ดร.อาณัติ ลีมัคเดช
ผู้ช่วยศาสตราจารย์ประจำภาควิชาการเงิน
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
กรรมการผู้ทรงคุณวุฒิ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

Trust Model และ รูปแบบการกำกับผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ในประเทศไทย

[บทคัดย่อ]

บทความนี้ทำการสำรวจรูปแบบของบริการผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ หรือ Certificate Authority (CA) ในประเทศไทย 3 ราย โดยทำการเปรียบเทียบระเบียบวิธีปฏิบัติของแต่ละรายในการให้บริการใบรับรองอิเล็กทรอนิกส์ รวมทั้งการนำไปเทียบกับวิธีการปฏิบัติของ Verisign ซึ่งเป็น CA ที่ผู้ใช้บริการมากที่สุดในปัจจุบัน แม้ว่า CA จะเป็นองค์ประกอบสำคัญของการทำพาณิชย์อิเล็กทรอนิกส์ แต่ประเทศไทยยังขาดระบบการรับรองร่วมกันระหว่าง CA แต่ละราย รวมทั้งรูปแบบการกำกับที่ชัดเจนจากภาครัฐ เพื่อสร้างความเชื่อมั่นและความสะดวกแก่ผู้ใช้บริการ บทความนี้ได้เสนอรูปแบบของ Trust Model 5 รูปแบบ เพื่อเป็นแนวทางการสร้างระบบการรับรองร่วมกันระหว่าง CA การสำรวจของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเห็นว่ารูปแบบหนึ่งของ Trust Model คือ Root CA เป็นรูปแบบที่ผู้ใช้เห็นว่ามีความเหมาะสมกับประเทศไทย นอกจากนั้นยังสนับสนุนให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้ทำหน้าที่ Root CA ของประเทศไทย

ผู้เขียนขอขอบคุณ ผู้ช่วยวิจัย คุณปรารถนา อมรฉัตร บริษัท เวโลคอล (ประเทศไทย) จำกัด ในการค้นหาข้อมูลและประสานงาน

1. ภาพรวม

การใช้งานอินเทอร์เน็ตในระยะเริ่มแรกนั้น ไม่ได้เน้นพัฒนาด้านระบบรักษาความปลอดภัยของข้อมูลบนเครือข่ายมากนัก เนื่องจากในช่วงนั้นเครือข่ายอินเตอร์เน็ต ถูกใช้ในการติดต่อสื่อสารระหว่างกลุ่มนักวิจัยในมหาวิทยาลัยและสถาบันต่างๆ ไม่กี่กลุ่ม ซึ่งมีความรู้จักคุ้นเคยกันและมีความเชื่อถือต่อกันและกัน ดังนั้นข้อมูลที่รับ - ส่งบนเครือข่ายอินเตอร์เน็ต จึงเป็นลักษณะของข้อมูลที่ไม่มีการเข้ารหัสลับใดๆ หรือที่เรียกกันว่า Cleartext แต่เมื่อเครือข่ายอินเทอร์เน็ตถูกนำมาใช้งานในเชิงพาณิชย์มากขึ้นตั้งแต่ พ.ศ. 2536 เป็นต้นมา การติดต่อสื่อสารขยายวงกว้างจึงเกิดความจำเป็นในการพัฒนาการสื่อสารบนเครือข่ายอินเทอร์เน็ตที่มีความปลอดภัยมากขึ้น

พ.ศ. 2537 บริษัท Netscape ซึ่งเป็นผู้พัฒนาโปรแกรมเว็บบราวเซอร์ได้คิดค้นมาตรฐานในการส่งข้อมูลแบบปลอดภัยบนเครือข่ายอินเทอร์เน็ตเรียกว่า Secure Socket Layer (SSL) ซึ่งเป็นการเข้ารหัสข้อมูลบนเครื่องคอมพิวเตอร์ของผู้ส่งก่อนที่ข้อมูลจะถูกส่งไปยังเครือข่ายอินเตอร์เน็ต ดังนั้นหากมีผู้ดักจับข้อมูลเหล่านั้น ก็จะไม่สามารถอ่านได้ เพราะเฉพาะผู้รับข้อมูลปลายทางที่ถูกระบุเท่านั้น จึงจะสามารถถอดรหัสข้อมูลเหล่านั้นได้

การพัฒนา SSL ก่อให้เกิดรูปแบบของพาณิชย์อิเล็กทรอนิกส์ในลักษณะร้านค้าที่สามารถรับคำสั่งซื้อและรับชำระเงินจากลูกค้าได้เลย จากเดิมซึ่งเป็นเพียงการแสดงภาพรายการสินค้า และยังคงใช้ช่องทางปกติในการสั่งซื้อสินค้าเท่านั้น เนื่องจากผู้ซื้อมีความมั่นใจในการส่งข้อมูลที่เป็นความลับเช่นหมายเลขบัตรเครดิตให้แก่ผู้ขายผ่านเครือข่ายอินเทอร์เน็ตเพื่อชำระเงินมากขึ้น เว็บไซต์พาณิชย์อิเล็กทรอนิกส์สำคัญ เช่น Amazon.com และ eBay.com กำเนิดขึ้นใน พ.ศ. 2538 และได้รับความนิยมอย่างรวดเร็ว

การเข้ารหัสและถอดรหัสข้อมูลภายใต้ระบบ SSL นั้น ถูกพัฒนาภายใต้เทคโนโลยีที่เรียกว่ากุญแจแบบอสมมาตร (Asymmetric Key) กล่าวคือผู้ใช้งานจะมีกุญแจ 2 ชุด คือ กุญแจส่วนตัว (Private Key) และ กุญแจสาธารณะ (Public Key) เมื่อใช้กุญแจใดเข้ารหัสข้อมูลแล้ว จะต้องใช้กุญแจอีกอันหนึ่งถอดรหัสข้อมูลเท่านั้น ไม่สามารถใช้กุญแจอันเดียวกันเข้ารหัสและถอดรหัสได้ การสร้างกุญแจอสมมาตรนี้จะมีวิธีการทางคณิตศาสตร์ที่มั่นใจได้ว่าผู้ใช้งานไม่สามารถหาวิธีสร้างกุญแจอันหนึ่งขึ้นมาโดยทราบข้อมูลของกุญแจอีกอันหนึ่งได้ ภาคผนวก ก จะให้รายละเอียดเพิ่มเติมของระบบกุญแจอสมมาตร เปรียบเทียบกับระบบกุญแจสมมาตร

บริษัท Netscape ได้นำ SSL มาใช้ในการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ต โดยใช้หลักการที่ว่าเว็บไซต์ที่เป็นผู้รับข้อมูลนั้นจะมีการสร้างกุญแจอสมมาตรขึ้นมา และเผยแพร่กุญแจสาธารณะของตน ในขณะที่เก็บกุญแจส่วนตัวของตนนั้นเป็นความลับ เมื่อมีผู้ต้องการส่งข้อมูลมาที่เว็บไซต์นี้ ผู้ส่งข้อมูลจะเรียกกุญแจสาธารณะของเว็บไซต์นั้นมาเข้ารหัสข้อมูลที่ส่ง ดังนั้นข้อมูลที่ส่งออกจากเครื่องคอมพิวเตอร์สู่เครือข่ายอินเทอร์เน็ตขณะนี้จึงถูกเข้ารหัสเรียบร้อยแล้ว และจะถูกถอดรหัสได้โดยใช้กุญแจส่วนตัวของเว็บไซต์ที่ผู้ส่งต้องการเท่านั้น หากมีผู้ดักจับข้อมูลที่เข้ารหัสนี้บนเครือข่ายอินเทอร์เน็ตได้ ก็จะไม่สามารถอ่านข้อมูลได้ เพราะไม่มีกุญแจส่วนตัวของเว็บไซต์นั่นเอง

อย่างไรก็ตาม จุดอ่อนสำคัญของระบบนี้คือการเผยแพร่กุญแจสาธารณะบนเครือข่ายอินเทอร์เน็ตนั้น ใครก็สามารถสร้างกุญแจอสมมาตรขึ้นมาและอ้างตนเองเป็นบุคคลอื่นได้ ดังนั้นความมั่นคงของระบบจึงจำเป็นต้องเกิดรูปแบบของการให้ความไว้วางใจหรือ Trust Model ขึ้นเพื่อสร้างความเชื่อมั่นระหว่างผู้รับ - ส่งข้อมูล Trust Model มีหลากหลายรูปแบบ ซึ่งพอจะจำแนกเป็นกลุ่มใหญ่ๆ ได้สองกลุ่ม

กลุ่มที่หนึ่ง คือรูปแบบ Peer - to - Peer Network นั่นคือผู้ที่สื่อสารกันในกลุ่มจะรับรองกันเอง เช่น ก รู้จักกับ ข และ ค และให้การรับรองว่าผู้ถือกุญแจสาธารณะที่อ้างตนเป็น ข และ ค นั้นเป็นบุคคลตามที่กล่าวอ้างจริง ต่อมา เมื่อ ข และ ค สื่อสารกันก็จะเชื่อถือว่ากำลังติดต่อกับบุคคลที่กล่าวอ้างจริง เพราะทั้งคู่เชื่อถือ ก ทั้ง ข และ ค อาจรู้จักคนอื่นเพิ่มเติมอีก เมื่อให้การรับรองผู้ใด ผู้ที่สื่อสารในเครือข่ายนั้นก็จะเชื่อถือกันโดยอัตโนมัติ รูปแบบนี้มักใช้กับเทคโนโลยีการสื่อสารระบบเปิดเช่น Pretty Good Privacy (PGP)

กลุ่มที่สอง คือรูปแบบ Certificate Authority (CA) ในรูปแบบนี้จะเป็นการรับรองโดยผ่านบุคคลที่สามที่ทุกคนเชื่อถือ นั่นคือ CA โดย CA จะต้องตรวจสอบตัวตนของผู้ขอการรับรองอย่างละเอียด เนื่องจาก CA จะมีข้อผูกพันทางกฎหมายหากรับรองผิดคน

จะเห็นว่ารูปแบบที่สองนั้นจะมีความน่าเชื่อถือมากกว่ารูปแบบที่หนึ่ง เพราะมีการตรวจสอบตัวตน และมีข้อผูกมัดทางกฎหมายหากมีการรับรองผิดคน จึงเหมาะกับการทำธุรกรรมในวงกว้างมากกว่ากลุ่มแรก ซึ่งทิศทางการพัฒนา Trust Model ของทุกประเทศจะเป็นในรูปแบบนี้มากกว่า เราอาจเรียกรูปแบบนี้ว่า Public Key Infrastructure หรือ PKI ซึ่งสามารถเขียนเป็นความสัมพันธ์ได้ว่า

PKI = Asymmetric Key + CA

ภายใต้ระบบนี้ เมื่อเว็บไซต์สร้างกุญแจอสมมาตรของตนเองขึ้นมาแล้ว จะส่งกุญแจสาธารณะของตนไปให้ CA ทำการรับรอง ในกระบวนการรับรองนี้ CA จะต้องทำการตรวจสอบด้วยวิธีการต่างๆ ให้แน่ใจได้ว่ากุญแจสาธารณะที่ผู้ขอทำการรับรองส่งมานั้น เป็นของตนเองตามที่กล่าวอ้างจริง เมื่อตรวจสอบแล้ว CA จะนำกุญแจส่วนตัวของตนเข้ารหัสกุญแจสาธารณะของเว็บไซต์แล้วนำไปเผยแพร่ผ่านเครื่องคอมพิวเตอร์บนเครือข่ายอินเทอร์เน็ตของ CA เพื่อให้ผู้ใช้ทั่วไปที่ต้องการส่งข้อมูลไปให้เว็บไซต์นั้นขอกุญแจสาธารณะมาเข้ารหัสได้ ภายใต้ระบบ PKI นี้ จะเห็นว่าผู้ขอกุญแจสาธารณะมั่นใจได้ว่ากุญแจสาธารณะนั้นเป็นของเว็บไซต์หรือบุคคลที่กล่าวอ้างจริง เพราะเชื่อถือใน CA ที่รับรองกุญแจสาธารณะนั้น เราอาจเรียกกุญแจสาธารณะที่ CA รับรอง และเผยแพร่บนเครือข่ายอินเทอร์เน็ตนี้ว่า **"ใบรับรองอิเล็กทรอนิกส์"** ได้

