บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 บทนำ

เทคโนโลยีสารสนเทศขององค์กรตลอดจนมาตรการในการรักษาความปลอดภัยนั้นมีการเปลี่ยนแปลงอยู่เสมอการเลือกใช้เทคโนโลยีด้านความปลอดภัยที่เหมาะสมแก่องค์กรทั้งในเรื่องของ TCO (Total Cost of Ownership) และ ROI (Return On Investment) จากข้อมูลของ Gartner เรื่อง Hype Cycle for Information Security 2004 [5] ปัญหาด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศยังเป็นประเด็นสำคัญที่ผู้บริหารต้องให้ความสนใจและจัดการอย่างเป็นระบบ ดังนั้นมาตรฐานขั้นตอนการปฏิบัติในการควบคุมจึงถือเป็นเรื่องสำคัญที่ควรจะศึกษาและกำหนดเป็นมาตรฐานในเรื่องของความปลอดภัยในการใช้งานระบบสารสนเทศในองค์กรเพื่อให้เกิดประสิทธิผลและประสิทธิภาพสูงสุดในการนำระบบกุญแจคู่สาธารณะมาใช้งาน

ในบทนี้จะนำเสนอถึงมาตรฐานต่างๆที่มีการนำไปใช้งานในด้านความปลอดภัยของข้อมูลที่เป็นที่ยอมรับในปัจจุบันตลอดจนงานวิจัยที่เกี่ยวข้องกุญแจรหัสส่วนตัวและใบรับรองอิเล็กทรอนิกส์ การนำเอากุญแจรหัสส่วนตัวไปใช้งานและผลทางด้านของกฎหมายว่าด้วยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ2544 . ขั้นตอนการยอมรับและความเชื่อถือของผู้บริหารที่จะยอมรับมาตรฐานหรือขั้นตอน การปฏิบัติในด้านความปลอดภัย

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 มาตรฐานความปลอดภัย

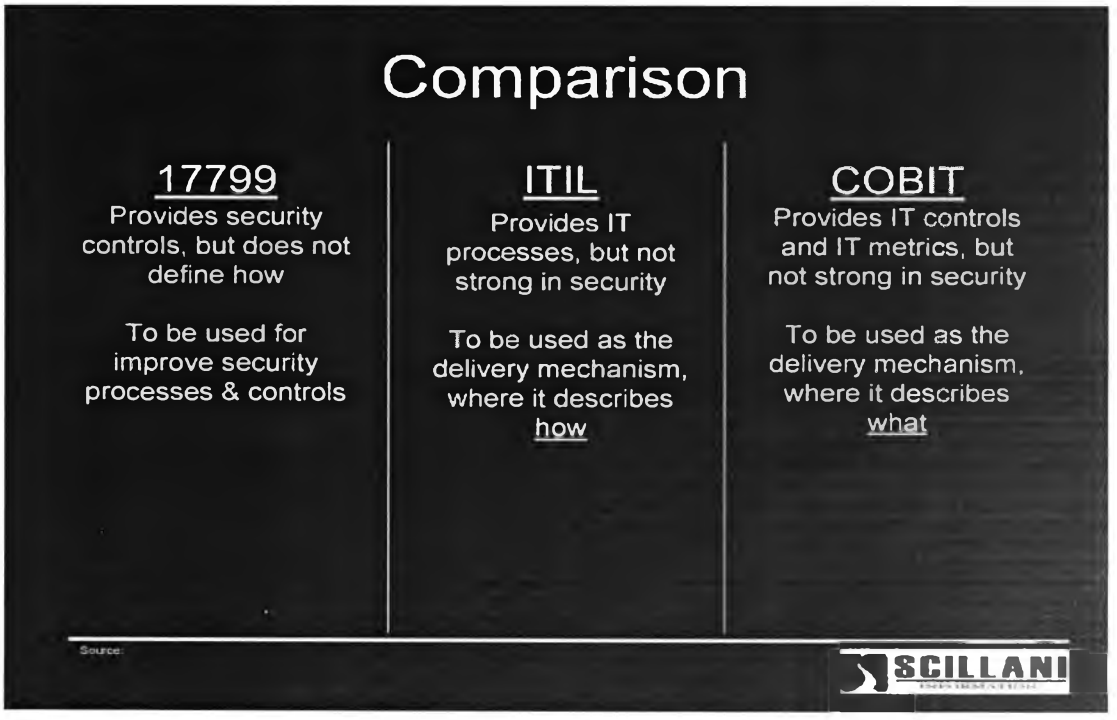
ในปี พ.ศ .2546 คณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ได้นำมาตรฐาน ISO/IEC17799 :2000 (First Edition) หรือ BS7799-1 [1] ในแนวทางในการกำหนดมาตรฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทยเพื่อให้เป็นแนวทางเสริมสร้างการรักษาความปลอดภัยให้กับหน่วยงานหรือองค์กรที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์โดยกำหนดมาตรฐานออกเป็น 3 ระดับ คือ ระดับ1 ควรปฏิบัติ 31 ข้อ, ระดับ 2 ควรปฏิบัติ 104 ข้อ และระดับ 3 ซึ่งเป็นระดับความปลอดภัยสูงสุด ควรปฏิบัติทั้งหมด 144 ข้อ [5]

ปัจจุบันได้มีการนำมาตรฐาน ISO/IEC17799 : 2005 [2] มาปฏิบัติในองค์กร ซึ่งในขณะนี้องค์กรทั่วโลกกำลังให้ความสนใจเรื่องความปลอดภัยระบบเทคโนโลยีสารสนเทศ ใน

ประเทศญี่ปุ่นนั้น มีองค์กรได้รับการรับรองมาตรฐาน BS7799-2 ไปแล้วกว่า 900 องค์กร แสดงให้เห็นถึงความสำคัญของการนำมาตรฐานด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศมาใช้งาน

