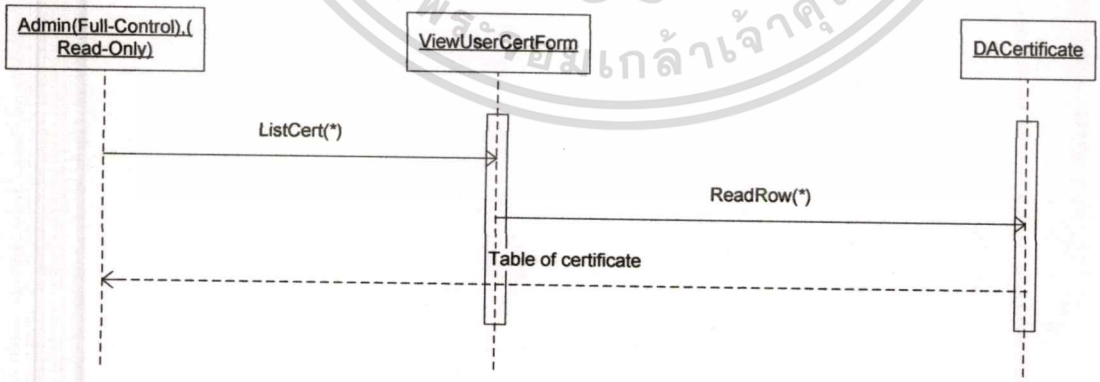


รูปที่ 3.13 ซีเควนซ์ไดอะแกรม Deny User Certificate

- **ซีเควนซ์ไดอะแกรม View User Certificate**

เมื่อผู้ดูแลระบบต้องการดูใบรับรองของผู้ใช้ทั้งหมดจะมีการทำงาน ดังรูปที่ 3.14

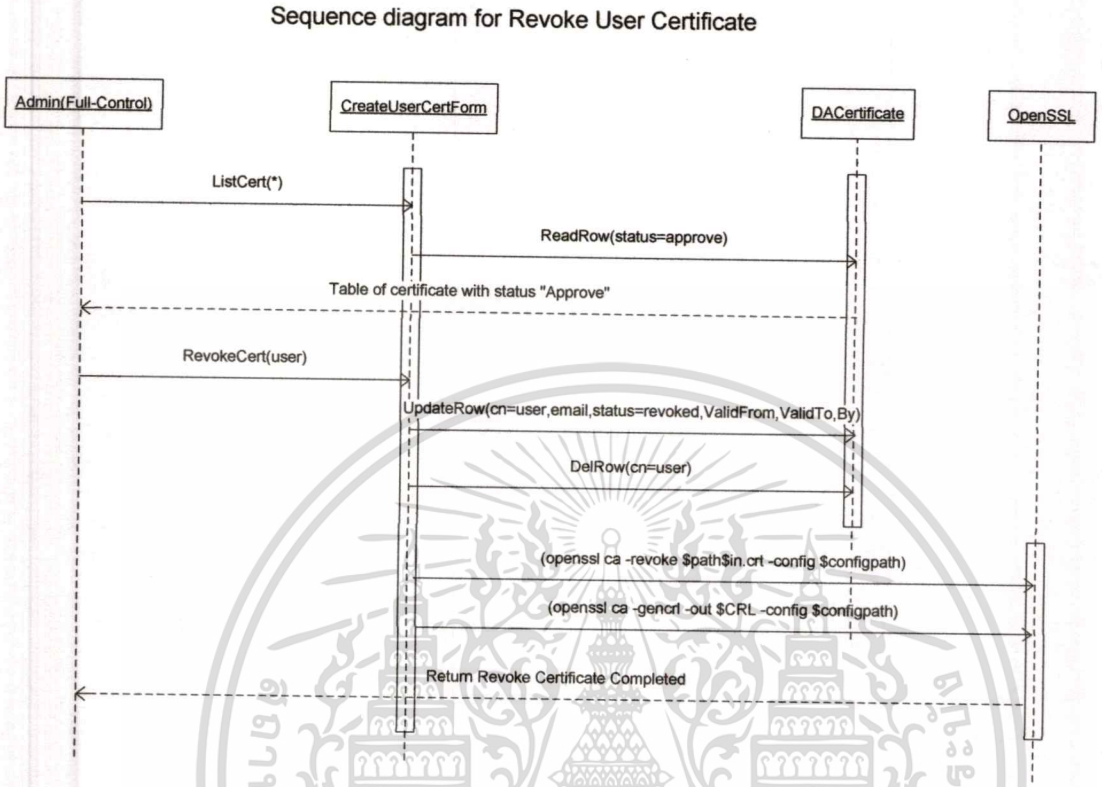
Sequence diagram for View User Certificate



รูปที่ 3.14 ซีเควนซ์ไดอะแกรม View User Certificate

- **ซีเควนซ์ไดอะแกรม Revoke User Certificate**

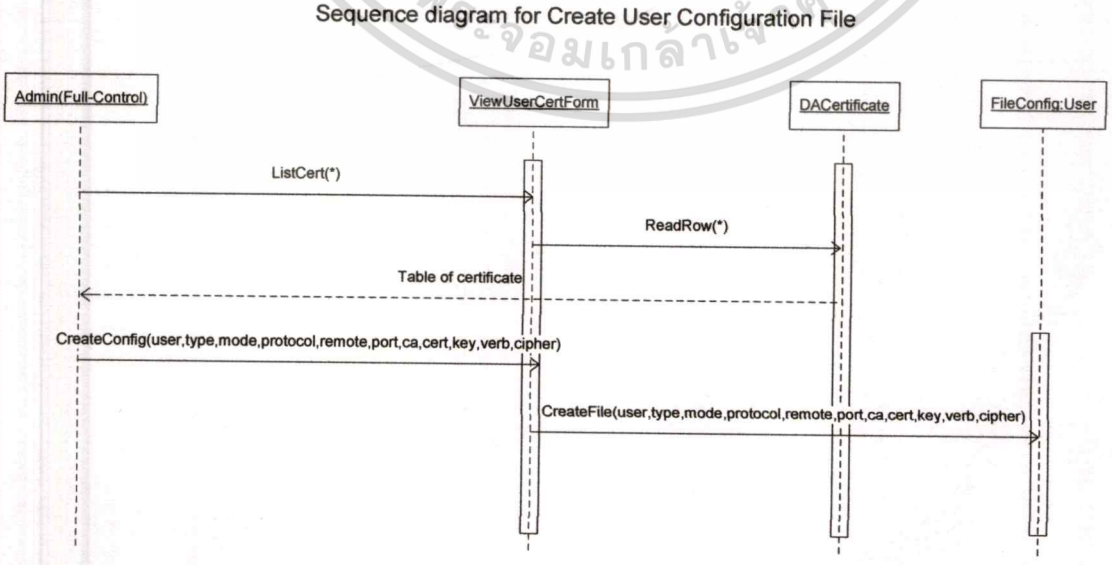
เมื่อผู้ดูแลระบบสิทธิ์สูงสุดต้องการยกเลิกใบรับรองของผู้ใช้จะมีการทำงาน ดังรูปที่ 3.15



รูปที่ 3.15 ซีเควนซ์ไดอะแกรม Revoke User Certificate

- **ซีเควนซ์ไดอะแกรม Create User Certificate File**

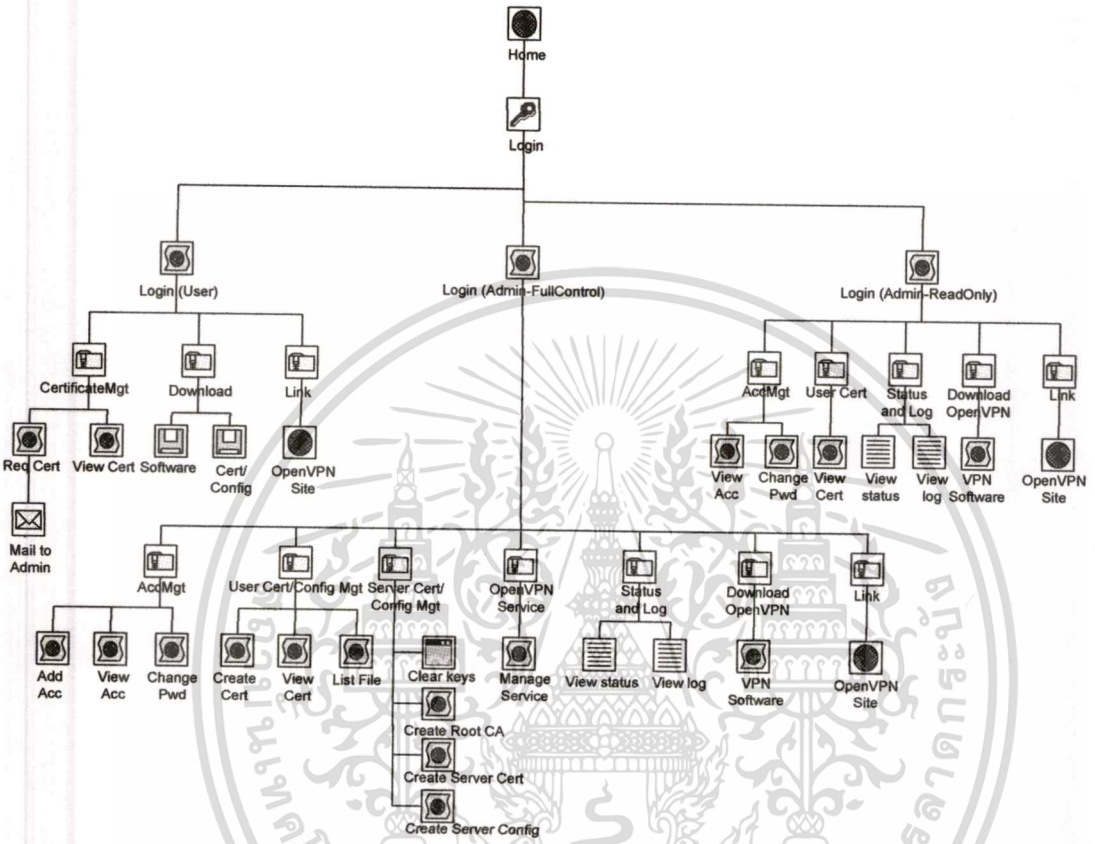
เมื่อผู้ดูแลระบบสิทธิ์สูงสุดต้องการสร้างไฟล์คอนฟิกของผู้ใช้จะมีการทำงาน ดังรูปที่ 3.16



รูปที่ 3.16 ซีเควนซ์ไดอะแกรม Create User Configuration File

3.4.6 การออกแบบโครงสร้างเว็บไซต์ (Website Mapping Design)

แผนภาพโครงสร้างเว็บไซต์ของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บมีดังนี้ ดังแสดงในรูปที่ 3.17



รูปที่ 3.17 แผนภาพโครงสร้างเว็บไซต์ของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัว

บทที่ 4
การออกแบบฐานข้อมูล

การออกแบบฐานข้อมูลสำหรับโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บนั้น เพื่อให้สามารถแสดงรายละเอียดได้อย่างถูกต้องและเข้าใจในระบบได้นั้น สามารถนำเสนอผ่านแบบจำลองอีอาร์ไดอะแกรม เพื่อแสดงให้เห็นถึงความสัมพันธ์ของข้อมูลที่เกิดขึ้น และจะแสดงรายละเอียดของข้อมูลผ่านพจนานุกรมข้อมูล รวมถึงโครงสร้างข้อมูลที่เก็บเป็นไฟล์ด้วย ดังแสดงรายละเอียดดังต่อไปนี้

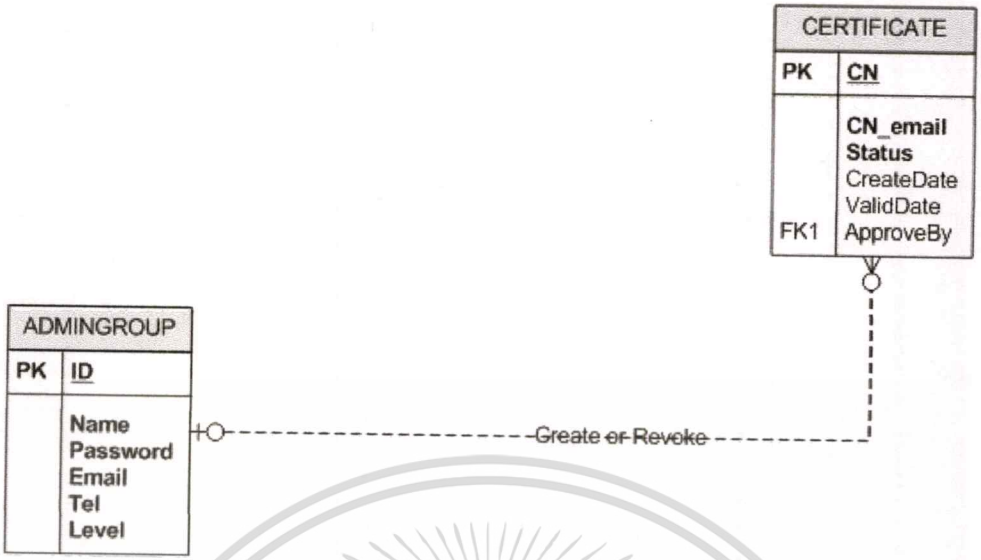
4.1 อีอาร์ไดอะแกรม

ในโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บนั้น มีการออกแบบความสัมพันธ์ระหว่างเอนทิตีที่เกิดขึ้น ซึ่งมีเอนทิตีที่เกี่ยวข้องในระบบดังตารางที่ 4.1

ตารางที่ 4.1 เอนทิตีโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

ลำดับที่	เอนทิตี	คำอธิบายเอนทิตี
1	ADMINGROUP	เอนทิตีข้อมูลของผู้ดูแลระบบ
2	CERTIFICATE	เอนทิตีข้อมูลใบรับรองดิจิตอลของผู้ใช้

จากเอนทิตีของโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ที่ได้แสดงไว้ตามตารางข้างต้นนั้น เอนทิตีเหล่านี้มีความสัมพันธ์กัน โดยจะแสดงความสัมพันธ์ของเอนทิตีเหล่านี้ผ่านอีอาร์ไดอะแกรม ซึ่งมีรายละเอียด ดังแสดงตามรูปที่ 4.1



รูปที่ 4.1 อีอาร์ไดอะแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

สำหรับความสัมพันธ์ระหว่างเอนทิตีแต่ละตัวของระบบ จะมีความสัมพันธ์กัน ดังนี้

- **ADMINGROUP กับ CERTIFICATE** มีความสัมพันธ์กันแบบ 1:M หมายถึง ผู้ดูแลระบบ 1 คน สามารถสร้างหรือยกเลิกใบรับรองให้ผู้ใช้ได้หลายคน ในขณะที่ใบรับรองของผู้ใช้ 1 คน สามารถถูกสร้างหรือยกเลิกโดยผู้ดูแลระบบได้เพียง 1 คนเท่านั้น

4.2 พจนานุกรมข้อมูล

จากอีอาร์ไดอะแกรมที่ได้นั้นสามารถแปลงเอนทิตีให้เป็นฐานข้อมูลเชิงสัมพันธ์ได้ โดยนำเสนอผ่านพจนานุกรมข้อมูลที่จะแสดงให้เห็นรายละเอียดของข้อมูลต่างๆที่เกี่ยวข้องกับการทำงานของระบบ ซึ่งได้เป็นตารางที่มีความสัมพันธ์กันทั้งหมด 2 ตาราง ดังรายการตามตารางที่ 4.2

ตารางที่ 4.2 รายการตารางของโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

ตารางที่	ชื่อตาราง	คำอธิบายตาราง
1	ADMINGROUP	ตารางที่ใช้เก็บข้อมูลของผู้ดูแลระบบ
2	CERTIFICATE	ตารางที่ใช้เก็บข้อมูลของใบรับรองดิจิตอลของผู้ใช้

จากตารางของระบบทั้ง 2 ตารางข้างต้นนั้น เมื่อมากำหนดคุณสมบัติต่างๆของแต่ละตาราง ได้แก่ ฟิลด์ข้อมูล ชนิดของข้อมูล ขนาดข้อมูล และการอ้างอิงข้อมูลไปยังตารางที่มีความสัมพันธ์กัน เพื่อนำข้อมูลเหล่านี้ไปพัฒนาเป็นโปรแกรมใช้งานของระบบ โดยเราจะอธิบายรายละเอียดคุณสมบัติของตารางไว้ที่พจนานุกรมข้อมูลดังรายละเอียดในตารางที่ 4.3 ถึงตารางที่ 4.4 ดังนี้

ตารางที่ 4.3 ADMINGROUP ข้อมูลของผู้ดูแลระบบ

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	ความยาว	คีย์	ตารางอ้างอิง
Id	เป็นค่าที่เพิ่มขึ้นทีละ 1 โดยอัตโนมัติ	Int	5	PK	
Name	ชื่อผู้ดูแลระบบ	Varchar	15		
Password	รหัสผ่านของผู้ดูแลระบบ	Varchar	16		
Email	อีเมลล์ของผู้ดูแลระบบ	Varchar	20		
Tel	เบอร์โทรศัพท์ของผู้ดูแลระบบ	Varchar	15		
Level	สิทธิ์ในการเข้าระบบ	Varchar	20		

ตารางที่ 4.4 CERTIFICATE – ข้อมูลใบรับรองดิจิตอลของผู้ใช้

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	ความยาว	คีย์	ตารางอ้างอิง
CN	ชื่อผู้ใช้ (Logon name)	Varchar	15	PK	
CN_Email	อีเมลล์ของผู้ใช้	Varchar	20		
Status	สถานะของใบรับรอง	Varchar	20		
Create_Date	วันและเวลาที่สร้างใบรับรอง	Varchar	30		
Valid_Date	วันหมดอายุของใบรับรอง	Varchar	30		
Approve_By	ผู้ดูแลระบบที่สร้างหรือยกเลิกใบรับรอง	Varchar	15	FK	ADMINGROUP

4.3 โครงสร้างข้อมูลแบบไฟล์

โครงงานนี้นอกจากมีการเก็บข้อมูลแบบฐานข้อมูล ยังเก็บข้อมูลในรูปแบบของไฟล์ด้วยซึ่งได้แก่คอนฟิกไฟล์ของผู้ใช้และของเซิร์ฟเวอร์ ดังแสดงในตารางที่ 4.5 - 4.7

ตารางที่ 4.5 โครงสร้างข้อมูลของไฟล์คอนฟิกของผู้ใช้

ชื่อแอททริบิวต์	คำอธิบาย
Client	ชนิดของผู้ใช้จะมี 2 แบบคือ client หรือ server
Dev	ชนิดของ interface ที่ใช้ในการเชื่อมต่อมีให้เลือก 2 แบบคือ Tun และ Tap ตัวอย่างเช่น Dev tun หรือ Dev tap
Proto	ชนิดของโปรโตคอลที่ใช้มีให้เลือก 2 แบบคือ TCP และ UDP ตัวอย่างเช่น Proto UDP หรือ Proto TCP
Remote	เป็นการระบุไอพีแอดเดรสและพอร์ตของวีพีเอ็นเซิร์ฟเวอร์ ตัวอย่างเช่น Remote 192.168.1.99 1194
Ca	เป็นการระบุที่เก็บไฟล์ใบรับรองของ CA ตัวอย่างเช่น Ca ca.crt
Cert	เป็นการระบุที่เก็บไฟล์ใบรับรองของผู้ใช้ ตัวอย่างเช่น Cert user01.crt
Key	เป็นการระบุที่เก็บไฟล์คีย์ส่วนตัวของผู้ใช้ ตัวอย่างเช่น Key user01.key
Verb	เป็นการระบุระดับในการเก็บล็อกซึ่งมีค่าตั้งแต่ 0-9 ตัวอย่างเช่น Verb 0
Cipher	เป็นการระบุอัลกอริทึมในการเข้ารหัสซึ่งมีให้เลือก 3 แบบคือ BF-CBC AES-128-CBC DEC-EDE3-CBC ซึ่งต้องเหมือนกันทั้งไคลเอ็นท์และเซิร์ฟเวอร์ ตัวอย่างเช่น Cipher BF-CBC

ตารางที่ 4.6 โครงสร้างข้อมูลของไฟล์คอนฟิกของเซิร์ฟเวอร์ชนิด Tap

ชื่อแอททริบิวต์	คำอธิบาย
Mode	ชนิดของผู้ใช้จะมี 2 แบบคือ client หรือ server ตัวอย่างเช่น Mode Server
TLS-Server	เป็นการระบุว่าต้องการใช้การเข้ารหัสโดยอาศัยหลักการของ TLS ตัวอย่างเช่น TLS-Server
Dev	ชนิดของ interface ที่ใช้ในการเชื่อมต่อมีให้เลือก 2 แบบคือ Tun และ Tap ตัวอย่างเช่น Dev tun หรือ Dev tap
Proto	ชนิดของโปรโตคอลที่ใช้มีให้เลือก 2 แบบคือ TCP และ UDP ตัวอย่างเช่น Proto UDP หรือ Proto TCP
Port	เป็นการระบุพอร์ตของวีพีเอ็นเซิร์ฟเวอร์ ตัวอย่างเช่น Port 1194
Ca	เป็นการระบุที่เก็บไฟล์ใบรับรองของ CA ตัวอย่างเช่น Ca ca.crt
Cert	เป็นการระบุที่เก็บไฟล์ใบรับรองของเซิร์ฟเวอร์ ตัวอย่างเช่น Cert server.crt
Key	เป็นการระบุที่เก็บไฟล์คีย์ส่วนตัวของเซิร์ฟเวอร์ ตัวอย่างเช่น Key server.key
Dh	เป็นการระบุที่เก็บไฟล์คีย์ Deffie Hellman ตัวอย่างเช่น Dh dh1024.pem
ifconfig	เป็นการระบุไอพีแอดเดรสและมาร์สของวีพีเอ็นเซิร์ฟเวอร์ ตัวอย่างเช่น ifconfig 10.100.1.1 255.255.255.0
Ifconfig-pool	เป็นการระบุช่วงไอพีแอดเดรสและมาร์สที่จะจ่ายให้ไคลเอ็นท์ ตัวอย่างเช่น ifconfig-pool 10.100.1.101 10.100.1.200 255.255.255.0
Duplicate-cn	เป็นการตรวจสอบว่ามีผู้ใช้ใบรับรองเดียวกันเข้าใช้พร้อมกันหรือไม่ ถ้ามีจะเข้าได้แค่คนแรกคนเดียว
Keep Alive	เป็นการ ping ตรวจสอบสถานะการเชื่อมต่อทุกกี่วินาทีโดยมี timeout อยู่ที่กี่วินาที

	ตัวอย่างเช่น Keep Alive 10 120
Max-client	เป็นการกำหนดจำนวนสูงสุดในการเชื่อมต่อพร้อมกัน ตัวอย่างเช่น Max-Client 100
Status	เป็นการระบุไฟล์ที่ OpenVPN จะเก็บค่าสถานะ ตัวอย่างเช่น Status openvpn-status.log
Log	เป็นการระบุไฟล์ที่ OpenVPN จะเก็บ]Hvd ตัวอย่างเช่น Status openvpn.log
Verb	เป็นการระบุระดับในการเก็บล็อกซึ่งมีค่าตั้งแต่ 0-9 ตัวอย่างเช่น Verb 0
Crl-verify	เป็นการกำหนดให้เซิร์ฟเวอร์ตรวจสอบใบรับรองที่ถูกยกเลิกไปแล้วไม่ให้สามารถเข้าใช้งานได้ ตัวอย่างเช่น Crl-verify crl.pem
Cipher	เป็นการระบุอัลกอริทึมในการเข้ารหัสซึ่งมีให้เลือก 3 แบบคือ BF-CBC AES-128-CBC DEC-EDE3-CBC ซึ่งต้องเหมือนกันทั้งไคลเอ็นท์และเซิร์ฟเวอร์ ตัวอย่างเช่น Cipher BF-CBC
Push	เป็นการส่งค่าได้แก่ Routing table และ DNS ไปยังไคลเอ็นท์ ตัวอย่างเช่น push "route 172.19.1.0 255.255.255.0 10.100.1.1" push "dhcp-option DNS 172.19.1.50"

ตารางที่ 4.7 โครงสร้างข้อมูลของไฟล์คอนฟิกของเซิร์ฟเวอร์ชนิด Tun

ชื่อแอททริบิวต์	คำอธิบาย
Dev	ชนิดของ interface ที่ใช้ในการเชื่อมต่อมีให้เลือก 2 แบบคือ Tun และ Tap ตัวอย่างเช่น Dev tun หรือ Dev tap
Proto	ชนิดของโปรโตคอลที่ใช้มีให้เลือก 2 แบบคือ TCP และ UDP ตัวอย่างเช่น Proto UDP หรือ Proto TCP
Port	เป็นการระบุพอร์ตของวีพีเอ็นเซิร์ฟเวอร์ ตัวอย่างเช่น Port 1194
Ca	เป็นการระบุที่เก็บไฟล์ใบรับรองของ CA ตัวอย่างเช่น Ca ca.crt

Cert	เป็นการระบุที่เก็บไฟล์ใบรับรองของเซิร์ฟเวอร์ ตัวอย่างเช่น Cert server.crt
Key	เป็นการระบุที่เก็บไฟล์คีย์ส่วนตัวของเซิร์ฟเวอร์ ตัวอย่างเช่น Key server.key
Dh	เป็นการระบุที่เก็บไฟล์คีย์ Deffie Hellman ตัวอย่างเช่น Dh dh1024.pem
Server	เป็นการระบุช่วงไอพีแอดเดรสและมาร์สที่จะจ่ายให้ไคลเอ็นท์แบบ Point-to-Point โดยไอพีแอดเดรสแรกจะเป็นของเซิร์ฟเวอร์ ตัวอย่างเช่น server 10.100.1.0 255.255.255.0
Duplicate-cn	เป็นการตรวจสอบว่ามีผู้ใช้ใบรับรองเดียวกันเข้าใช้พร้อมกันหรือไม่ ถ้ามีจะเข้าได้แค่คนแรกคนเดียว
Keep Alive	เป็นการ ping ตรวจสอบสถานะการเชื่อมต่อทุกกี่วินาทีโดยมี timeout อยู่ที่กี่วินาที ตัวอย่างเช่น Keep Alive 10 120
Max-client	เป็นการกำหนดจำนวนสูงสุดในการเชื่อมต่อพร้อมกัน ตัวอย่างเช่น Max-Client 100
Status	เป็นการระบุไฟล์ที่ OpenVPN จะเก็บค่าสถานะ ตัวอย่างเช่น Status openvpn-status.log
Log	เป็นการระบุไฟล์ที่ OpenVPN จะเก็บ]Hvd ตัวอย่างเช่น Status openvpn.log
Verb	เป็นการระบุระดับในการเก็บล็อกซึ่งมีค่าตั้งแต่ 0-9 ตัวอย่างเช่น Verb 0
Crl-verify	เป็นการกำหนดให้เซิร์ฟเวอร์ตรวจสอบใบรับรองที่ถูกยกเลิกไปแล้วไม่ให้สามารถเข้าใช้งานได้ ตัวอย่างเช่น Crl-verify crl.pem
Cipher	เป็นการระบุอัลกอริทึมในการเข้ารหัสซึ่งมีให้เลือก 3 แบบคือ BF-CBC AES-128-CBC DEC-EDE3-CBC ซึ่งต้องเหมือนกันทั้งไคลเอ็นท์และเซิร์ฟเวอร์ ตัวอย่างเช่น Cipher BF-CBC
Push	เป็นการส่งค่าได้แก่ Routing table และ DNS ไปยังไคลเอ็นท์

	ตัวอย่างเช่น push "route 172.19.1.0 255.255.255.0" push "dhcp-option DNS 172.19.1.50"