บทบาทของ CA จึงนับว่ามีความสำคัญอย่างสูงต่อการทำธุรกรรมแบบอิเล็กทรอนิกส์ทั้งบนเครือข่ายอินเทอร์เน็ตและนอกเครือข่ายอินเทอร์เน็ตมาก กฎหมายที่รับรองการทำธุรกรรมอิเล็กทรอนิกส์ประเทศต่างๆ รวมทั้งประเทศไทย ซึ่งมี พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ให้การยอมรับต่อการใช้ระบบ PKI ในการระบุตัวตนของผู้ที่เกี่ยวข้องกับธุรกรรมอิเล็กทรอนิกส์ และล้วนมีบทบัญญัติในการควบคุมกิจกรรมของ CA

อย่างไรก็ตาม ในประเทศหนึ่งสามารถมี CA มากกว่าหนึ่งราย เพื่อให้การสื่อสารสามารถเกิดขึ้นในวงกว้าง CA จะต้องมี Trust Model เพื่อทำการรับรองซึ่งกันและกัน บทความนี้จะเน้นศึกษาในเรื่อง Trust Model ระหว่าง CA โดยเปรียบเทียบ Trust Model รูปแบบต่างๆ

บทความนี้แบ่งเป็น 5 ส่วน ในส่วนถัดไปจะกล่าวถึง CA สำคัญในประเทศไทย โดยเน้นที่ CA ที่ดำเนินการโดยบริษัทที่มีรัฐบาลเกี่ยวข้องในฐานะผู้ถือหุ้นใหญ่ ในส่วนที่ 3 จะเปรียบเทียบระเบียบวิธีปฏิบัติของ CA ในการตรวจสอบและรับรองกุญแจสาธารณะ ส่วนที่ 4 นำเสนอผลสำรวจความคิดเห็นของข้าราชการต่อรูปแบบการกำกับ CA ในประเทศไทย และสรุปด้วยบทวิเคราะห์

2. ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ (CA) ในประเทศไทย

ปัจจุบันประเทศไทยมีผู้ให้บริการใบรับรองอิเล็กทรอนิกส์เชิงพาณิชย์ไม่มากนัก[1] ในบทความนี้จะจำกัดการศึกษาเฉพาะผู้ให้บริการรายใหญ่ 3 ราย ซึ่งแต่ละผู้ให้บริการ มีผลิตภัณฑ์ที่แตกต่างกันไป ดังนี้

2.1 บมจ. ทีโอที (TOT) แบ่งการให้บริการออกเป็น 3 ประเภท ได้แก่

2.1.1 TOT CA SSL : ออกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Sever) หรือเว็บไซต์เพื่อใช้ในการรับรองและรักษาความปลอดภัยของข้อมูลในการรับส่งข้อมูลให้กับ Server

2.1.2 TOT CA Standard : ออกให้กับบุคคลทั่วไปหรือนิติบุคคล เพื่อใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ และการเข้ารหัสข้อมูลในการรับส่งข้อมูลผ่านทางอินเตอร์เน็ต

2.1.3 TOT CA Mail : ออกให้กับบุคคลทั่วไปหรือนิติบุคคลเพื่อใช้ในการลงรายมือชื่ออิเล็กทรอนิกส์บน E - Mail

2.2 บมจ. กสท โทรคมนาคม (CAT) แบ่งการให้บริการออกเป็น 3 ประเภท ได้แก่

2.2.1 Personal Certificate : ออกให้กับบุคคลธรรมดาหรือนิติบุคคล

[1] นอกจากผู้ให้บริการใบรับรองอิเล็กทรอนิกส์เชิงพาณิชย์ ประเทศไทยยังมี CA ที่สร้างระบบขึ้นใช้งานกับหน่วยงานที่เกี่ยวข้องเอง เช่น ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน ซึ่งอยู่นอกเหนือการพิจารณาในบทความนี้

2.2.2 Enterprise Certificate : ออกให้กับบุคคลธรรมดาหรือนิติบุคคล

2.2.3 VPN Certificate : ให้การรับรองอุปกรณ์ที่ใช้ในการรับ-ส่งข้อมูลแบบปลอดภัย เช่น เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์ Router หรือ Firewall เพื่อให้แน่ใจว่าอุปกรณ์ดังกล่าวเป็นของบุคคลหรือนิติบุคคลที่กล่าวอ้างจริง

2.3 สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (GITS)

2.3.1 Personal Certificate Service : ออกให้กับบุคคลธรรมดา

2.3.2 Web Server Certification Service : ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องให้บริการเว็บ สำหรับสร้างช่องทางสื่อสารแบบปลอดภัยระหว่างเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server) และเครื่องใช้บริการ (Client)

2.3.3 CA Hosting / Virtual CA Service : บริการรับฝากระบบบริการใบรับรองอิเล็กทรอนิกส์ เป็นบริการที่ทางหน่วยงานภาครัฐดำเนินการเป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

3. วิธีปฏิบัติของผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ในประเทศไทย

ตามที่ได้กล่าวในส่วนที่หนึ่งว่าระบบ PKI นั้น ไม่ได้หมายถึงการเข้ารหัสด้วยกุญแจอสมมาตรแต่เพียงอย่างเดียว ความมั่นคงของระบบนี้ขึ้นกับ CA ที่ผู้ใช้ระบบทุกคนเชื่อถือว่าจะทำการตรวจสอบกุญแจสาธารณะที่รับรองว่าเป็นของบุคคลหรือเว็บไซต์ที่ขอรับรองจริง

ในการดำเนินธุรกิจของ CA จะเกี่ยวข้องกับกิจกรรมที่สำคัญ 5 กิจกรรม ได้แก่

1. การตรวจสอบตัวบุคคลหรือเว็บไซต์ที่ขอรับการรับรอง CA จะต้องมีวิธีการที่เชื่อถือได้ว่าผู้ขอรับการรับรองนั้นเป็นบุคคลตามที่กล่าวอ้างจริง

2. การสร้างกุญแจอสมมาตร การรับรองเว็บไซต์นั้น ผู้ขอรับการรับรองจะมีเจ้าหน้าที่เทคนิกที่มีความรู้สามารถสร้างกุญแจอสมมาตรเองได้ และส่งเฉพาะกุญแจสาธารณะมาให้ CA รับรอง กิจกรรมด้านนี้ของ CA จึงไม่ค่อยน่าเป็นห่วงเท่าไร เพราะหากมีการรั่วไหลของกุญแจส่วนตัว จะต้องเกิดจากฝั่งของผู้ขอรับการรับรองเท่านั้น แต่ในการรับรองบุคคล ซึ่งส่วนใหญ่ขาดความรู้ที่จะสร้างกุญแจอสมมาตรเอง CA จะต้องเป็นผู้สร้างให้ทั้งกุญแจส่วนตัว และกุญแจสาธารณะ CA จะต้องมีวิธีการสร้างความมั่นใจได้ว่าจะไม่มีการทำสำเนากุญแจส่วนตัวที่สร้างขึ้นไว้นี้ด้วยวิธีการใดๆ ทั้งสิ้น

3. การเผยแพร่กุญแจ CA จะต้องนำกุญแจสาธารณะที่ตนเองรับรอง ด้วยการเข้ารหัสด้วยกุญแจส่วนตัวของตน ไปเผยแพร่บนเครื่องคอมพิวเตอร์ซึ่งผู้ใช้สามารถเรียกใช้งานเพื่อทำการตรวจสอบ หรือใช้เข้ารหัสข้อมูล และเครื่องคอมพิวเตอร์นี้ต้องสามารถเข้าถึงโดยมาตรฐานที่ได้รับการยอมรับได้ (โดยส่วนใหญ่ใช้มาตรฐาน LDAP)

4. การเพิกถอนใบรับรองอิเล็กทรอนิกส์ เมื่อมีเหตุสงสัยว่ากุญแจส่วนตัวของตนรั่วไหลหรือสูญหาย เจ้าของจะต้องรีบแจ้ง CA เพื่อให้ทำการยกเลิกใบรับรองอิเล็กทรอนิกส์สำหรับกุญแจส่วนตัวนั้น ในกิจกรรมนี้ CA จะต้องมีวิธีการที่น่าเชื่อถือว่าจะสามารถรับแจ้งข้อมูลการขอเพิกถอนจากเจ้าของใบรับรองฯตัวจริง และสามารถนำรายการที่เพิกถอนแล้วเผยแพร่บนเครื่องคอมพิวเตอร์ที่สามารถเข้าถึงผ่านเครือข่ายอินเทอร์เน็ตได้ในเวลาที่รวดเร็ว

5. การต่ออายุใบรับรองอิเล็กทรอนิกส์ ใบรับรองอิเล็กทรอนิกส์ส่วนใหญ่มีอายุเพียง 1 ปี เมื่อครบกำหนดแล้ว CA จะต้องกำหนดระเบียบวิธีปฏิบัติว่าจะตรวจสอบตัวตนผู้ขอต่ออายุใบรับรองให้มั่นใจได้ว่าเป็นบุคคลนั้นจริง

CA จะระบุวิธีการปฏิบัติของตนต่อกิจกรรมทั้ง 5 ด้านนี้ไว้ใน CPS (Certificate Practice Statement) ซึ่งสามารถเรียกดูได้จากเว็บไซต์ของผู้ให้บริการ CPS ที่แต่ละ CA ใช้จะเป็นหัวใจสำคัญในการสร้างระบบ Trust Model ของแต่ละ CA เพราะ CPS ที่ใช้ควรจะมีการปฏิบัติที่รัดกุมใกล้เคียงกัน มิฉะนั้น CA ที่มีข้อปฏิบัติทาง CPS ที่ผ่อนคลาย จะทำให้ความเชื่อมั่นในระบบน้อยลง และเป็นข้ออ้างให้ CA รายอื่นไม่ต้องการเข้าสู่ระบบเพื่อรับรองข้าม CA กันด้วย

ตารางที่ 1 เปรียบเทียบ CPS ของผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ในไทย 3 ราย และบริษัท Verisign ซึ่งเป็น CA ที่มีผู้ใช้บริการมากที่สุดในโลก