ISACA และ IT Governance Institute ได้กำหนดมาตรฐาน CobiT [3] ขึ้นมาเพื่อเป็นแนวคิดและแนวทางปฏิบัติของผู้บริหารระบบสารสนเทศ และขณะเดียวกันก็เป็นแนวทางปฏิบัติสำหรับผู้ตรวจสอบระบบสารสนเทศด้วยโครงสร้างของมาตรฐาน CobiT นั้นแบ่งออกเป็น 4 กระบวนการหลัก ประกอบด้วย High Level Control Objective ทั้งหมด 34หัวข้อ และ Detail Control Objective แบ่งแยกย่อยอีกทั้งหมด 318 หัวข้อย่อย [4]

มาตรฐาน ITIL ได้ถูกพัฒนามาโดย การบริหารงานด้านสารสนเทศOGC (Office of Government Commerce) พัฒนาร่วมกับ BSI (British Standard Institute) มีวัตถุประสงค์ในการสร้าง Best Practice สำหรับกระบวนการบริหารงานบริการด้านสารสนเทศ (IT Service Management) มาตรฐาน ITIL กล่าวถึง "Best Practice" ในการบริหารจัดการงานให้บริการด้านระบบสารสนเทศที่ควรจะเป็นและมีประสิทธิภาพและ ประสิทธิผลชัดเจน เช่น มาตรฐานด้าน Service Support และ Service Delivery ตลอดจน การกำหนด SLA (Service Level Agreement) เป็นต้น ITIL ได้แสดงการผูกโยงเปรียบเทียบกันระหว่าง ISO 17799 และ COBIT [6] แสดงส่วนที่สอดคล้องสัมพันธ์หรือส่วนที่สำคัญของมาตรฐานข้างต้นดังรูปที่ 2.1



รูปที่ 2.1 **การเปรียบเทียบมาตรฐาน** ISO, ITIL **และ** COBIT [6]

งานวิจัยในเรื่อง ISO/IEC 17799 Compliant ? [9] ได้กล่าวถึงสถานะของความปลอดภัยในปัจจุบันภาพรวามของบริษัทหรือองค์กรขนาดใหญ่ของการดำเนินธุรกิจ อธิบายในมาตรฐานของ ISO ว่ามีขอบเขตและขั้นตอนครอบคลุมพื้นที่การทำงานส่วนใดตลอดจนทำการออกแบบคำถามสำรวจถึงหัวข้อในมาตรฐานว่าได้มีการปฏิบัติกันหรือไม่อย่างไร

HIPAA Final Security Standards [10] เป็นมาตรฐานหนึ่งที่ได้รับความนิยม ซึ่งงานวิจัยนี้จะทำการเปรียบเทียบมาตรฐานความปลอดภัย 2 มาตรฐานคือ HIPAA กับ ISO/IEC 17799 ว่าการที่เราใช้งานในมาตรฐานใดมาตรฐานหนึ่งแล้วควรหรือจำเป็นหรือไม่ที่จะต้องใช้มาตรฐานอื่นควบคู่ไปด้วยหรือเป็นการเพียงพอแล้วที่จะใช้มาตรฐานใดมาตรฐานหนึ่งเท่านั้น

ใน Who Do You Trust ? [11] ได้กล่าวถึงเรื่องความเชื่อถือในด้านบุคลากร ว่าใครที่เราจะเชื่อถือได้ ข้อควรระวังต่างๆทั้งเรื่องผู้ดูแลระบบ พนักงาน บริษัทตัวแทนจำหน่าย ตลอดจนที่ปรึกษา ว่าเราควรที่จะมีความเชื่อถือได้อย่างไร

Best practice เป็นรูปแบบที่ควรปฏิบัติตาม ในเรื่องความปลอดภัยก็มีอยู่มากมายที่ได้แนะนำ ในงานวิจัย Teaching Security Best Practices by Architecting and Administering an IT Security Lab [12] นั้น ได้ทำการทดลองในห้องทดลองของมหาวิทยาลัยเพื่อเป็นแนวทางในการใช้งานทางด้านความปลอดภัยของนักศึกษาที่ได้นำเอา Best practice มาใช้

2.2.2 งานวิจัยลายมือชื่อและใบรับรอง

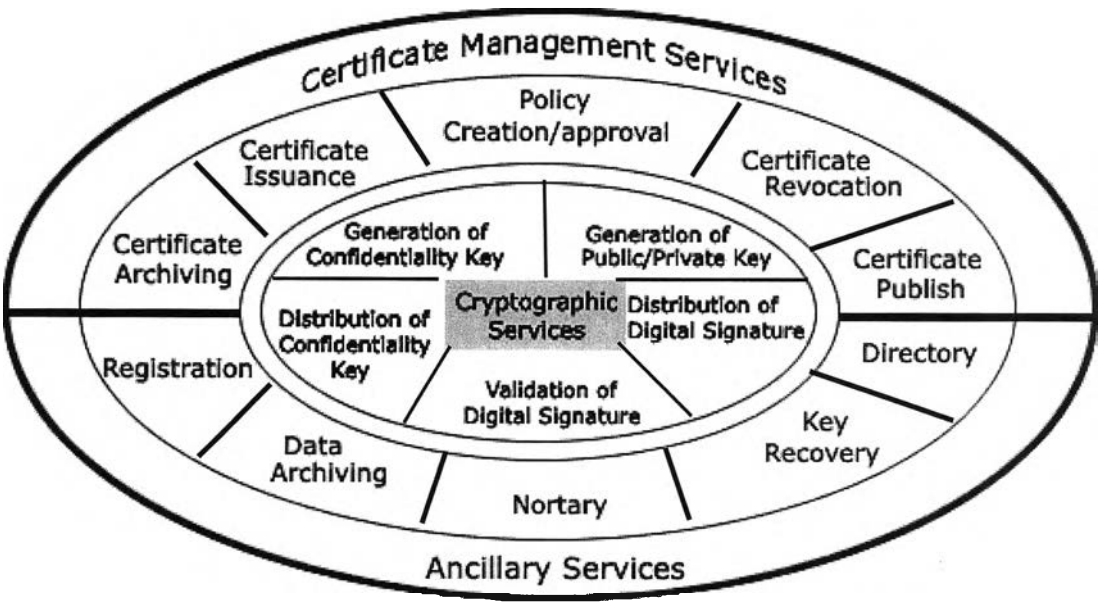
ลายมือชื่อและใบรับรองอิเล็กทรอนิกส์ [7] เป็นการประยุกต์ใช้เทคโนโลยีที่ช่วยในการรักษาความปลอดภัย เทคโนโลยีการเข้ารหัสที่ใช้กุญแจรหัสลับ (Secret key) คู่กับกุญแจสาธารณะ (Public key) หรือที่เรียกสั้นๆว่า "เทคโนโลยีการเข้ารหัส ด้วยกุญแจสาธารณะ" ซึ่งในการกระทำธุรกรรมทางด้านอิเล็กทรอนิกส์ต่างๆ เช่นธุรกรรมพานิชย์อิเล็กทรอนิกส์ (E-Commerce) ตลอดจนถึงการสื่อสารการแลกเปลี่ยนข้อมูลข่าวสารทางอิเล็กทรอนิกส์กันนั้นจะต้องมีองค์ประกอบพื้นฐานในด้านความปลอดภัยอยู่ทั้งหมด 4 ด้านด้วยกันคือ 1.การระบุตัวบุคคล (Authenticity) 2. การรักษาความลับ (Confidentiality) 3. การรักษาความถูกต้องสมบรูณ์ (Integrity) และ 4. การป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation) [7] ดังแสดงในตารางที่ 2.1