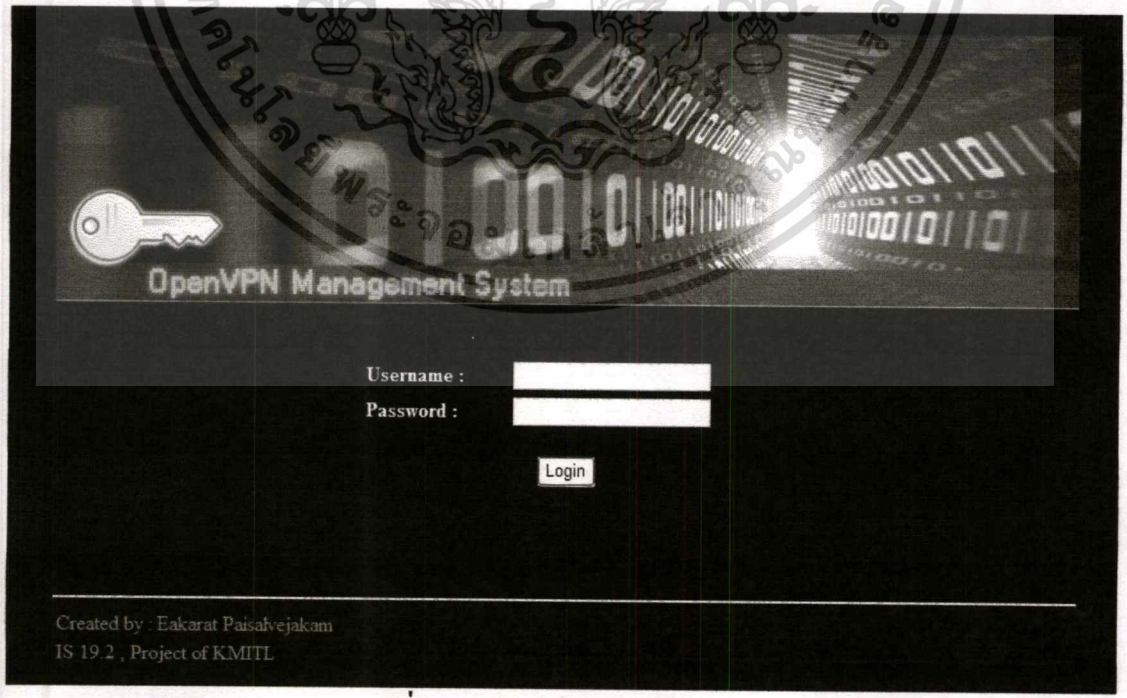
บทที่ 5
การออกแบบส่วนต่อประสานกับผู้ใช้

ส่วนการติดต่อกับผู้ใช้งานของโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บนั้น แบ่งออกเป็น 3 ส่วน คือ ส่วนติดต่อกับผู้ดูแลระบบที่มีสิทธิ์สูงสุด (Full-Control) ส่วนติดต่อกับผู้ดูแลระบบที่มีสิทธิ์ดูข้อมูลได้อย่างเดียว (Read-Only) และส่วนติดต่อกับผู้ใช้งาน

5.1 การออกแบบส่วนติดต่อกับผู้ดูแลระบบที่มีสิทธิ์สูงสุด (Full-Control)

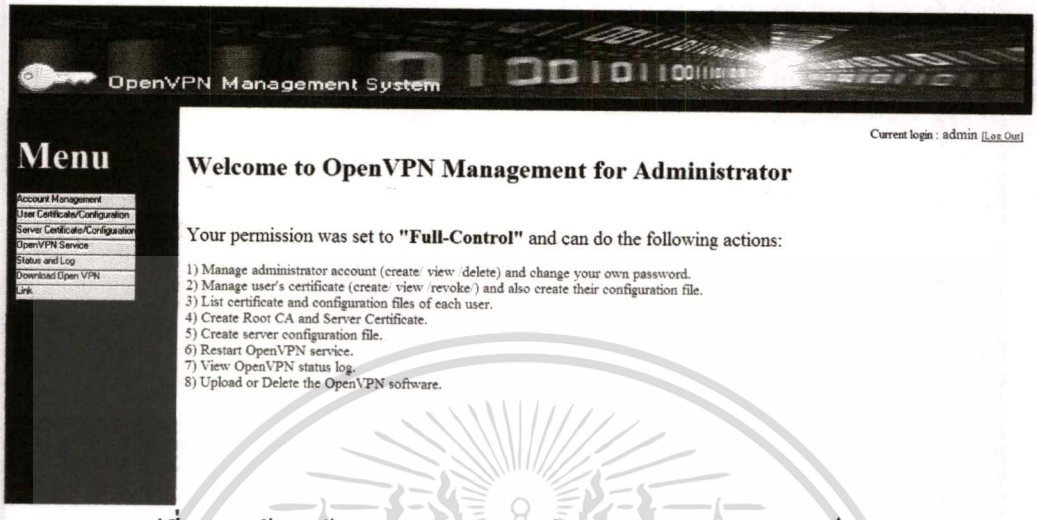
หน้าจอสำหรับจัดการข้อมูลต่าง ๆ ของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ในส่วนนี้จะมีฟังก์ชันการใช้งานหลักทั้งหมดของผู้ดูแลระบบ ได้แก่ การจัดการข้อมูลในการเข้าใช้งานของผู้ดูแลระบบ การจัดการเรื่องใบรับรองดิจิตอลของผู้ใช้งานและเซิร์ฟเวอร์ การสร้างไฟล์คอนฟิกผู้ใช้งานและเซิร์ฟเวอร์ การจัดการเรื่องการให้บริการของ OpenVPN การดูสถานะและล็อกของ OpenVPN การจัดการเรื่องการให้บริการดาวน์โหลดซอฟต์แวร์ โดยมีหน้าจอหลักของระบบ ดังต่อไปนี้

หน้าจอล็อกอินของระบบซึ่งจะเป็นหน้าจอที่ใช้ในการตรวจสอบสิทธิ์ผู้ใช้งาน ว่าสามารถจะเข้ามาใช้งานได้หรือไม่และมีสิทธิ์ในการใช้งานได้อย่างไรบ้าง แสดงดังรูปที่ 5.1



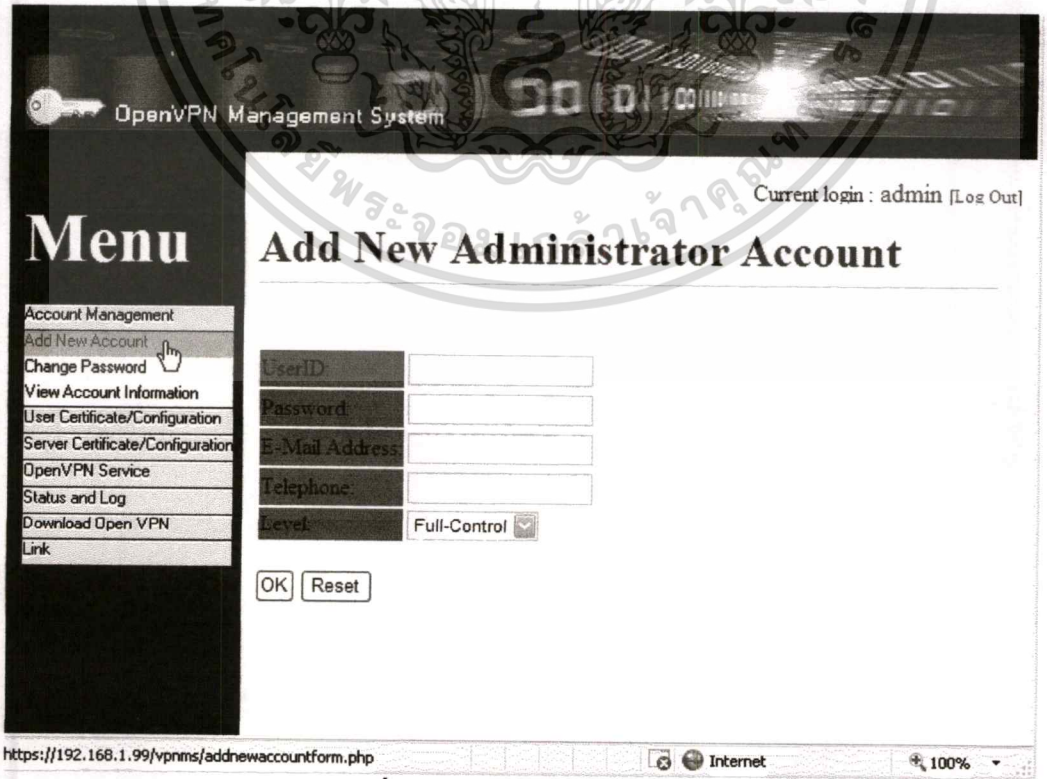
รูปที่ 5.1 หน้าจอล็อกอินเข้าสู่ระบบ

เมื่อล็อกอินเข้าสู่ระบบเรียบร้อยแล้ว จะปรากฏหน้าจอต้อนรับพร้อมบอกว่าผู้ล็อกอินเข้ามามีสิทธิ์อะไร สามารถทำอะไรได้บ้าง รวมถึงบอกว่าล็อกอินเข้ามาด้วยชื่ออะไร แสดงดังรูปที่ 5.2



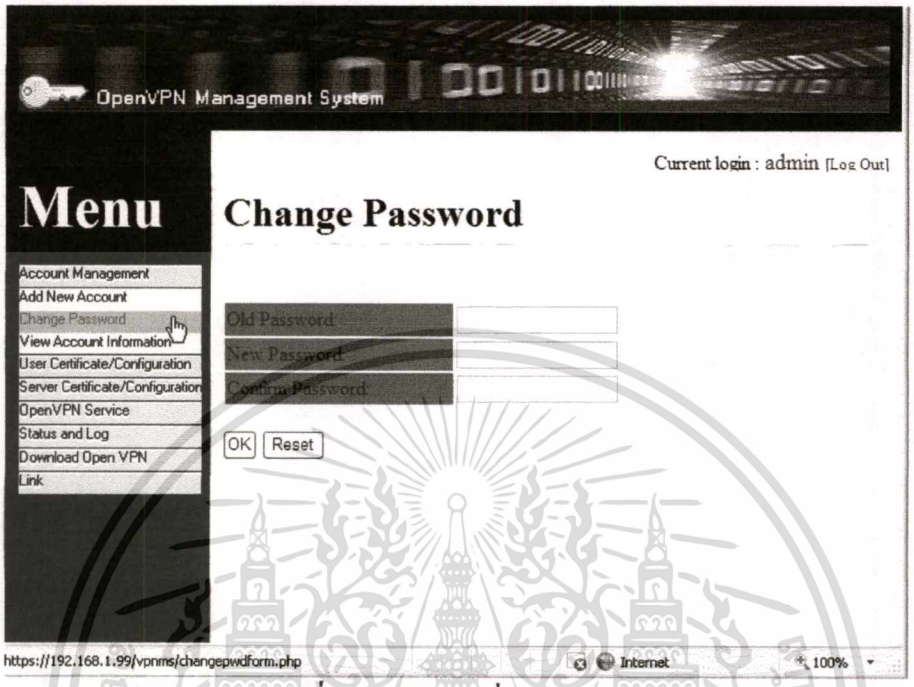
รูปที่ 5.2 หน้าจอต้อนรับหลังจากการล็อกอินเข้าระบบด้วยสิทธิ์สูงสุด

เมื่อต้องการเพิ่มผู้ดูแลระบบ สามารถทำได้โดยเข้าไปที่เมนู Account Management จากนั้นเลือก Add New Account โดยใส่ชื่อผู้ดูแลระบบ รหัสผ่าน อีเมลล์ เบอร์โทรศัพท์ และสิทธิ์ซึ่งมีให้เลือก 2 แบบคือ Full-Control กับ Read-Only แสดงดังรูปที่ 5.3



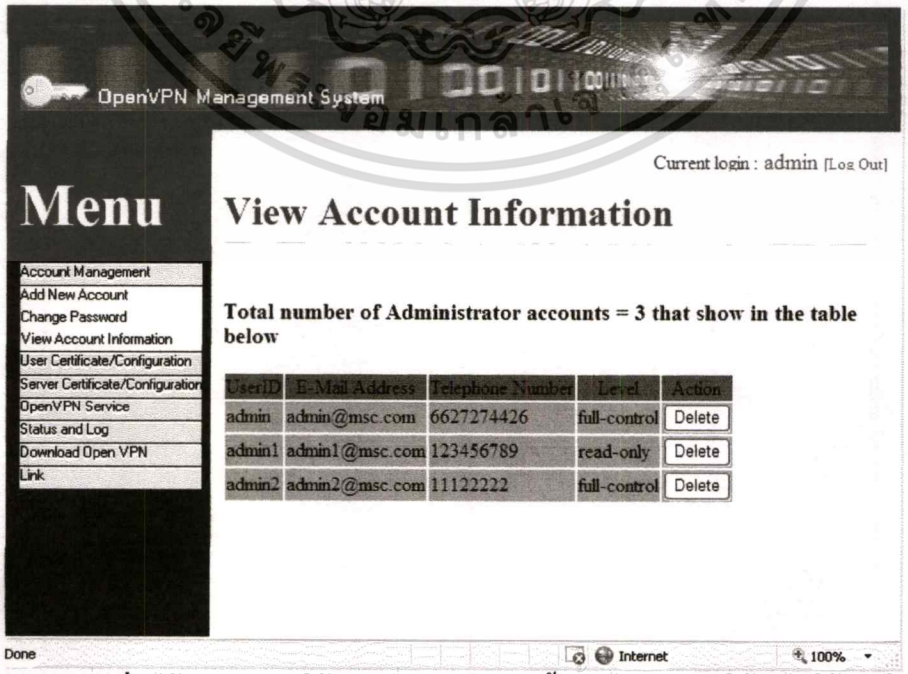
รูปที่ 5.3 หน้าจอเพิ่มผู้ดูแลระบบ

หากต้องการเปลี่ยนรหัสผ่านของตนเอง สามารถทำได้โดยเข้าไปที่เมนู Account Management จากนั้นเลือก Change Password โดยใส่รหัสผ่านเดิม และรหัสผ่านใหม่ หน้าจอดังแสดงในรูป 5.4



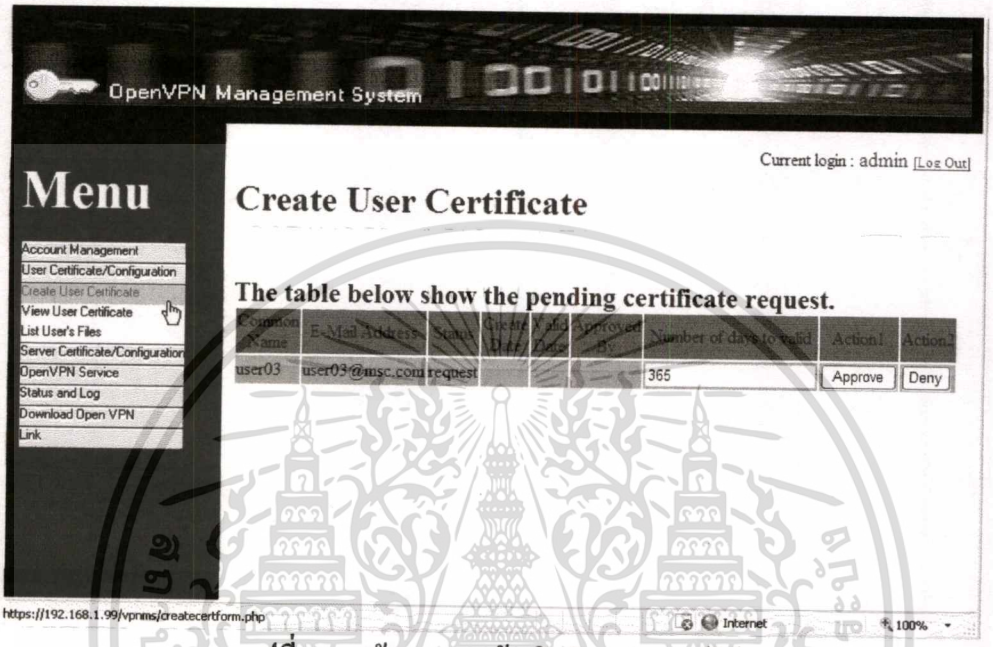
รูปที่ 5.4 หน้าจอเปลี่ยนรหัสผ่าน

เมื่อต้องการดูข้อมูลว่ามีผู้ดูแลระบบทั้งหมดมีกี่คนและมีใครบ้าง สามารถทำได้โดยเข้าไปที่เมนู Account Management จากนั้นเลือก View Account Information นอกจากนี้ยังสามารถลบผู้ดูแลระบบที่ไม่ต้องการได้อีกด้วย ดังแสดงในรูปที่ 5.5



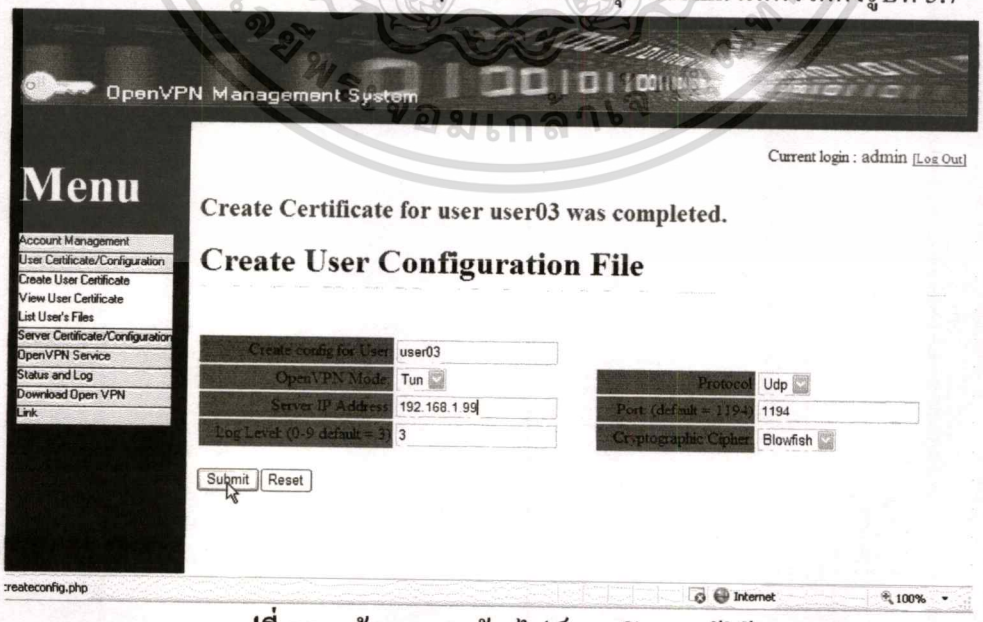
รูปที่ 5.5 หน้าจอดูข้อมูลของผู้ดูแลระบบทั้งหมดสำหรับสิทธิ์สูงสุด

เมื่อต้องการสร้างใบรับรองให้ผู้ใช้งาน (ต้องมีการร้องขอจากผู้ใช้งานก่อน) สามารถทำได้โดยเข้าไปที่เมนู User Certificate/ Configuration จากนั้นเลือก Create User Certificate ถ้ามีการร้องขอแล้วยังไม่มีการ approve หรือ deny ก็จะแสดงตารางที่ค้างอยู่ จากนั้นถ้าต้องการสร้างใบรับรองให้ใส่จำนวนวันที่ต้องการแล้วกดปุ่ม Approve หรือถ้าไม่ต้องการออกใบรับรองให้กดปุ่ม Deny ดังแสดงในรูปที่ 5.6



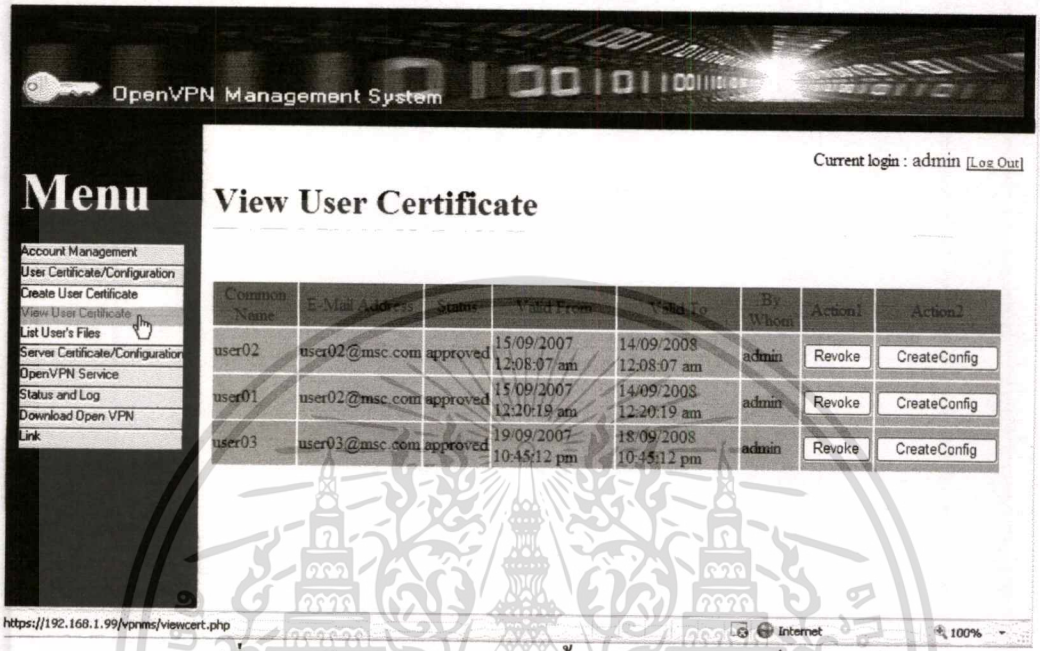
รูปที่ 5.6 หน้าจอการสร้างใบรับรองของผู้ใช้

หลังจากสร้างใบรับรองเสร็จจะเป็นการสร้างไฟล์คอนฟิกของผู้ใช้ โดยให้ใส่ไอพีแอดเดรสของเซิร์ฟเวอร์ และค่าคอนฟิกต่างๆ จากนั้นให้กดปุ่ม Submit แสดงได้ดังรูปที่ 5.7



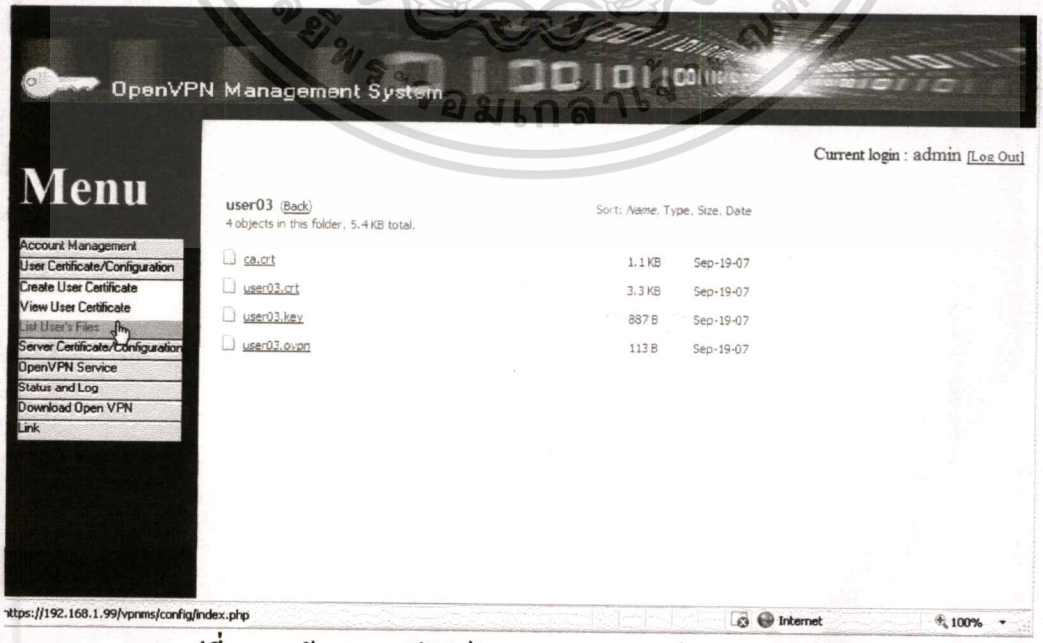
รูปที่ 5.7 หน้าจอการสร้างไฟล์คอนฟิกของผู้ใช้

เมื่อต้องการดูรายละเอียดของใบรับรองทั้งหมดที่มีอยู่ สามารถทำได้โดยเข้าไปที่เมนู User Certificate/ Configuration จากนั้นเลือก View User Certificate นอกจากนี้ยังสามารถยกเลิกใบรับรองได้ โดยกดปุ่ม Revoke รวมถึงสามารถสร้างไฟล์คอนฟิกของผู้ใช้งานได้อีกโดยกดปุ่ม Create config แสดงดังรูปที่ 5.8



รูปที่ 5.8 หน้าจอการดูใบรับรองทั้งหมดสำหรับสิทธิ์สูงสุด

เมื่อต้องการดูไฟล์ที่สร้างขึ้นมาทั้งหมดทั้งใบรับรองและไฟล์คอนฟิกของผู้ใช้ทั้งหมด สามารถทำได้โดยเข้าไปที่เมนู User Certificate/ Configuration จากนั้นเลือก List User's Files แสดงดังรูปที่ 5.9

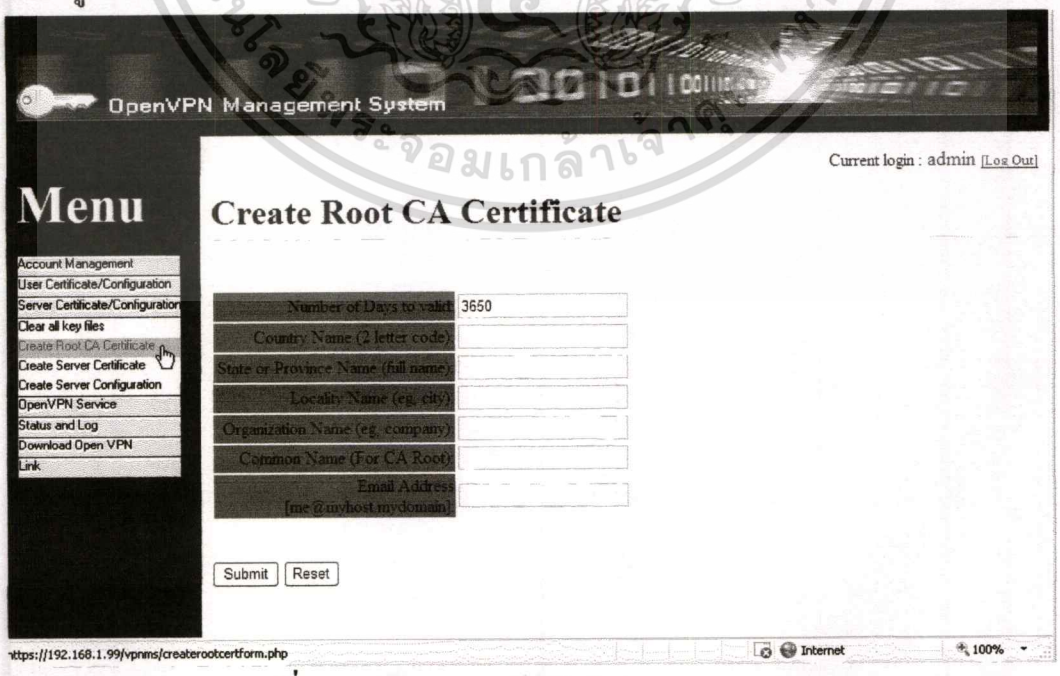


รูปที่ 5.9 หน้าจอการดูไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้

เมื่อต้องการสร้างใบรับรองของเซิร์ฟเวอร์ใหม่ทั้งหมด โดยต้องการลบไฟล์ใบรับรองของเก่าทิ้งทั้งหมดก่อน สามารถทำได้โดยเข้าไปที่เมนู Server Certificate/ Configuration จากนั้นเลือก Clear All Key Files และกดปุ่ม Remove ดังแสดงในรูปที่ 5.10