ตารางที่ 1 เปรียบเทียบ CPS ของ TOT, CAT, GITS และ Verisign

	การตรวจสอบ	การสร้างกุญแจ	การเผยแพร่ข้อมูล	การเพิกถอนใบรับรอง	การต่ออายุใบรับรอง
TOT	การขอใบรับรองต้องทำด้วยตนเอง - กรอกข้อมูลเพื่อขอใบรับรองและแนบเอกสารประกอบการขอ ได้แก่ สำเนาบัตรประจำตัวประชาชนหรือเอกสารทางราชการที่มีรูปถ่ายผู้ขอใช้บริการ - ระบุรูปแบบของการขอจัดเก็บว่าต้องการแบบ Smart Card หรือ Diskette - ลงลายมือชื่อรับรองเอกสาร - ผู้ขอออกใบรับรอ ใส่ PIN สำหรับรักษาความปลอดภัยของ Private Key	- การออกรหัสกุญแจและใบรับรองทำขึ้นในเครื่องของ ทศท. โดยพนักงานของ ทศท. โดยมีตัวแทนที่ได้รับอนุญาต ทศท. เป็นพยานเมื่อมีการทำรหัสกุญแจ, ใบรับรอง และรับผิดชอบในการข้อมูลทั้งหมดเข้าสู่ระบบการให้บริการ - ใบรับรองอิเล็กทรอนิกส์ในรูปแบบของ Smart Card หรือ Diskette โดย Smart Card มีอายุการใช้งาน 2 ปี และในรูปแบบ Diskette มีอายุการใช้งาน 1 ปี	- ประกาศนโยบายการออกใบรับรองและ CPS บนเว็บไซต์ ทศท. เท่านั้น - มี LDAP Server	- แจ้งผู้ออกใบรับรองทางโทรศัพท์และทำเป็นลายลักษณ์อักษรภายใน 48 ชั่วโมง นับแต่การแจ้งทางโทรศัพท์	- ผู้ออกใบรับรองต้องแจ้งล่วงหน้าเป็นหนังสือ และ/หรือ โดยวิธีการทางอิเล็กทรอนิกส์ไม่น้อยกว่า 30 วันก่อนครบอายุการใช้งาน
CAT	สามารถลงทะเบียนได้ 2 ทาง - เว็บไซต์ http://catca.cattelecom.com กรอกแบบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล - ยื่นเอกสารและหลักฐานแก่เจ้าหน้าที่รับลงทะเบียน ได้แก่ สำเนาบัตรประจำตัวราชการหรือสำเนาบัตรประชาชนและหนังสือรับรองการทำงาน*	- ผู้ให้บริการบันทึกข้อมูลผู้ขอใช้บริการลงไดเร็กทอรี และระบบจะส่งรหัสผ่านเริ่มต้น (One time Password) และรหัสติดตั้ง (มีอายุการใช้งาน 14 วัน) ผ่านทางจดหมายอิเลกทรอนิกส์ - เข้าเว็บไซต์ http://catca.cattelecom.com เพื่อกรอกรหัสอ้างอิงและรหัสติดตั้ง จากนั้นทำการตรวจสอบข้อมูลที่ปรากฏในใบรับรอง	- ทำการเผยแพร่ข้อมูลผ่านทางเว็บไซต์ CAT CA http://catca.cattelecom.com - มี LDAP Server	สามารถทำได้ 2 ทาง 1. แจ้งเพิกถอนแบบออนไลน์ โดยเข้าเว็บไซต์ http://catca.cattelecom.com 2. กรอกแบบคำขอเพิกถอน โดยพิมพ์แบบคำขอเพิกถอนพร้อมลงลายมือชื่อกำกับ** ** ผู้ให้บริการออกใบรับรองจะดำเนินการเมื่อได้รับคำขอเพิกถอนจากผู้ใช้บริการหรือเจ้าหน้าที่รับลงทะเบียน หรือได้	- ผู้ออกใบรับรองต้องแจ้งล่วงหน้าเป็นหนังสือ และ/หรือ โดยวิธีการทางอิเล็กทรอนิกส์ไม่น้อยกว่า 30 วันก่อนครบอายุการใช้งาน

	การตรวจสอบ	การสร้างกุญแจ	การเผยแพร่ข้อมูล	การเพิกถอนใบรับรอง	การต่ออายุใบรับรอง
CAT	* กรณีแบบคำขอสมัครใช้บริการแบบกระดาษ (ไม่ได้กรอกผ่านทางเว็บไซต์) เจ้าหน้าที่รับลงทะเบียนจะเป็นผู้ดำเนินการกรอกรายละเอียดต่างๆ ของผู้ขอใช้บริการ ทั้งนี้ผู้ขอใช้บริการจำเป็นต้องทำการลงลายมือชื่อในแบบคำขอที่เจ้าหน้าที่รับลงทะเบียนเป็นผู้พิมพ์ด้วย	- ระบบจะทำการสร้างกุญแจคู่โดยเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการจะบันทึกและเก็บข้อมูลอิเล็กทรอนิกส์ของกุญแจส่วนตัว และส่งของมูลอิเล็กทรอนิกส์ของกุญแจสาธารณะไปยังระบบให้บริการของ CAT โดยอัตโนมัติ - ใบรับรองอิเล็กทรอนิกส์มี 2 รูปแบบของ Diskette, CD-Rom หรือ Smart Card โดยมีอายุการใช้งาน 1 ปี		รับคำสั่งโดยชอบด้วยกฎหมายโดยแจ้งเป็นลายลักษณ์อักษรภายใน 48 ชั่วโมง	
GITS	- เข้าไปกรอกข้อมูลที่เว็บไซต์ http://gca.thaigov.net - กรอกข้อมูลทั้งหมดและทำการพิมพ์แบบฟอร์ม นำแบบคำขอสมัครใช้บริการใบรับรองอิเล็กทรอนิกส์และลงลายมือชื่อในแบบคำขอ พร้อมแนบหลักฐานการสมัคร ได้แก่ สำเนาบัตรประจำตัวประชาชนพร้อมหนังสือรับรองการเป็นพนักงานมาส่งยังเจ้าหน้าที่รับลงทะเบียน	- ผู้ให้บริการบันทึกข้อมูลผู้ขอใช้บริการลงไดเร็กทอรี และระบบจะส่งรหัสผ่านเริ่มต้น (One time Password) และรหัสติดตั้ง (มีอายุการใช้งาน 14 วัน) ผ่านทางไปรษณีย์อิเล็กทรอนิกส์ - เข้าเว็บไซต์ http://gca.thaigov.net เพื่อกรอกรหัสอ้างอิงและรหัสติดตั้ง จากนั้นทำการตรวจสอบข้อมูลที่ปรากฏในใบรับรอง - ระบบจะทำการสร้างกุญแจคู่โดยเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการจะบันทึกและเก็บข้อมูลอิเล็กทรอนิกส์ของกุญแจ	การเผยแพร่ข้อมูลผ่านทางเว็บไซต์ของ G-CA http://gca.thaigov.net - มี LDAP Server	- เข้าไปที่เว็บไซต์ http://gca.thaigov.net เพื่อกรอกข้อมูลและพิมพ์แบบฟอร์มใบเพิกถอน นำไปส่งยังเจ้าหน้าที่รับลงทะเบียน จะมีผลการเพิกถอนใบรับรองภายใน 2 วัน - กรณีที่ไม่สามารถเข้าระบบได้ สามารถติดต่อมายังผู้ให้บริการทางโทรศัพท์ เพื่อดำเนินการขอเพิกถอนใบรับรอง โดยผู้ให้บริการจะมีกระบวนการตรวจสอบข้อมูลส่วนตัวเพื่อยืนยันผู้ใช้ และต้องนำแบบฟอร์มการเพิกถอนใบรับรองมายื่นในภายหลัง	- ผู้ออกใบรับรองต้องแจ้งล่วงหน้าเป็นหนังสือ และ/หรือโดยวิธีการทางอิเล็กทรอนิกส์ ไม่น้อยกว่า 30 วันก่อนครบอายุการใช้งาน

	การตรวจสอบ	การสร้างกุญแจ	การเผยแพร่ข้อมูล	การเพิกถอนใบรับรอง	การต่ออายุใบรับรอง
		ส่วนตัวและส่งของมูลอิเล็กทรอนิกส์ของกุญแจสาธารณะไปยังระบบให้บริการของ G-CA โดยอัตโนมัติ - ใบรับรองอิเล็กทรอนิกส์มี 2 รูปแบบของ Diskette, CD-Rom หรือ Smart Card โดยมีอายุการใช้งาน 1 ปี			
Verisign	ผู้สมัครขอใช้บริการสามารถขอรับบริการผ่านเว็บไซต์ได้ แต่จะต้องส่งเอกสารราชการที่เกี่ยวกับการระบุตัวตนของตนเองให้ Verisign ตรวจสอบก่อน ในกรณีนิติบุคคล ต้องส่งเอกสารแสดงการจดทะเบียน วัตถุประสงค์การประกอบการ ทั้งนี้ Verisign อาจรอขอเอกสารเพิ่มเติมเพื่อการตรวจสอบได้อีก	จะเป็นผู้สร้างกุญแจคู่ให้กับทางผู้ขอใช้บริการใบรับรองอิเล็กทรอนิกส์ ในสื่อรูปแบบต่างๆ ในกรณีการรับรองเว็บไซต์ ผู้ขอรับการรับรองจะสร้างกุญแจอสมมาตรด้วยตนเอง แล้วส่งเฉพาะกุญแจสาธารณะให้ Verisign รับรอง ปัจจุบัน Verisign รับรองเว็บไซต์ราว 500,000 เว็บไซต์	- จะเผยแพร่ข้อมูลที่ถูกเก็บเอาไว้ผ่านเว็บไซต์ http://www.verisign.com/repository/ - ระบบสามารถตรวจสอบใบรับรองอัตโนมัติผ่าน LDAP Server ได้	- ผู้ให้บริการจะไม่อนุญาตให้ผู้ใช้บริการที่ถูกเพิกถอนเข้าสู่ข้อมูลที่ถูกเพิกถอนหรือข้อมูลที่เกี่ยวกับใบรับรองโดยปราศจากการยินยอมของผู้ให้บริการเป็นลายลักษณ์อักษร - ผู้ใช้บริการต้องร้องขอคำเพิกถอนกับผู้ให้บริการสำหรับ Managed PKI Customer ผู้ใช้บริการจะต้องติดต่อกับเจ้าหน้าที่ฝ่ายเอกสารของ Managed PKI เพื่อขอยกเลิก	- ผู้ออกใบรับรองต้องแจ้งล่วงหน้าภายใน 30 วันก่อนหรือหลังวันที่ใบรับรองหมดอายุโดยวิธีการทางอิเล็กทรอนิกส์ - หากเกิน 30 วันหลังจากหมดอายุ ผู้ออกใบรับรองจะแจ้งโดยวิธีการทางอิเล็กทรอนิกส์

4. Trust Model ของการรับรองข้าม CA

การติดต่อสื่อสารโดยใช้ใบรับรองอิเล็กทรอนิกส์ที่ออกโดยต่างผู้ให้บริการกันมักจะพบปัญหาเรื่องความเชื่อถือ เพราะทุกผู้ให้บริการต่างมีมาตรฐานของตัวเองที่ต่างกัน ทำให้บางครั้งผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการต่างกันทำการติดต่อกัน เกิดปัญหาขึ้น กล่าวคือไม่สามารถยืนยันตัวตนที่แท้จริงได้ เพราะไม่มีข้อมูลของผู้ใช้บริการที่ออกโดยผู้ให้บริการอีกราย เพื่อแก้ปัญหาดังกล่าวจึงต้องมีการสร้างความสัมพันธ์ขึ้น โดยรูปแบบการเชื่อมโยงแบ่งเป็น 5 ประเภทหลัก

