บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

โครงสร้างพื้นฐานระบบกุญแจสาธารณะเป็นระบบที่เกี่ยวข้องกับการจัดการกุญแจสาธารณะ สำหรับใช้ในกระบวนการการเข้ารหัสแบบใช้กุญแจสาธารณะ ซึ่งมีความเกี่ยวข้องกับทฤษฎีพื้นฐานด้านวิทยาการการเข้ารหัสต่าง ๆ คือ

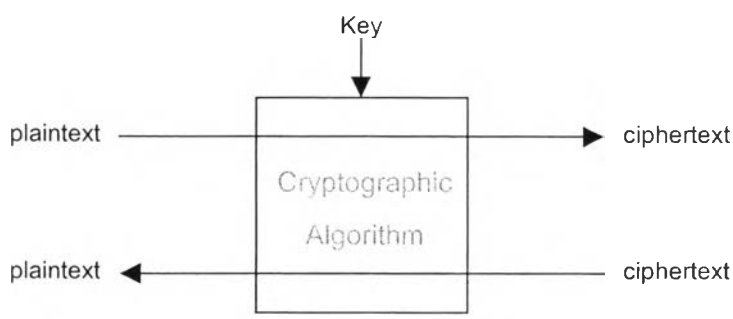
1) วิทยาการการเข้ารหัสลับ (Cryptography)

2) โครงสร้างพื้นฐานระบบกุญแจสาธารณะ (Public Key Infrastructure)

2.1. วิทยาการการเข้ารหัสลับ (Cryptography)

2.1.1. การเข้ารหัสแบบกุญแจลับ (Secret Key Cryptography)

การเข้ารหัสแบบกุญแจลับเป็นวิทยาการที่เกี่ยวข้องกับการเข้ารหัสและถอดรหัสด้วยการใช้กุญแจเพียงหนึ่งดอก โดยกระบวนการเข้ารหัสจะเริ่มจากการนำข้อมูลที่ต้องการเข้ารหัส (Plaintext) และกุญแจลับ (Secret Key) มาผ่านวิธีการเข้ารหัส (Cryptographic Algorithm) ได้ผลเป็นข้อมูลที่ถูกเข้ารหัส (Ciphertext) กระบวนการถอดรหัสจะเป็นกระบวนการย้อนกลับของกระบวนการเข้ารหัส โดยเริ่มจากการนำข้อมูลที่ถูกเข้ารหัส และกุญแจลับที่ใช้ในการเข้ารหัสข้อมูลชุดนั้น มาผ่านวิธีการถอดรหัสซึ่งเป็นวิธีเดียวกับการเข้ารหัสข้อมูลชุดนั้น ได้ผลเป็นข้อมูลก่อนการเข้ารหัส ดังแสดงในรูปที่ 2.1 การเข้ารหัสแบบกุญแจลับอาจเรียกอีกชื่อหนึ่งว่า การเข้ารหัสแบบสมมาตร (Symmetric Cryptography)[3]



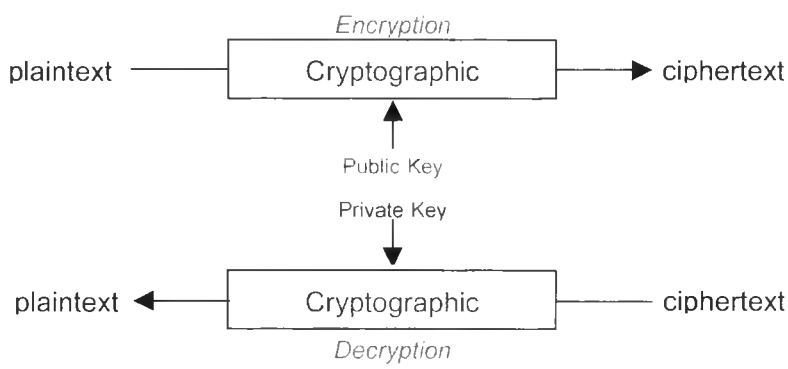
รูปที่ 2.1 การเข้ารหัสและถอดรหัสแบบกุญแจลับ

2.1.2. การเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography)