คุณสมบัติ	คำอธิบาย
การระบุตัวบุคคล (Authenticity)	ความสามารถระบุตัวบุคคลว่าเป็นบุคคลตามที่ได้กล่าวอ้างหรือมีอำนาจหน้าที่ตามที่ได้อ้างถึง

คุณสมบัติ	คำอธิบาย
การรักษาความลับ (Confidentiality)	ความสามารถในการรักษาความลับของข้อมูลมิให้ถูกเปิดเผย
การรักษาความถูกต้องสมบรูณ์ (Integrity)	ความสามารถในการรักษาความถูกต้องครบถ้วนของข้อมูลมิให้มีการแก้ไขโดยไม่ปรากฏร่องรอย
การป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation)	ความสามารถในการห้ามการปฏิเสธความรับผิดชอบจากฝ่ายต่างๆที่เกี่ยวข้องว่าไม่ได้มีการรับ-ส่งข้อมูลของตน

ตารางที่ 2.1 คุณสมบัติของกุญแจคู่สาธารณะ

องค์กรออกใบรับรองโดยทั่วไปหรือ CA (Certification Authority) จะมีบทบาทหน้าที่ในการให้บริการอยู่หลายด้าน เช่นด้านเทคโนโลยีการสร้างรหัสกุญแจคู่สาธารณะ การออกใบรับรอง การประกาศใบรับรอง การเรียกคืนกรณีกุญแจรหัสรับที่ออกใบรับรองได้มีปัญหาซึ่งอาจเกิดจากการสูญสาย ถูกขโมย ตลอดจนบริการเสริมต่างดังรูปที่ 2.2



รูปที่ 2.2 การบริการขององค์กรออกใบรับรอง [7]

ปัจจุบัน ผู้ให้บริการออกใบรับรองหรือ CA (Certification Authority) ในประเทศไทยมี สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) สังกัดสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช)กระทรวงวิทยาศาสตร์และเทคโนโลยี ได้จัดทำ G-CA (Government Certification Authority) ซึ่งเป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยอาศัยเทคโนโลยีหลักที่เรียกว่าโครงสร้างพื้นฐานระบบกุญแจสาธารณะ (Public Key Infrastructure – KPI) ซึ่งจะประกอบด้วยกุญแจรหัสส่วนตัว (Private Key) และ กุญแจสาธารณะ (Public Key) เป็นพื้นฐานสำคัญ โดย G-CA จะทำการรับรองข้อมูลต่างๆรวมทั้งกุญแจสาธารณะของบุคคลนั้น ซึ่งจะใช้กุญแจสาธารณะนี้ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) เพื่อใช้ในการยืนยันตัวบุคคล จาก News Letter online ฉบับที่ 9 : กุมภาพันธ์ 2549 - เมษายน 2549 หัวข้อ " Special Report New Vision From GITS Director " ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศภาครัฐได้กล่าวถึงการบริการของ G-CA ไว้ว่า "สำหรับบริการ CA ซึ่งคาดว่าภายในปีนี้จะได้รับการ Certified เป็นมาตรฐาน ซึ่งจะเป็นหน่วยงานแรกของประเทศไทยในการได้รับมาตรฐานในการให้บริการ CA ซึ่งจุดนี้เป็นขั้นตอนต่อไปในการที่จะทำให้ สบทร.มีการบริหารจัดการที่เป็นมาตรฐานได้" ดังนั้น ถ้า G-CA ของ สบทร. ได้รับการ Certified แล้ว น่าจะเป็นหน่วยงานหลัก ที่มีความน่าเชื่อถือในการให้บริการออกใบรับรองอิเล็กทรอนิกส์ภายในประเทศและพัฒนาต่อไปจนมีความน่าเชื่อถือใช้งานในระดับประเทศเพื่อการได้รับการยอมรับในระดับสากล ซึ่งในปัจจุบันประเทศไทยยังไม่มีหน่วยงานที่ทำหน้าที่ในการออกใบรับรองอิเล็กทรอนิกส์ที่มีการนำไปใช้ในธุรกรรมทางอิเล็กทรอนิกส์ในด้านการเงินที่มีมูลค่าในระดับเป็นร้อยล้านบาท จากงานวิจัยของ ดร.ราม ปิยะเกตุ และคณะ ในโครงการศึกษาวิเคราะห์พัฒนาการของ ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ ได้ทำการวิจัย ภาพรวมของพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย[22] ได้กล่าวว่า "จากการศึกษาพบว่า การได้รับการรับรองความน่าเชื่อถือของเว็บไซต์ของธุรกิจ ยังอยู่ในระดับต่ำมาก กล่าวคือธุรกิจส่วนใหญ่ยังขาดการรับรองความน่าเชื่อถือของเว็บไซต์ เช่น VeriSign, Truste, หรือ BBB เป็นต้น ดังนั้นจึงอาจเป็นอุปสรรคต่อการทำ ธุรกรรมกับลูกค้าในต่างประเทศได้" และ ถ้าในกรณีที่อธิการบดีจุฬาลงกรณ์จะต้องทำธุรกรรมอิเล็กทรอนิกส์ที่มีมูลค่ามหาศาลนั้น การเลือกใช้บริการของ CA เพื่อการยืนยันหรือรับรองความปลอดภัยของข้อมูล ในการทำธุรกรรมอิเล็กทรอนิกส์นั้นต้องเลือก CA ที่มีความน่าเชื่อถือในระดับสากล ดังตัวอย่างของสถาบันการเงินที่ให้ความสำคัญกับความเชื่อถือของผู้ให้บริการออกใบรับรองมากเช่น ธนาคารกรุงเทพ มีการใช้บริการของ Verisign Inc. Verisign Certificate ซึ่งเป็นใบรับรองที่ออกโดยบริษัท Verisign Inc. ในการนำมาใช้ทำธุรกรรมอิเล็กทรอนิกส์ เป็นต้น ซึ่งแม้แต่ในเอกสารเผยแพร่ของ สบทร. ใน G-CA Technology White Paper ยังกล่าวไว้ว่า "ปัจจุบันผู้ให้บริการออกใบรับรองมีหลายราย แต่ในการติดต่อกันระหว่างผู้ใช้ใบรับรองอิเล็กทรอนิกส์ซึ่งได้รับการรับรองโดยผู้ให้บริการออกใบรับรองคน