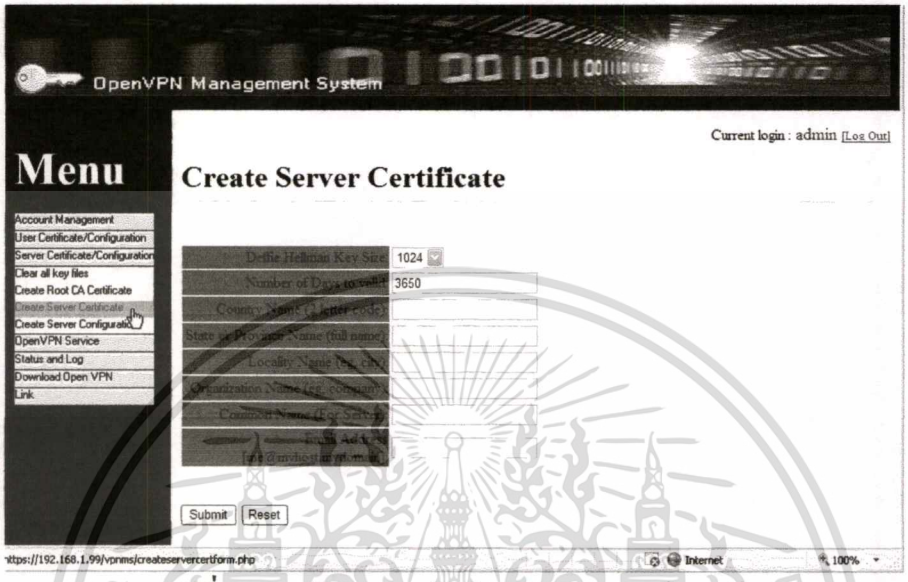
รูปที่ 5.10 หน้าจอการลบไฟล์ใบรับรองทั้งหมดที่มีในเซิร์ฟเวอร์

เมื่อต้องการสร้างใบรับรองของ Root CA ใหม่ สามารถทำได้โดยเข้าไปที่เมนู Server Certificate/ Configuration จากนั้นเลือก Create Root CA Certificate แล้วใส่ข้อมูลต่างๆเช่น จำนวนวัน ประเทศ จังหวัด ชื่อเมือง ชื่อบริษัท ชื่อของ Root CA และอีเมลล์ จากนั้นกดปุ่ม Submit ดังแสดงในรูปที่ 5.11



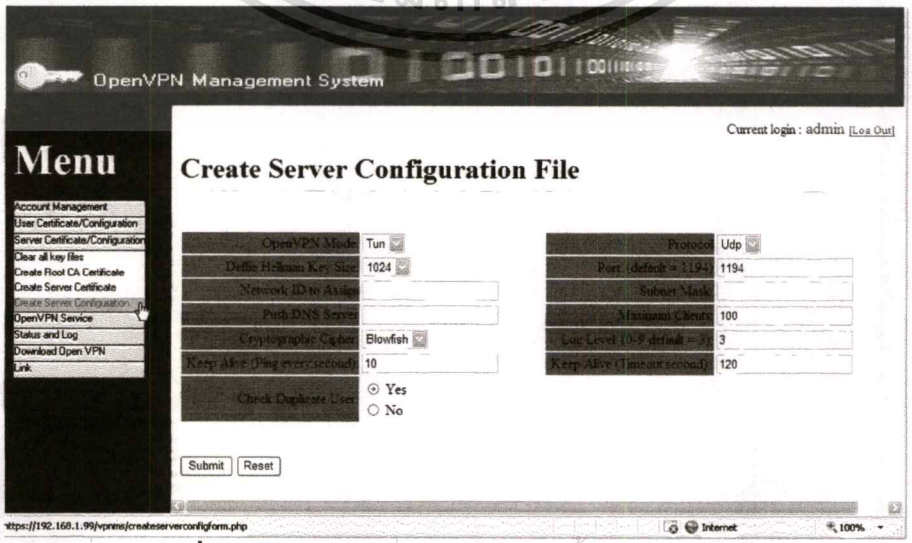
รูปที่ 5.11 หน้าจอการสร้างใบรับรองของ Root CA

เมื่อต้องการสร้างใบรับรองของเซิร์ฟเวอร์ใหม่ สามารถทำได้โดยเข้าไปที่เมนู Server Certificate/ Configuration จากนั้นเลือก Create Server Certificate แล้วใส่ข้อมูลต่างๆเช่น ขนาดของคีย์ จำนวนวัน ประเทศ จังหวัด ชื่อเมือง ชื่อบริษัท ชื่อของเซิร์ฟเวอร์ และอีเมลล์ จากนั้นกดปุ่ม Submit ดังแสดงในรูปที่ 5.12



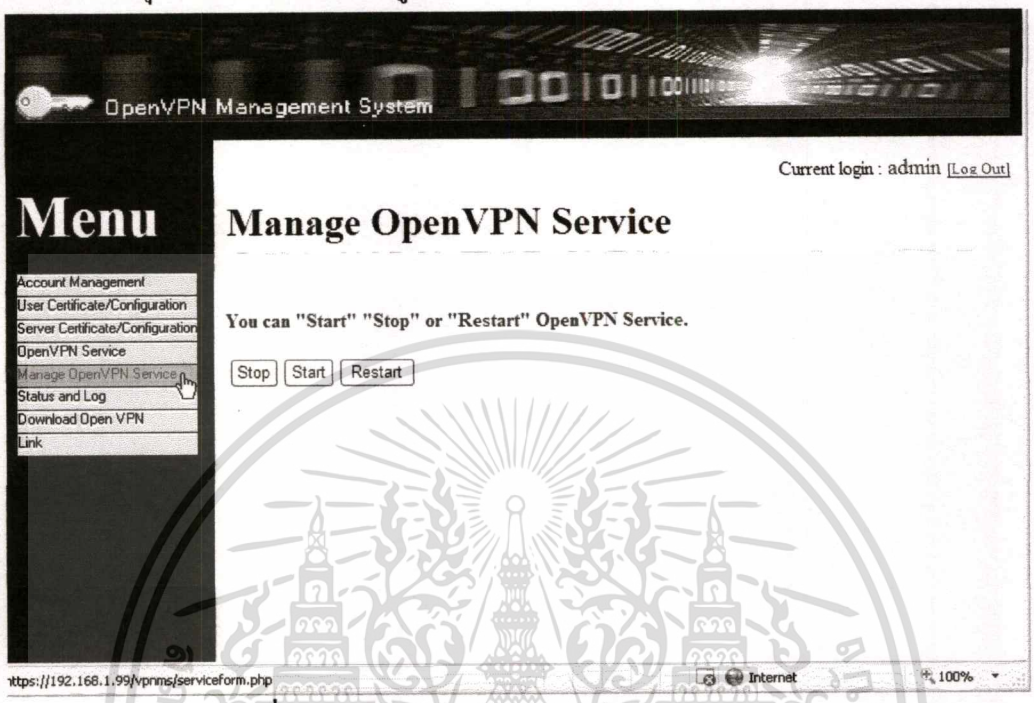
รูปที่ 5.12 หน้าจอการสร้างใบรับรองของเซิร์ฟเวอร์

หากต้องการสร้างไฟล์คอนฟิกของเซิร์ฟเวอร์ สามารถทำได้โดยเข้าไปที่เมนู Server Certificate/ Configuration จากนั้นเลือก Create Server Configuration แล้วใส่ข้อมูลต่างๆได้แก่ โหมดของ OpenVPN โปรโตคอลที่ใช้ ขนาดของคีย์ พอร์ตที่ใช้ ช่วงของไอพีแอดเดรสที่จะแจกให้ผู้ใช้ ดีเอนเอสเซิร์ฟเวอร์ที่จะแจกให้ผู้ใช้ จำนวนผู้ใช้ที่มากที่สุดในการเชื่อมต่อพร้อมกัน ชนิดของการเข้ารหัส ระดับในการเก็บล็อก ค่าในการตรวจสอบสถานะ และกำหนดผู้ใช้งานห้ามมีใบรับรองเดียวกันเข้าใช้งานพร้อมกัน ดังแสดงในรูปที่ 5.13



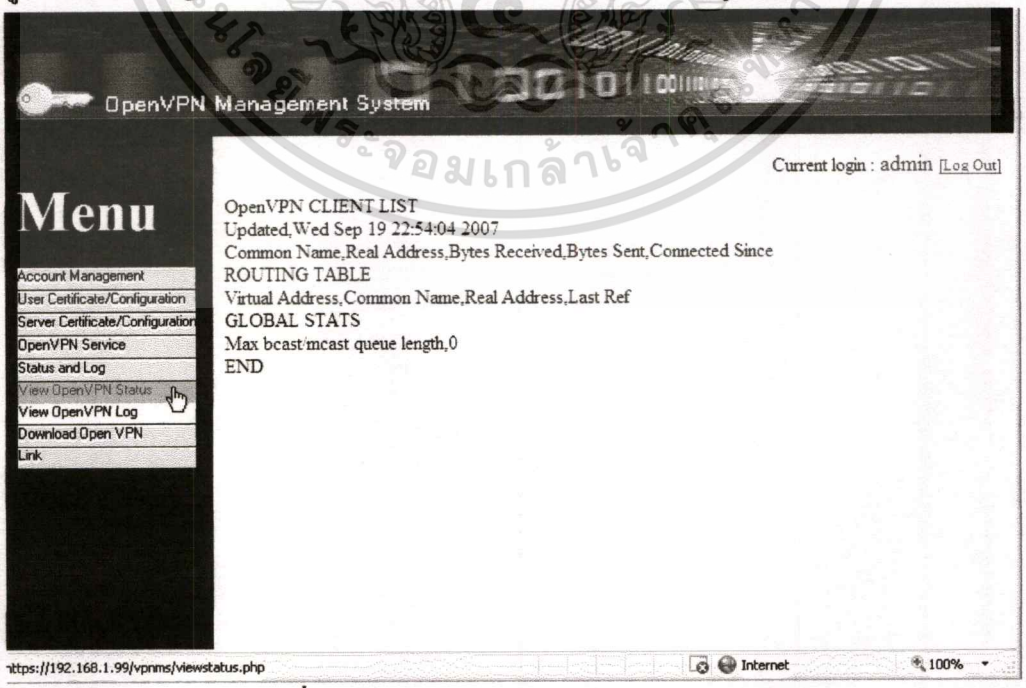
รูปที่ 5.13 หน้าจอการสร้างไฟล์คอนฟิกของเซิร์ฟเวอร์

เมื่อมีการเปลี่ยนค่าไฟล์คอนฟิกของเซิร์ฟเวอร์ทุกครั้งต้องมีการรีสตาร์ทเซอร์วิสของ OpenVPN สามารถทำได้โดยเข้าไปที่เมนู OpenVPN Service จากนั้นเลือก Manage OpenVPN Service แล้วกดปุ่ม Restart ดังแสดงในรูปที่ 5.14



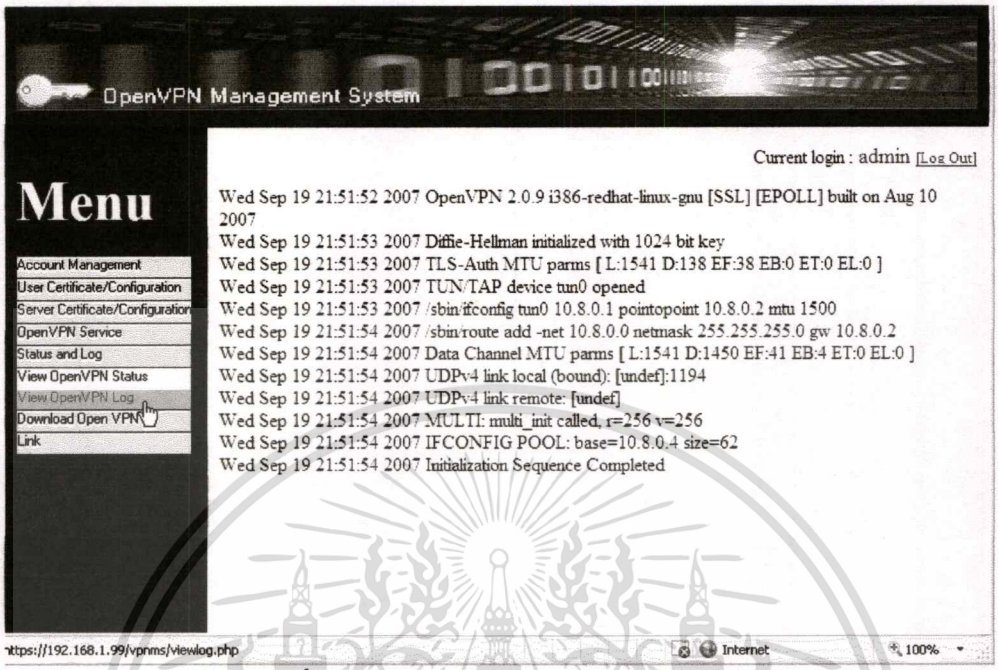
รูปที่ 5.14 หน้าจอการจัดการเซอร์วิสของ OpenVPN

หากต้องการดูสถานะว่าขณะนี้มีใครเชื่อมต่อเข้ามาใช้งานอยู่บ้าง สามารถทำได้โดยเข้าไปที่เมนู Status and Log จากนั้นเลือก View OpenVPN Status แสดงดังรูปที่ 5.15



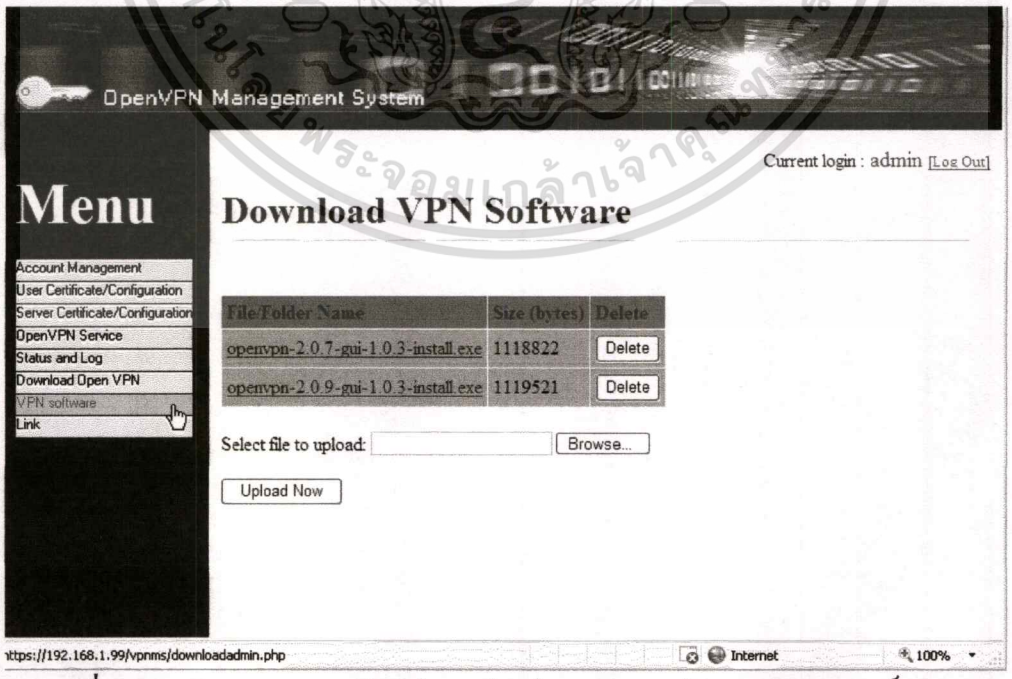
รูปที่ 5.15 หน้าจอการดูสถานะของ OpenVPN

หากต้องการดูล็อกของ OpenVPN สามารถทำได้โดยเข้าไปที่เมนู Status and Log จากนั้นเลือก View OpenVPN Log ดังแสดงในรูปที่ 5.16



รูปที่ 5.16 หน้าจอการดูล็อกของ OpenVPN

หากต้องการจัดการซอฟต์แวร์ OpenVPN เพื่อให้บริการดาวน์โหลด สามารถสามารถทำได้โดยเข้าไปที่เมนู Download OpenVPN แล้วเลือก VPN Software ซึ่งสามารถอัพโหลดหรือลบไฟล์บนเซิร์ฟเวอร์ได้ ดังแสดงในรูปที่ 5.17



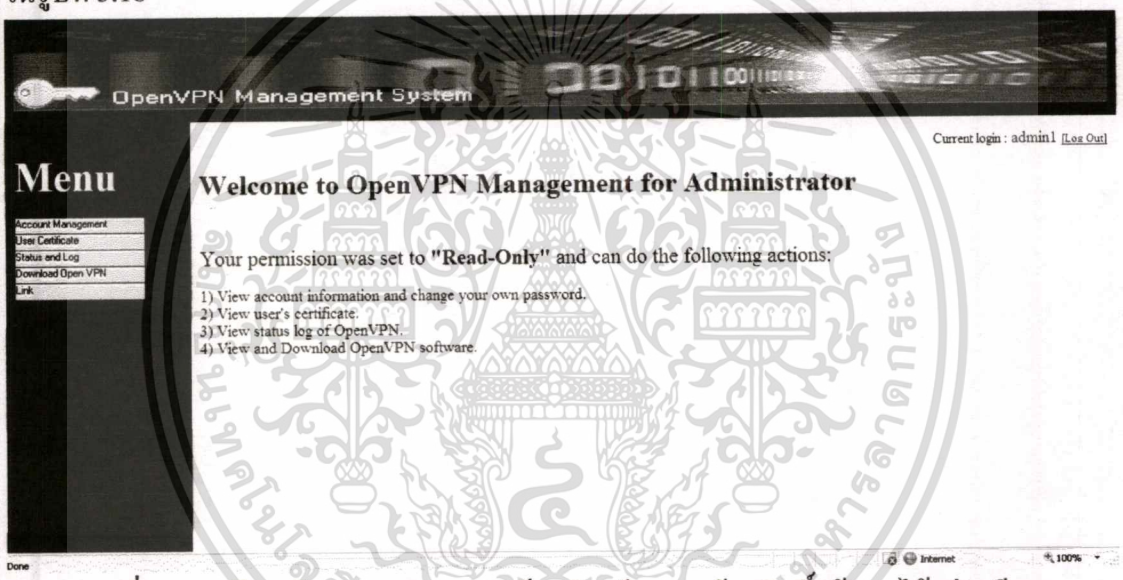
รูปที่ 5.17 หน้าจอการจัดการไฟล์ซอฟต์แวร์สำหรับดาวน์โหลดสำหรับสิทธิ์สูงสุด

หากต้องเข้าไปยังเว็บไซต์ของ OpenVPN สามารถเข้าไปจากเมนู Link แล้ว OpenVPN Help

5.2 การออกแบบส่วนติดต่อกับผู้ดูแลระบบที่มีสิทธิ์ดูข้อมูลได้อย่างเดียว (Read-Only)

หน้าจอสำหรับจัดการข้อมูลต่าง ๆ ของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ในส่วนนี้จะมีฟังก์ชันการใช้งานน้อยกว่าแบบ Full-Control ซึ่งจะดูข้อมูลได้อย่างเดียว ได้แก่ การดูข้อมูลของผู้ดูแลระบบ การดูใบรับรองดิจิตอลของผู้ใช้งาน การดูการให้บริการดาวน์โหลดซอฟต์แวร์ การดูสถานะและล็อกของ OpenVPN โดยมีหน้าจอหลักของระบบ ดังต่อไปนี้

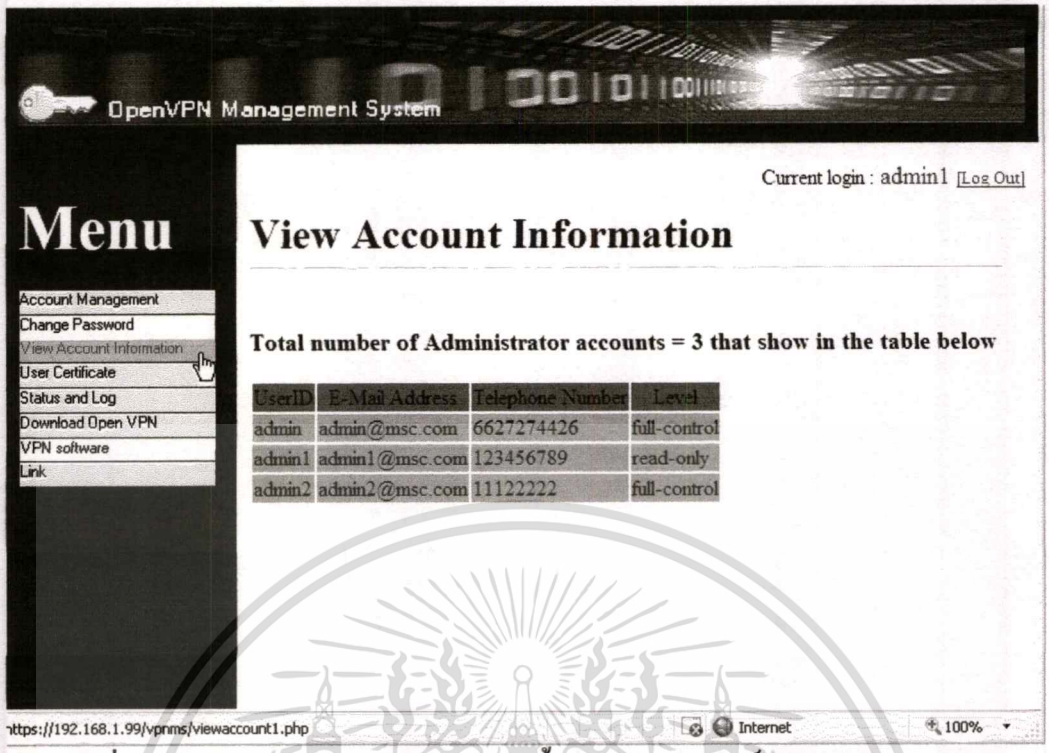
หน้าจอต้อนรับสำหรับผู้ดูแลระบบที่มีสิทธิ์ดูข้อมูลได้อย่างเดียวหลังจากล็อกอิน ดังแสดงในรูปที่ 5.18



รูปที่ 5.18 หน้าจอต้อนรับหลังจากการล็อกอินเข้าระบบด้วยสิทธิ์ดูข้อมูลได้อย่างเดียว

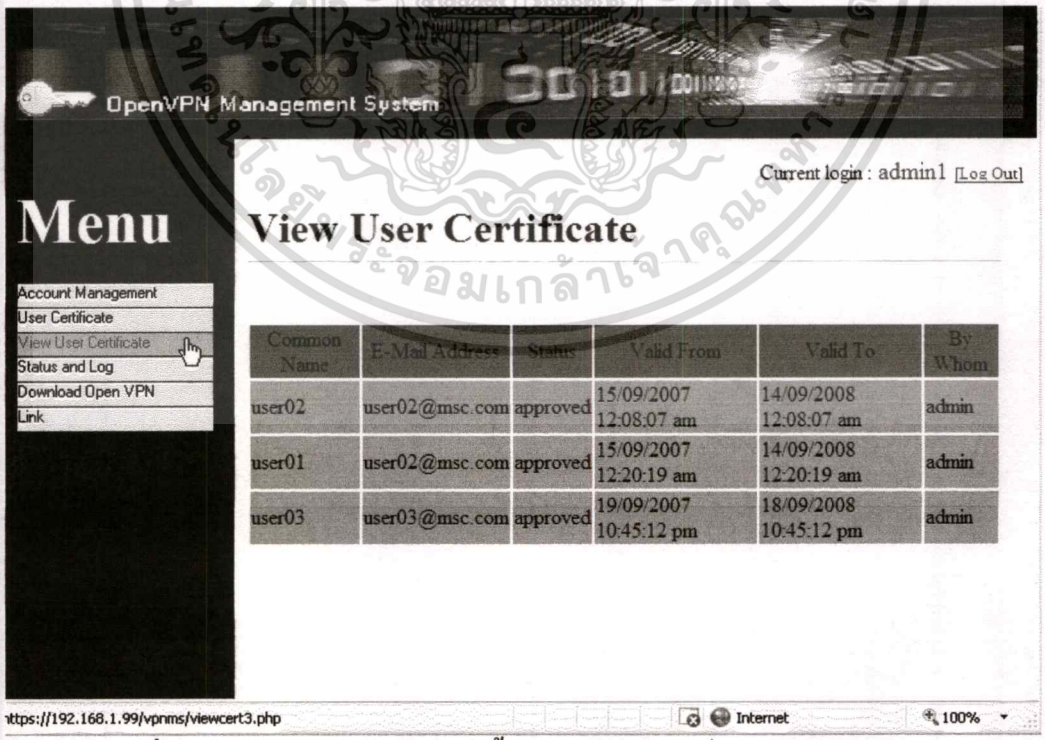
สามารถเปลี่ยนรหัสผ่านของตนเองเหมือนกับผู้ดูแลระบบแบบสิทธิ์สูงสุด

เมื่อต้องการดูข้อมูลว่ามีผู้ดูแลระบบทั้งหมดมีกี่คนและมีใครบ้าง สามารถทำได้โดยเข้าไปที่เมนู Account Management จากนั้นเลือก View Account Information สามารถ ดังแสดงในรูปที่ 5.19



รูปที่ 5.19หน้าจอดูข้อมูลของผู้ดูแลระบบทั้งหมดสำหรับสิทธิ์ดูข้อมูลได้อย่างเดียว

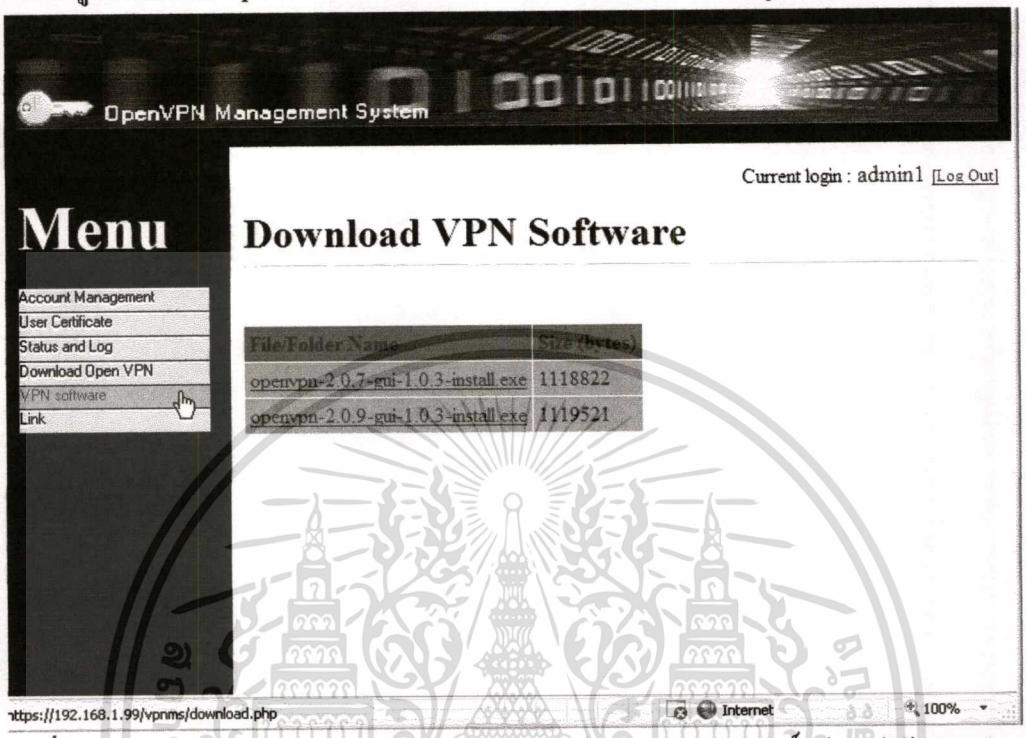
เมื่อต้องการดูรายละเอียดของใบรับรองทั้งหมดที่มีอยู่ สามารถทำได้โดยเข้าไปที่เมนู User Certificate จากนั้นเลือก View User Certificate ดังแสดงในรูปที่ 5.20



รูปที่ 5.20 หน้าจอการดูใบรับรองทั้งหมดสำหรับสิทธิ์ดูข้อมูลได้อย่างเดียว

สามารถดูสถานะและล็อกของ OpenVPN ได้เหมือนกับผู้ดูแลระบบแบบสิทธิ์สูงสุด

หากต้องการดูซอฟต์แวร์ OpenVPN เพื่อให้บริการดาวน์โหลด สามารถสามารถทำได้โดยเข้าไปที่เมนู Download OpenVPN แล้วเลือก VPN Software ดังแสดงในรูปที่ 5.21