การเข้ารหัสแบบกุญแจสาธารณะเป็นวิทยาการที่เกี่ยวข้องกับการเข้ารหัสและถอดรหัสด้วยการใช้กุญแจสองดอกซึ่งเป็นคู่กัน หรือกล่าวอีกนัยหนึ่งคือ กุญแจทั้งสองจะมีความสัมพันธ์ทางคณิตศาสตร์ซึ่งกันและกัน โดยกุญแจดอกหนึ่งเรียกว่ากุญแจส่วนตัว (Private Key) เป็นกุญแจที่ต้องเก็บเป็นความลับเฉพาะบุคคล ส่วนกุญแจอีกดอกหนึ่งเรียกว่ากุญแจสาธารณะ (Public Key) สามารถเปิดเผยสู่สาธารณะได้ การเข้ารหัสแบบกุญแจสาธารณะต่างจากการเข้ารหัสแบบกุญแจลับตรงที่ ถ้าใช้กุญแจดอกหนึ่งในการเข้ารหัส ต้องใช้กุญแจอีกดอกหนึ่งซึ่งเป็นคู่กันในการถอดรหัส การเข้ารหัสแบบกุญแจสาธารณะจึงถูกเรียกอีกชื่อหนึ่งว่า การเข้ารหัสแบบอสมมาตร (Asymmetric Cryptography)[3]

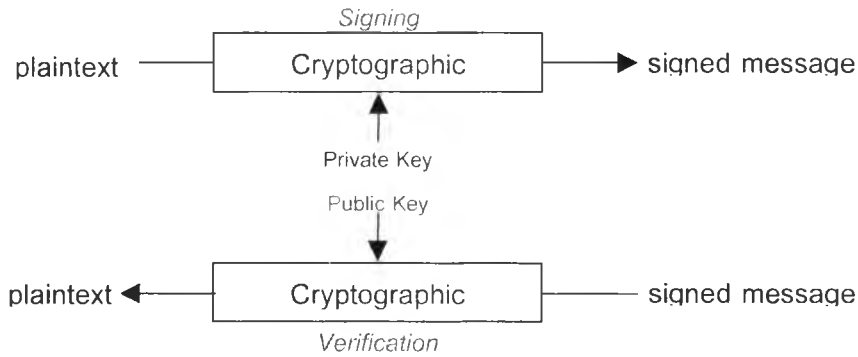
การประยุกต์ใช้การเข้ารหัสแบบกุญแจสาธารณะมีอยู่ 2 ลักษณะคือ การใช้กุญแจสาธารณะในการเข้ารหัสและใช้กุญแจส่วนตัวในการถอดรหัส เรียกกระบวนการดังกล่าวว่ากระบวนการเข้ารหัสและถอดรหัส (Encryption and Decryption) ในทางกลับกัน ถ้าใช้กุญแจส่วนตัวในการเข้ารหัสและใช้กุญแจสาธารณะในการถอดรหัส เรียกกระบวนการดังกล่าวว่ากระบวนการลงลายมือชื่อและการทวนสอบ (Signing and Verification)

กระบวนการเข้ารหัสและถอดรหัสเริ่มจากการนำข้อมูลที่ต้องการเข้ารหัส (Plaintext) และกุญแจสาธารณะ มาผ่านวิธีการเข้ารหัส (Cryptographic Algorithm) ได้ผลเป็นข้อมูลที่ถูกเข้ารหัส (Ciphertext) กระบวนการถอดรหัสเริ่มจากการนำข้อมูลที่ถูกเข้ารหัส และกุญแจส่วนตัว มาผ่านวิธีการถอดรหัส ได้ผลเป็นข้อมูลก่อนการเข้ารหัส ดังแสดงในรูปที่ 2.2



รูปที่ 2.2 การเข้ารหัสและถอดรหัสแบบกุญแจสาธารณะ

กระบวนการลงลายมือชื่อเริ่มจากการนำข้อมูลที่ต้องการลงลายมือชื่อ (Plaintext) และกุญแจส่วนตัว มาผ่านวิธีการเข้ารหัส ได้ผลเป็นข้อมูลที่ลงลายมือชื่อ (Signed Message) ส่วนกระบวนการทวนสอบเริ่มจากการนำข้อมูลที่ลงลายมือชื่อ และกุญแจสาธารณะ มาผ่านวิธีการถอดรหัส ได้ผลเป็นข้อมูลก่อนลงลายมือชื่อ ดังแสดงในรูปที่ 2.3