แต่ละแห่งจะมีปัญหาในเรื่องของความเชื่อในตัวบุคคล เนื่องจากผู้ให้บริการออกใบรับรองแต่ละแห่งจะใช้มาตรฐานต่างกันเช่นมาตรฐานในการตรวจสอบบุคคล มาตรฐานในด้านการรักษาความปลอดภัยระบบให้บริการใบรับรองอิเล็กทรอนิกส์ " ในความคิดเห็นของผู้วิจัย มาตรฐานที่ได้รับการยอมรับนำไปใช้งานในระดับสากลก็มีหลายมาตรฐาน แต่ละมาตรฐานก็มีจุดประสงค์ที่แตกต่างกันออกไปการได้รับรองมาตรฐานใดมาตรฐานหนึ่งไม่ได้ครอบคลุมถึงมาตรฐานอื่นๆด้วยโดยส่วนมากแล้วจะมีการนำมาตรฐานหนึ่งเป็นหลักแล้วนำมาตรฐานอื่นมาใช้ร่วมกันเพื่อเสริมความปลอดภัยให้มากขึ้นแต่ก็ไม่มีกรอบเพื่อเป็นแนวทางในการนำมาตรฐานมาใช้งานร่วมกัน งานวิจัยนี้ก็เป็นกรอบแนวทางขั้นตอนการปฏิบัติที่สามารถนำไปประยุกต์ใช้งานของกุญแจรหัสส่วนตัวในหน่วยงานต่างๆได้

2.2.3 ลักษณะการควบคุมความปลอดภัย

ในทางปฏิบัตินั้นเราสามารถที่กำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้ 5 ระดับ [8] ดังนี้คือ

1 การพิสูจน์ตัวตน (Authentication) คือการที่สามารถพิสูจน์และระบุว่าเป็นบุคคลที่ได้อ้างถึงหรือไม่ซึ่งจะมีอยู่ 2 ขั้นตอนคือ

1.1 การระบุตัวตน (Identification)

1.2 การพิสูจน์ตัวตน (Authentication)

1.1 การระบุตัวตน (Identification) จะต้องดูหลักฐานที่ผู้กล่าวอ้างนำมาใช้ ซึ่งจะต้องสามารถบ่งบอกได้ว่าคนที่กล่าวอ้างนั้นเป็นใคร (Actual identity) และสามารถที่จะแสดงหลักฐานทางด้านอิเล็กทรอนิกส์ ที่บ่งบอกข้อมูลของบุคคลที่อ้างอิงนั้นได้ (Electronic identity) ซึ่งในแต่ละบุคคลอาจมีมากกว่า 1 หลักฐาน

1.2 การพิสูจน์ตัวตน (Authentication mechanisms) วิธีในการพิสูจน์ตัวตนจะต้องทราบถึงข้อกำหนดอยู่ 3 ส่วนด้วยกันคือ

1.2.1 สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด

1.2.2 สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน

1.2.3 สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ ม่านตา เสียง

ในการพิสูจน์ตัวตนนั้นจะนำคุณลักษณะทั้ง 3 มาใช้ในการยืนยันในหลักฐานที่ผู้กล่าวอ้างอ้างถึงแต่การนำมาใช้เพียงอย่างหนึ่งในระบบ (Single-factor authentication) ก็ยังมีข้อจำกัดในการนำไปใช้งานเช่น สิ่งที่คุณมี (Possession factor) อาจเกิดการสูญหายหรือถูกการปลอมหรือ

สร้างขึ้นมาได้อย่างเหมือนต้นฉบับ สิ่งที่คุณรู้ (Knowledge factor) อาจถูกดักหรือถูกขโมย สิ่งที่คุณเป็น (Biometric factor) อาจมีความปลอดภัยมากกว่าสองอย่างข้างต้นแต่ก็ก็มีข้อจำกัดในการใช้งานหรือมีปัจจัยในการใช้งาน

2 การกำหนดสิทธิ์ (Authorization) เป็นขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้างโดยที่ต้องทราบว่าบุคคลที่กล่าวอ้างนั้นคือใคร ตามขบวนการขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าในการพิสูจน์ตัวตนนั้นถูกต้อง

3 การเข้ารหัส (Encryption) เป็นการเก็บข้อมูลส่วนบุคคลแยกจากบุคคลอื่นที่ไม่ได้รับอนุญาตมีอยู่ 2 ส่วนที่สำคัญที่จะทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ "การกำหนดสิทธิ์" และ "การพิสูจน์ตัวตน" เพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นและจะต้องแน่ใจได้ว่าบุคคลที่อ้างนั้นเป็นใคร ได้รับอนุญาตในการเข้ามาดูข้อมูลได้หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่ได้ทำการเข้ารหัสไว้