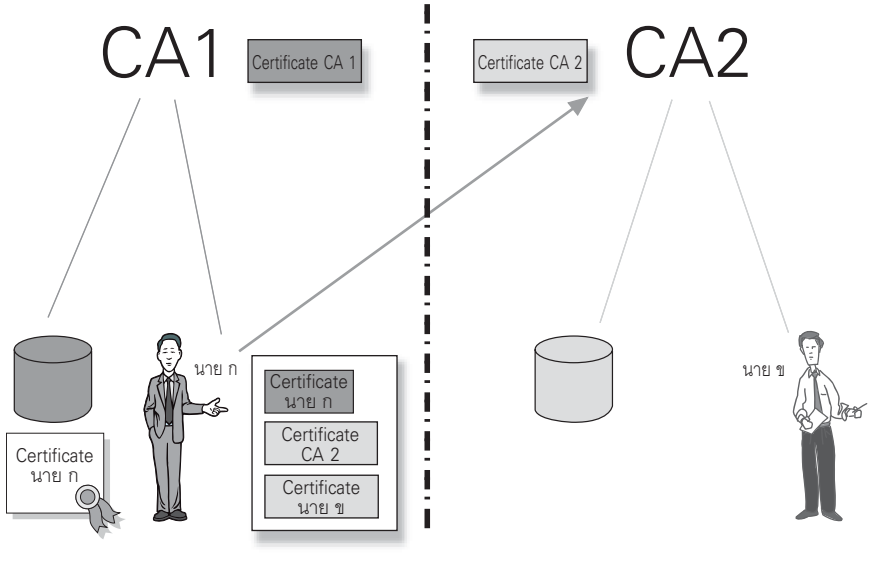
4.1 Cross Recognition

ระบบนี้บุคคลผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์ และผู้ที่เกี่ยวข้องเป็นผู้ตัดสินใจเลือกว่าจะมอบความไว้วางใจให้กับ CA รายใดบ้างด้วยตนเอง โดยเป็นผู้ติดตั้งกุญแจสาธารณะ (Public Key) ของผู้ให้บริการใบรับรองอิเล็กทรอนิกส์บนโปรแกรมของตนเอง

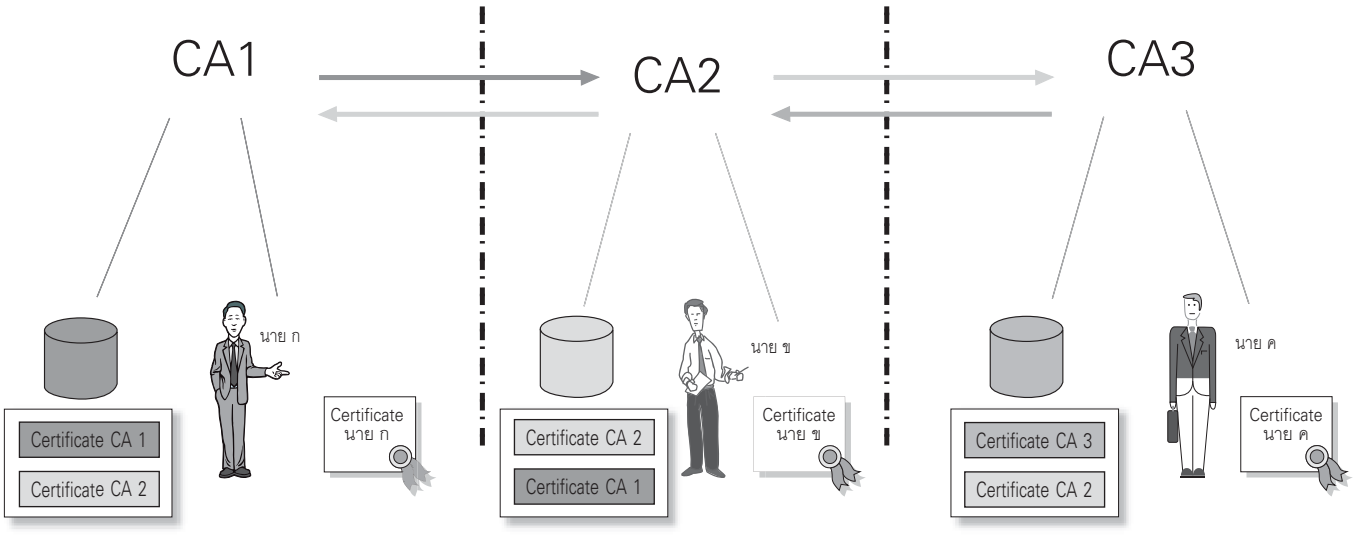
จากรูปที่ 1 ผู้ใช้บริการ CA1 ต้องการทำธุรกรรมกับผู้ใช้บริการ CA2 ผู้ใช้บริการ CA1 สามารถทำการติดตั้ง Public Key ของ CA2 ได้บนโปรแกรมของตน ใน Certificate Trust Lists

4.2 Cross Certification

ระบบนี้เป็นการสร้างความสัมพันธ์ระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยผู้ให้บริการเลือกที่จะออกใบรับรองให้แก่กัน



รูปที่ 1 ความสัมพันธ์ระหว่างผู้ใช้กับผู้ให้บริการใบรับรองอื่น

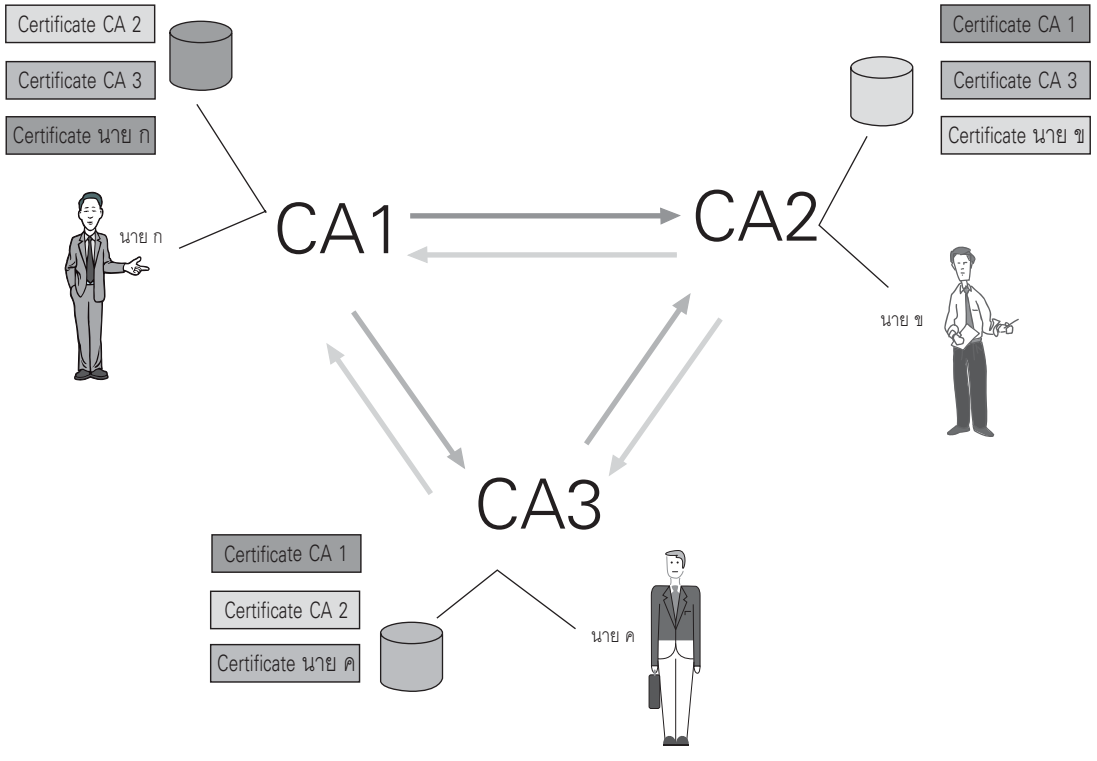


รูปที่ 2 ความสัมพันธ์ระหว่างผู้ให้บริการใบรับรอง

จากรูปเมื่อนาย ก. ต้องการติดต่อกับนาย ข. นาย ก. สามารถเข้าไปค้นหาใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ CA2 ผ่านทางไดเร็กทอรีของผู้ให้บริการ CA1 ได้โดยตรง เพื่อใช้ในการตรวจสอบใบรับรองอิเล็กทรอนิกส์ของนาย ข. ว่ามาจากผู้ให้บริการ CA2 จริง ดังรูปที่ 2

4.3 Mesh Trust

เป็นเครือข่ายโครงข่ายที่เชื่อมโยงระหว่างกลุ่มของผู้ให้บริการ และการตรวจสอบแต่ผู้ให้บริการสามารถติดต่อกันได้เองโดยตรง ดังรูปที่ 3



รูปที่ 3 ความสัมพันธ์ระหว่างผู้ให้บริการใบรับรอง แบบ Mesh Trust

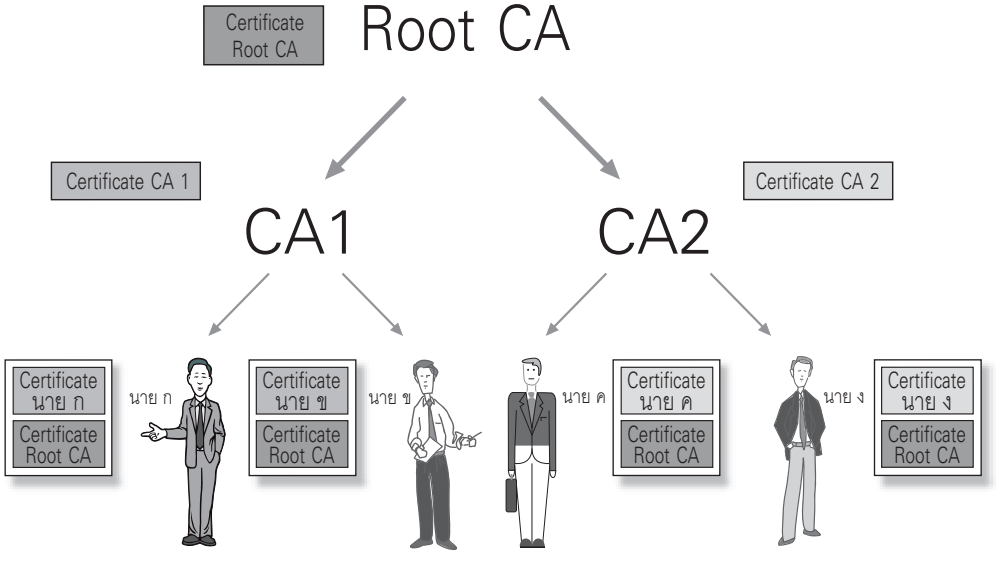
4.4 Hierarchy Trust (Root CA)

เป็นระบบความสัมพันธ์ที่ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ที่เป็นที่รู้จักและได้รับความไว้วางใจจากผู้ให้บริการใบรับรองอิเล็กทรอนิกส์รายอื่นๆ มากที่สุด ตั้งตนเป็นผู้ให้บริการชั้นสูงสุด (Root CA) เพื่อทำการรับรองผู้ให้บริการรายอื่นๆ (Subordinate CA) โดยใช้กุญแจส่วนตัวของผู้ให้บริการชั้นสูงสุดออกใบรับรอง และในการออกใบรับรองให้กับผู้ใช้บริการ จะต้องส่งใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการในชั้นที่สูงกว่าให้กับผู้ใช้ ที่ขอใบรับรองอิเล็กทรอนิกส์ด้วย ดังรูปที่ 4