รูปที่ 2.3 การลงลายมือชื่อและการทวนสอบ

2.1.3. ฟังก์ชันแฮช (Hash Function)

ฟังก์ชันแฮชเป็นกระบวนการทางคณิตศาสตร์ที่ทำหน้าที่แปลงข้อมูลที่มีความยาวใด ๆ เป็นชุดของตัวเลขที่มีขนาดคงที่ ฟังก์ชันแฮชมีคุณลักษณะดังนี้

1) เป็นฟังก์ชันที่ง่ายต่อการคำนวณและใช้เวลาน้อยในการแปลงข้อมูลใด ๆ เป็นตัวเลขที่มีขนาดคงที่ค่าหนึ่ง

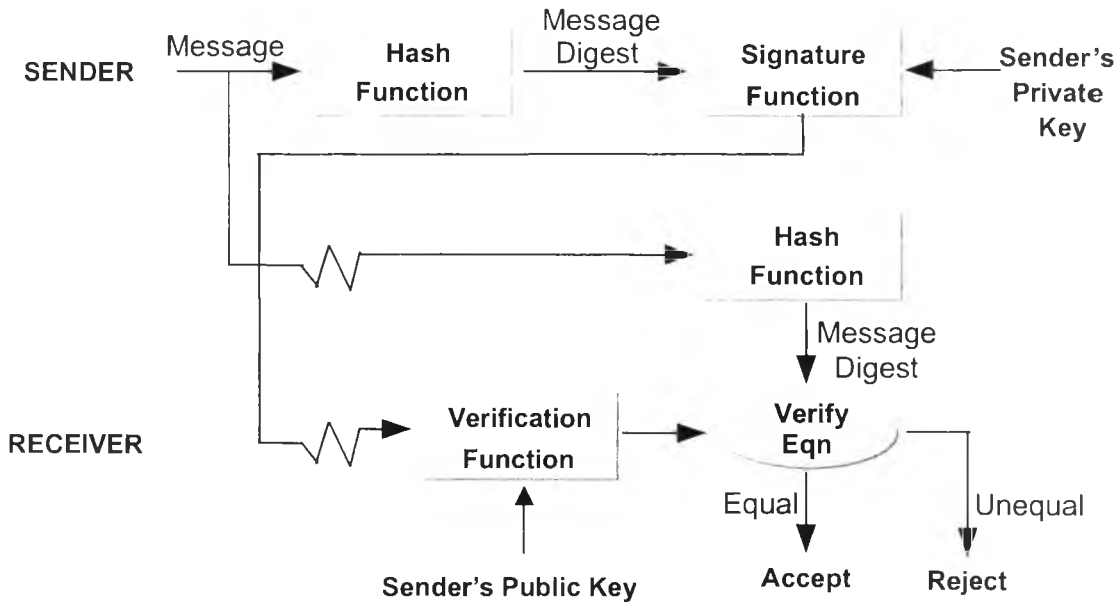
2) ไม่มีวิธีการแปลงค่าตัวเลขที่ได้จากการคำนวณฟังก์ชันแฮช กลับมาเป็นข้อมูลดั้งเดิม

3) ไม่มีวิธีการคำนวณค่าแฮชของข้อมูลที่ต่างกัน 2 ชุด ให้ได้ค่าแฮชเดียวกัน

ฟังก์ชันแฮชมักรู้จักกันในนาม การย่อยข้อมูล (Message Digests) หรือ การแปลงคาแบบทางเดียว (One-way Transformations)[3]

2.1.4. ลายมือชื่อดิจิตอล (Digital Signature)

