สารบัญภาพ

	หน้า
รูปที่ 2-1 ระบบรับส่งสารด่วนแบบเพียร์ทูเพียร์	6
รูปที่ 2-2 ระบบรับส่งสารด่วนแบบ Server-based	7
รูปที่ 3-1 แสดง Security Pyramid 1	10
รูปที่ 3-2 แผนผังแสดงกระบวนการการพิสูจน์ตัวตน 2	11
รูปที่ 4-1 ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจ	15
รูปที่ 4.2 ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตน	16
รูปที่ 4-3 การส่งข้อมูลเข้าไปใน Hash function	16
รูปที่ 4-4 การเข้ารหัสเมสเซสไดเจสต์ด้วยกุญแจส่วนตัวเพื่อเป็นการลงลาย	17
รูปที่ 4-5 ขั้นตอนการเปรียบเทียบความถูกต้อง	17
รูปที่ 5-1 จะใช้ ขบวนการสร้างการเชื่อมต่อโดย SSL แบบเข้ารหัสอย่างเดียว	20
รูปที่ 5-2 แสดงสภาวะในการรับส่งข้อมูลของไคล์เอ็นต์ตามกระบวนการของ SSL โพรโตคอล	24
รูปที่ 5-3 แสดงสภาวะในการรับส่งข้อมูลของเซิร์ฟเวอร์ตามขบวนการของ SSL โพรโตคอล	25
รูปที่ 5-4 แสดงการโจมตีแบบแมนอินเดอะมิดเดิล (Man-in-the-middle)	27
รูปที่ 5-5 แสดงสองข้อความใหม่ที่ใช้สำหรับการพิสูจน์ตนของเซิร์ฟเวอร์	28
รูปที่ 5-6 การใช้ระบบพิสูจน์ตนอย่างเดียว	29
รูปที่ 5-7 แสดงการพิสูจน์ตนและเข้ารหัสของฝั่งไคลเอ็นต์	30
รูปที่ 5-8 ผู้ร้องขอจำเป็นต้องมี ใบรับรองสิทธิ์ของผู้ออก	35
รูปที่ 5-9 ผู้ร้องขอส่งคำร้องไปยังผู้ออกเพื่อให้ผู้ออกทำการ sign ใบรับรองสิทธิ์	35
รูปที่ 5-10 ผู้ร้องขอได้รับ ใบรับรองสิทธิ์	36
รูปที่ 5-11 แสดงการสื่อสารโดยใช้ใบรับรองสิทธิ์	37
รูปที่ 5-12 แสดงการพิสูจน์ใบรับรองสิทธิ์โดยฝั่งเซิร์ฟเวอร์	38
รูปที่ 6-1 แสดงถึงความสำคัญของ alias	40
รูปที่ 6-3 การสร้าง KeyStore ด้วย keytool	43
รูปที่ 6-4 การตรวจสอบข้อมูลภายใน KeyStore ที่ถูกสร้างขึ้นด้วย keytool	44