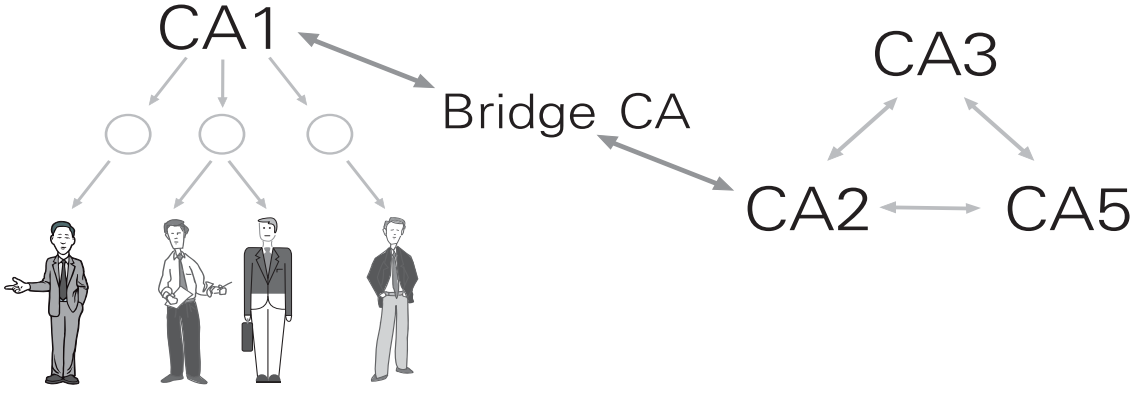
4.5 Bridge CA

เป็นระบบความสัมพันธ์ที่ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์กลาง (Bridge CA) เป็นศูนย์กลางหรือตัวกลางในการติดต่อผู้ให้บริการแต่ละรูปแบบ เช่น จากรูปที่ 5 Bridge CA จะทำหน้าที่เป็นตัวกลางระหว่างระบบ Hierarchy Trust และ Mesh Trust

Trust Model ในรูปแบบทั้ง 5 นี้มีข้อดีข้อเสียแตกต่างกัน ซึ่งได้สรุปไว้ในตารางที่ 2



รูปที่ 4 ความสัมพันธ์ระหว่างผู้ให้บริการใบรับรอง แบบ Hierarchy Trust หรือ Root CA



รูปที่ 5 ความสัมพันธ์ระหว่างผู้ให้บริการใบรับรอง แบบ Bridge CA

ตารางที่ 2 ตารางแสดงการเปรียบเทียบ Trust Model แบบต่างๆ

	ข้อดี	ข้อเสีย
Cross Recognition	- ไม่จำเป็นต้องมีการตกลงระหว่างผู้ให้บริการใบรับรองอิเล็กทรอนิกส์	- ยุ่งยากในการใช้งาน เพราะผู้ใช้ต้องติดตั้ง Public Key ของ CA แต่ละรายเข้าไปในโปรแกรมของตนเอง - มีความเสี่ยงสูง เพราะเป็นการตัดสินใจโดยผู้ใช้เพียงคนเดียวเท่านั้น ในการเลือกเชื่อถือ CA รายใด
Cross Certification	- ได้รับความเชื่อมั่นในด้านความปลอดภัยของข้อมูล - สะดวกกับผู้ใช้งาน เพราะไม่ต้องติดตั้งอะไรเพิ่มเติม	- ระบบบริการของทั้งสอง CA จะต้องเป็นซอฟต์แวร์เดียวกันหรือรองรับมาตรฐานเดียวกัน
Mesh Trust	- เหมาะกับโครงสร้างที่ไม่แน่นอน - หากกุญแจของ CA รายใดรายหนึ่งหาย จะไม่กระทบทั้งระบบ	- การตรวจสอบใบรับรองจะยุ่งยาก ซับซ้อนสำหรับ CA
Hierarchy Trust (Root CA)	- เหมาะกันระบบที่มีโครงสร้างองค์กรที่แน่นอน - การดูแลควบคุมมาตรฐานค่อนข้างสะดวก เพราะดูแลเฉพาะ Subordinate CA เท่านั้น	- ฐานข้อมูลใหญ่และซับซ้อน ยากต่อการดูแล - กรณีที่ Root CA เกิดข้อผิดพลาดในการออกใบรับรอง จะกระทบกระเทือนกับทั้งระบบ
Bridge CA	- เหมาะกับโครงสร้างที่เป็นแบบผสมระหว่าง Mesh และ Strict Hierarchy	- ฐานข้อมูลใหญ่และซับซ้อน ยากต่อการดูแล

5. ผลการสำรวจความคิดเห็นเกี่ยวกับโครงการใบรับรองอิเล็กทรอนิกส์เพื่อข้าราชการ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ทก.) ร่วมกับสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ จัดงานสัมมนาหัวข้อ "ใบรับรองอิเล็กทรอนิกส์เพื่อข้าราชการ" ขึ้น ในวันที่ 24 กันยายน 2547 ณ โรงแรมมิราเคิล แกรนด์ คอนเวนชั่น ผู้เข้าร่วมงานสัมมนา ประกอบด้วย ผู้อำนวยการฝ่ายสารสนเทศและผู้อำนวยการกองการเจ้าหน้าที่ของหน่วยราชการทุกแห่ง รวม 361 คน

ในงานสัมมนาดังกล่าว ได้มีการจัดทำแบบสอบถาม เพื่อสำรวจความคิดเห็นของข้าราชการจากหน่วยงานต่างๆ ที่เข้าร่วมประชุม เกี่ยวกับการดำเนินการกำกับ CA ในรูปแบบ Root CA แบบสอบถาม มีจำนวน 8 ข้อ คำถาม 7 ข้อแรกเป็นการถามความคิดเห็นของผู้ร่วมสัมมนาในประเด็นต่างๆ โดยให้เลือกตอบว่า "เห็นด้วยอย่างยิ่ง" "เห็นด้วย" "เห็นด้วยปานกลาง" "ไม่เห็นด้วย" และ "ไม่เห็นด้วยอย่างยิ่ง" ส่วนคำถามข้อสุดท้ายเป็นคำถามเปิด ให้ผู้ตอบแบบสอบถามแสดงข้อเสนอแนะต่อกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในการดำเนินโครงการใบรับรองอิเล็กทรอนิกส์เพื่อข้าราชการ ภายหลังการสัมมนามีผู้ร่วมตอบแบบสอบถาม จำนวนทั้งสิ้น 193 ราย ผลสรุปจากแบบสอบถามเกี่ยวกับการใช้ใบรับรองอิเล็กทรอนิกส์ในภาครัฐมีดังนี้

ผู้ตอบแบบสอบถามจำนวน 83 ราย หรือร้อยละ 43.01 ***เห็นด้วยอย่างยิ่ง***ที่ประเทศไทยจะใช้รูปแบบการกำกับ CA แบบ Root CA รองลงมา จำนวนร้อยละ 38.86 เห็นด้วยกับแนวคิดดังกล่าว มีเพียงร้อยละ 2.07 ที่ไม่เห็นด้วยอย่างยิ่งหากประเทศไทยจะใช้รูปแบบการกำกับผู้ให้บริการใบรับรองอิเล็กทรอนิกส์หรือ CA แบบ Root CA

ผู้ตอบแบบสอบถามจำนวน 79 ราย หรือ ร้อยละ 40.93 ***เห็นด้วยอย่างยิ่ง*** ที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจะเป็นหน่วยงานกำกับ CA มีเพียงร้อยละ 2.59 ที่ไม่เห็นด้วยที่ ทก. จะเป็นหน่วยงานกำกับ CA โดยเสนอให้หน่วยงานอื่นเป็นผู้กำกับ เช่น ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) กระทรวงมหาดไทย ภาคเอกชน องค์กรอิสระ กระทรวงยุติธรรม หรือหน่วยงานที่มีหน้าที่ทางด้านกฎหมาย โดย ทก. เป็นผู้สนับสนุนเทคโนโลยี

ในส่วนของการรับรองหน่วยงานที่ทำหน้าที่ในการออกใบรับรองอิเล็กทรอนิกส์ ผู้ตอบแบบสอบถามส่วนใหญ่ คือ ร้อยละ 24.87 ไม่เห็นด้วยหาก ทก. จะรับรองเฉพาะ CA ภาครัฐเท่านั้น มีเพียงร้อยละ 18.65 ที่เห็นด้วยอย่างยิ่งในการให้ ทก. รับรองเฉพาะภาครัฐเท่านั้น

สำหรับการพิจารณาการรับรอง CA ภาคเอกชน ผู้ตอบแบบสอบถามกว่าร้อยละ 80 เห็นสมควรให้ ทก. กำหนดเงื่อนไขการรับรอง โดยพิจารณาจาก CPS (ระเบียบ วิธีการ บริหารใบรับรองอิเล็กทรอนิกส์) ของ CA รายนั้น กล่าวคือ มีแบบสอบถามร้อยละ 40.41 ที่เลือกตอบว่า ***เห็นด้วยอย่างยิ่ง*** และแบบสอบถามร้อยละ 39.90 ระบุว่า ***เห็นด้วย*** มีแบบสอบถามเพียงร้อยละ 3.11 เท่านั้นที่ ***ไม่เห็นด้วยอย่างยิ่ง*** หาก ทก. จะใช้ CPS เป็นเงื่อนไขในการพิจารณารับรอง CA ภาคเอกชน

เมื่อสอบถามความเห็นเกี่ยวกับการรับรอง CA ภาคเอกชนโดยการพิจารณาจากทุนจดทะเบียนของเอกชนรายนั้น พบว่า ผู้ตอบแบบสอบถามจำนวน 60 ราย หรือ 31.09% เลือกตอบว่า ***ไม่แสดงความเห็น*** รองลงมา ผู้ตอบแบบสอบถามสนับสนุนแนวคิดที่ว่า หาก ทก. จะต้องรับรอง CA ภาคเอกชนควรกำหนดเงื่อนไขการรับรองจากทุนจดทะเบียน โดยมีจำนวนผู้ตอบแบบสอบถามที่ตอบว่า ***เห็นด้วย*** และ ***เห็นด้วยอย่างยิ่ง*** คิดเป็นร้อยละ 23.83 และ 17.62 ตามลำดับ

สำหรับประเด็นการออกใบรับรองอิเล็กทรอนิกส์ให้กับข้าราชการนั้น ผู้ตอบแบบสอบถามร้อยละ 36.79 และ 22.28 ***เห็นด้วยอย่างยิ่ง*** และ***เห็นด้วย*** หาก ทก. พิจารณาออกใบรับรองอิเล็กทรอนิกส์ให้กับข้าราชการต่ำกว่าระดับ 8 มีเพียงร้อยละ 4.15 ที่ตอบว่า ***ไม่เห็นด้วยอย่างยิ่ง*** กับแนวคิดดังกล่าว ทั้งนี้มีผู้ตอบแบบสอบถามคิดเป็น ร้อยละ 20.73 ที่***ไม่แสดงความเห็น*** เกี่ยวกับระดับข้าราชการที่ควรได้รับใบรับรองอิเล็กทรอนิกส์

6. บทวิเคราะห์

บทความนี้ได้สำรวจรูปแบบของผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ หรือ CA ในประเทศไทย 3 บริษัท โดยเน้นการพิจารณาระเบียบวิธีปฏิบัติ (CPS) ในการให้บริการของ CA แต่ละราย เนื่องจาก CA จัดเป็นรากฐานสำคัญของการทำธุรกรรมอิเล็กทรอนิกส์ ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 การพัฒนา CA ในประเทศไทยจึงเป็นสิ่งจำเป็น