4 การรักษาความสมบูรณ์ (Integrity) หมายถึงการยืนยันและรับรองได้ว่าข้อมูลจะไม่ถูกทำการเปลี่ยนแปลงแก้ไขหรือถูกทำลายไปจากต้นฉบับ (source) ไม่ว่าจะโดยเหตุบังเอิญหรือถูกเปลี่ยนแปลงโดยเจตนาที่ส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูล คือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะเข้าควบคุมการจัดการของข้อมูลได้

5 การตรวจสอบ (Aaudit) คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ที่สามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและเที่ยงตรง การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

รูปที่ 2.3 **ความปลอดภัยแบบปิรามิด** [8]

ในการกำหนดและควบคุมทั้งบุคคลที่สามารถเข้าสู่ระบบและเข้าสู่ข้อมูลภายในระบบ และเพื่อกระทำการใดได้บ้าง อนุญาตตามระดับชั้นของความสำคัญของข้อมูล รวมไปถึงการจัดเก็บพฤติกรรมการใช้งานระบบของบุคคลนั้นต่อข้อมูลบนระบบทั้งหมด

ในการพิสูจน์ตัวตนนั้น จะมีวิธีการในการพิสูจน์ตัวตนอยู่ด้วยกันหลายวิธี ซึ่งแต่ละวิธีที่ใช้ในการพิสูจน์นั้นจะมีข้อดีและข้อเสียที่แตกต่างกันขึ้นอยู่กับเงื่อนไขและสภาพแวดล้อมด้วยกันหลายด้านการเปรียบเทียบการพิสูจน์ตัวตนของแต่ละวิธีการได้แสดงไว้พอสังเขปดังในตารางที่ 2.1

คอมพิวเตอร์ได้รับการพัฒนาไปในทิศทางที่ใช้เทคโนโลยีไร้สายมากขึ้นปัญหาที่ถูกนำเสนอขึ้นมาในเรื่องของความเชื่อถือได้ของการสื่อสาร ในด้านของความปลอดภัย โดยงานวิจัยของ Kumar Tanganathan ได้นำเสนอ "Trustworthy Pervasive Computing: The Hard Security Problem" [16] ได้ให้ข้อสังเกตุอยู่ 5 ส่วนด้วยกันคือ 1.เรากำลังติดต่ออยู่กับใคร 2.ข้อมูลส่วนบุคคลได้รับการปกป้องหรือไม่ 3.ความเชื่อถือได้ของอุปกรณ์ที่เรากับติดต่อสื่อสารอยู่ 4. ระบบได้เตรียมสภาพแวดล้อมในการใช้งานแค่ไหน และ 5. การสื่อสารในลักษณะกระจายแบบนี้มีความเชื่อถือได้แค่ไหน

การพิสูจน์ตัวตน	**ข้อดี**	**ข้อเสีย**
ไม่มีการพิสูจน์ตัวตนตน	ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ	ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่
การพิสูจน์ตัวตนโดยใช้รหัสผ่าน	สามารถใช้ได้กับทุกระบบ	จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็นสาธารณะหรือไม่มีการเข้ารหัสข้อมูล
การพิสูจน์ตัวตนโดยใช้ PIN	● ง่ายต่อการจำและความปลอดภัยค่อนข้างดี)บัตร ATM) ● สามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่าง ปลอดภัย	● ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN ● ไม่สามารถใช้กับต่างระบบกันได้ ● การดูแลรักษา PIN อาจถูกขโมยหรือทำซ้ำได้
การพิสูจน์ตัวตนโดยใช้ password	● จะมีความปลอดภัยมากกว่าการใช้การจำ	● การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน

การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
authenticators หรือ tokens แบบอะซิงโครนัส	รหัสผ่าน แบบธรรมดา ● ไม่ต้องใช้เครื่องอ่านการ์ด ● เป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับวิธีการใช้การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens	● authenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้ไม่สามารถป้องกันผู้ที่ละเมิดเข้ามาในระบบได้ ● การใช้งานค่อนข้างยุ่งยากกว่าวิธีการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password) ● ขนาดของข้อมูลมีขนาดใหญ่กว่าเดิมมากอาจเป็นปัญหาในการใช้งาน
การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล	มีความปลอดภัยสูงเพราะเลียนแบบกันได้ยาก	● ระบบมีความซับซ้อนสูง ● ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย ● ค่าใช้จ่ายค่อนข้างสูงเมื่อเทียบกับวิธีอื่นๆ ● ไม่สามารถเปลี่ยนแปลงได้ ● เป็นข้อมูลที่เปิดเผย ● เสียหายหรือถูกทำลายแล้วไม่สามารถกู้คืนหรือสำรอง
การพิสูจน์ตัวตนโดยวิธี One-Time Password	ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก	● ไม่สะดวกต่อการใช้งานเพราะผู้ใช้ต้องจำรหัสผ่านหลายตัว ● ถ้าผู้ใช้จำรหัสผ่านไม่ได้ หรือทำรหัสผ่านสูญหาย ก็ไม่สามารถเข้าใช้ระบบได้

การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
การพิสูจน์ตัวตนโดยการเข้ารหัสแบบคู่รหัสกุญแจ	● การจัดการกุญแจทำได้ปลอดภัย เพราะ ใช้กุญแจในการเข้ารหัส	● ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
	และถอดรหัสต่างกัน ● สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์	• ต้องใช้ระบบที่สนับสนุนการทำงาน
การพิสูจน์ตัวตนโดยการใช้ลายเซ็นดิจิตอล	● สามารถระบุตัวผู้ส่งได้ชัดเจน ● ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามาถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่	ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
การพิสูจน์ตัวตนโดยวิธี zero-knowledge proofs	● ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้และเซิร์ฟเวอร์เท่านั้นที่ทราบ	● ความซับซ้อนของระบบเพิ่มขึ้นตามความสามารถของระบบ