ลายมือชื่อดิจิตอลเป็นข้อมูลทางอิเล็กทรอนิกส์ชุดหนึ่งที่เกิดจากการนำข้อมูลชุดใด ๆ มาผ่านฟังก์ชันแฮช และนำค่าแฮชที่ได้ไปผ่านการเข้ารหัสแบบกุญแจสาธารณะ โดยใช้กุญแจส่วนตัวของผู้ที่ทำหน้าที่ลงลายมือชื่อได้เป็นลายมือชื่อดิจิตอลดังแสดงในรูปที่ 2.4 และเนื่องจากลายมือชื่อดิจิตอลเป็นข้อมูลที่ขึ้นอยู่กับข้อมูลดั้งเดิม หากข้อมูลดั้งเดิมถูกแก้ไขจะทำให้ลายมือชื่อดิจิตอลไม่เหมือนเดิม ดังนั้นจะเห็นได้ว่าลายมือชื่อดิจิตอลทำหน้าที่หลักที่สำคัญ 2 ประการได้แก่ พิสูจน์ผู้ลงลายมือชื่อ และพิสูจน์ว่าข้อมูลไม่ได้ถูกแก้ไข[4]

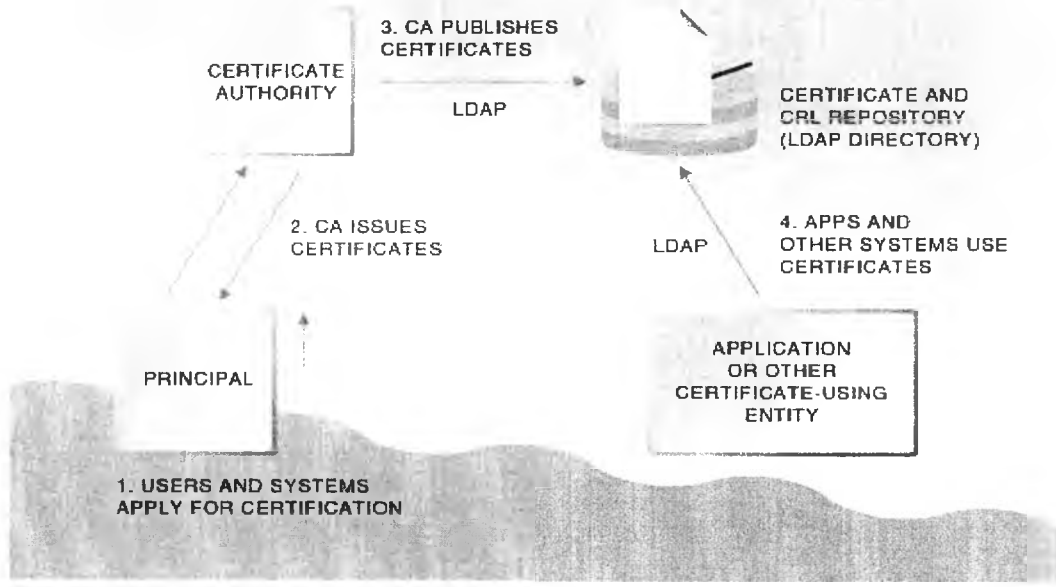


รูปที่ 2.4 ขั้นตอนการตรวจสอบลายมือชื่อดิจิตอล

2.2. โครงสร้างพื้นฐานระบบกุญแจสาธารณะ (Public Key Infrastructure)

โครงสร้างพื้นฐานระบบกุญแจสาธารณะเป็นระบบที่ใช้สำหรับการเผยแพร่ *กุญแจสาธารณะที่มีความน่าเชื่อถือ* ออกไปในระบบเครือข่าย เพื่อใช้ในกระบวนการเข้ารหัสแบบกุญแจสาธารณะ เนื่องจากหากขาดความน่าเชื่อถือของกุญแจสาธารณะจะทำให้ระบบขาดความน่าเชื่อถือ[5] โครงสร้างพื้นฐานระบบกุญแจสาธารณะทำหน้าที่หลัก 2 ประการได้แก่

1) การเชื่อมโยงกุญแจสาธารณะเข้ากับผู้เป็นเจ้าของ ซึ่งอาจเป็นบุคคล หน่วยงาน หรือทรัพยากรในระบบเครือข่าย รวมถึงการจัดเก็บ ดูแล บำรุงรักษา ให้กุญแจสาธารณะมีความน่าเชื่อถืออยู่เสมอ
2) การแจกจ่ายกุญแจสาธารณะที่มีความน่าเชื่อถือไปยังผู้ใช้งาน