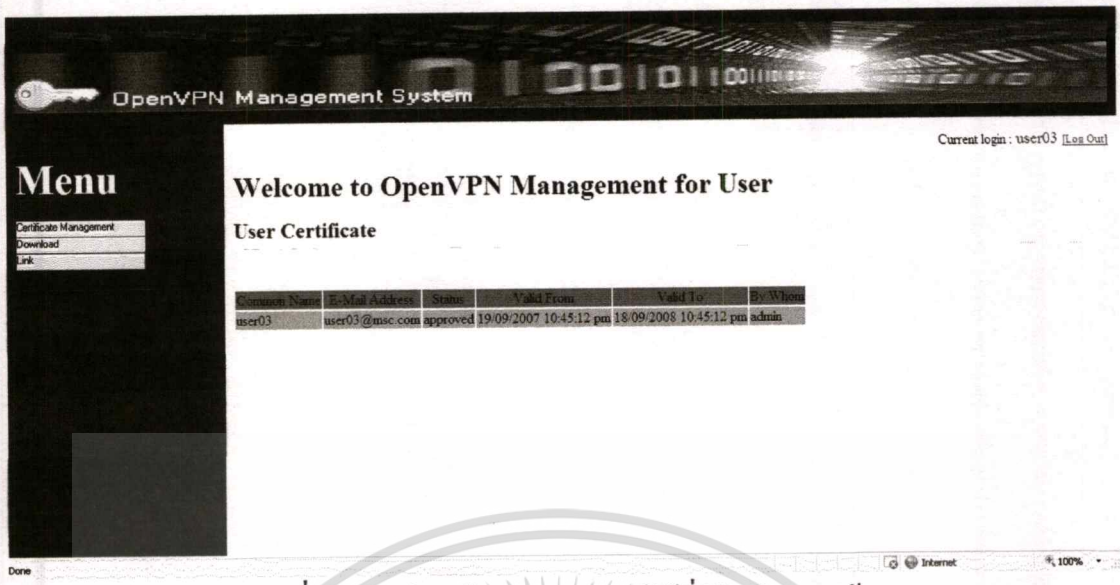


รูปที่ 5.21 หน้าจอการดูไฟล์ซอฟต์แวร์สำหรับดาวน์โหลดสำหรับสิทธิ์ดูข้อมูลได้อย่างเดียว

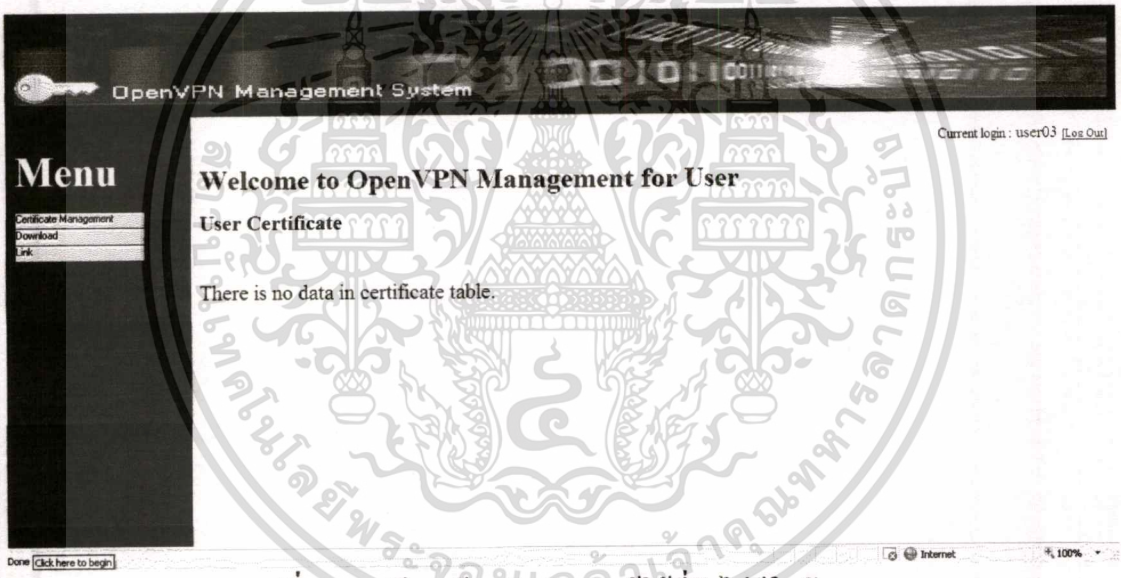
5.3 การออกแบบส่วนติดต่อกับผู้ใช้

หน้าจอสำหรับจัดการข้อมูลต่าง ๆ ของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ในส่วนนี้จะมีฟังก์ชันการใช้งานเฉพาะของผู้ใช้เท่านั้น ซึ่งได้แก่ การร้องขอและดูใบรับรองดิจิตอลของผู้ใช้งาน การดาวน์โหลดไฟล์ใบรับรองและไฟล์คอนฟิก การดาวน์โหลดซอฟต์แวร์ OpenVPN โดยมีหน้าจอหลักของระบบ ดังต่อไปนี้

การล็อกอินของผู้ใช้นั้นจะผ่านการพิสูจน์ตัวตนจาก Microsoft Active Directory โดยหน้าจอต้อนรับสำหรับหลังจากล็อกอิน ดังแสดงในรูปที่ 5.22 และ 5.23

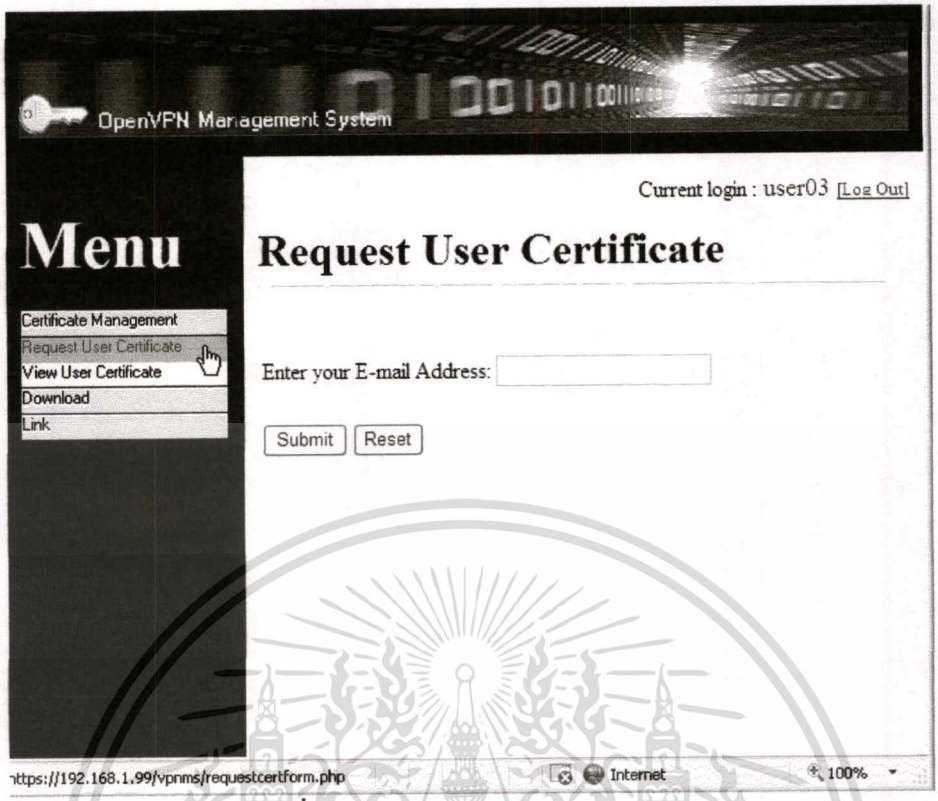


รูปที่ 5.22 หน้าจอต้อนรับสำหรับผู้ใช้ที่มีใบรับรองแล้ว

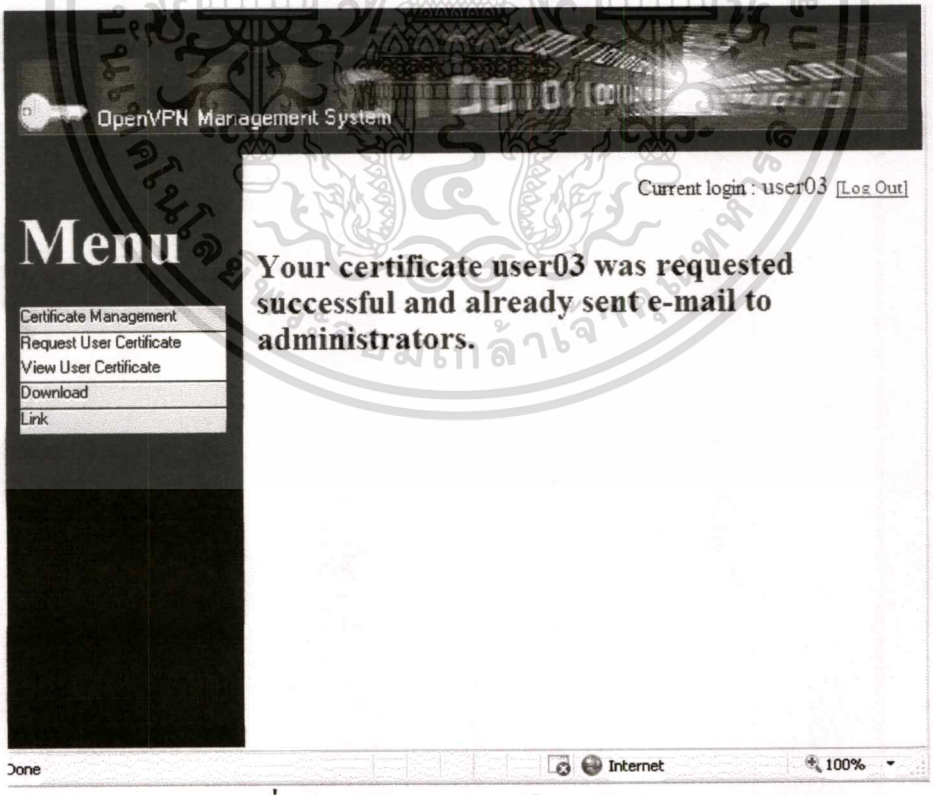


รูปที่ 5.23 หน้าจอต้อนรับสำหรับผู้ใช้ที่ยังไม่มีใบรับรอง

เมื่อเข้าสู่ระบบแล้วผู้ใช้ยังไม่มีใบรับรอง สามารถร้องขอไปได้โดยไปที่เมนู Certificate Management จากนั้นเลือก Request User Certificate แล้วใส่อีเมลล์ของตน ดังแสดงในรูปที่ 5.24 และ 5.25

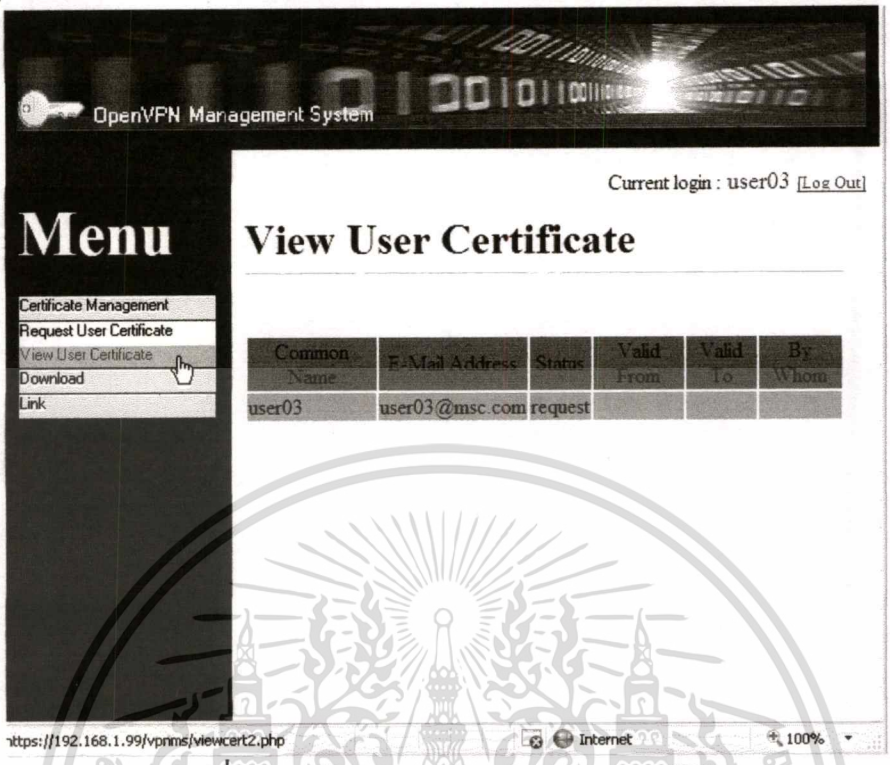


รูปที่ 5.24 หน้าจอการร้องขอใบรับรอง



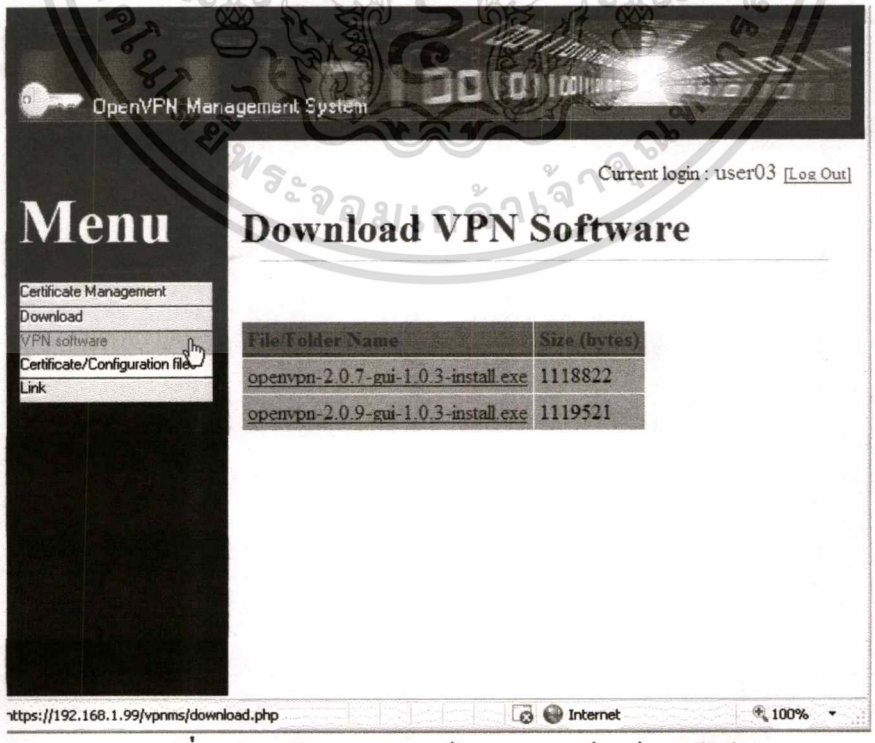
รูปที่ 5.25 หน้าจอหลังการร้องขอใบรับรอง

ผู้ใช้สามารถตรวจสอบสถานะของใบรับรองได้โดยไปที่เมนู ดังแสดงในรูปที่ 5.26



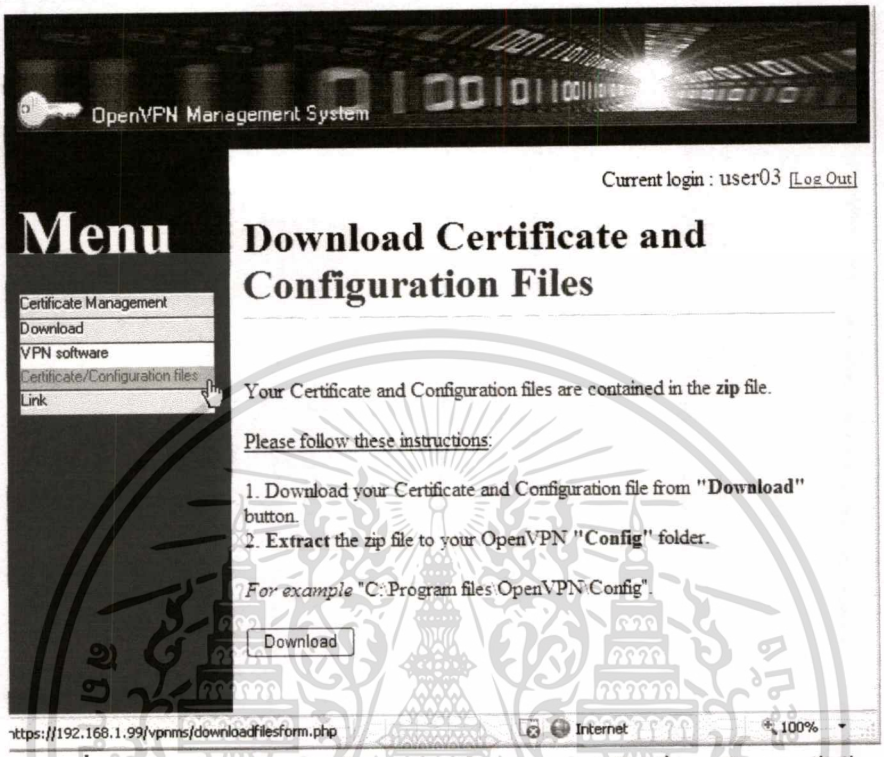
รูปที่ 5.26 หน้าจอการดูข้อมูลใบรับรองของผู้ใช้

ผู้ใช้สามารถเข้าไปดาวน์โหลดซอฟต์แวร์ OpenVPN เพื่อนำไปติดตั้งได้โดยไปที่เมนู Download แล้วเลือก VPN Software ดังแสดงในรูปที่ 5.27

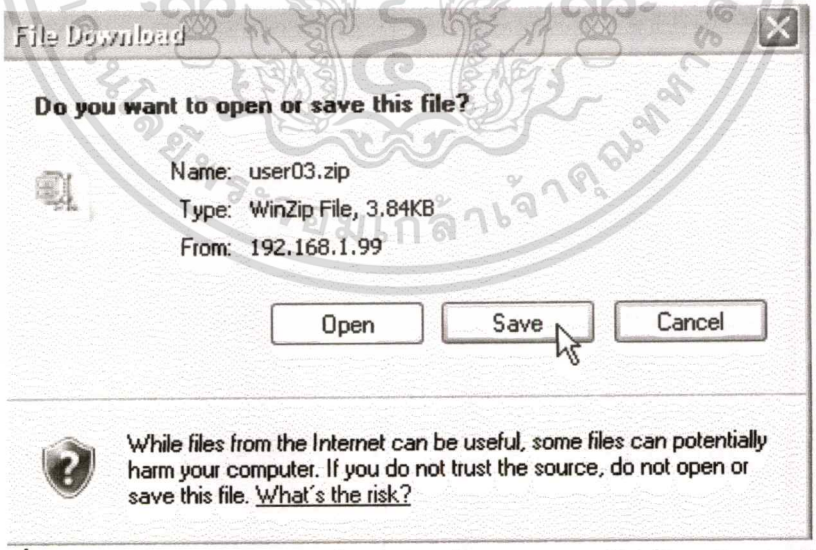


รูปที่ 5.27 หน้าจอการดาวน์โหลดซอฟต์แวร์ของผู้ใช้

ผู้ใช้สามารถเข้าไปดาวน์โหลดไฟล์ใบรับรองและไฟล์คอนฟิก เพื่อนำไปใช้งานได้โดยไปที่เมนู Download แล้วเลือก Certificate/ Configuration Files โดยการดาวน์โหลดจะเป็นไฟล์ซิปดังแสดงในรูปที่ 5.28 และ 5.29



รูปที่ 5.28 หน้าจอการดาวน์โหลดไฟล์ใบรับรองกับไฟล์คอนฟิกของผู้ใช้



รูปที่ 5.29 หน้าจอหลังการดาวน์โหลดไฟล์ใบรับรองกับไฟล์คอนฟิกของผู้ใช้

บทที่ 6
การพัฒนาระบบ

6.1 เครื่องมือที่ใช้ในการพัฒนาระบบ

- PHP, HTML, Java Script เป็นภาษาที่ใช้ในการพัฒนาโครงงาน
- ระบบปฏิบัติการ Red Hat Enterprise Linux เป็นระบบปฏิบัติการหลักที่ใช้ในการพัฒนาระบบ
- Apache Web Server ใช้เป็นเว็บเซิร์ฟเวอร์บนระบบปฏิบัติการ Red Hat Enterprise Linux
- MySQL ใช้เป็นฐานข้อมูลเชิงสัมพันธ์บนระบบปฏิบัติการ Red Hat Enterprise Linux
- PhpMyAdmin เป็นเว็บอินเทอร์เฟสในการจัดการฐานข้อมูล MySQL
- โปรแกรม OpenVPN ใช้เป็นวีพีเอ็นเซิร์ฟเวอร์บนระบบปฏิบัติการ Red Hat Enterprise Linux
- Microsoft Active Directory ใช้เพื่อให้บริการพิสูจน์ตัวตนผ่านไดเร็คทอรีเซอร์วิส
- โมดูล PHP ที่สนับสนุนการใช้งาน LDAP และ OpenSSL
- โปรแกรม Edit Plus เป็นเท็กซ์อิดิเตอร์ที่ใช้ในการเขียนโปรแกรม
- โปรแกรม Microsoft Word ใช้ในการเขียนเอกสารประกอบการพัฒนาโครงงาน
- โปรแกรม Microsoft Visio ใช้ในการออกแบบวาดภาพประกอบคำอธิบาย
- Microsoft Internet Explorer ใช้เป็นบราวเซอร์หลักในการทดสอบโครงงาน
- Lotus Notes/ Domino ใช้เป็นอีเมลล์เซิร์ฟเวอร์เพื่อใช้ทดสอบในการส่งอีเมลล์
- โปรแกรม VMWare ใช้ในการสร้างสภาพแวดล้อมการทำงานในการพัฒนาระบบ

6.2 การพัฒนาระบบ

6.2.1 สถาปัตยกรรมของระบบ

สถาปัตยกรรมของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บนั้น มีแนวทางการการอิมพลีเมนต์ระบบ โดยมีองค์ประกอบ ดังต่อไปนี้

6.2.1.1 รายละเอียดฮาร์ดแวร์ ซอฟต์แวร์ที่ใช้พัฒนาระบบ

สำหรับความต้องการด้านองค์ประกอบแต่ละส่วนทางฮาร์ดแวร์และซอฟต์แวร์ที่ใช้พัฒนาระบบนั้น มีรายละเอียดความต้องการตามตารางที่ 6.1

ตารางที่ 6.1 ความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์สำหรับเซิร์ฟเวอร์ OpenVPN

เครื่องคอมพิวเตอร์แม่ข่าย (OpenVPN Server/ WebServer) 1 เครื่อง	
หน่วยประมวลผล	มี Processor ที่มีประสิทธิภาพในการประมวลผลเทียบเท่าหรือดีกว่า Intel Pentium 4 ที่ Clock Speed ไม่น้อยกว่า 1.5 GHz
หน่วยความจำ	ขนาดไม่ต่ำกว่า 256 MB
ฮาร์ดดิสก์	ขนาดความจุไม่ต่ำกว่า 10 GB
Network Interface	มี 10/100 Ethernet Interface อย่างน้อย 2 ชุด
Port	1 Serial Port, 1 Parallel Port , 2 USB Port
อื่นๆ	ซีดีรอมไดร์ฟ จอภาพ คีย์บอร์ด เมาส์
ระบบปฏิบัติการ	Red Hat Enterprise Linux 4
ซอฟต์แวร์	- OpenVPN เวอร์ชัน 2.0.9 - Apache Web Server เวอร์ชัน 2.0.52 - MySQL เวอร์ชัน 4.1.12 - ตัวแปลภาษา PHP เวอร์ชัน 4.3.9 - OpenSSL เวอร์ชัน 0.9.7A - OpenLDAP เวอร์ชัน 20213

ตารางที่ 6.2 ความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์สำหรับเครื่องไคลเอนท์

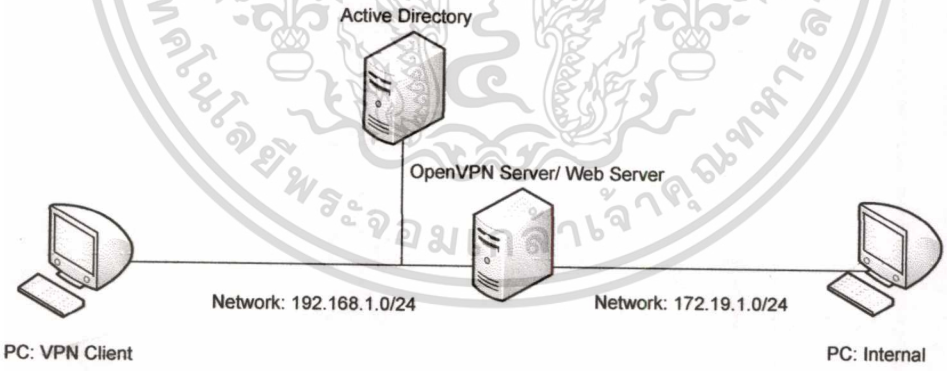
เครื่องคอมพิวเตอร์สำหรับผู้ใช้ (เครื่องไคลเอนท์) 1 เครื่อง	
หน่วยประมวลผล	มี Processor ที่มีประสิทธิภาพในการประมวลผลเทียบเท่าหรือดีกว่า Intel Pentium 4 ที่ Clock Speed ไม่น้อยกว่า 1.5 GHz
หน่วยความจำ	ขนาดไม่ต่ำกว่า 256 MB
ฮาร์ดดิสก์	ขนาดความจุไม่ต่ำกว่า 30 GB
Network Interface	มี 10/100 Ethernet Interface อย่างน้อย 1 ชุด
Port	1 Serial Port, 1 Parallel Port , 2 USB Port
อื่นๆ	มีชิ้นส่วนอุปกรณ์ที่สำคัญได้แก่ ซีดีรอมไดร์ฟ จอภาพ คีย์บอร์ด เมาส์
ระบบปฏิบัติการ	Windows XP Professional
ซอฟต์แวร์	Microsoft Internet Explorer เวอร์ชัน 6 ขึ้นไป

ตารางที่ 6.3 ความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์สำหรับเครื่อง Microsoft Active Directory

เครื่องคอมพิวเตอร์สำหรับเซิร์ฟเวอร์ (Microsoft Active Directory) 1 เครื่อง	
หน่วยประมวลผล	มี Processor ที่มีประสิทธิภาพในการประมวลผลเทียบเท่าหรือดีกว่า Intel Pentium 4 ที่ Clock Speed ไม่น้อยกว่า 1.5 GHz
หน่วยความจำ	ขนาดไม่ต่ำกว่า 512 MB
ฮาร์ดดิสก์	ขนาดความจุไม่ต่ำกว่า 30 GB
Network Interface	มี 10/100 Ethernet Interface อย่างน้อย 1 ชุด
Port	1 Serial Port, 1 Parallel Port , 2 USB Port
อื่นๆ	มีชิ้นส่วนอุปกรณ์ที่สำคัญได้แก่ ซีดีรอมไดร์ฟ จอภาพ คีย์บอร์ด เมาส์
ระบบปฏิบัติการ	Microsoft Windows Server 2003 Enterprise Edition
ซอฟต์แวร์	- Active Directory 2003 - เซอร์วิส DNS

6.2.1.2 สถาปัตยกรรมเครือข่ายของระบบ

การออกแบบสถาปัตยกรรมเครือข่ายของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บนั้น จากการวิเคราะห์การทำงานของระบบ พบว่าการทำงานจะเป็นงานที่เชื่อมต่อ ตามรูปที่ 6.1



รูปที่ 6.1 สถาปัตยกรรมเครือข่ายของระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