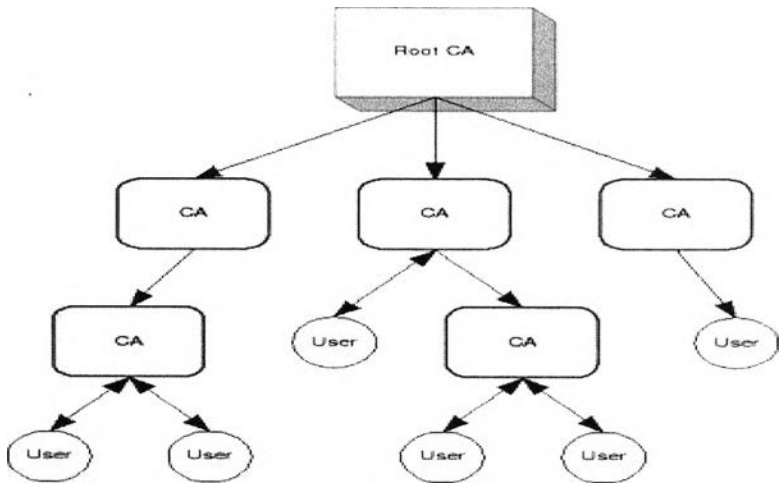
ตารางที่ 2.2 ตารางการเปรียบเทียบการพิสูจน์ตัวตน

2.2.4 รูปแบบการรับรองระหว่างหน่วยงาน

การใช้ใบรับรองอิเล็กทรอนิกส์หรือ ลายมือชื่ออิเล็กทรอนิกส์ ที่ใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์นั้นเพื่อยืนยันตัวบุคคลและความถูกต้องของข้อมูลโดยที่อาศัยใบรับรองจากผู้บริการออกใบรับรองอิเล็กทรอนิกส์นั้นจะมีผู้ให้บริการในการออกใบรับรองอยู่หลากหลาย ทำให้เกิดมีรูปแบบการรับรองระหว่างกันหลายมาตรฐานขึ้น ซึ่งพอจะสรุปรูปแบบต่างๆดังต่อไปนี้ [7]

2.2.4.1 Root CA/Hierarchy Model

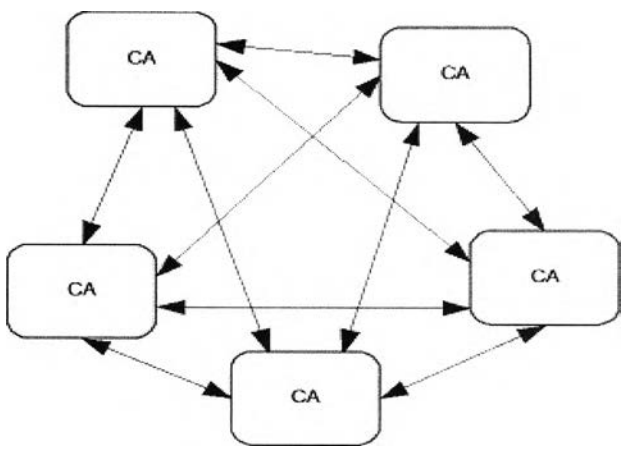
เป็นรูปแบบพื้นฐานที่ไม่ยุ่งยากซับซ้อน สร้างรูปแบบการมอบความไว้วางใจแบบนี้ได้ง่าย (ประเทศไทยเลือกใช้รูปแบบนี้ ประกาศวันที่ 20 กรกฎาคม 2547) โดยจะเป็นรูปแบบความสัมพันธ์ที่ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ที่เป็นที่ยอมรับหรือรู้จักและได้รับการไว้วางใจตั้งผู้ให้การรับรองระดับสูงสุดเพื่อให้การรับรองผู้รับรองในลำดับชั้นอื่นๆรองลงมา



รูปที่ 2.4 Root CA Model

2.2.4.2 Cross-Certification (Mesh)

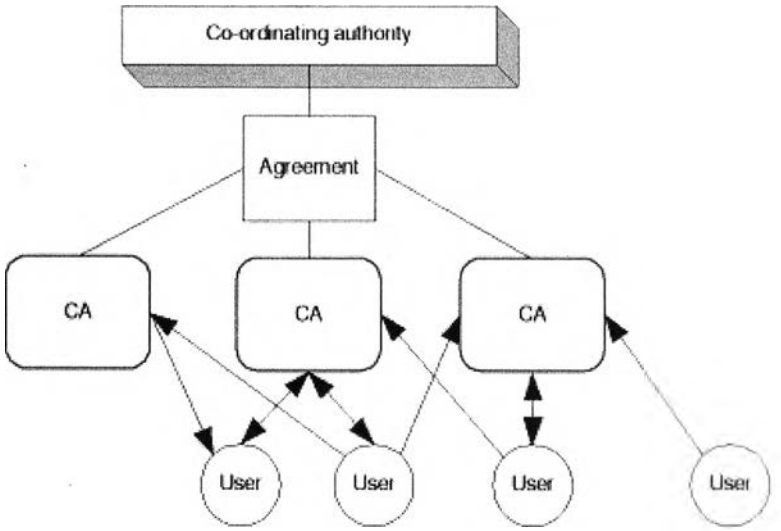
ผู้ให้บริการจะออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการซึ่งกันและกันทำให้ผู้ที่เป็นสมาชิกของหน่วยงานรับรองของตนสามารถค้นหาใบรับรองอิเล็กทรอนิกส์ของผู้ที่ตนติดต่อด้วยดังรูปที่ 4.4