รูปที่ 2.5 โครงสร้างพื้นฐานระบบกุญแจสาธารณะ

2.2.1. องค์ประกอบของโครงสร้างพื้นฐานระบบกุญแจสาธารณะ

โครงสร้างพื้นฐานระบบกุญแจสาธารณะโดยทั่วไปมีองค์ประกอบพื้นฐานด้วยกัน 6 ส่วนได้แก่

1) ใบรับรองกุญแจสาธารณะ (Public Key Certificate) – ใบรับรองกุญแจสาธารณะเป็นข้อมูลอิเล็กทรอนิกส์ที่ใช้เชื่อมโยงกุญแจสาธารณะกับผู้เป็นเจ้าของกุญแจสาธารณะนั้น โดยใบรับรองจะถูกลงลายมือชื่ออิเล็กทรอนิกส์โดยหน่วยงานที่เชื่อถือได้ (CA)

2) รายการเพิกถอนใบรับรอง (Certificate Revocation List หรือ CRL) – รายการเพิกถอนใบรับรองเป็นรายการใบรับรองที่ถูกเพิกถอนจากระบบ

3) หน่วยออกใบรับรอง (Certificate Authority หรือ CA) – หน่วยออกใบรับรองมีหน้าที่ออกใบรับรองกุญแจสาธารณะให้กับบุคคล หน่วยงาน หรือทรัพยากรในระบบและทำหน้าที่เพิกถอนใบรับรอง

4) หน่วยรับรองบุคคล (Registration Authority หรือ RA) – หน่วยรับรองบุคคลเป็นหน่วยที่ได้รับความไว้วางใจจากหน่วยออกใบรับรองให้ทำหน้าที่ในการรวบรวมข้อมูลผู้ร้องขอใบรับรอง และตรวจสอบความมีตัวตนของผู้ขอใบรับรอง โดยหน่วยรับรองบุคคลอาจเป็นส่วนหนึ่งของหน่วยออกใบรับรองหรือเป็นหน่วยอิสระก็ได้

5) หน่วยเก็บรักษาใบรับรอง (Certificate Repository) – หน่วยเก็บรักษาใบรับรองเป็นแหล่งเก็บใบรับรองอิเล็กทรอนิกส์และรายการเพิกถอนใบรับรอง

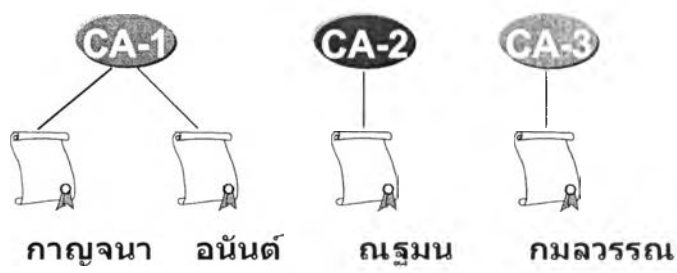
6) ผู้ใช้ใบรับรอง (Certificate User) – ผู้ใช้ใบรับรองเป็นหน่วยที่ใช้กุญแจสาธารณะของ บุคคล หน่วยงาน หรือทรัพยากรในระบบ เพื่อใช้ในกระบวนการเข้ารหัสแบบกุญแจสาธารณะ

2.2.2. สถาปัตยกรรมของหน่วยออกใบรับรอง

โดยทั่วไปสถาปัตยกรรมที่ใช้สำหรับการออกใบรับรองมักจะมีลักษณะดังสถาปัตยกรรมพื้นฐาน 3 แบบต่อไปนี้

2.2.2.1. สถาปัตยกรรมแบบหน่วยออกใบรับรองเดี่ยว (Single CA Architecture)