บทความนี้ได้ให้แนวคิดเบื้องต้นการพิจารณารูปแบบการกำกับ CA โดยคำนึงถึงประเด็นการสร้างมาตรฐานเดียวกัน การรับรองร่วมกัน เพื่อให้ผู้ใช้บริการ CA ต่างรายกัน สามารถทำธุรกรรมกันได้ มาตรา 32 ใน พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ได้ให้อำนาจแก่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในการออกกฎหมายเพื่อควบคุมผู้ประกอบการที่เกี่ยวข้องกับการทำธุรกรรมอิเล็กทรอนิกส์ได้ ซึ่ง CA จัดเป็นธุรกิจที่มีความสำคัญลำดับต้นๆ ที่จะต้องมีการกำกับดูแล อย่างไรก็ตาม ผู้ใช้ใบรับรองอิเล็กทรอนิกส์ในการทำธุรกรรมจะต้องเข้าใจว่าขอบเขตของ CA นั้นจะรับผิดชอบต่อการระบุตัวตนหรือเว็บไซต์ที่ทำธุรกรรมด้วยเท่านั้น CA จะไม่คำนึงถึงความน่าเชื่อถือหรือเครดิตของบุคคลที่ได้รับการรับรองนั้น การรับรองข้าม CA กันนั้น จำเป็นต้องมีการเลือกรูปแบบ Trust Model ที่เหมาะสม ซึ่งบทความนี้ได้นำเสนอทางเลือกรูปแบบต่างๆ 5 รูปแบบ

นอกจากการทำธุรกรรมอิเล็กทรอนิกส์ในภาคเอกชนแล้ว การทำธุรกรรมอิเล็กทรอนิกส์ในภาครัฐก็จัดเป็นองค์ประกอบที่สำคัญในการกระตุ้นให้เกิดการทำธุรกรรมอิเล็กทรอนิกส์ เพราะนอกจากจะเป็นการอำนวยความสะดวกแก่ประชาชนแล้ว รัฐบาลยังสามารถประหยัดค่าใช้จ่ายได้ด้วย ในปัจจุบัน หน่วยงานรัฐบาลบางแห่งได้ทำหน้าที่เป็น CA เพื่อออกใบรับรองอิเล็กทรอนิกส์ในการรับรองตัวตนของผู้รับบริการรายใหญ่ อย่างไรก็ตาม การที่หน่วยงานรัฐบาลแต่ละหน่วยจัดทำใบรับรองอิเล็กทรอนิกส์ของตนเอง อาจทำให้เกิดปัญหาด้านมาตรฐานที่แตกต่างกัน และค่าใช้จ่ายที่สูง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงได้ริเริ่มโครงการใบรับรองอิเล็กทรอนิกส์เพื่อข้าราชการ โดยออกใบรับรองอิเล็กทรอนิกส์ให้แก่ข้าราชการระดับ 8 ขึ้นไป ทุกหน่วยงาน จำนวน 50,000 ใบ ซึ่งบทความนี้ได้เสนอผลสำรวจความคิดเห็นของข้าราชการต่อรูปแบบการกำกับ ซึ่งส่วนใหญ่เห็นว่าหากประเทศไทยเลือกใช้ Trust Model แบบ Root CA แล้ว กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารควรทำหน้าที่เป็นผู้ดูแล Root CA นี้ โดยมีประเด็นปลีกย่อย ที่น่าสนใจหลายด้าน ซึ่งสรุปไว้ในภาคผนวก ข.

จากการพิจารณา Trust Model ของการรับรองข้าม CA ในรูปแบบต่างๆ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้มีมติให้เลือกรูปแบบ Root CA เป็นแนวทางการกำกับ CA ของประเทศไทย ซึ่งรูปแบบนี้มีข้อดีที่เด่นชัดคือการจัดการที่ง่ายกว่า นอกจากนี้ เมื่อคำนึงถึงการรับรอง CA ข้ามประเทศ รูปแบบ Root CA ยังสามารถทำได้สะดวกกว่าด้วย เช่น หากนักธุรกิจไทยต้องการทำธุรกรรมกับนักธุรกิจในเกาหลีใต้ ซึ่งใช้ระบบ Root CA ในการกำกับเหมือนกัน เพียงแต่ Root CA ของทั้งสองประเทศทำการรับรองร่วมกันด้วยวิธี Cross Certification เท่านั้น ผู้ที่อยู่ในระบบ CA ทั้งหมด ไม่ว่าจะเกิดจากผู้ให้บริการรายใด ก็จะรู้จักกันโดยอัตโนมัติ นอกจากนี้ยังมีข้อดีในประเด็นด้านการกำกับทางพฤตินัย เพราะหาก CA รายใดไม่ปฏิบัติตามกรอบ CPS ที่ตกลงกันไว้ อันจะเป็นเหตุให้ความเชื่อถือในระบบลดลง Root CA สามารถใช้ดุลยพินิจยกเลิกการให้การรับรอง CA ดังกล่าว ซึ่งจะก่อให้เกิดความเสียหายทางธุรกิจของ CA นั้นอย่างมาก เพราะใบรับรองอิล็กทรอนิกส์ที่ออกให้ลูกค้าทั้งหมดจะถูกถอนการรับรองโดยอัตโนมัติ การกำกับแบบนี้จะทำให้สามารถดูแล CA ได้มากกว่าการบังคับทางนิตินัยด้วยพระราชกฤษฎีกาประกอบมาตรา 32

ผู้ทำหน้าที่ Root CA ควรมีความเป็นกลาง และไม่ประกอบธุรกิจ ดังนั้นหน่วยงานภาครัฐที่เหมาะสมในการจัดตั้ง Root CA น่าจะเป็นกระทรวงวิทยาศาสตร์และเทคโนโลยี หรือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยขอบข่ายงานกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ควรจะเป็นผู้ดูแล นอกจากนี้รัฐมนตรีว่าการฯ ยังทำหน้าที่ประธานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์โดยตำแหน่งด้วย ซึ่งจะทำให้การกำกับดูแล CA มีผลทั้งทางพฤตินัยและนิตินัยตามที่ได้กล่าวมาแล้ว

อย่างไรก็ตาม จุดอ่อนสำคัญของรูปแบบ Root CA คือจะต้องคอยดูแลให้ CPS ที่แต่ละ CA ใช้มีมาตรฐานอยู่ในระดับเท่าเทียมกัน ประเด็นที่ Root CA ควรพิจารณาดำเนินการจึงมีอยู่ 3 ประเด็นหลัก

ประเด็นที่ 1 ทำการร่าง CPS ทั้งของ Root CA เอง และ CA เพื่อใช้เป็นแนวทางให้ CA เกิดความเชื่อถือในการปฏิบัติงานของ Root CA และให้ CA ทุกรายใช้ร่าง CPS นี้เป็นกรอบการปฏิบัติขั้นต่ำที่ CA ทุกรายจะต้องปฏิบัติตาม

ประเด็นที่ 2 กำหนดกรอบขั้นต่ำในการอนุญาตให้ประกอบธุรกิจ CA ในประเทศไทย เกณฑ์ที่ใช้ในต่างประเทศมักจะใช้ยอดเงินลงทุน และจำนวนพนักงาน เฉพาะส่วนที่ให้บริการ CA เป็นเงื่อนไขสำคัญ เพราะต้องการให้ผู้ประกอบธุรกิจ CA นั้นมีความน่าเชื่อถือ อย่างไรก็ตาม ประเทศไทยอาจจะเลือกการสร้างกฎเกณฑ์ที่ครอบคลุมในเชิงพาณิชย์ด้วย เพื่อให้เกิดการแข่งขันที่เป็นธรรม ประกอบกับด้านความมั่นคงของระบบ มิฉะนั้นจะเกิดผู้ให้บริการน้อยรายอันจะทำให้เกิดการผูกขาดได้ นอกจากนี้ยังควรให้มีข้อยกเว้นสำหรับการประกอบกิจกรรม CA ที่ไม่แสวงผลกำไร เช่นการรับรองภายในหน่วยงานเดียวกันเอง หรือการรับรองโดยหน่วยงานภาครัฐ

ประเด็นที่ 3 Root CA จะต้องสร้างความเชื่อถือให้เกิดขึ้นในระบบของตนอย่างสูง นอกจากการลงทุนทางเทคโนโลยี และสร้าง CPS ที่เข้มงวดแล้ว Root CA จะต้องแสดงความน่าเชื่อถือผ่านองค์กรที่ผู้ใช้งานเชื่อ เช่นการรับรองข้าม Root CA ในต่างประเทศ และการให้บริษัทผู้ผลิตซอฟต์แวร์เช่น Microsoft รับรองโดยบรรจุกุญแจสาธารณะของ Root CA ไว้ใน List of Trusted CA ของผลิตภัณฑ์ ซึ่งการทำแบบนี้ จะทำให้เกิดผลต่อการใช้งานทันที และประเทศยังสามารถเงินตราต่างประเทศได้มาก เพราะในปัจจุบันนี้เว็บไซต์ของไทยทุกแห่งที่ทำธุรกรรมอิเล็กทรอนิกส์ผ่านอินเทอร์เน็ตยังต้องใช้ CA ต่างประเทศรับรอง เนื่องจากไม่มี CA รายใดในประเทศได้รับการรับรองโดย Microsoft ทำให้ไม่สามารถนำใบรับรองอิเล็กทรอนิกส์มาใช้งานในวงกว้างได้

แม้ว่าประเทศไทยจะมีการใช้งานพาณิชย์อิเล็กทรอนิกส์มานานแล้ว แต่จะพบว่าระดับการพัฒนายังไม่อยู่ในระดับที่น่าพอใจ รวมทั้งการพัฒนารัฐบาลอิเล็กทรอนิกส์ที่จะให้ประชาชนรับบริการผ่านอินเทอร์เน็ตนั้นแทบจะเป็นศูนย์ ทั้งนี้อุปสรรคสำคัญคือการขาดระบบสร้างความเชื่อถือ ที่จะทำให้เกิดการทำธุรกรรมในวงกว้างและมีผลผูกพันทางกฎหมายได้ บทความนี้นำเสนอแนวทางการสร้าง Trust Model ระหว่าง CA และวิเคราะห์แนวทางที่หน่วยงานที่รับผิดชอบควรปฏิบัติ เพื่อส่งเสริมการทำธุรกรรมอิเล็กทรอนิกส์ในประเทศไทย

เอกสารอ้างอิง

Atreya, M., B. Hammond, S. Paine, P. Starrett, and S. Wu, *Digital Signatures,* 2002, McGraw-Hill.