รูปที่ 2.5 Root CA Model

2.2.4.3 Cross- Recognition

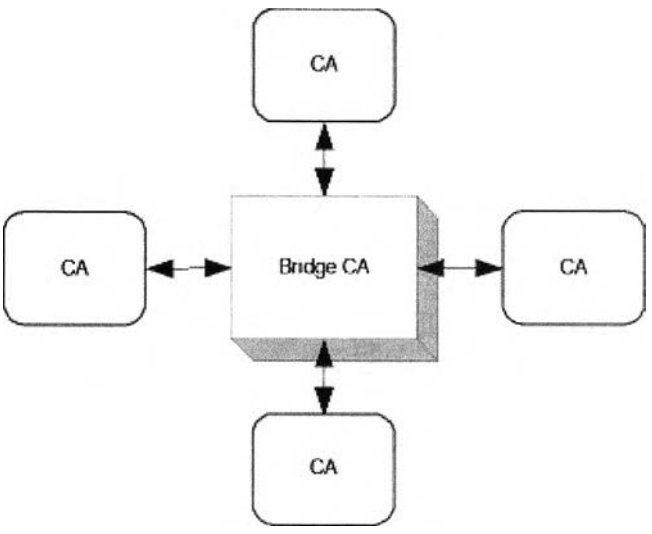
ความสัมพันธ์แบบนี้นั้นขึ้นอยู่กับผู้ที่ใช้บริการใบรับรองอิเล็กทรอนิกส์และ ผู้ที่เกี่ยวข้องจะเป็นผู้ตัดสินใจเลือกที่จะมอบความไว้วางใจของตนให้กับผู้ให้บริการออกใบรับรองรายใดบ้าง ซึ่งจะทำการติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการรับรองรายอื่น



รูปที่ 2.6 Cross- **Recognition**

2.2.4.4 Bridge CA

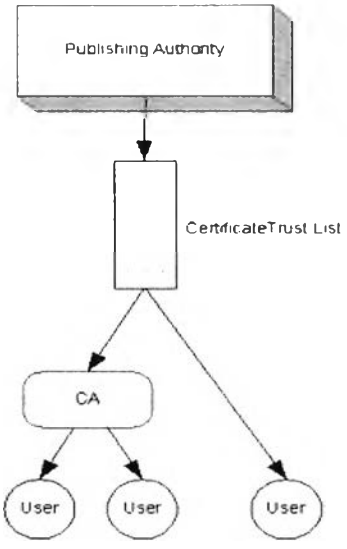
เป็นความสัมพันธ์ในรูปแบบที่มีผู้ให้บริการในการออกใบรับรองอิเล็กทรอนิกส์เป็นศูนย์กลางในการเชื่อมโยงติดต่อกับผู้ให้บริการรายอื่นๆ



รูปที่ 2.7 Bridge CA

2.2.4.5 Certificate Trust List

คือการประกาศกลุ่มรายชื่อของผู้ออกใบรับรอง (Certificate Trust List) ที่น่าเชื่อถือ



รูปที่ 2.8 Certificate Trust List

กฎหมายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [13] ได้กำหนดถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ในด้านผลบังคับว่าควรมีลักษณะหรือการกระทำได้ที่อยู่ภายใต้กฎหมายนี้ ซึ่งธุรกรรมทางอิเล็กทรอนิกส์หมายถึงการกระทำโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือเพียงบางส่วน [14] ตลอดจนไปถึงการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) [15] ว่าข้อมูลใดที่ไม่ควรจะทำการเปิดเผยเช่นในการเข้าเว็บไซต์บางแห่งจำกัดอายุเท่านั้นแต่ข้อมูลอื่นเช่น ที่อยู่ ชื่อ ก็ไม่ควรที่จะต้องถูกเปิดเผยด้วยเป็นต้น

2.3 ทฤษฎีการยอมรับและกระบวนการยอมรับ

การยอมรับหรือความไว้วางใจของผู้บริหารระดับสูงขององค์กรนั้นมีปัจจัย หรือองค์ประกอบอยู่หลายส่วนด้วยกัน ซึ่งการยอมรับและไว้วางใจนั้นจะนำไปสู่ความเชื่อมั่นของผู้บริหารที่จะนำขั้นตอนการปฏิบัติงานที่น่าเชื่อถือได้เพื่อการได้มาและการใช้งานของกุญแจรหัสส่วนตัวไปใช้งาน ดังนั้นต้องให้ผู้บริหารเกิดการยอมรับก่อน ซึ่งในการที่จะทำให้ผู้บริหารจะเกิดการยอมรับได้นั้นต้องเข้าใจถึงความหมายและกระบวนการของการยอมรับเสียก่อนซึ่งมีผู้ได้ให้ความหมายและแนวคิดเกี่ยวกับการยอมรับหลายท่านดังนี้

การยอมรับ คือการที่ได้เรียนรู้โดยผ่านการศึกษา สามารถบรรยายได้โดยผ่านขั้นการรับรู้ กระบวนการยอมรับจะเกิดขึ้นได้หากมีการเรียนรู้ด้วยตนเองและการเรียนรู้นั้นจะได้ผลเมื่อ

บุคคลนั้นได้ทดลองปฏิบัติ เมื่อแน่ใจแล้วว่าสิ่งประดิษฐ์นั้นสามารถให้ประโยชน์อย่างแน่นอนเขาจึงกล้าลงทุนกับงานประดิษฐ์นั้น [18]

การยอมรับนวัตกรรม หมายถึง การตัดสินใจที่จะนำนวัตกรรมนั้นไปใช้อย่างเต็มที่เพราะนวัตกรรมนั้นเป็นวิถีทางที่ดีกว่าและมีประโยชน์กว่าการยอมรับนวัตกรรมของบุคคลเกิดขึ้นเป็นกระบวนการเริ่มต้นตั้งแต่ได้สัมผัสนวัตกรรมถูกชักจูงให้ยอมรับนวัตกรรมตัดสินใจยอมรับหรือปฏิเสธ ปฏิบัติตามการตัดสินใจ และยืนยันการปฏิบัตินั้นกระบวนการนี้อาจกินเวลาช้าหรือเร็วขึ้นอยู่กับปัจจัยที่สำคัญคือ ตัวบุคคลและคุณลักษณะของนวัตกรรม (Roger 1983:11อ้างในกรกฎ) [19]

ได้มีการนำเสนอแนวคิดเกี่ยวกับการยอมรับสิ่งใหม่ และนำไปปฏิบัติของมนุษย์ว่าการศึกษาเป็นขบวนการสังคมอย่างหนึ่งที่ช่วยพัฒนาคุณสมบัติของบุคคล เช่น ความรู้ ค่านิยม ทัศนคติ ทำให้เป็นสมาชิกของสังคมได้และช่วยให้รับรู้การเปลี่ยนแปลง มีความเข้าใจในสิ่งใหม่ๆได้ง่าย บุคคลที่มีการศึกษาสูง อ่านหนังสือมากตลอดจนรับรู้ข่าวสารต่างๆอยู่ตลอดเวลาจะมีการยอมรับการปฏิบัติในสิ่งใหม่ๆ มากกว่าผู้ที่ที่มีการศึกษาน้อยและไม่ใฝ่ใจอ่านหนังสือ ไม่รู้จักเสาะแสวงหาข่าวสารเพิ่มเติม การติดต่อสัมพันธ์กับเจ้าหน้าที่ทั้งความสัมพันธ์ทางแนวตั้ง ได้แก่การติดต่อกับหน่วยงานต่างๆที่อยู่นอกชุมชนของตนเอง