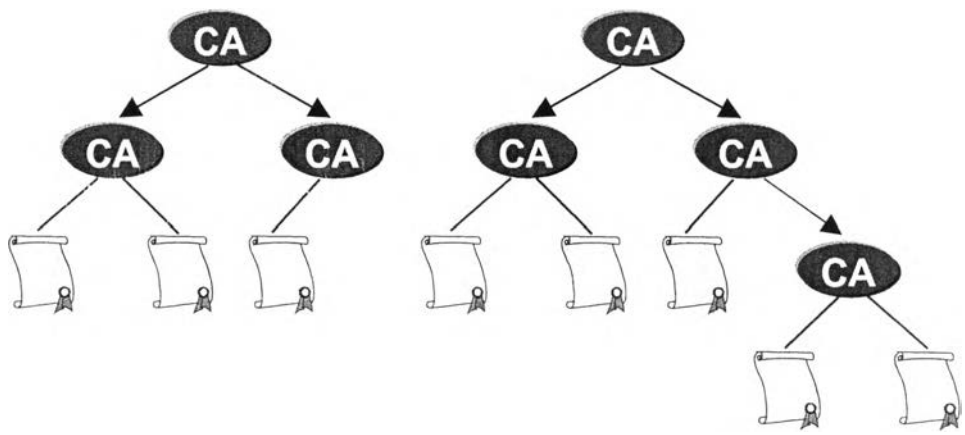
สถาปัตยกรรมแบบนี้จะมีหน่วยออกใบรับรองเพียงหน่วยเดียวดังแสดงในรูปที่ 2.6 ซึ่งทำหน้าที่ให้กับผู้ใช้งานทั้งระบบ ส่งผลให้สถาปัตยกรรมดังกล่าวมีความง่ายต่อการนำไปใช้งาน แต่มีจุดด้อยคือขาดความสามารถในการรองรับการขยายระบบเพื่อสนับสนุนระบบที่มีขนาดใหญ่[6][7][8][9]



รูปที่ 2.6 สถาปัตยกรรมแบบหน่วยออกใบรับรองเดี่ยว

2.2.2.2. สถาปัตยกรรมแบบจัดลำดับชั้น (Hierarchical Architecture)

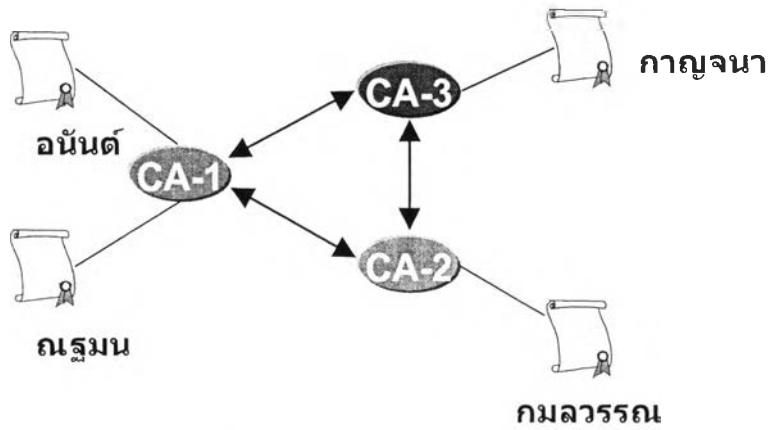
สถาปัตยกรรมแบบนี้จะมีหน่วยออกใบรับรองหลายหน่วย โดยมีหน่วยหนึ่งทำหน้าที่เป็น Root CA และมีลักษณะการเชื่อมโยงในลักษณะทิศทางเดียวดังแสดงในรูปที่ 2.7 สถาปัตยกรรมดังกล่าวมีจุดเด่นในด้านความสามารถในการขยายระบบที่ดี เส้นทางของใบรับรองจะสั้น ง่ายต่อการค้นหาเส้นทางใบรับรองเนื่องจากมีลักษณะการเชื่อมต่อแบบทิศทางเดียว อย่างไรก็ดีสถาปัตยกรรมดังกล่าวยังมีจุดด้อยคือหากกุญแจส่วนตัวของ Root CA ถูกเปิดเผยจะทำให้ทั้งระบบขาดความน่าเชื่อถือ นอกจากนี้การจัดสร้างสถาปัตยกรรมแบบนี้อาจเป็นไปได้ยากในทางปฏิบัติ รวมถึงการเชื่อมโยงโครงสร้างที่มีอยู่แล้วหลายระบบเข้าหากันเพื่อเปลี่ยนมาเป็นสถาปัตยกรรมแบบนี้อาจเป็นไปได้ยากเช่นเดียวกัน[6][7][8][9]