ภาคผนวก ก
การเข้ารหัสแบบกุญแจอสมมาตร

การสื่อสารแบบปลอดภัยบนเครือข่ายอินเทอร์เน็ตโดยใช้มาตรฐาน SSL ยึดรูปแบบการเข้ารหัสด้วยวิธีกุญแจอสมมาตร เพื่อให้เกิดความเข้าใจ ภาคผนวกนี้จะอธิบายและเปรียบเทียบวิธีเข้ารหัสแบบกุญแจสมมาตรและอสมมาตร

- **ระบบเข้ารหัสแบบกุญแจสมมาตร** (Symmetric-key Cryptography)

การเข้ารหัสแบบกุญแจสมมาตร หมายถึง การใช้กุญแจ 1 ตัวในการเข้ารหัสและถอดรหัส ดังนั้นทั้งผู้ส่งที่ 1 และผู้รับข้อความที่ 1 จะต้องมีกุญแจเก็บไว้โดยเป็นความลับระหว่างกัน ถ้าผู้ส่งที่ 1 ต้องการส่งข้อความให้ผู้รับข้อความที่ 2 ต้องทำการสร้างกุญแจระหว่างกันใหม่อีกครั้ง

จากรูปที่ 6 นาย ก. ทำการสร้างกุญแจขึ้นมา 1 ดอก เพื่อเก็บไว้สำหรับตนเองและนาย ข. เมื่อนาย ก. ต้องการส่งข้อมูลที่เป็นความลับให้นาย ข. นาย ก. ต้องทำการเข้ารหัส (Encrypt) ข้อมูลโดยใช้กุญแจ นาย ข. จะสามารถอ่านข้อมูลที่นาย ก. ส่งมาได้นั้น ต้องใช้กุญแจดอกเดียวกันในการถอดรหัส (Decrypt) จึงสามารถอ่านข้อมูลที่นาย ก. ส่งมาให้ได้

ข้อดี

1. เหมาะกับผู้ใช้ที่มีจำนวนน้อย สามารถกระจายกุญแจได้ทั่วถึงกัน

2. การเข้าและถอดรหัสข้อมูลทำได้รวดเร็ว เพราะกระบวนการเข้ารหัสและถอดรหัสที่ใช้ไม่ได้สลับซับซ้อน

3. ขนาดของข้อมูลหลังจากทำการเข้ารหัสแล้วมีขนาดไม่ใหญ่มาก

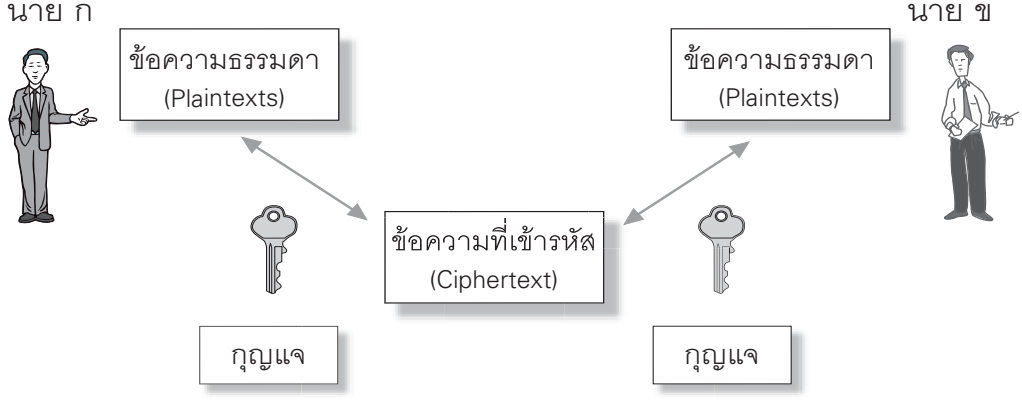
ข้อเสีย

1. การจัดการกับกุญแจลับ (Key Management) ยุ่งยากและซับซ้อน เพราะทุกครั้งที่ทำการติดต่อกับผู้รับข้อความคนใหม่ต้องทำการสร้างกุญแจคู่ใหม่ทุกครั้ง

2. การส่งมอบกุญแจลับ เนื่องจากการเข้ารหัสวิธีนี้ต้องใช้กุญแจลับ 1 ดอกต่อผู้รับ 1 คน ดังนั้นถ้าผู้ส่งข้อความต้องติดต่อกับคนมากๆ ผู้ส่งต้องส่งกุญแจลับที่ใช้ไปให้กับทุกคน

3. ความปลอดภัยของข้อมูลน้อย ในกรณีที่มีผู้ไม่ประสงค์ดีรู้รหัสกุญแจนี้ สามารถนำไปถอดรหัส และนำข้อมูลไปใช้ได้เลย

ระบบเข้ารหัสแบบกุญแจสมมาตร



รูปที่ 6 ระบบการเข้ารหัสแบบกุญแจสมมาตร

- **ระบบเข้ารหัสแบบกุญแจอสมมาตร** (Asymmetric-key cryptography)

การเข้ารหัสแบบกุญแจอสมมาตร หมายถึง การใช้กุญแจคู่ในการเข้ารหัสและถอดรหัส โดยประกอบด้วย กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) กุญแจลูกหนึ่งใช้เข้ารหัสและอีกลูกหนึ่งที่เป็นคู่กุญแจเท่านั้นจะสามารถใช้ในการถอดรหัสได้

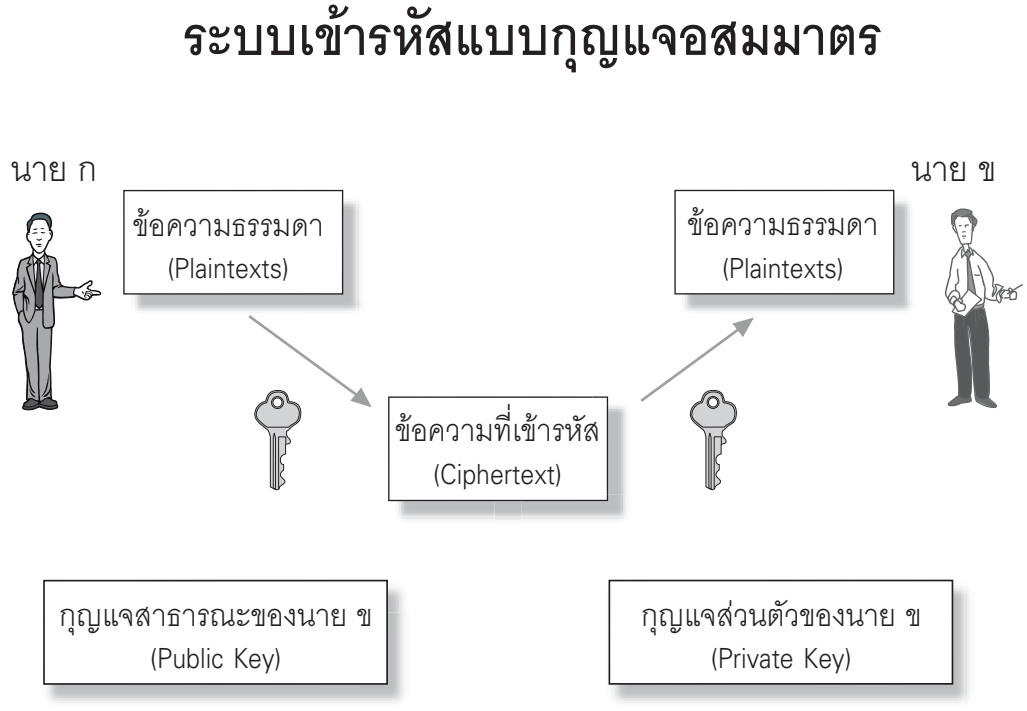
จากรูปที่ 7 นาย ข. ต้องทำการสร้างคู่กุญแจของตัวเองขึ้นมาก่อน เมื่อนาย ก. ต้องการส่งข้อมูลที่เป็นความลับให้นาย ข. นาย ก. ต้องไปเอากุญแจสาธารณะของนาย ข. ที่ถูกเก็บไว้ที่ระบบเพื่อนำมาทำการเข้ารหัส (Encrypt) และส่งข้อมูลมาที่นาย ข. นาย ข. ต้องใช้กุญแจส่วนตัว (Private Key) ของตนในการถอดรหัส (Decrypt) ถึงจะสามารถอ่านข้อมูลจาก นาย ก. ได้ หาก นาย ก. ต้องการส่งข้อมูลให้กับบุคคลอื่นอีกก็สามารถนำกุญแจสาธารณะของบุคคลนั้นมาเข้ารหัสได้เลย โดยไม่ต้องกังวลวิธีการส่งมอบกุญแจลับเพื่อถอดรหัสให้

ข้อดี

1. การจัดการกับกุญแจทำได้ง่าย ผู้ส่งสารสามารถใช้กุญแจสาธารณะ (Public Key) ของผู้รับกี่คนก็ได้ เพื่อส่งสารให้ เพราะมีเพียงผู้รับแต่ละคนซึ่งมีกุญแจส่วนตัวของตนเองเท่านั้นจึงจะถอดรหัสได้
2. ความปลอดภัยของข้อมูลสูง กรณีมีผู้ไม่ประสงค์ดีทราบรหัสกุญแจสาธารณะ (Public Key) ก็ไม่สามารถถอดรหัสข้อมูลและนำไปใช้ได้
3. การกระจายกุญแจ สามารถทำได้อย่างกว้างขวาง

ข้อเสีย

1. การเข้ารหัสและถอดรหัสข้อมูลใช้เวลามาก เพราะว่ากระบวนการเข้ารหัสและถอดรหัสที่ใช้ค่อนข้างจะสลับซับซ้อนมาก
2. ขนาดข้อมูลหลังจากทำการเข้ารหัสแล้ว มีขนาดใหญ่กว่าเดิมมาก เพราะฉะนั้นจะเป็นปัญหาในการใช้งาน



รูปที่ 7 ระบบการเข้ารหัสแบบกุญแจอสมมาตร

ภาคผนวก ข
สรุปผลแบบสอบถามในงานสัมมนา “ใบรับรองอิเล็กทรอนิกส์เพื่อข้าราชการ”

1. ท่านเห็นว่าประเทศไทยควรใช้รูปแบบการกำกับ CA แบบ Root CA หรือไม่

	เห็นด้วยอย่างยิ่ง (5)	เห็นด้วย (4)	ปานกลาง (3)	ไม่เห็นด้วย (2)	ไม่เห็นด้วยอย่างยิ่ง (1)	ไม่แสดงความเห็น
จำนวน	83	75	25	5	4	1
(%)	43.01	38.86	12.95	2.59	2.07	0.52

2. ท่านเห็นว่ากระทรวงเทคโนโลยีสารสนเทศและการสื่อสารควรเป็นหน่วยงานกำกับ CA หรือไม่

	เห็นด้วยอย่างยิ่ง (5)	เห็นด้วย (4)	ปานกลาง (3)	ไม่เห็นด้วย (2)	ไม่เห็นด้วยอย่างยิ่ง (1)	ไม่แสดงความเห็น
จำนวน	79	77	21	7	5	4
(%)	40.93	39.90	10.88	3.63	2.59	2.07

3. การรับรอง CA ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารควรรับรองเฉพาะ CA ภาครัฐเท่านั้น

	เห็นด้วยอย่างยิ่ง (5)	เห็นด้วย (4)	ปานกลาง (3)	ไม่เห็นด้วย (2)	ไม่เห็นด้วยอย่างยิ่ง (1)	ไม่แสดงความเห็น
จำนวน	36	35	38	48	35	1
(%)	18.65	18.13	19.69	24.87	18.13	0.52

4. หากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารต้องรับรอง CA ภาคเอกชน ควรกำหนดเงื่อนไขการรับรองโดยพิจารณาจาก CPS (ระเบียบ วิธีการ บริหารใบรับรองอิเล็กทรอนิกส์) ของ CA รายนั้น

	เห็นด้วยอย่างยิ่ง (5)	เห็นด้วย (4)	ปานกลาง (3)	ไม่เห็นด้วย (2)	ไม่เห็นด้วยอย่างยิ่ง (1)	ไม่แสดงความเห็น
จำนวน	78	77	26	2	6	4
(%)	40.41	39.90	13.47	1.04	3.11	2.07

5. หากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารต้องรับรอง CA ภาคเอกชนควรกำหนดเงื่อนไขการรับรอง โดยพิจารณาจากทุนจดทะเบียนของเอกชนรายนั้น

	เห็นด้วยอย่างยิ่ง (5)	เห็นด้วย (4)	ปานกลาง (3)	ไม่เห็นด้วย (2)	ไม่เห็นด้วยอย่างยิ่ง (1)	ไม่แสดงความเห็น
จำนวน	34	46	39	5	9	60
เปอร์เซนต์	17.62	23.83	20.21	2.59	4.66	31.09