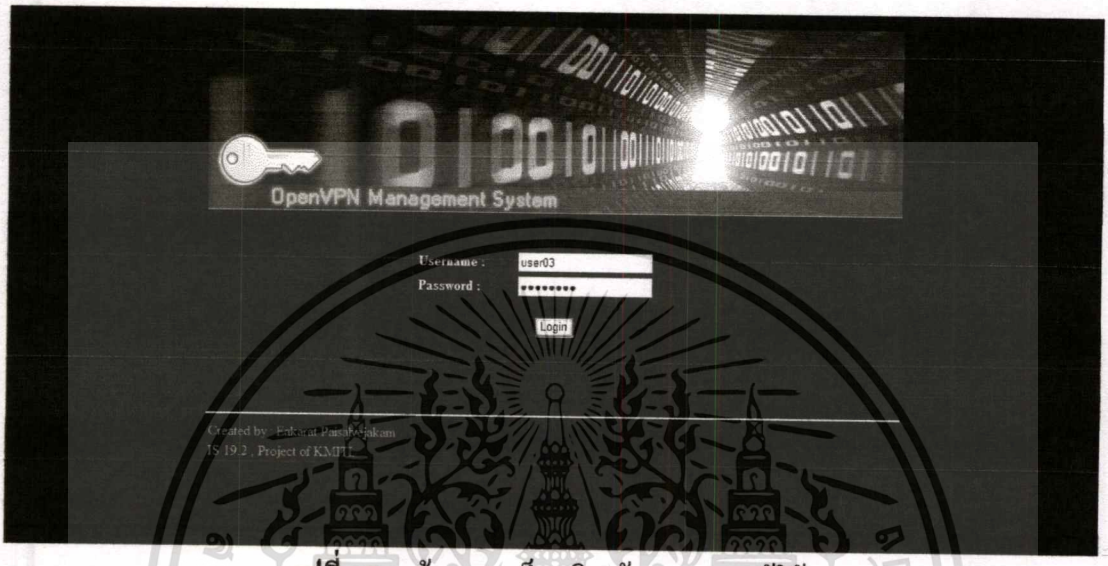
6.3 การทดสอบการใช้งานระบบ

ในส่วนของการทดสอบระบบนั้น จะทดสอบตามหัวข้อดังนี้

- การร้องขอและการอนุมัติหรือปฏิเสธการออกใบรับรองของผู้ใช้งาน
- การสร้างไฟล์คอนฟิกของผู้ใช้งาน
- การดาวน์โหลดซอฟต์แวร์ ใบรับรอง และไฟล์คอนฟิก ของผู้ใช้งาน

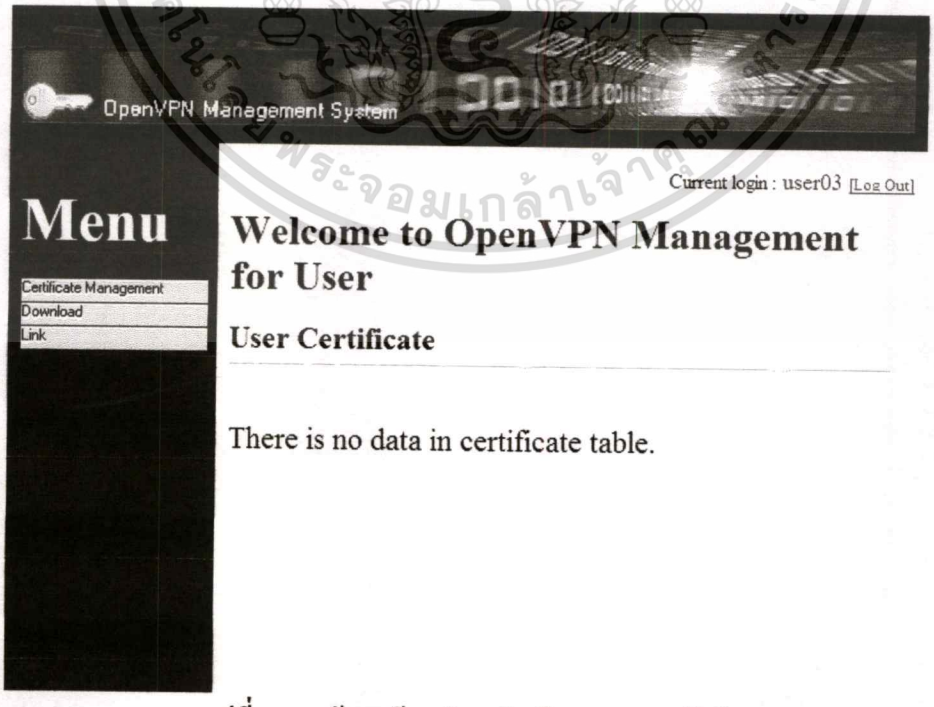
- การยกเลิกใบรับรองโดยผู้ดูแลระบบ

6.3.1 การทำงานจะเริ่มจากผู้ใช้ล็อกอินเข้าระบบโดยผ่านเว็บบราวเซอร์ไปยังระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ดังรูปที่ 6.2



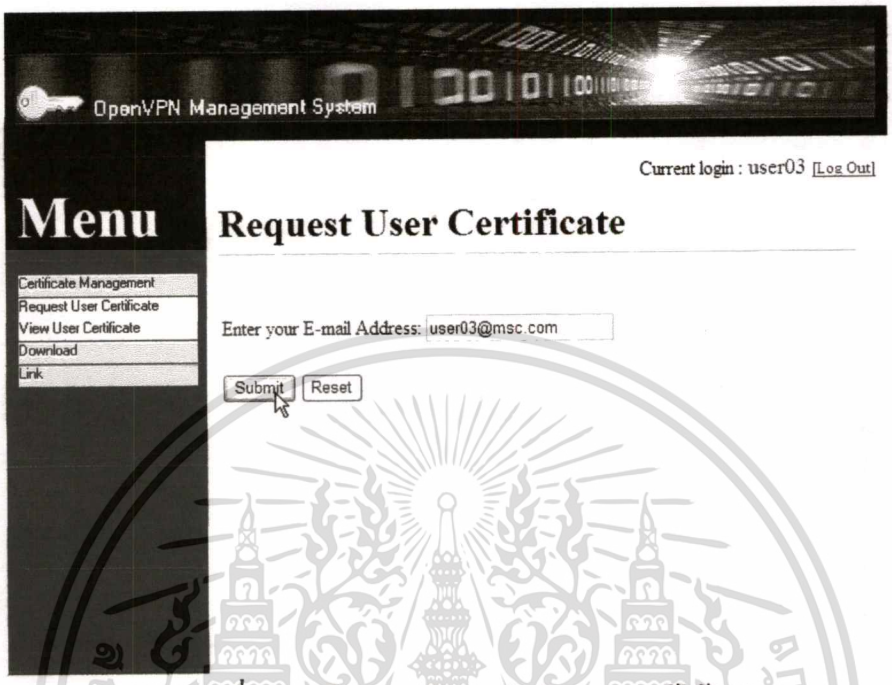
รูปที่ 6.2 หน้าจอการล็อกอินเข้าระบบของผู้ใช้

6.3.2 หลังจากที่ผู้ใช้งานล็อกอินเข้าระบบ ถ้าผู้ใช้ยังไม่มีการขอใบรับรองมาก่อนจะแสดง ดังรูปที่ 6.3



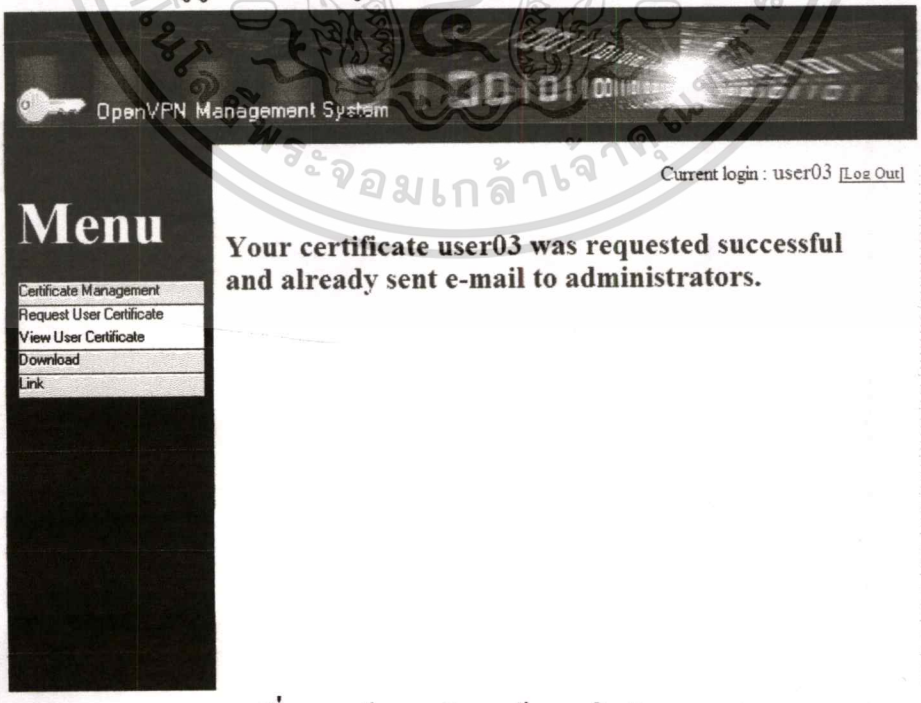
รูปที่ 6.3 หน้าจอต้อนรับหลังเข้าระบบของผู้ใช้

6.3.3 หลังจากนั้นผู้ใช้งานจะร้องขอใบรับรองโดยไปที่เมนู Request User Certificate แล้วใส่อีเมลล์ของผู้ใช้ลงไปแล้วกดปุ่ม Submit ดังรูปที่ 6.4

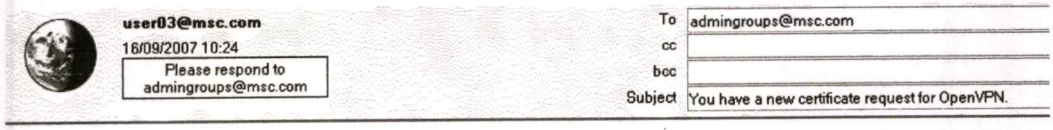


รูปที่ 6.4 หน้าจอการร้องขอใบรับรองของผู้ใช้

6.3.4 หลังจากนั้นระบบจะส่งการร้องขอโดยการไปอัพเดทสถานะในฐานข้อมูลและส่งเมลล์การร้องขอไปถึงผู้ดูแลระบบ ดังรูปที่ 6.5-6.6



รูปที่ 6.5 หน้าจอหลังจากร้องขอใบรับรอง



The user user03 request you to create user's certificate.
If you have any issues, please reply-to user03@msc.com

รูปที่ 6.6 หน้าจอข้อมูลการร้องขอใบรับรองผ่านอีเมลล์

6.3.5 หลังจากนั้นผู้ใช้สามารถดูสถานะของใบรับรองได้จากเมนู View User Certificate ดังรูปที่ 6.7

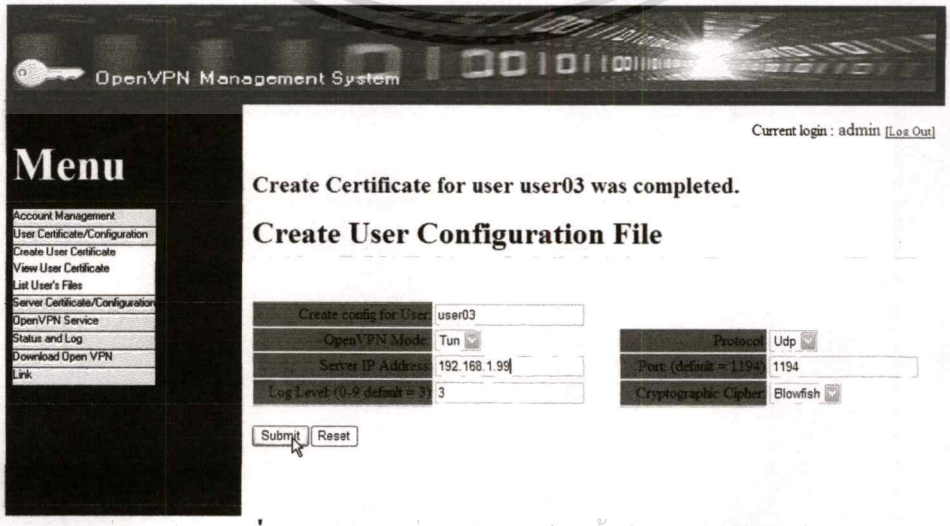
รูปที่ 6.7 หน้าจอการดูสถานะใบรับรองของผู้ใช้

6.3.6 หลังจากนั้นผู้ดูแลระบบสามารถอนุมัติหรือปฏิเสธใบรับรองได้จากเมนู Create User Certificate ซึ่งถ้าเป็นการอนุมัติจะต้องใส่จำนวนวันที่จะอนุมัติด้วยว่าจะให้ใบรับรองมีอายุกี่วัน ดังรูปที่ 6.8

รูปที่ 6.8 หน้าจอการอนุมัติใบรับรองของผู้ใช้

6.3.7 หลังจากที่ผู้ดูแลระบบอนุมัติใบรับรองแล้วก็จะเป็นการสร้างไฟล์คอนฟิกของผู้ใช้ ซึ่งมีรายละเอียด ดังรูปที่ 6.9

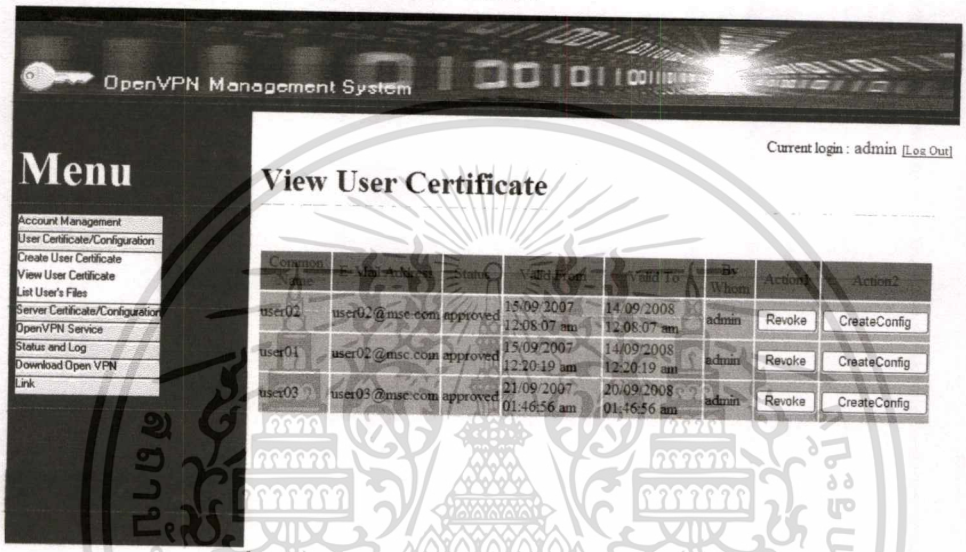
- OpenVPN Mode จะมีให้เลือก 2 แบบ คือ Tun (Routed Mode) และ Tap(Bridge Mode) ซึ่งในที่นี้จะใช้ Tun
- Protocol จะมีให้เลือก 2 แบบคือ UDP และ TCP ซึ่งในที่นี้จะใช้ UDP
- Server IP Address เป็นการระบุเซิร์ฟเวอร์ของ OpenVPN
- Port เป็นการระบุพอร์ตของเซิร์ฟเวอร์ OpenVPN ที่จะติดต่อด้วย
- Log Level เป็นการกำหนดระดับในการเก็บล็อกมีให้เลือกตั้งแต่ 0 – 9
- Cryptography Cipher เป็นการกำหนดอัลกอริทึมในการเข้ารหัสซึ่งต้องเหมือนกันทั้งฝั่งเซิร์ฟเวอร์และไคลเอนท์ มีให้เลือกคือ Blowfish, AES, 3DES



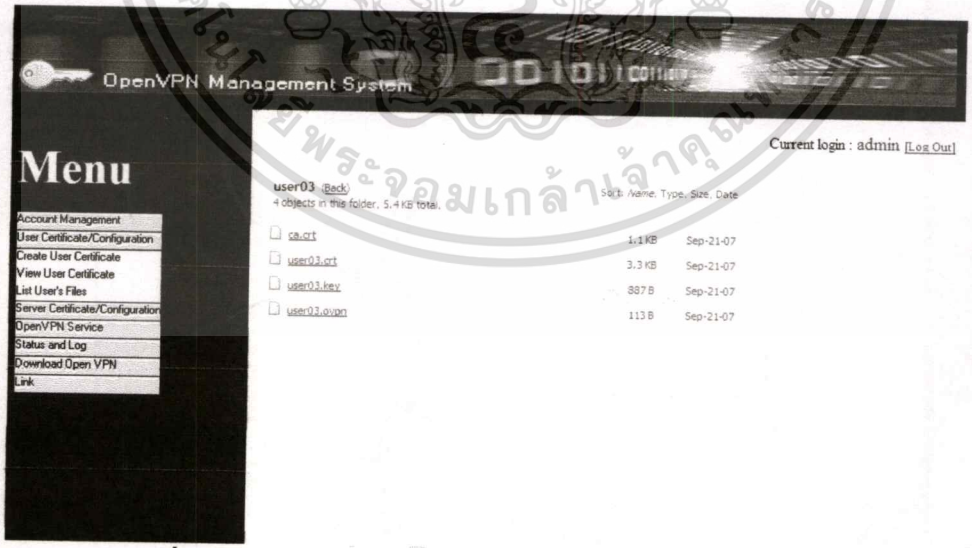
รูปที่ 6.9 หน้าจอการสร้างไฟล์คอนฟิกของผู้ใช้

6.3.8 หลังจากที่ผู้ดูแลระบบสร้างใบรับรองและไฟล์คอนฟิกเรียบร้อยแล้วสามารถดูได้จากเมนู View User Certificate ซึ่งจะบอกสถานะ วันหมดเริ่มต้น วันหมดอายุของใบรับรอง และ List User's Files ซึ่งมีรายละเอียด ดังรูปที่ 6.10-6.11

- Ca.crt คือไฟล์ใบรับรองของ RootCA
- User03.crt คือไฟล์ใบรับรองของ User03
- User03.key คือไฟล์กุญแจส่วนตัวของ User03
- User03.ovpn คือไฟล์คอนฟิกของ User03



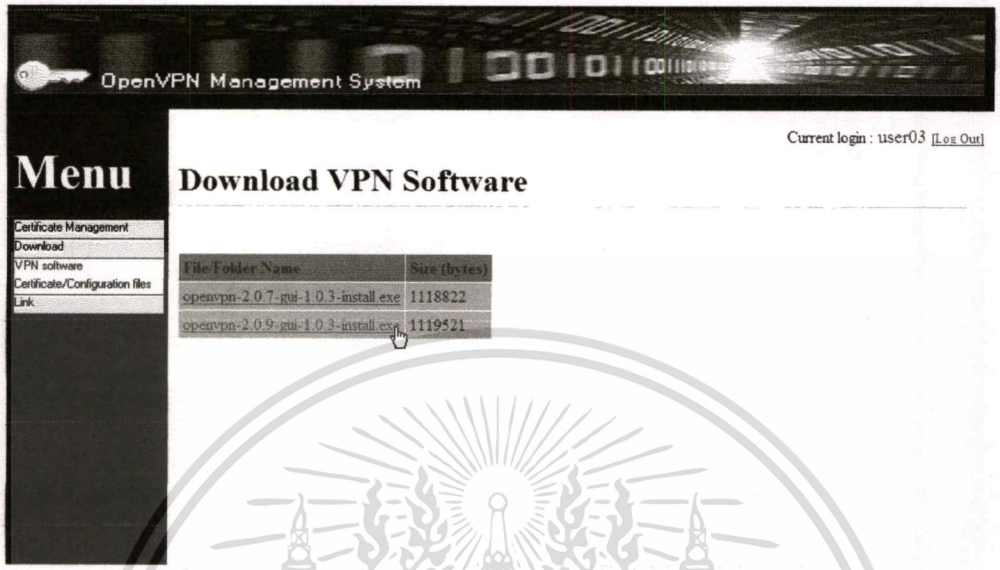
รูปที่ 6.10 หน้าจอการดูใบรับรองทั้งหมดของผู้ใช้



รูปที่ 6.11 หน้าจอการดูไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้

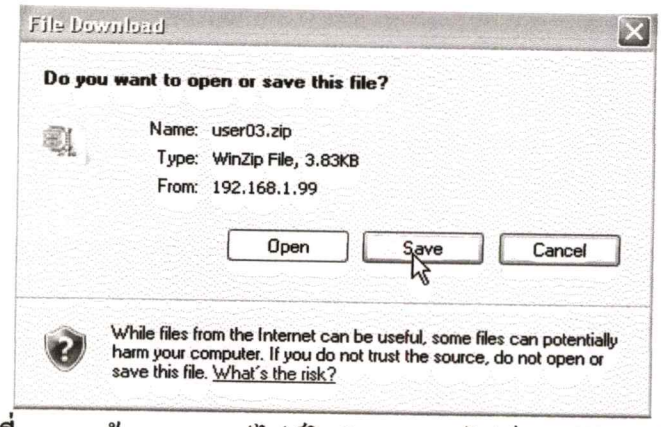
6.3.9 จากนั้นผู้ใช้งานล็อกอินเข้าระบบอีกครั้ง ถ้าต้องการดาวน์โหลดซอฟต์แวร์ OpenVPN ก็ให้เลือกเมนู Download-> VPNSoftware แต่ถ้าต้องการดาวน์โหลดไฟล์ใบรับรองและไฟล์คอน

ฟิกให้ไปที่เมนู Download-> Certificate/ Configuration files แล้วกด Download ซึ่งจะเป็นไฟล์ซิป โดยผู้ใช้งานต้องนำไป extract ไว้ที่โฟลเดอร์ config ของโปรแกรม OpenVPN ดังรูปที่ 6.12-6.15

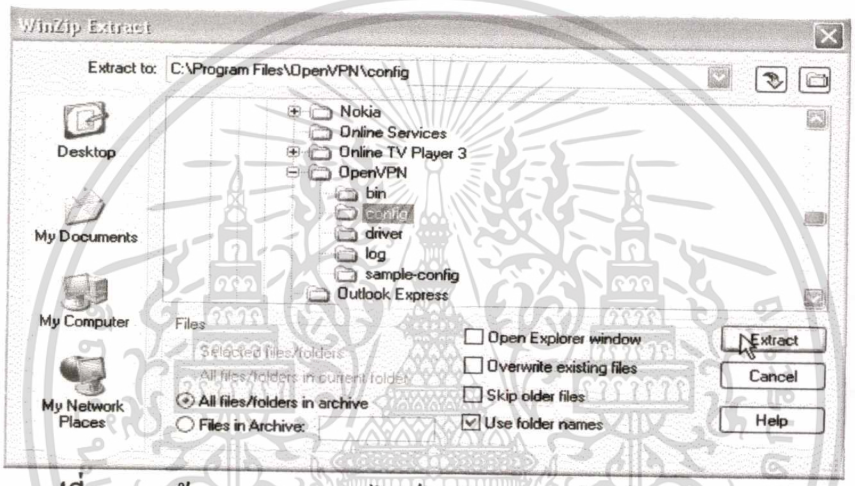


รูปที่ 6.12 หน้าจอการดาวน์โหลดซอฟต์แวร์ OpenVPN ของผู้ใช้

รูปที่ 6.13 หน้าจอการดาวน์โหลดไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้

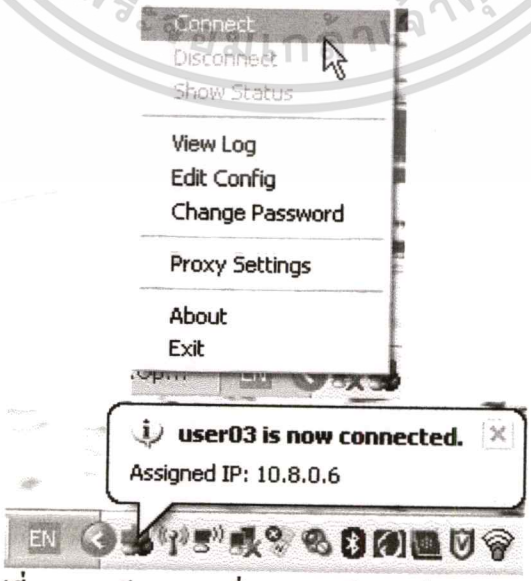


รูปที่ 6.14 หน้าจอการเซฟไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้



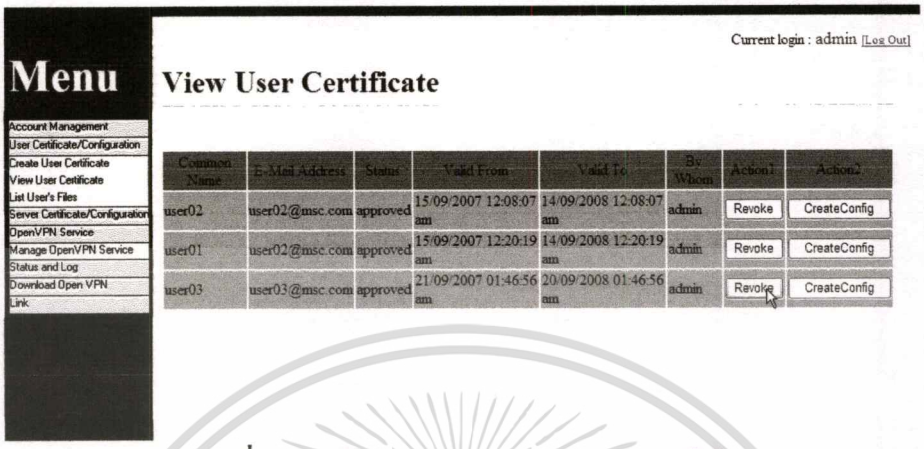
รูปที่ 6.15 หน้าจอการ extract ไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้

6.3.10 จากนั้นผู้ใช้งานเลือก Connect ที่ไอคอน OpenVPN บน task bar ก็จะสามารถติดต่อกับเซิร์ฟเวอร์ OpenVPN ได้ ดังรูปที่ 6.16



รูปที่ 6.16 หน้าจอการเชื่อมต่อเซิร์ฟเวอร์ OpenVPN

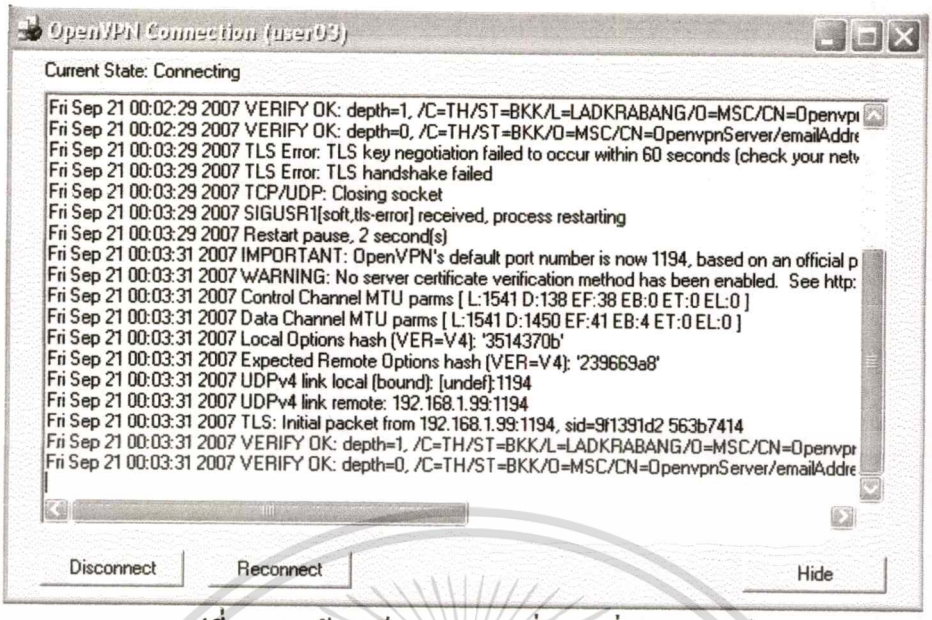
6.3.11 ถ้าผู้ดูแลระบบต้องการยกเลิกใบรับรองของผู้ใช้สามารถทำได้โดยไปที่เมนู View User Certificate แล้วกดปุ่ม Revoke ที่ผู้ใช้ที่ต้องการยกเลิกใบรับรอง ดังรูปที่ 6.17