รูปที่ 2.7 สถาปัตยกรรมแบบจัดลำดับชั้น

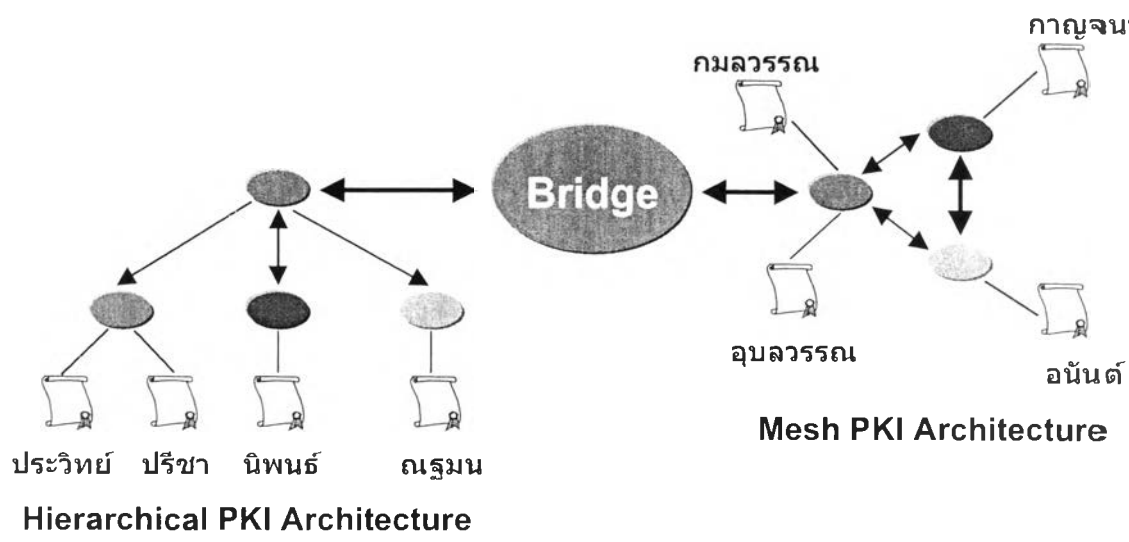
2.2.2.3. สถาปัตยกรรมแบบตาข่าย (Mesh Architecture)

สถาปัตยกรรมแบบนี้มีหน่วยออกใบรับรองหลายหน่วย และเชื่อมโยงกันในลักษณะสองทิศทางดังแสดงในรูปที่ 2.8 สถาปัตยกรรมดังกล่าวมีจุดเด่นคือง่ายต่อการจัดสร้าง ทนทานต่อความเสียหายของระบบ และง่ายต่อการปรับเปลี่ยนระบบหากหน่วยออกใบรับรองหน่วยใดขาดความน่าเชื่อถือ และมีจุดด้อยคือการสร้างเส้นทางใบรับรองเป็นเรื่องซับซ้อนเนื่องจากการเชื่อมโยงมีลักษณะเป็นสองทิศทาง[6][7][8][9]



รูปที่ 2.8 สถาปัตยกรรมแบบตาข่าย

นอกจากสถาปัตยกรรมพื้นฐานทั้ง 3 แบบ ทางรัฐบาลสหรัฐได้มีความพยายามคิดค้นสถาปัตยกรรมใหม่ ๆ เพื่อให้มีความเหมาะสมกับโลกแห่งความเป็นจริงมากยิ่งขึ้น โดยได้คิดค้นและทดลองใช้สถาปัตยกรรมแบบใหม่ชื่อ Bridge Certificate Authority (BCA) [6] ดังแสดงในรูปที่ 2.9 ซึ่งมีความแตกต่างจากสถาปัตยกรรมแบบตาข่ายที่ BCA ไม่ได้ทำหน้าที่เป็นหน่วยออกใบรับรอง เป็นแต่เพียงจุดเชื่อมต่อของหลาย ๆ โครงสร้าง สถาปัตยกรรมดังกล่าวมีความซับซ้อนในการหาเส้นทางใบรับรองน้อยกว่าสถาปัตยกรรมแบบตาข่าย แต่ซับซ้อนมากกว่าสถาปัตยกรรมแบบจัดลำดับชั้น



รูปที่ 2.9 สถาปัตยกรรมแบบ Bridge