6. ท่านเห็นด้วยหรือไม่ว่ากระทรวงเทคโนโลยีสารสนเทศควรออกใบรับรองอิเล็กทรอนิกส์ให้แก่ข้าราชการต่ำกว่าระดับ 8 ด้วย

	เห็นด้วย อย่างยิ่ง (5)	เห็นด้วย (4)	ปานกลาง (3)	ไม่เห็นด้วย (2)	ไม่เห็นด้วย อย่างยิ่ง (1)	ไม่แสดง ความเห็น
จำนวน	71	43	20	11	8	40
(%)	36.79	22.28	10.36	5.70	4.15	20.73

7. ข้อเสนอแนะต่อกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในการดำเนินโครงการใบรับรองอิเล็กทรอนิกส์เพื่อข้าราชการ แบ่งเป็นข้อเสนอแนะในด้านต่างๆ ดังนี้

การดำเนินโครงการ Root CA

- ควรมีการประชาสัมพันธ์โครงการอย่างกว้างขวาง เพื่อให้กลุ่มผู้บริหาร หัวหน้าส่วนงาน และข้าราชการตระหนักถึงความสำคัญของระบบ และผลักดันให้มีการใช้งานอย่างจริงจัง
- ควรมีการกำหนดลักษณะงานนำร่อง เพื่อนำระบบมาใช้แนวทางเดียวกัน
- มีกรอบระยะเวลาดำเนินงานที่ชัดเจน
- ควรกำหนดมาตรฐานของเครือข่ายขององค์กรที่จะเข้าร่วมโครงการ
- ควรพิจารณาเรื่องลิขสิทธิ์การใช้งานโปรแกรมด้วย
- ส่วนงานต่างๆ ต้องมีพื้นฐานระบบเอกสารเป็นไอทีทั้งหมด หรือใช้งานเอกสารอิเล็กทรอนิกส์ จึงจะทำให้เกิดประโยชน์สูงสุด
- ควรออกใบรับรองอิเล็กทรอนิกส์ให้กับเจ้าหน้าที่ที่จะต้องรับผิดชอบในการติดตั้งดูแลระบบของแต่ละหน่วยงาน หรือพิจารณาตามความจำเป็นในการใช้งาน และความเกี่ยวข้องของงานที่ปฏิบัติ
- ควรมีการสนับสนุนให้มีการใช้งานใบรับรองอิเล็กทรอนิกส์อย่างจริงจัง เริ่มตั้งแต่การใช้งานระบบใดระบบหนึ่งเพื่อแสดงให้เห็นประโยชน์และกระตุ้นให้เกิดการใช้งานอย่างจริงจัง
- ใบรับรองอิเล็กทรอนิกส์ควรเชื่อมโยงกับระบบ Web Mail ของหน่วยงานได้
- ควรรวมใบรับรองอิเล็กทรอนิกส์ใน Smart Card (บัตรประชาชนอัจริยะอเนกประสงค์) เพื่อประหยัดงบประมาณ
- ควรมีการสนับสนุนงบประมาณด้าน CA Software, Hardware และเครือข่ายของหน่วยงานต่างๆ
- หาหนทางในการสร้างความมั่นใจทางด้านความปลอดภัยในการใช้งาน เพื่อสร้างความมั่นใจให้กับข้าราชการมากยิ่งขึ้น
- ควรมีการดำเนินงานอย่างต่อเนื่อง และมีการสนับสนุนจากผู้บริหารระดับสูง เพื่อให้การดำเนินโครงการเป็นไปอย่างมีประสิทธิภาพสูงสุด
- Root CA ควรครอบคลุมทั้ง CA ภาครัฐและเอกชน
- การออกใบรับรองฯ ควรมีความเข้มงวด สำหรับผู้ที่ทำธุรกรรมที่สำคัญๆ เท่านั้น

กฎระเบียบ

- ควรมีการปรับปรุง กฎ ระเบียบ และวิธีปฏิบัติต่างๆ สนับสนุนให้ลดการใช้กระดาษในหน่วยงาน
- การก่อตั้งหรือจัดตั้งสถาบันที่ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ควรแยกตามสาขาหรือประเภทขององค์กร เช่น ธนาคาร ผู้ที่เป็น CA ควรเป็นสมาคมธนาคารไทย ส่วน Root CA ควรมีเพียงองค์กรเดียวที่ทำหน้าที่ดูแลในภาพรวม ซึ่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นองค์กรที่เหมาะสมที่สุด
- สำหรับ CA ภาคเอกชน Root CA ควรออกกฎเกณฑ์อย่างกว้างๆ เพื่อเป็นกรอบให้ CA ภาคเอกชนดำเนินการด้วยมาตรฐานเดียวกัน

- Root CA by MICT ไม่ควรมีบทบาทในการรับผิดชอบความเสียหายที่เกิดขึ้น แต่ควรมีบทบาทในการกำกับโดยเป็นผู้ดูแล CA หรือออกกฎเกณฑ์หรือระเบียบให้แก่ CA ยึดถือปฏิบัติ ความเสียหายที่อาจเกิดขึ้นควรให้ CA เป็นผู้ชดใช้ความเสียหายแก่ผู้ใช้โดยตรง
- อายุใบรับรองอิเล็กทรอนิกส์ที่ Root CA ออกให้กับ CA ควรกำหนดเป็นเทอม 3-5 ปี ส่วนระหว่าง CA กับผู้ใช้งานไม่ควรเกิน 1 ปี
- การเพิกถอนใบรับรองของ CA จาก Root CA ไม่ควรเพิกถอนได้โดยง่าย เพราะจะส่งผลกระทบต่อผู้ใช้งานของแต่ละ CA นั้นๆ ในวงกว้าง การเพิกถอนควรมีคณะกรรมการย่อยใน Root CA พิจารณาคำร้องเรียนนั้นๆ
- Root CA by MICT ไม่ควรเรียกเก็บค่าธรรมเนียมอย่างยิ่ง ควรให้เป็น Infrastructure ของประเทศ นอกจากนี้ควรกำหนดนโยบายการเรียกเก็บค่าธรรมเนียมที่เหมาะสมให้แก่ CA ยึดถือปฏิบัติกับผู้ใช้งานใน CA แต่ละแห่ง
- การใช้กฎหมายรับรองต้องสร้างความเชื่อมั่นให้แก่ผู้บริหารว่าการแจกจ่ายและจัดเก็บ key เป็นไปอย่างปลอดภัยสูงสุด จึงจะทำให้ความน่าเชื่อถือในเชิงกฎหมายมากขึ้น
- การต่ออายุใบรับรองอิเล็กทรอนิกส์ของ CA ควรทำโดยอัตโนมัติ
- บุคคลทั่วไปควรมีใบรับรองอิเล็กทรอนิกส์ด้วย
- ทก. ควรร่วมกับสำนักนายกรัฐมนตรี และ สำนักงานข้าราชการพลเรือน (กพ.) แก้ไขกฎระเบียบด้านสารบรรณเพื่อให้สามารถนำระบบไปรษณีย์อิเล็กทรอนิกส์มาใช้อย่างแพร่หลายมากขึ้น
- การกำกับดูแล CA ควรมีหน่วยงานที่เกี่ยวข้องเข้าร่วมรับผิดชอบด้วย เช่น NECTEC กระทรวงมหาดไทย ฯลฯ
- ควรมีความชัดเจนเกี่ยวกับกฎหมายที่เข้ามาควบคุม CA เช่น การกำหนดความรับผิดชอบ ความปลอดภัยของข้อมูล
- ให้มีมาตรการและระเบียบปฏิบัติบังคับให้ส่วนราชการทำธุรกรรมอิเล็กทรอนิกส์ แบบ Secure Mail

การจัดอบรม

- จัดอบรมอย่างต่อเนื่อง เพื่อแนะนำรายละเอียดการใช้งาน
- มีการจัดอบรมการใช้งานให้กับข้าราชการที่ใช้ใบรับรองอิเล็กทรอนิกส์ทุกคน
- ควรให้ CA จัดอบรมที่หน่วยงานต่างๆ
- ควรจัดการอบรมให้กับบุคลากรฝ่ายนิติการด้วย เพราะหากมีปัญหาทางกฎหมายหรือวินัย บุคคลเหล่านี้จะต้องมีความรู้พื้นฐานในเรื่องเหล่านี้ด้วย

แนวทางการใช้งานใบรับรองอิเล็กทรอนิกส์

- ควรมีการประยุกต์ใช้กับระบบสารบรรณอิเล็กทรอนิกส์และระบบ GFMIS และระบบอื่นๆ เพื่อที่เจ้าหน้าที่จะได้ใช้ใบรับรองฯ เพียงใบเดียวในการใช้งานทุกระบบงาน
- ควรมีการออกใบรับรองอิเล็กทรอนิกส์ให้กับข้าราชการในทุกระดับ และสามารถใช้ร่วมกับระบบ Web Based ได้
- เร่งดำเนินการรับรอง CA ให้สามารถใช้กับต่างประเทศได้จะทำให้มีการใช้งานมากขึ้น
- การเปิดซองประมูล การจัดจ้างหรือการทำธุรกรรมต่างๆ สามารถกระทำผ่าน e-mail ได้
- ควรให้ใช้งานใบรับรองฯ ร่วมกับธนาคารได้ด้วย

ความรับผิดชอบของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

- ทก. ควรเป็นหน่วยงานหลักหรือหน่วยงานกลางที่รับผิดชอบเกี่ยวกับ CA ในทุกๆ เรื่อง เนื่องจากมีอำนาจ งบประมาณ และบุคลากรที่จะสามารถดำเนินการในนโยบายต่างๆ ได้ดีกว่า
- ทก. ควรเป็นเจ้าภาพ จัดสัมมนาให้ความรู้และความชัดเจนในการใช้ใบรับรองฯ ควบคู่กับเรื่อง พ.ร.บ. หรือกฎหมาย โดยเชิญข้าราชการระดับ 9-11 ทุกหน่วยงาน เนื่องจากเป็นเรื่องยากที่เจ้าหน้าที่จะถ่ายทอดให้กับผู้บริหารเข้าใจได้
- การดูแลและให้ความช่วยเหลือหน่วยงานราชการ ควรมีความต่อเนื่องและชัดเจน
- จัดทำข่าวสาร จุลสารต่างๆ เพื่อเผยแพร่ข้อมูล ข่าวสาร และประชาสัมพันธ์โครงการ
- ทก. ควรประเมินว่าหน่วยงานใดที่มีงานหรือความเหมาะสมที่จะใช้ใบรับรองอิเล็กทรอนิกส์ตามภาระงานที่หน่วยงานรับผิดชอบ โดยหาหน่วยงานนำร่องเพื่อให้มีการใช้งานอย่างจริงจัง
- ควรนำเสนอหน่วยงานต้นแบบ และจัดให้หน่วยงานอื่นๆ มาดูงาน โดยเฉพาะ ทก. ควรเป็นต้นแบบให้หน่วยงานอื่นปฏิบัติตาม
- ทก. ควรดูแลระบบไปรษณีย์ของหน่วยราชการทั้งหมด
- ทก. ตั้งงบประมาณดูแล CA ภาครัฐทั้งหมด
- หาก ทก. ต้องรับรอง CA ภาคเอกชน ทก. ควรมี CPS กลางเพื่อเป็นมาตรฐานในการพิจารณาว่าจะรับรอง CA ภาคเอกชนรายนั้นได้
- ให้บริการแก่หน่วยงานภาครัฐ โดยไม่เสียค่าใช้จ่าย