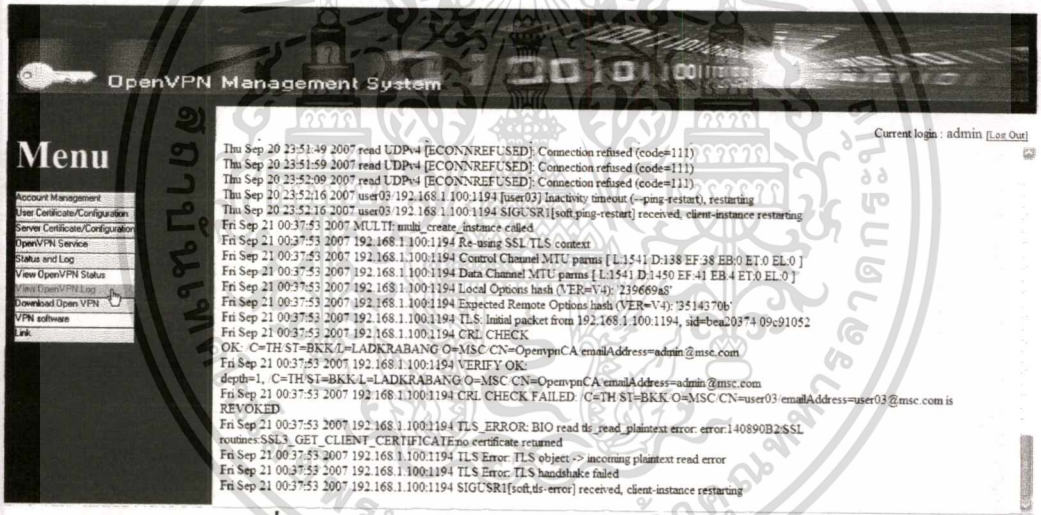
รูปที่ 6.17 หน้าจอการยกเลิกใบรับรองของผู้ใช้

6.3.12 หลังจากที่ใบรับรองถูกยกเลิกแล้ว ผู้ใช้จะไม่สามารถติดต่อเซิร์ฟเวอร์ Open VPN ได้อีก ดังรูปที่ 6.17-6.19

รูปที่ 6.18 หน้าจอหลังการยกเลิกใบรับรองของผู้ใช้



รูปที่ 6.19 หน้าจอล็อกของการเชื่อมต่อฝั่งไคลเอนท์



รูปที่ 6.20 หน้าจอล็อกของการเชื่อมต่อฝั่งเซิร์ฟเวอร์

บทที่ 7
บทสรุปและข้อเสนอแนะ

7.1 สรุปโครงการ

ในโครงการนี้ได้ดำเนินการศึกษาข้อมูล ทฤษฎี และมาตรฐานเทคโนโลยีที่เกี่ยวกับการสร้างเครือข่ายเสมือนส่วนตัว รวมถึงการการพัฒนาโปรแกรมการจัดการเครือข่ายเสมือนส่วนตัวผ่านเว็บ และเทคโนโลยีที่เกี่ยวข้อง เช่น และการพัฒนาโปรแกรมด้วยภาษา PHP, Java Script และ HTML โดยนำความรู้ที่ได้มาออกแบบและพัฒนาโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ โดยในระหว่างขั้นตอนการวิเคราะห์และออกแบบโปรแกรมก็ได้ทำการศึกษาเกี่ยวกับ UML เพื่อออกแบบระบบให้ถูกต้อง และได้นำทฤษฎีแนวคิดเทคโนโยลีต่าง ๆ ที่เกี่ยวข้องมาพัฒนาเป็นระบบ เพื่อให้ได้ระบบที่สามารถใช้จัดการเซิร์ฟเวอร์ OpenVPN ได้จริง ซึ่งถือว่าเป็นระบบที่ก่อเกิดความสะดวกและรวดเร็วกับผู้ใช้งานมากขึ้น ตอบสนองต่อการใช้งานของยุคปัจจุบัน

จากการพัฒนาโครงการทำให้เข้าใจถึงหลักการทำงานของเครือข่ายเสมือนส่วนตัวว่ามีหลักการทำงานอย่างไร มีรูปแบบการใช้งานกี่ประเภท อีกทั้งยังได้เข้าใจถึงความสามารถของฟังก์ชันของโปรแกรมโอเพ่นวีพีเอ็น (OpenVPN) และการนำฟังก์ชันเหล่านี้มาใช้งานให้เกิดประโยชน์ในโครงงาน รวมถึงการพัฒนาในส่วนการบริหารจัดการเพื่อให้สามารถใช้งานได้ง่ายขึ้น ในการพัฒนาโครงงานนี้นั้น สามารถสรุปความสามารถได้ดังนี้

- สามารถเพิ่มหรือลบผู้ดูแลระบบได้
- สามารถพิสูจน์ตัวตนผู้ใช้งานผ่าน Microsoft Active Directory ได้
- ผู้ดูแลสามารถเปลี่ยนรหัสผ่านของตนเองได้
- ผู้ดูแลสามารถดูข้อมูลของผู้ดูแลระบบทั้งหมดได้
- ผู้ใช้สามารถร้องขอใบรับรองได้และจะมีการแจ้งเตือนไปหาผู้ดูแลระบบผ่านทางอีเมลล์
- ผู้ดูแลระบบสามารถอนุมัติแล้วสร้างใบรับรองของผู้ใช้ที่ร้องขอได้
- ผู้ดูแลระบบสามารถปฏิเสธสร้างใบรับรองของผู้ใช้ที่ร้องขอได้
- ผู้ดูแลระบบสามารถดูข้อมูลใบรับรองของผู้ใช้ได้
- ผู้ดูแลระบบสามารถยกเลิกใบรับรองของผู้ใช้ได้
- ผู้ใช้สามารถดูข้อมูลใบรับรองของตนเองได้
- ผู้ดูแลระบบสามารถสร้างไฟล์คอนฟิกของผู้ใช้และของเซิร์ฟเวอร์ได้
- ผู้ดูแลระบบสามารถสร้างใบรับรองของ RootCA และของเซิร์ฟเวอร์ได้

- ผู้ดูแลระบบสามารถรีสตาร์ทเซอร์วิสของ OpenVPN ได้
- ผู้ดูแลระบบสามารถดูสถานะและล็อกของ OpenVPN ได้
- ผู้ดูแลระบบสามารถจัดการซอฟต์แวร์ได้เช่นอัพโหลดและลบไฟล์
- ผู้ใช้สามารถดาวน์โหลดซอฟต์แวร์และไฟล์ใบรับรองและไฟล์คอนฟิกของตนเองได้

7.2 ข้อเสนอแนะในการพัฒนาต่อ

จากการทดสอบโปรแกรมพบว่าสามารถทำงานได้ตามฟังก์ชันที่ต้องการซึ่งเป็นความต้องการขั้นพื้นฐานในการจัดการเครือข่ายเสมือนส่วนตัว แต่อย่างไรก็ตามสามารถนำไปพัฒนาต่อเพื่อให้มีความสามารถมากกว่าเดิมได้โดยเพิ่มฟังก์ชันการจัดการที่ซับซ้อนมากขึ้นเช่น

1. เพิ่มฟังก์ชันการทำแชร์โหลด กล่าวคือผู้ใช้สามารถติดต่อเซิร์ฟเวอร์ OpenVPN ได้หลายตัวโดยมีการทำเรื่องของ Load Sharing
2. เพิ่มฟังก์ชันการทำงานการสร้างอุโมงค์โดยผ่าน Proxy
3. เพิ่มฟังก์ชันการพิสูจน์ตัวตนในการเชื่อมต่อ OpenVPN

บรรณานุกรม

ดร.บรรจง หะรังษี **ความรู้เบื้องต้นของการเข้ารหัสข้อมูล**

[Online].Available: http://www.thaicert.nectec.or.th/paper/encryption/intro_crypt.php

"OpenVPN". [Online]. Available: http://openvpn.net

ธีรภัทร มนตรีศาสตร์ OpenVPN เมื่อแอพลิเคชั่นจะตามคุณไปทุกที่

[Online].Available: http://www.itdestination.com/articles/openvpn/

อนรรฆนงค์ คุณมณี 2550. **Basic of PHP.** พิมพ์ครั้งที่ 1. นนทบุรี: ไอดีซีฯ.

Marcus Feilner. April 2006. **OpenVPN Building and Integrating Virtual Private Networks.**

Birmingham. : Packt Publishing.

ภาคผนวก ก

การติดตั้งระบบ

การติดตั้งเพื่อใช้งานระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัว นั้นจะมีรายละเอียดการติดตั้งดังนี้

1. การติดตั้งระบบโปรแกรม OpenVPN บนระบบปฏิบัติการ Red Hat Enterprise Linux 4

1.1 ดาวน์โหลดซอฟต์แวร์จาก http://openvpn.net/download.html โดยเลือกไฟล์ “openvpn-2.0.9.tar.gz”

1.2 จากนั้นให้สร้าง RPM โดยใช้คำสั่ง “rpmbuild -tb openvpn-2.0.9.tar.gz”

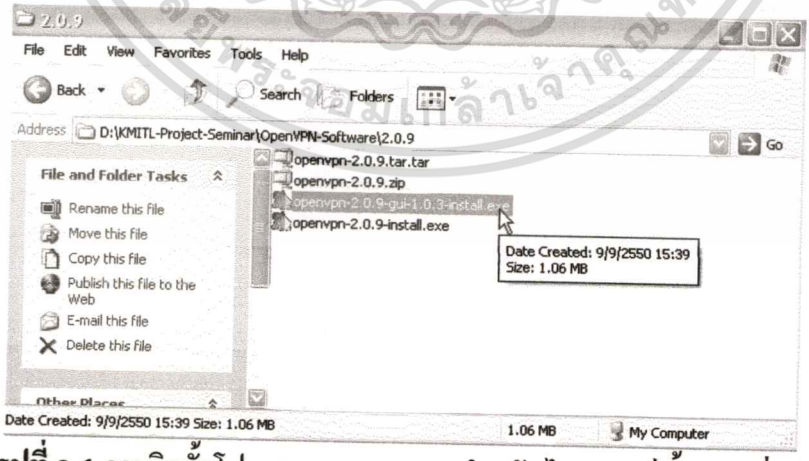
1.3 จากนั้นให้ติดตั้งโดยใช้คำสั่ง “rpm -ivh openvpn-2.0.9.rpm”

1.4 หลังจากติดตั้งเสร็จโปรแกรมจะอยู่ใน /usr/shar/doc/openvpn2.0.9 โดยให้ copy ไปที่ /etc/openvpn

1.5 หลังจากนั้นให้กำหนดให้เซอร์วิสของ OpenVPN สตาร์ทโดยอัตโนมัติหลังเซิร์ฟเวอร์สตาร์ท

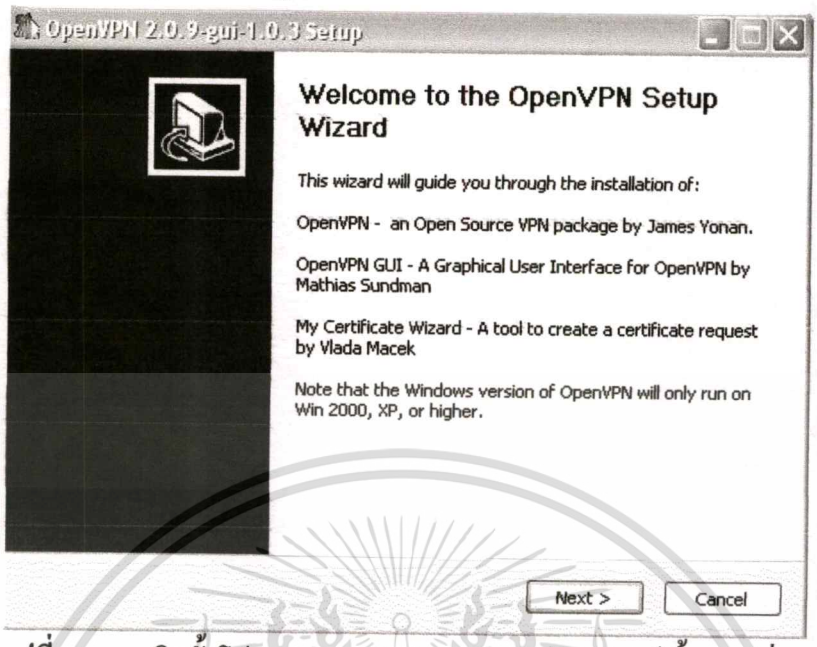
2. การติดตั้งระบบโปรแกรม OpenVPN สำหรับไคลเอนท์บนระบบปฏิบัติการ Windows

2.1 ดับเบิ้ลคลิ้กไฟล์ “Openvpn-2.0.9-gui-1.0.3-install.exe” ดังรูปที่ ก-1



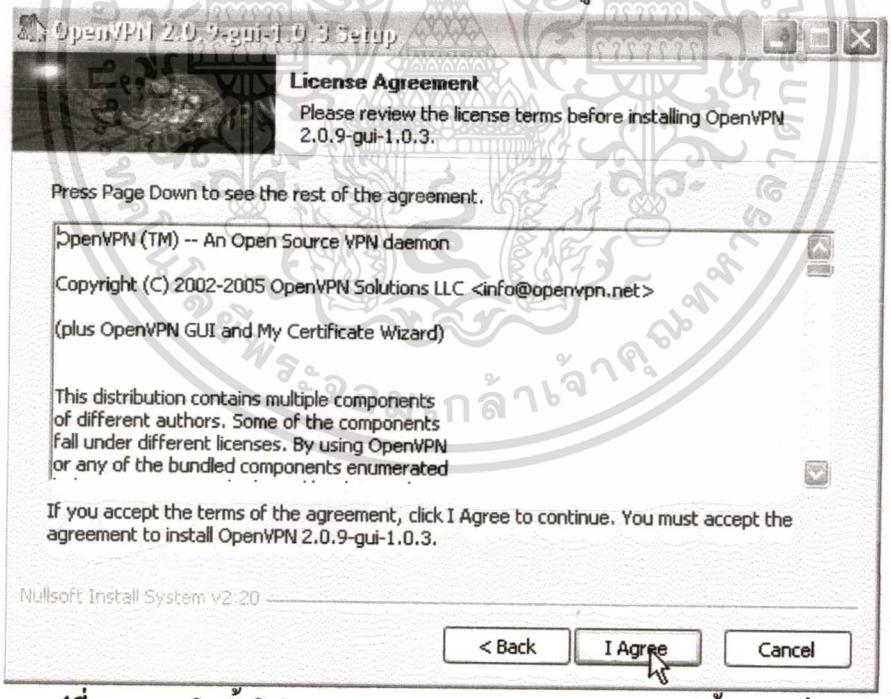
รูปที่ ก-1 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 1

2.2 จากนั้นให้กดปุ่ม Next ดังรูปที่ ก-2



รูปที่ ก-2 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 2

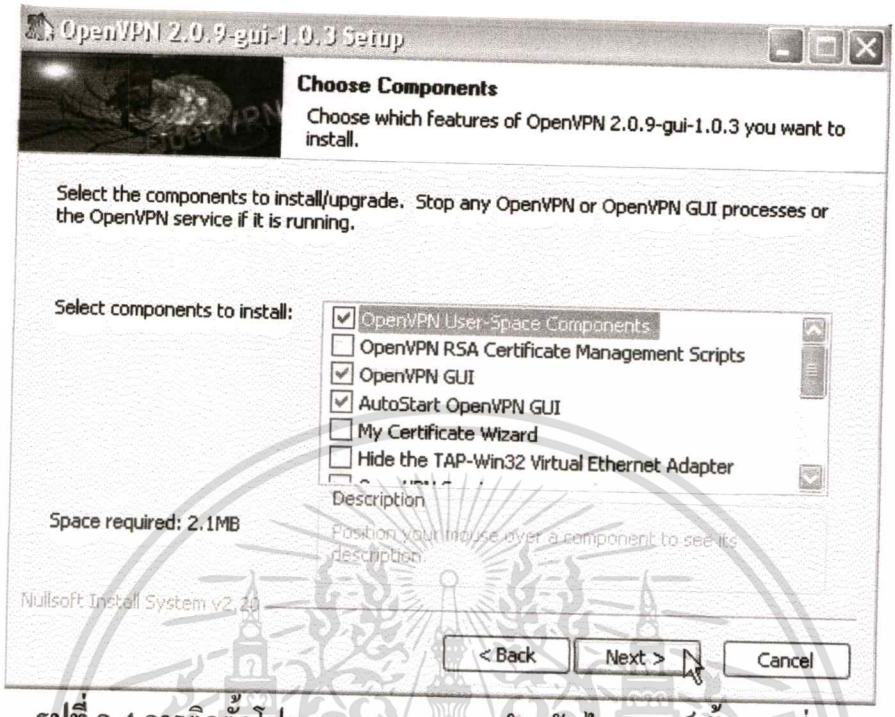
2.3 จากนั้นให้กดปุ่ม I Agree เพื่อยอมรับข้อตกลง ดังรูปที่ ก-3



รูปที่ ก-3 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 3

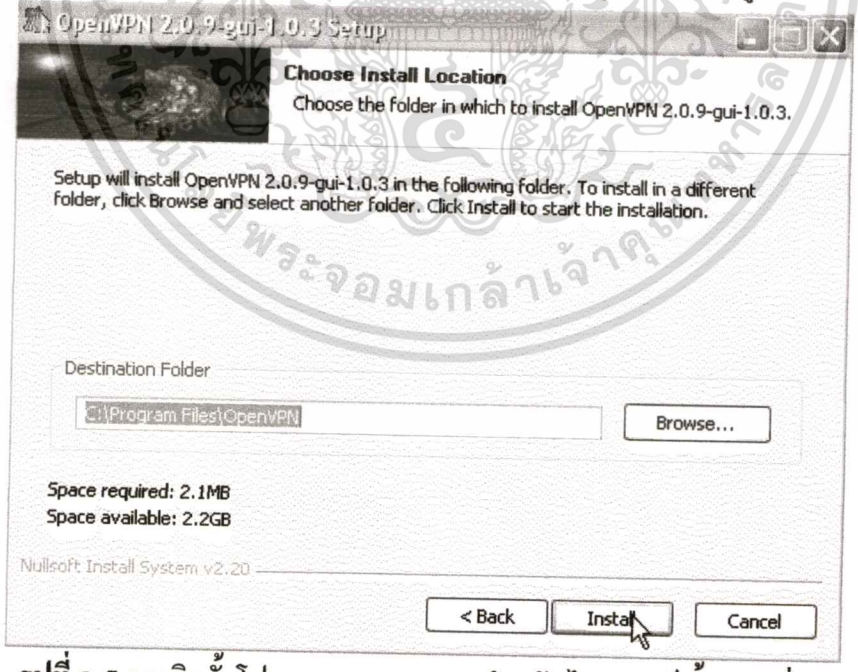
2.4 จากนั้นให้เลือกโมดูลที่จะลงได้แก่ "OpenVPN User-Space Component, OpenVPN GUI, AutoStart OpenVPN GUI, OpenVPN Fule Association, OpenSSL DLLs, OpenSSL

Utilities, TAP-Win32 Virtual Network Adapter, Add OpenVPN to Path, Add shotcut to start menu" ดังรูปที่ ก-4



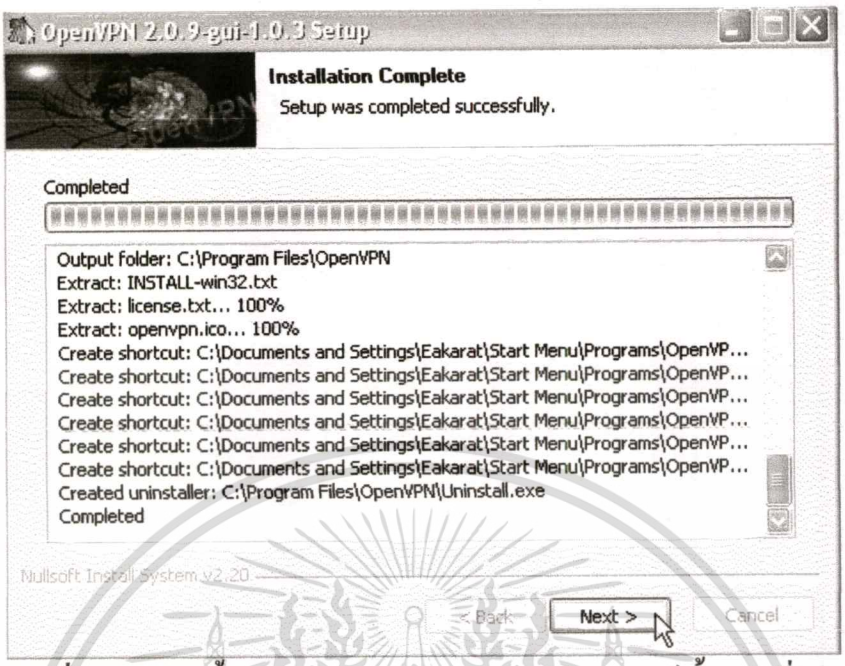
รูปที่ ก-4 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 4

2.5 จากนั้นให้เลือกว่าจะลงโปรแกรมที่ไหน จากนั้นกดปุ่ม Install ดังรูปที่ ก-5



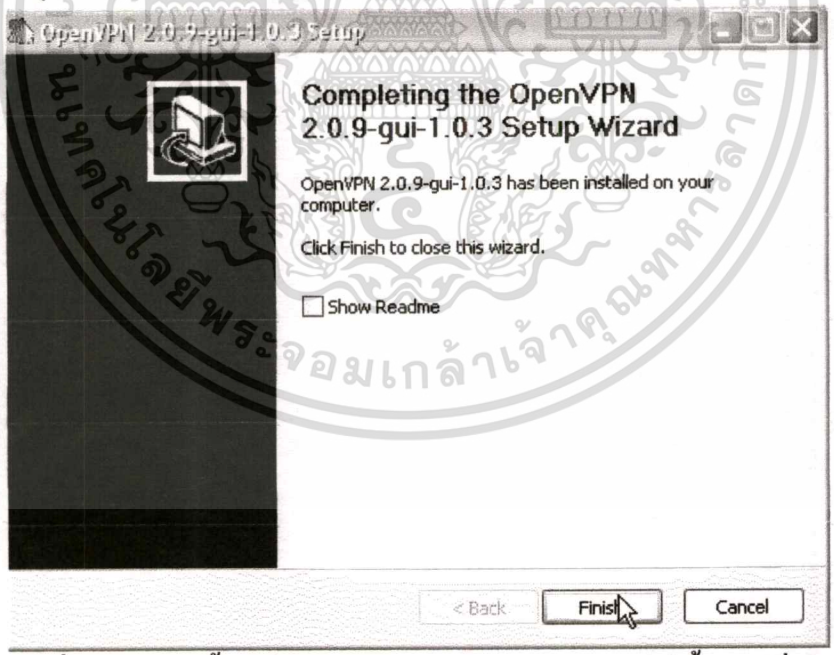
รูปที่ ก-5 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 5

2.6 จากนั้นรอจนกว่าจะติดตั้งเสร็จ แล้วกด Next ดังรูปที่ ก-6



รูปที่ ก-6 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 6

2.7 กดปุ่ม Finish เพื่อสิ้นสุดการติดตั้ง ดังรูปที่ ก-7



รูปที่ ก-7 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 7

2.8 ตรวจสอบที่ task bar จะมีไอคอนปรากฏ ดังรูปที่ ก-8

รูปที่ ก-8 การติดตั้งโปรแกรม OpenVPN สำหรับไคลเอนท์ ขั้นตอนที่ 8

3. การติดตั้งระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บบนระบบปฏิบัติการ Red Hat Enterprise Linux

3.1 หลังจากที่ติดตั้งเว็บเซิร์ฟเวอร์ Apache PHP MySQL และ PHPMyAdmin เรียบร้อยแล้ว ให้นำโปรแกรมระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ ไปเก็บไว้ที่ "/var/www/html/vpnms" ซึ่งจะเก็บ Source code ของโปรแกรมนี้ทั้งหมดไว้ ซึ่งจะมีรายละเอียดดังนี้

- /var/www/html/vpnms เป็นที่เก็บไฟล์ php ซึ่งเป็นโค้ดหลักของระบบนี้
- /var/www/html/vpnms/keys เป็นที่เก็บไฟล์ใบรับรองที่ใช้ในระบบ
- /var/www/html/vpnms/config เป็นที่เก็บไฟล์ใบรับรองและไฟล์คอนฟิกของผู้ใช้

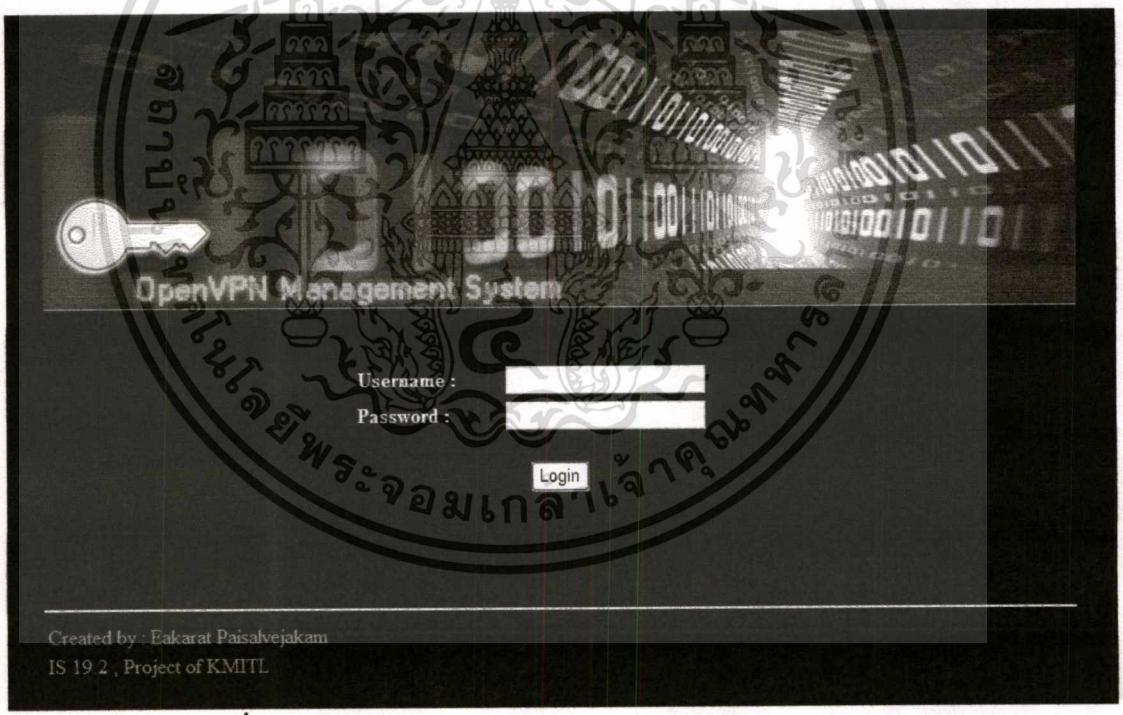
ภาคผนวก ข

คู่มือการใช้งานระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ

การใช้งานระบบดูแลและบริหารเครือข่ายเสมือนส่วนตัวผ่านเว็บ นั้นจะมีรายละเอียดการใช้งานดังนี้

1. การเข้าสู่ระบบ

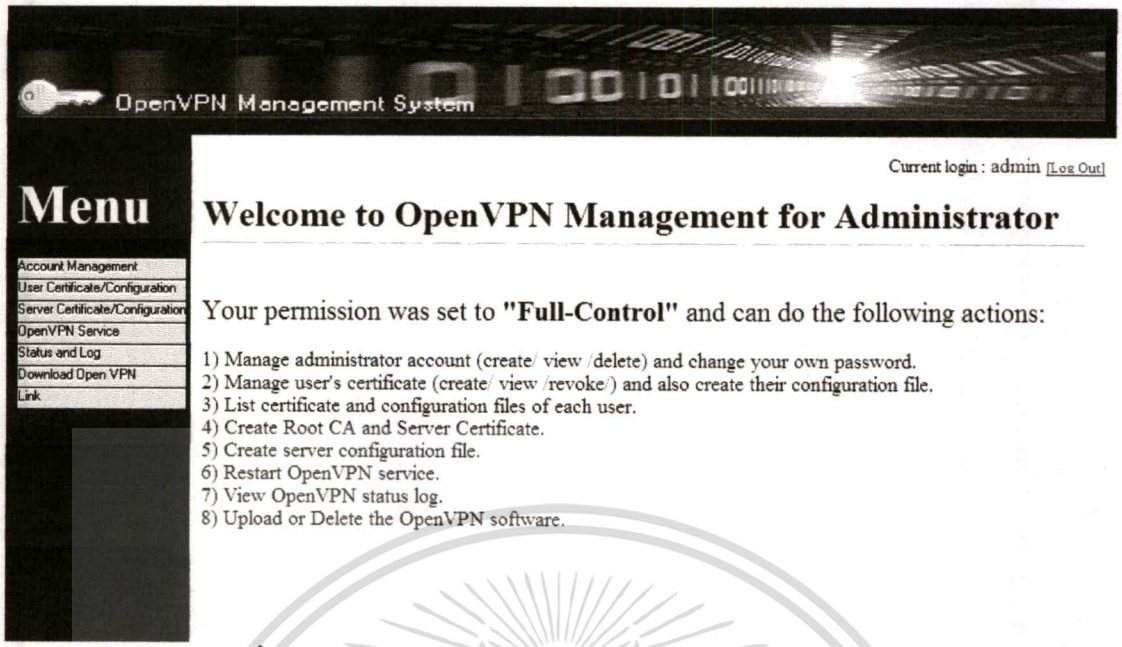
1.1 การล็อกอินเข้าสู่ระบบ เมื่อเริ่มต้นใช้งาน ระบบจะตรวจสอบสิทธิ์ในการใช้งาน ซึ่งผู้ใช้งานจะต้องใส่รหัสผู้ใช้งานและรหัสผ่านที่ถูกต้องและกดปุ่ม Login จึงจะสามารถเข้าใช้งานระบบได้โดยจะมีการแบ่งผู้ใช้ออกเป็น 3 ระดับคือ Admin (Full-Control) Admin(Read-Only) และ User