รูปที่ 6-5 การตรวจสอบข้อมูลอย่างละเอียดภายใน KeyStore ที่ถูกสร้างขึ้นด้วย keytool 44
รูปที่ 6-6 การสร้างใบร้องขอใบรับรองสิทธิ์จาก KeyStore ที่ถูกสร้างขึ้นด้วย keytool 44
รูปที่ 6-7 กาตรวจสอบใบร้องขอใบรับรองสิทธิ์ที่สร้างด้วย keytool 45
รูปที่ 6-8 การนำเข้าใบรับรองสิทธิ์ที่ไว้วางใจเข้ามาใน KeyStore 45
รูปที่ 6-9 การนำเข้าใบรับรองสิทธิ์ที่ไว้วางใจเข้ามาใน KeyStore 46
รูปที่ 7-1 การติดต่อระหว่าง IsagQ ด้วยกันในยุคก่อน 48
รูปที่ 7-2 การติดต่อระหว่าง IsagQ ด้วยกัน โดยมิได้ใช้ SSL Protocol 49
รูปที่ 7-3 การติดต่อระหว่าง IsagQ ด้วยกัน โดยใช้เฉพาะการแลกเปลี่ยนคีย์ 50
รูปที่ 7-4 IsagMQ & IsagQ ในยุคปัจจุบัน 51
รูปที่ 7-5 การติดต่อระหว่าง IsagQ กับ IsagQ โดยใช้ SSL Protocol 51
รูปที่ 7-6 การติดต่อระหว่าง IsagQ กับ IsagQ โดยมีการแลกเปลี่ยนคีย์และใบรับรองสิทธิ์ 52
รูปที่ 7-8 ช่องทางการสื่อสารแบบปลอดภัยของโปรแกรม 55
รูปที่ 7-9โครงสร้างของโปรแกรมแม่ข่ายสำหรับรับส่งสารด่วนแบบปลอดภัย 57
รูปที่ 7-10โครงสร้างของโปรแกรมลูกข่ายสำหรับรับส่งสารด่วนแบบปลอดภัย 58
รูปที่ 7-11โครงสร้างการติดต่อสื่อสารระหว่างโปรแกรมลูกข่ายด้วยกันเอง 59
รูปที่ 7-12 แสดงรูปแบบของโพรโตคอลที่ใช้สำหรับ IsagMQ และ IsagQ 61
รูปที่ 7-14 แสดงขั้นตอนที่ 1 ของการร้องขอใบรับรองสิทธิ์ 68
รูปที่ 7-15 แสดงขั้นตอนที่ 2 ของการร้องขอใบรับรองสิทธิ์ 69
รูปที่ 7-16 แสดงขั้นตอนที่ 3 ของการร้องขอใบรับรองสิทธิ์ 69
รูปที่ 7-17 ขั้นตอนสำหรับการเข้าใช้บริการ 74
รูปที่ 7-18 ขั้นตอนสำหรับการเพิ่มรายชื่อคู่สนทนาด้วยอีเมลแอดเดรส 75
รูปที่ 7-19 ขั้นตอนสำหรับการเพิ่มรายชื่อคู่สนทนาด้วยรหัสผู้ใช้ 77
รูปที่ 7-20 ขั้นตอนสำหรับการเปลี่ยนชื่อเล่นของผู้ใช้ 79
รูปที่ 7-21 ขั้นตอนสำหรับการตรวจสอบสถานะ 81
รูปที่ 7-22 ขั้นตอนสำหรับการรายงานความผิดพลาด 83
รูปที่ 7-23 ขั้นตอนสำหรับสิ้นสุดการใช้บริการ 84
รูปที่ 7-24 ขั้นตอนสำหรับการค้นหาสมาชิก 85
รูปที่ 7-25 ขั้นตอนสำหรับการลบรายชื่อคู่สนทนา 87
รูปที่ 7-26 ขั้นตอนสำหรับการเปลี่ยนสถานะของผู้ใช้ 89

รูปที่ 7-27 ขั้นตอนสำหรับการปฏิเสธคู่สนทนา 91
รูปที่ 7-28 ขั้นตอนสำหรับการตรวจสอบบัญชีรายชื่อที่รอคำยินยอม 93
รูปที่ 7-29 ขั้นตอนสำหรับการยินยอมตามคำร้องขอ 95
รูปที่ 7-30 ขั้นตอนสำหรับการส่งข้อความระหว่าง IsagQ ด้วยกัน 97
รูปที่ 7-31 ขั้นตอนสำหรับการส่งไฟล์ระหว่าง IsagQ ด้วยกัน 98
รูปที่ 7-32 ขั้นตอนสำหรับปฏิเสธการรับไฟล์ 100
รูปที่ 7-33 ขั้นตอนสำหรับการแสดงผลผิดพลาดในการส่งไฟล์ 101
รูปที่ 8-1 แสดงการดักจับการสถาปนาการเชื่อมต่อ ด้วย SSL ระหว่าง IsagMQ กับ IsagQ 102
รูปที่ 8-2 แสดงการดักจับข้อมูลที่ถูกเข้ารหัส ระหว่าง IsagMQ กับ IsagQ 103
รูปที่ 8-3 การดักจับการสถาปนาการเชื่อมต่อ ด้วย SSL ระหว่าง IsagMQ กับ IsagQ 104
รูปที่ 8-4 แสดงการดักจับข้อมูลที่ถูกเข้ารหัส ระหว่าง IsagQ กับ IsagQ 104