รูปที่ ข-1 หน้าจอตรวจสอบผู้ใช้งานก่อนเข้าใช้งานระบบ

2. ฟังก์ชันการใช้งานของ Admin (Full-Control)

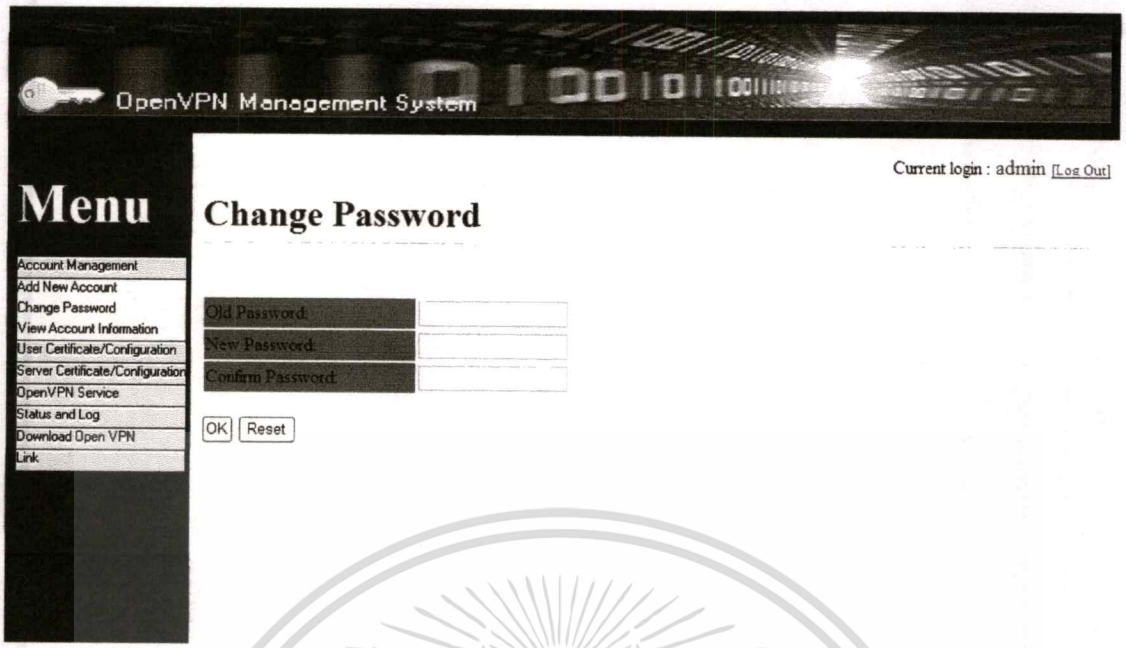
หลังจากที่ล็อกอินเข้าสู่ระบบแล้ว ในหน้าต้อนรับจะมีข้อความระบุว่าผู้ล็อกอินมีสิทธิ์ระดับไหนและมีสิทธิ์ทำอะไรได้บ้าง ดังรูปที่ ข-2



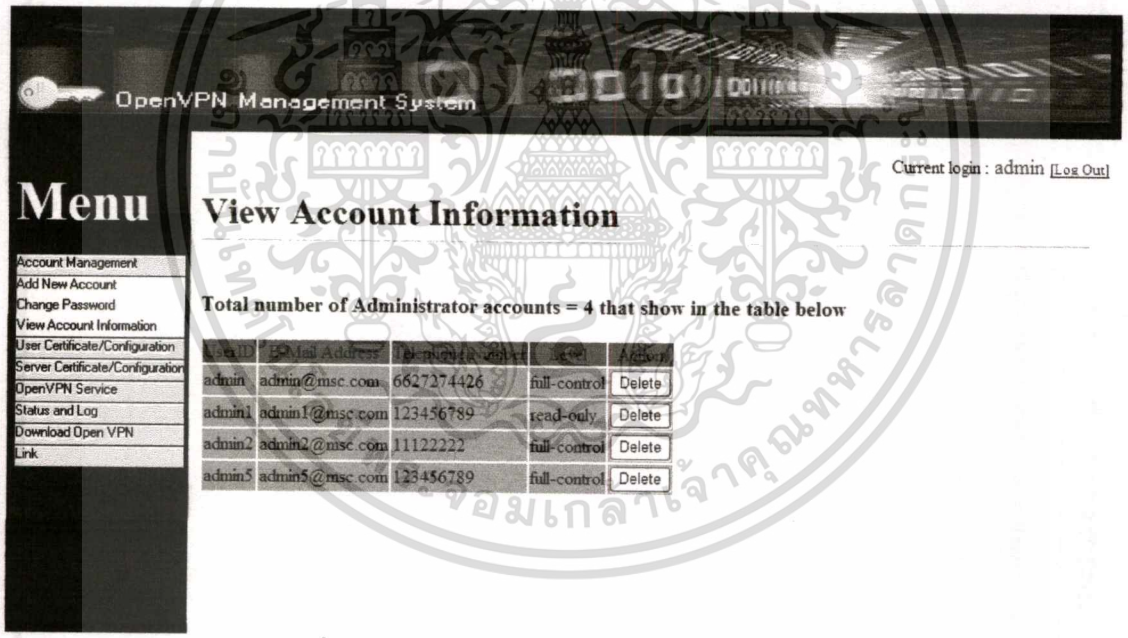
รูปที่ ข-2 หน้าจอแสดงหน้าต้อนรับของ Admin (Full-Control)

2.1 เมนู Account Management สำหรับสร้างผู้ดูแลระบบและการเปลี่ยนรหัสผ่าน ซึ่งประกอบด้วย ชื่อ รหัสผ่าน อีเมลล์ เบอร์โทรศัพท์และระดับของสิทธิ์ และในส่วนของการเปลี่ยนรหัสผ่านผู้ใช้งานต้องกรอกรหัสผ่านเดิมให้ถูกต้อง และกรอกรหัสผ่านใหม่ให้เหมือนกัน 2 ครั้งจึงจะสามารถเปลี่ยนรหัสผ่านใหม่ได้

รูปที่ ข-3 หน้าจอแสดง Add New Administrator Account



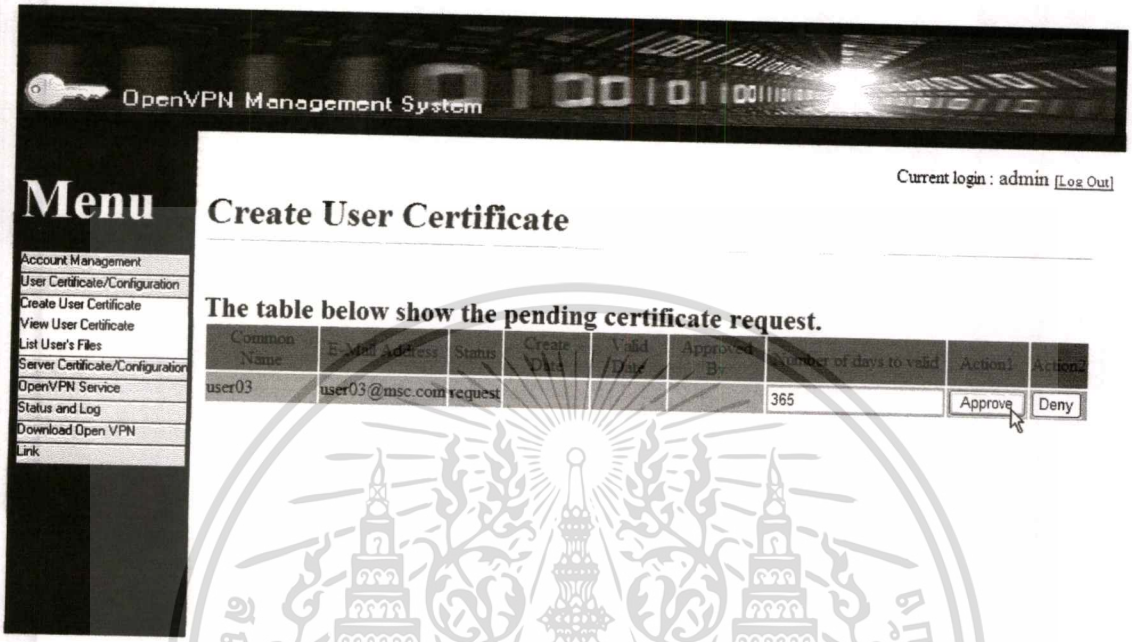
รูปที่ ข-4 หน้าจอแสดง Change Password



รูปที่ ข-5 หน้าจอแสดง View Account Information

2.2 เมนู User Certificate/ Configuration สำหรับอนุมัติและสร้างใบรับรองหรือปฏิเสธใบรับรอง การสร้างไฟล์คอนฟิกของผู้ใช้รวมถึงการเรียกดูไฟล์ของผู้ใช้ทั้งหมดด้วย

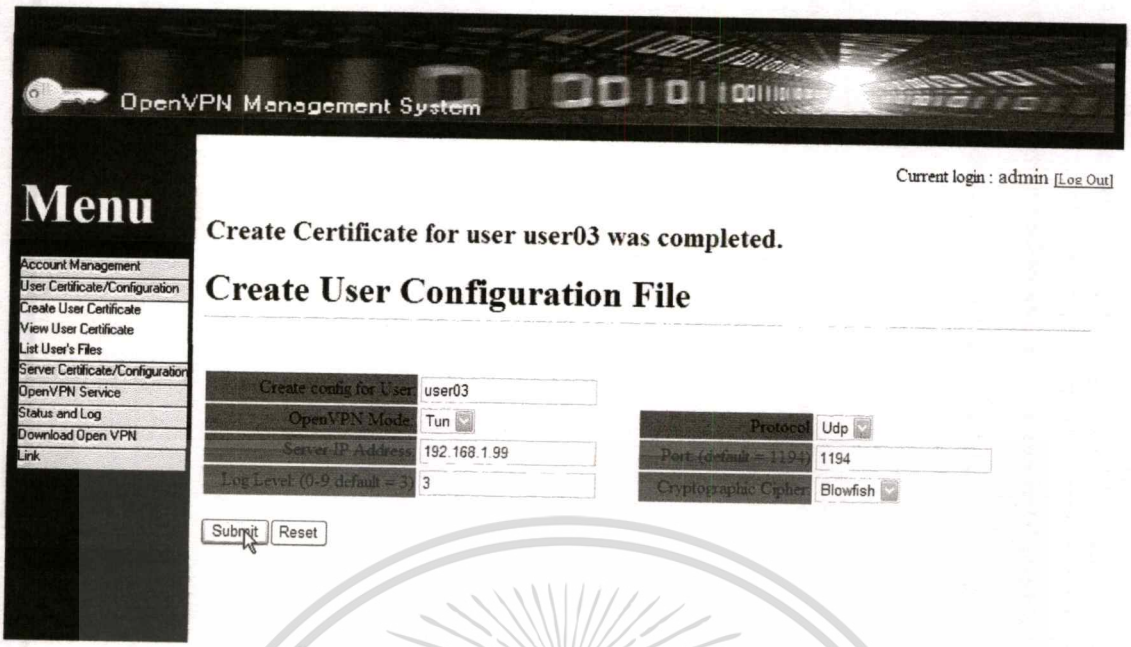
ในการสร้างใบรับรองของผู้ใช้จะต้องกำหนดจำนวนวันว่าใบรับรองจะมีอายุกี่วันเข้าไปในช่อง Number of days to valid ด้วย จากนั้นให้กดปุ่ม Approve เพื่ออนุมัติและสร้างใบรับรองหรือกด Deny เพื่อปฏิเสธใบรับรอง



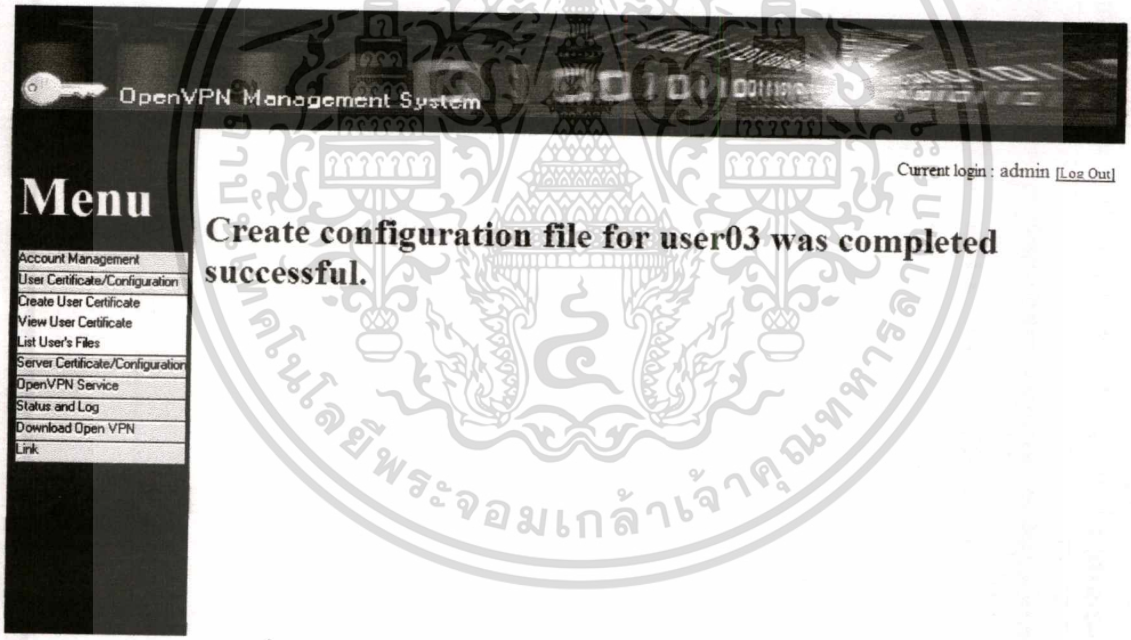
รูปที่ ข-6 หน้าจอแสดง Create User Certificate

หลังจากนั้นจะเป็นการสร้างไฟล์คอนฟิกของผู้ใช้ โดยต้องใส่ข้อมูลดังนี้

- Create config for user ให้ใส่ชื่อของ user ที่ต้องการสร้างไฟล์คอนฟิกซึ่งค่านี้จะเป็นชื่อไฟล์ด้วย
- OpenVPN Mode – ให้เลือก Tun หรือ Tap ซึ่งต้องสัมพันธ์กับค่าบนเซิร์ฟเวอร์ด้วย
- Protocol – ให้เลือกโปรโตคอลที่ใช้ว่าเป็น TCP หรือ UDP ซึ่งต้องสัมพันธ์กับค่าบนเซิร์ฟเวอร์ด้วย
- Server IP Address ให้ใส่ไอพีแอดเดรสของเซิร์ฟเวอร์ของ OpenVPN
- Port ให้ใส่พอร์ตของเซิร์ฟเวอร์ของ OpenVPN
- Log Level –ให้ใส่ค่าระดับในการเก็บล็อกตั้งแต่ 0 ถึง 9
- Cryptographic Cipher – ให้เลือกอัลกอริทึมในการเข้ารหัส ซึ่งต้องสัมพันธ์กับค่าบนเซิร์ฟเวอร์ด้วย



รูปที่ ข-7 หน้าจอแสดง Create User Configuration File



รูปที่ ข-8 หน้าจอแสดงผลหลังสร้าง User Configuration File

หลังจากสร้างไฟล์ใบรับรองและไฟล์คอนฟิกแล้วจะได้ไฟล์ทั้งหมด 4 ไฟล์ ดังต่อไปนี้

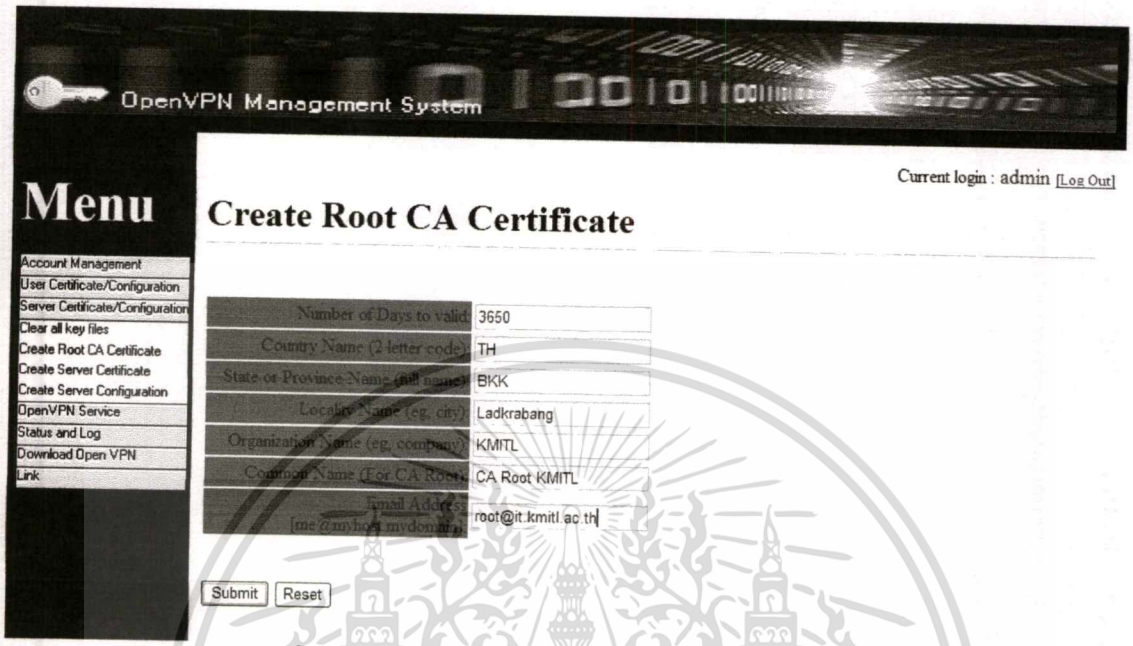
- Ca.crt คือใบรับรองของ CA
- Username.crt คือใบรับรองของผู้ใช้
- Username.key คือกุญแจส่วนตัวของผู้ใช้
- Username.ovpn คือไฟล์คอนฟิกของผู้ใช้

รูปที่ ข-9 หน้าจอแสดงผลการ List User Files

2.3 เมนู Server Certificate/ Configuration สำหรับลบคีย์ในระบบทั้งหมดและสร้างใบรับรองของCA Root และเซิร์ฟเวอร์ใหม่ รวมถึงการสร้างไฟล์คอนฟิกของเซิร์ฟเวอร์ด้วย

รูปที่ ข-10 หน้าจอแสดงผล Clear All Key Files

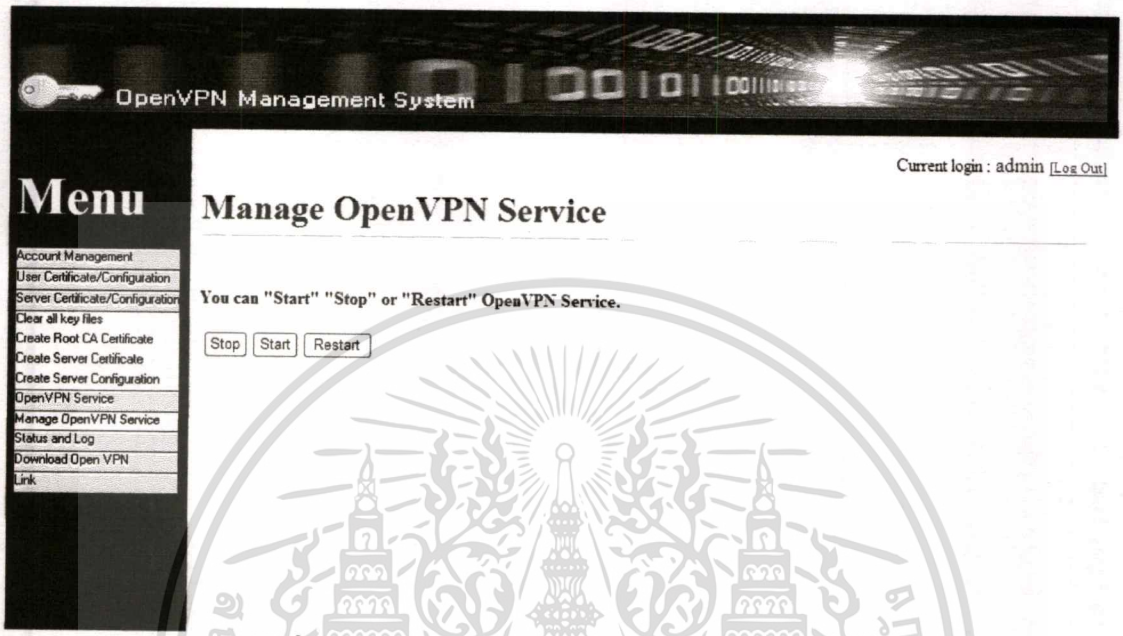
ในการสร้างใบรับรองของ Root CA และ Server นั้นต้องมีการใส่ข้อมูลเช่นจำนวนวันที่ valid ชื่อประเทศ ชื่อจังหวัด ชื่อเขต ชื่อองค์กร ชื่อใบรับรองและอีเมลล์แอดเดรส ในส่วนของเซิร์ฟเวอร์จะมีให้กำหนดขนาดของคีย์เพิ่มเติมด้วย



รูปที่ ข-11 หน้าจอแสดงผล Create Root CA Certificate

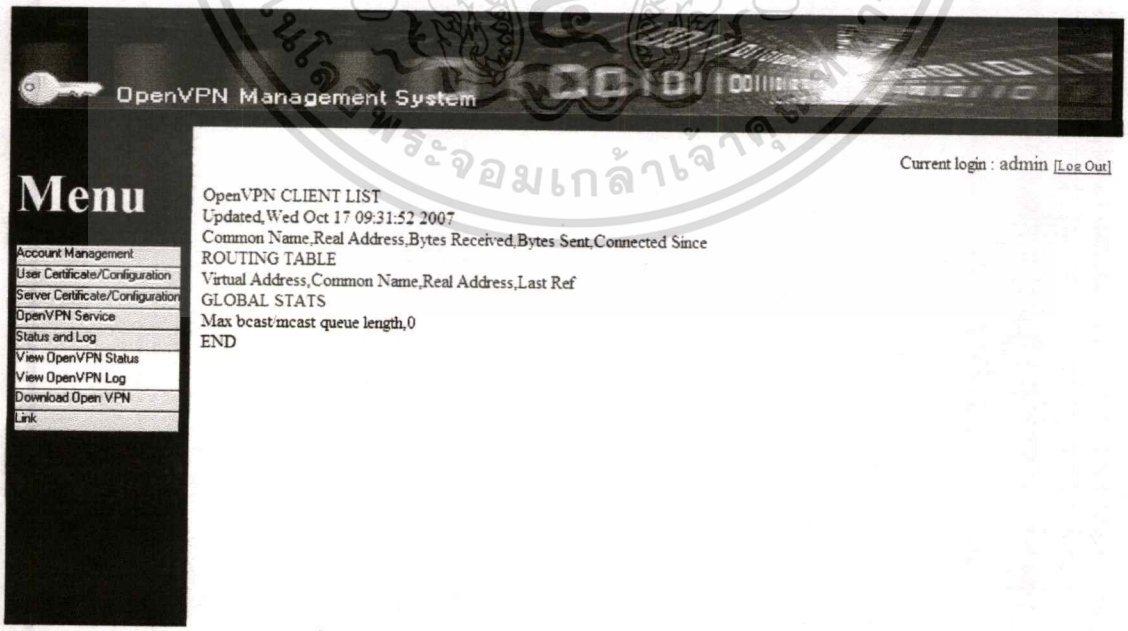
รูปที่ ข-12 หน้าจอแสดงผล Create Server Certificate

2.4 เมนู OpenVPN Service สำหรับเปิดและปิดเซอร์วิสของ OpenVPN Server เนื่องจากเมื่อมีการเปลี่ยนแปลงค่าในไฟล์คอนฟิกของเซิร์ฟเวอร์จะต้องทำการรีสตาร์ทเซอร์วิสเพื่อให้ใช้งานค่าใหม่ได้

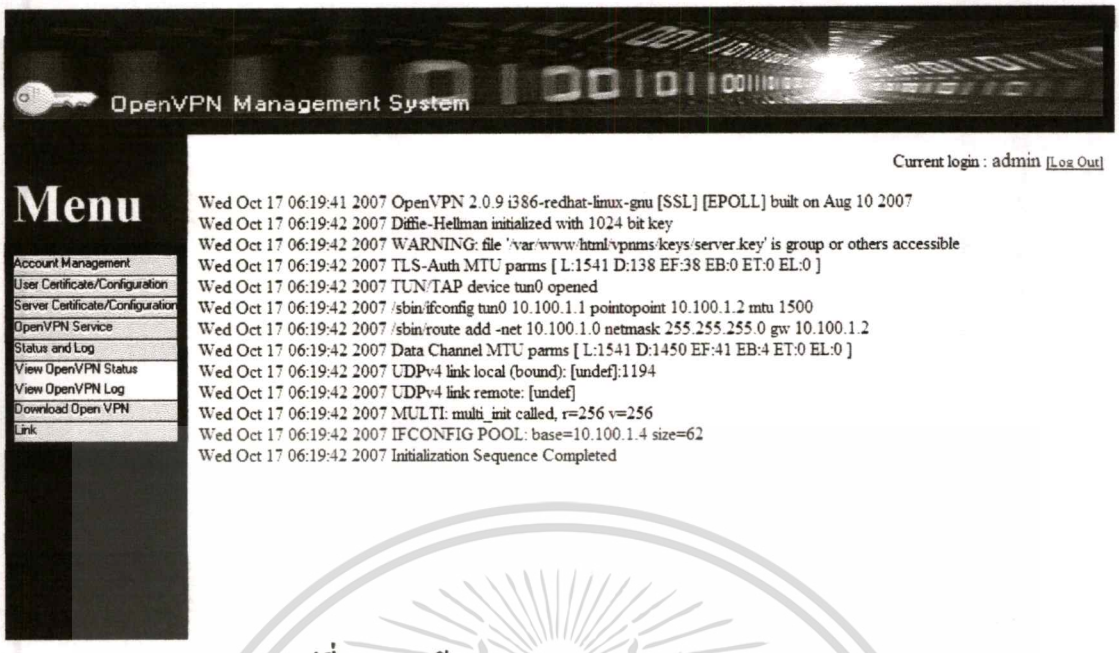


รูปที่ ข-13 หน้าจอแสดงผล Manage OpenVPN Service

2.5 เมนู Status and Log สำหรับตรวจสอบสถานะของผู้ใช้งานและดูล็อกของ OpenVPN Server ได้

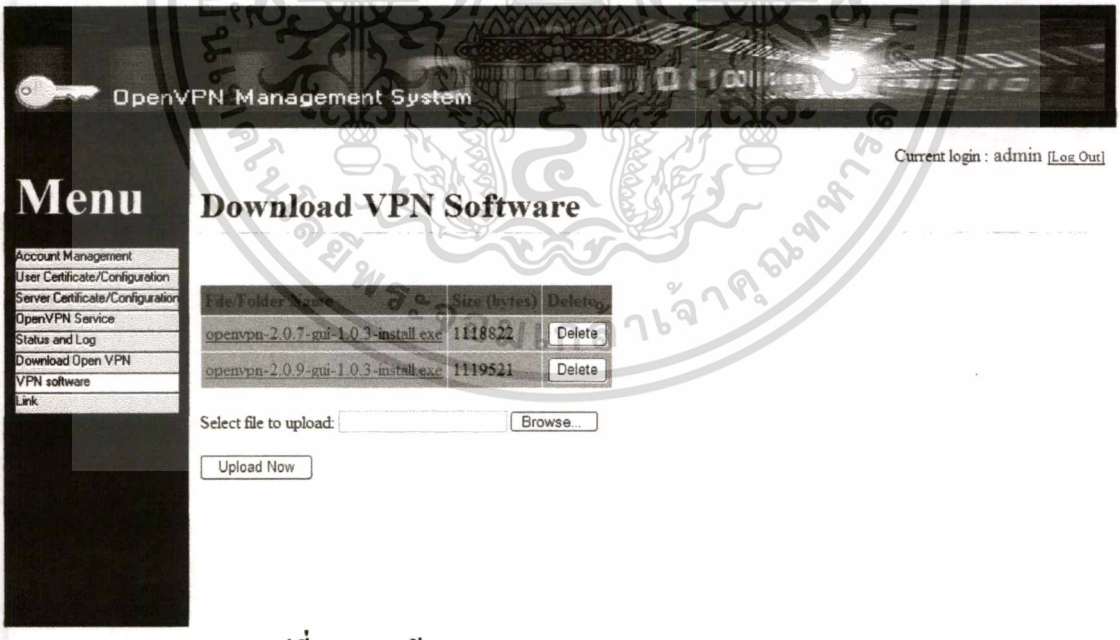


รูปที่ ข-14 หน้าจอแสดงผล View OpenVPN Status



รูปที่ ข-15 หน้าจอแสดงผล View OpenVPN Log

2.6 เมนู Download OpenVPN สำหรับบริหารจัดการการให้บริการในการดาวน์โหลดซอฟต์แวร์ OpenVPN Client โดยผู้ดูแลระบบสามารถเพิ่มหรือลบซอฟต์แวร์ออกจากระบบได้

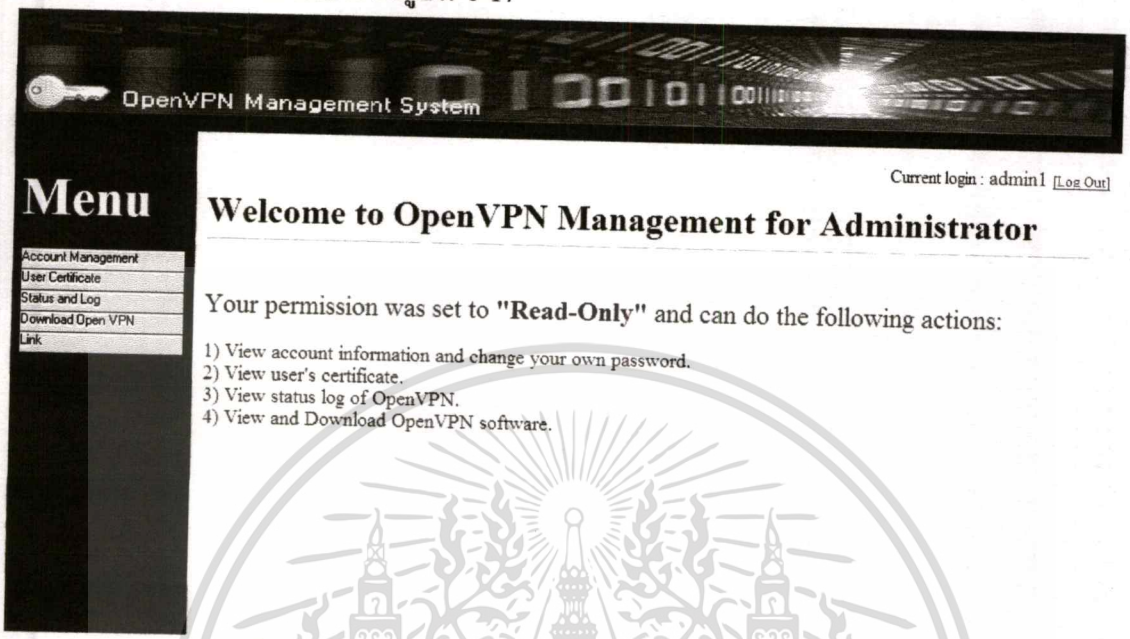


รูปที่ ข-16 หน้าจอแสดงผล Download VPN Software

2.7 เมนู Link สำหรับเข้าถึงเว็บไซต์ของ OpenVPN

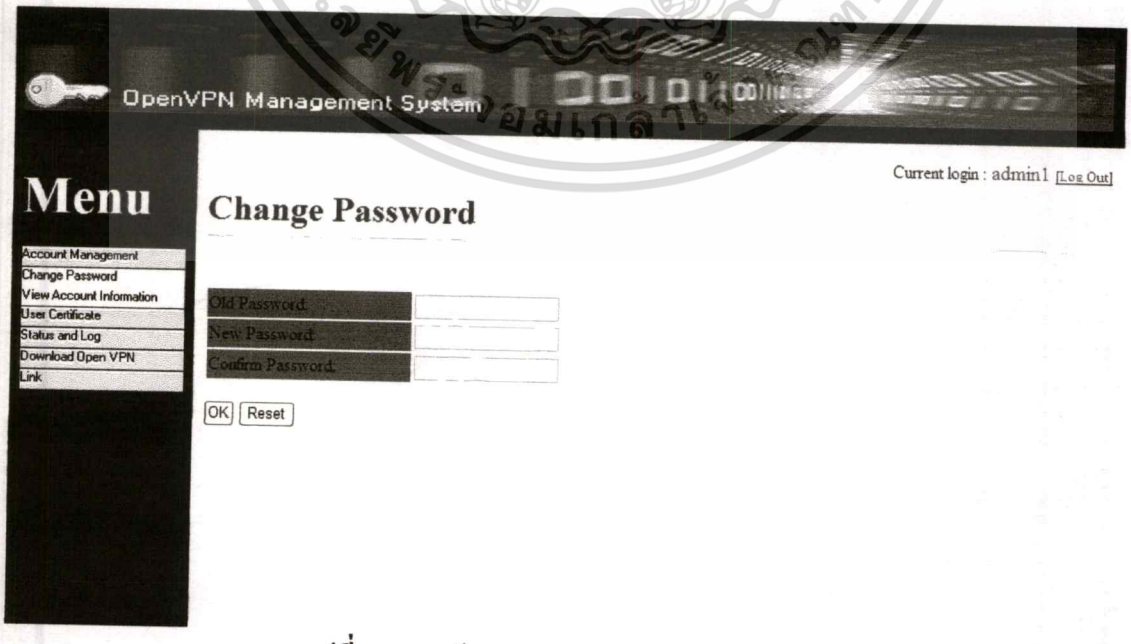
3. ฟังก์ชันการใช้งานของ Admin (Read-Only)

หลังจากที่ล็อกอินเข้าสู่ระบบแล้ว ในหน้าต้อนรับจะมีข้อความระบุว่าผู้ล็อกอินมีสิทธิ์ระดับไหนและมีสิทธิ์ทำอะไรได้บ้าง ดังรูปที่ ข-17

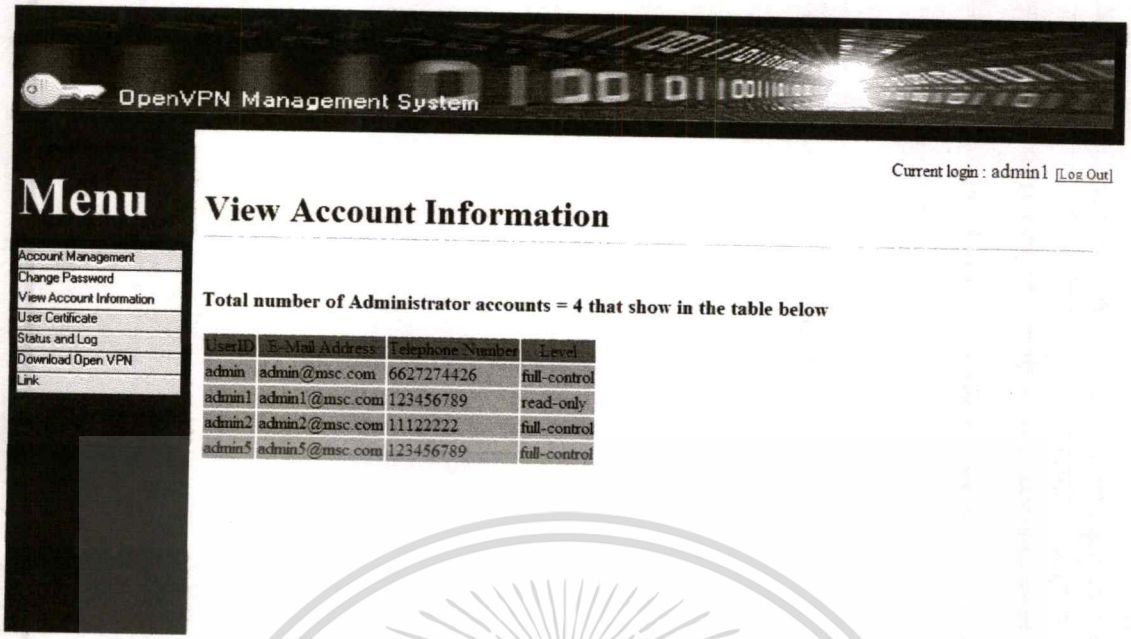


รูปที่ ข-17 หน้าจอแสดงหน้าต้อนรับของ Admin (Read-Only)

3.1 เมนู Account Management ดูข้อมูลผู้ดูแลระบบทั้งหมดรวมถึงเปลี่ยนรหัสผ่านของตน และในส่วนของการเปลี่ยนรหัสผ่านผู้ใช้งานต้องกรอกรหัสผ่านเดิมให้ถูกต้อง และกรอกรหัสผ่านใหม่ให้เหมือนกัน 2 ครั้งจึงจะสามารถเปลี่ยนรหัสผ่านใหม่ได้



รูปที่ ข-18 หน้าจอแสดงผล Change Password



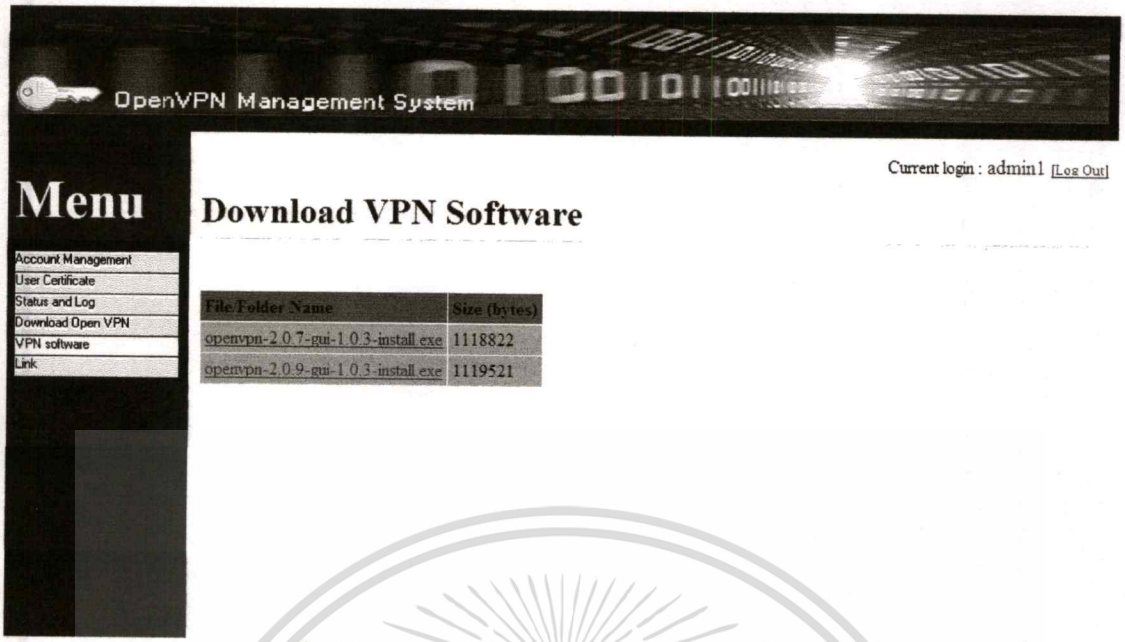
รูปที่ ข-19 หน้าจอแสดงผล View Account Information

3.2 เมนู User Certificate ดูข้อมูลใบรับรองของผู้ใช้ทั้งหมด

รูปที่ ข-20 หน้าจอแสดงผล View User Certificate

3.3 เมนู Status and Log สำหรับตรวจสอบสถานะของผู้ใช้งานและดูล็อกของ OpenVPN Server ได้ ซึ่งจะได้ผลเหมือนกับ Admin (Full-Control)

3.4 เมนู Download OpenVPN สำหรับดาวน์โหลดโปรแกรม OpenVPN Client ซึ่งจะไม่สามารถอัพโหลดไฟล์หรือลบไฟล์ทิ้งได้

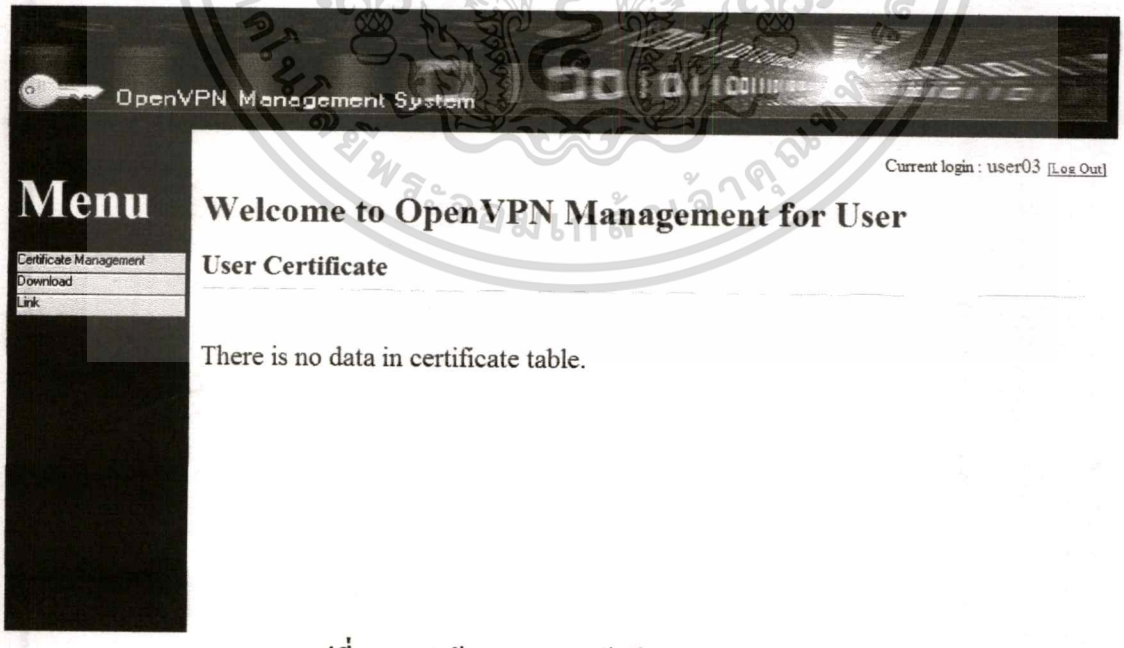


รูปที่ ข-21 หน้าจอแสดงผล Download VPN Software

3.5 เมนู Link สำหรับเข้าถึงเว็บไซต์ของ OpenVPN

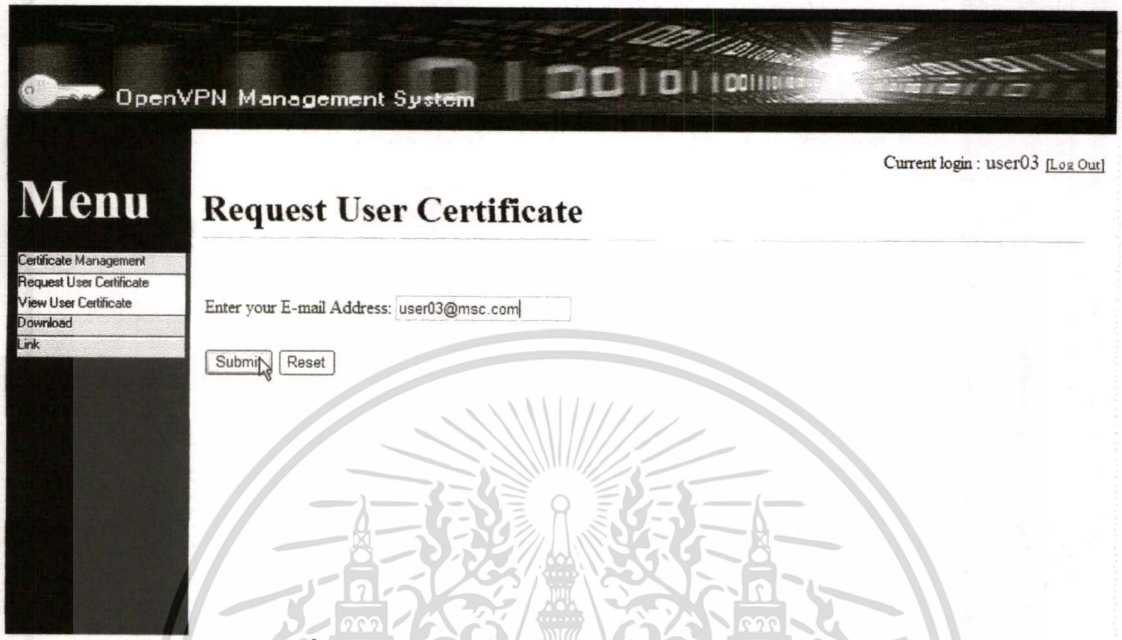
4. ฟังก์ชันการใช้งานของ User

หลังจากที่ล็อกอินเข้าสู่ระบบแล้ว ในหน้าต้อนรับจะมีข้อความระบุว่าผู้ล็อกอินมีใบรับรองหรือยัง ดังรูปที่ ข-22



รูปที่ ข-22 หน้าจอแสดงหน้าต้อนรับของ User

4.1 เมนู Certificate Management ผู้ใช้สามารถดูใบรับรองและร้องขอใบรับรองไปยังผู้ดูแลระบบได้ในกรณีที่ยังไม่มีใบรับรอง โดยระบบจะส่งอีเมลล์ไปยังผู้ดูแลระบบเพื่อดำเนินการต่อไป



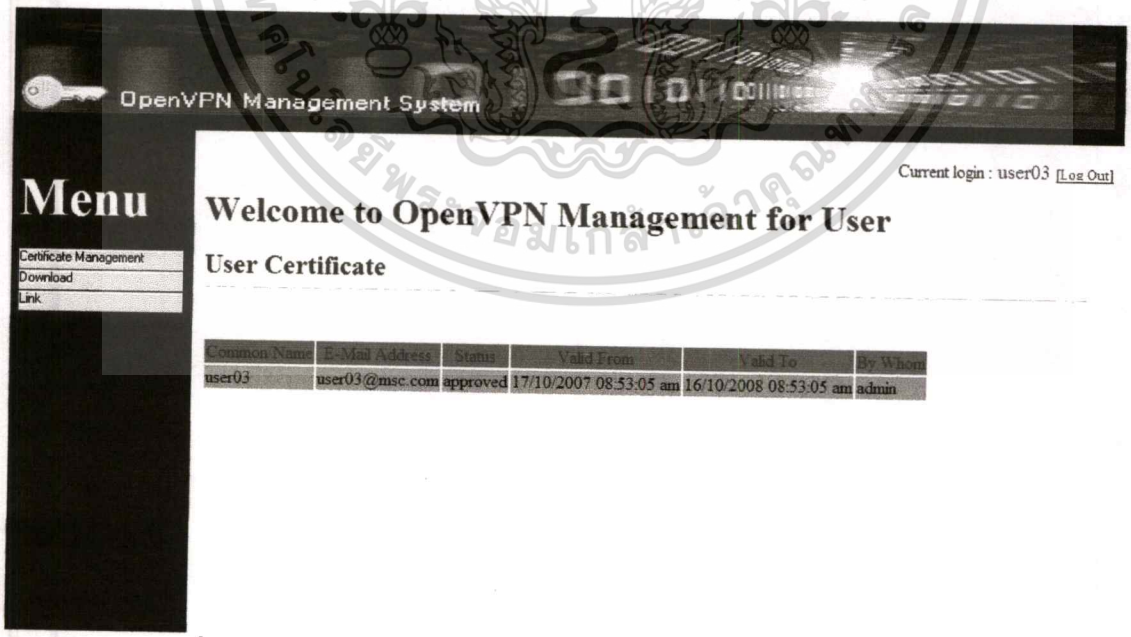
รูปที่ ข-23 หน้าจอแสดงผล Request User Certificate

รูปที่ ข-24 หน้าจอแสดงผลหลัง Request User Certificate แล้ว

หลังจากร้องขอใบรับรองแล้ว เมื่อเข้ามาดูที่สถานะของใบรับรองจะแสดงเป็น Request

รูปที่ ข-25 หน้าจอแสดงผล View User Certificate

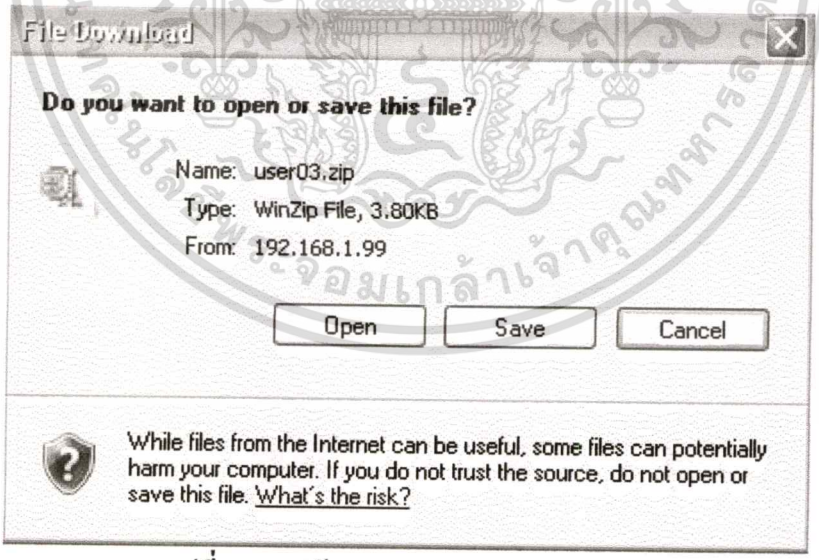
หลังจากที่ผู้ดูแลระบบอนุมัติและสร้างใบรับรองให้แล้ว สถานะจะเปลี่ยนเป็น Approved ซึ่งสามารถใช้งานได้แล้ว



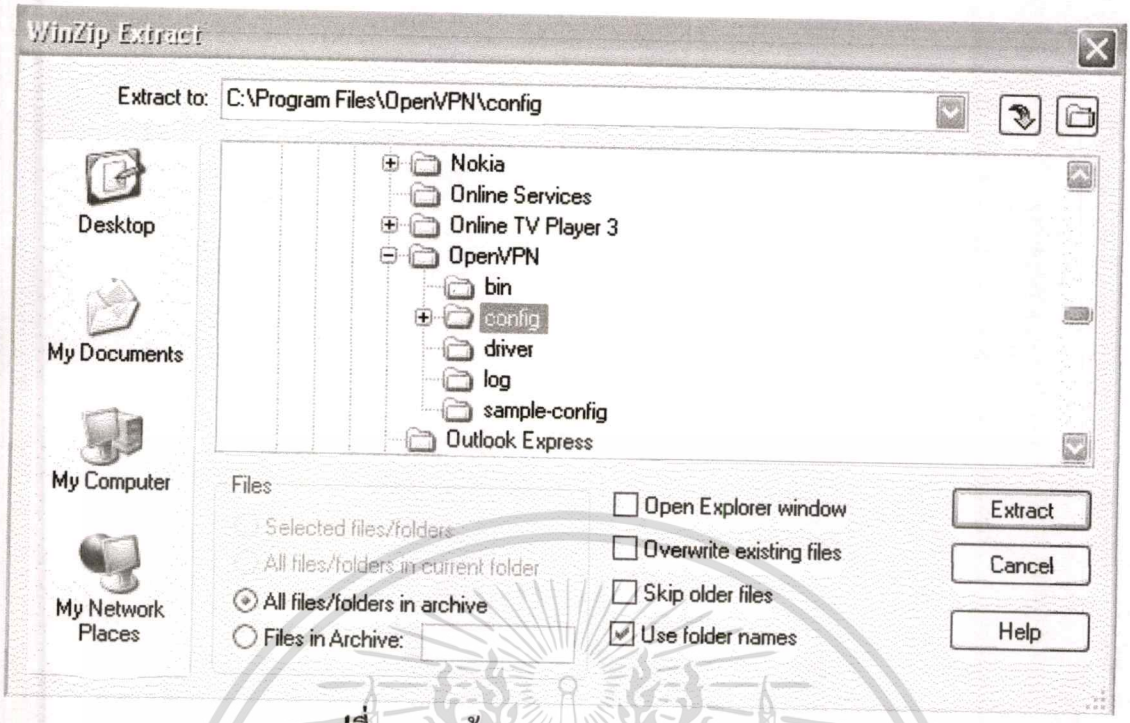
รูปที่ ข-26 หน้าจอแสดงหน้าต้อนรับของ User หลัง Approved ใบรับรอง

4.2 เมนู Download ผู้ใช้สามารถดาวน์โหลดโปรแกรม OpenVPN Client และใบรับรองและไฟล์คอนฟิกของตนเองได้โดยการดาวน์โหลดจะเป็นไฟล์ซิปซึ่งผู้ใช้จะต้อง extract ไปวางไว้ใน part config ของ OpenVPN เช่น C:\Program Files\OpenVPN\Config

รูปที่ ข-27 หน้าจอแสดงผล Download Certificate and Configuration File

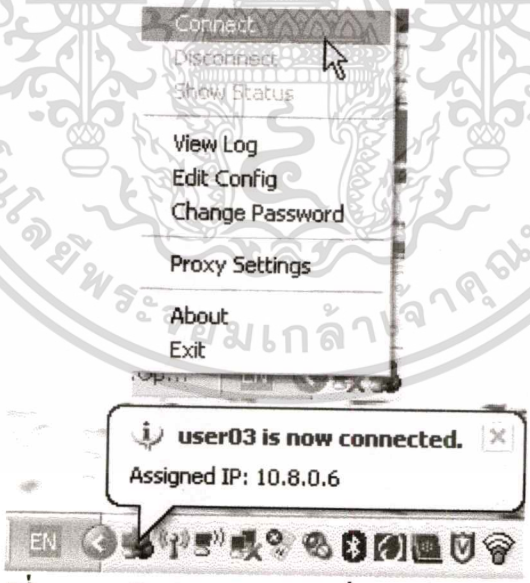


รูปที่ ข-28 หน้าจอแสดงผล File Download



รูปที่ ข-29 หน้าจอแสดงผล Winzip Extract

จากนั้นผู้ใช้งานเลือก Connect ที่ไอคอน OpenVPN บน task bar ก็จะสามารถติดต่อกับเซิร์ฟเวอร์ OpenVPN ได้



รูปที่ ข-30 หน้าจอแสดงผลการเชื่อมต่อ OpenVPN

ประวัติผู้เขียน

ชื่อผู้เขียน	นายเอกรัฐ ไพศาลเวชกรรม
สถานที่เกิด	จังหวัดกรุงเทพมหานคร
การศึกษา	ระดับปริญญาตรี
	วศ.บ. (วิศวกรรมศาสตรบัณฑิต)
	สาขาวิศวกรรมคอมพิวเตอร์
	มหาวิทยาลัยเกษตรศาสตร์
ประสบการณ์การทำงาน	บริษัท เมโทรซิสเต็มส์ คอร์ปอเรชัน จำกัด มหาชน