สรุปได้ว่า การยอมรับ หมายถึงกระบวนการที่บุคคลได้ตัดสินใจที่จะนำเอานวัตกรรมที่ได้มานั้นนำไปปฏิบัติใช้งานได้ตามที่บุคคลนั้นต้องการ โดยผ่านการศึกษาหาความรู้ มีทัศนคติที่ดีตัดสินใจเลือกและทดลองนำไปปฏิบัติจนถึงการยืนยันรับนวัตกรรมนั้นๆมาใช้

การยอมรับมีกระบวนการที่เป็นแนวคิดในการที่จะทำให้บุคคลเกิดการยอมรับโดยเฉพาะนวัตกรรมใหม่ๆที่เกิดขึ้นและ โรเจอร์ ยังได้กล่าวถึงกระบวนการยอมรับนวัตกรรมไว้ว่าเป็นกระบวนการที่เกิดขึ้นได้ 5 ขั้นคือ

1. ขั้นรับทราบ (Awareness) หมายถึง ระยะเริ่มแรกที่บุคคลรับทราบว่ามีแต่ยังไม่ทราบรายละเอียดของนวัตกรรม ถือว่าเป็นระดับที่ 1
2. ขั้นสนใจ (Interest Stage) หมายถึง ระยะที่บุคคลสนใจวัตกรรมและแสวงหารายละเอียดเกี่ยวกับนวัตกรรมมากยิ่งขึ้น ถือว่าเป็นระดับที่ 2
3. ขั้นประเมินค่า (Evaluation Stage) หมายถึง ระยะที่บุคคลจะประเมินคุณค่าของนวัตกรรมนั้นโดยคำนึงถึงผลดีผลเสียของการยอมรับหรือปฏิเสธนวัตกรรม ถือว่าเป็นระดับที่ 3
4. ขั้นทดลองใช้ (Trial Stage) หมายถึง การที่บุคคลตัดสินใจนำนวัตกรรมไปทดลองใช้ในวงจำกัดเพื่อประกอบการตัดสินใจว่าจะนำไปใช้อย่างเต็มที่ต่อไปหรือไม่ ถือว่าเป็นระดับที่ 4

5. ขั้นยอมรับ (Adoption Stage) หมายถึง การที่บุคคลตัดสินใจนำนวัตกรรมนั้นไปใช้อย่างเต็มที่และในการณีที่บุคคลใช้นวัตกรรมนั้นอยู่แล้วก็จัดว่าอยู่ในขั้นนี้ด้วย ถือว่าเป็นระดับ 5

โรเจอร์ยังได้กล่าวถึง แบบจำลองกระบวนการตัดสินใจเกี่ยวกับนวัตกรรม (A Model of The Innovation Decision Process) ประกอบด้วย 5 ขั้นตอนดังนี้

1. ขั้นความรู้ กระบวนการตัดสินใจเกี่ยวกับนวัตกรรมเริ่มต้นเมื่อบุคคลได้สัมผัสนวัตกรรมและเริ่มต้นศึกษาหาความรู้เพื่อทำความเข้าใจถึงหน้าที่ของนวัตกรรมนั้น ความรู้เกี่ยวกับนวัตกรรมที่บุคคลได้รับในขั้นนี้สามารถแบ่งได้เป็น 3 ประเภท

    1.1 ความรู้จักนวัตกรรม ความรู้ประเภทนี้เป็นความรู้ทำให้เกิดการตื่นตัวเกี่ยวนวัตกรรม เป็นความรู้ที่รู้ว่ามีวัตกรรมนั้นสามารถทำหน้าที่อะไรได้บ้าง

    1.2 ความรู้วิธีการใช้นวัตกรรม ความรู้ประเภทนี้ได้จากการติดต่อกับสื่อมวลชนการติดต่อกับหน่วยราชการที่ทำการเผยแพร่รวัตกรรม หรือเข้าร่วมประชุม ความรู้ประเภทนี้จะช่วยให้สามารถใช้นวัตกรรมได้อย่างถูกต้อง ยิ่งนวัตกรรมมีความสลับซับซ้อนมากขึ้นเท่าใด ความจำเป็นที่ต้องมีความรู้ประเภทนี้ก็ยิ่งมากขึ้นเท่านั้น การขาดความรู้ในด้านนี้จะนำไปสู่การปฏิเสธนวัตกรรมได้มากขึ้น

    1.3 ความรู้เกี่ยวกับหลักการของนวัตกรรม ความรู้ประเภทนี้เป็นความรู้กฎเกณฑ์เบื้องหลังชของนวัตกรรมซึ่งจะช่วยให้นวัตกรรมบรรลุ เช่น ความรู้เกี่ยวกับเชื้อโรคและการระบาดของเชื้อโรคซึ่งช่วยให้เข้าใจว่าทำไมการฉีดวัคซีนหรือการสร้างส้วมให้ถูกสุขลักษณะจะช่วยป้องกันเชื้อโรคได้

2. ขั้นการจูงใจ ในขั้นนี้บุคคลมีการสร้างทัศนคติที่ชอบหรือไม่ชอบนวัตกรรม กิจกรรมในสมองของบุคคลขั้นความรู้เป็นเรื่องของความคิดหรือการรู้ ส่วนกิจกรรมในสมองในขั้นการจูงใจเป็นเรื่องของอารมณ์หรือความรู้สึก ในขั้นนี้บุคคลจะมีพฤติกรรมสำคัญคือ แสวงหาแหล่งข่าวสารข้อมูล แสวงหาสาระข่าวข้อมูลที่รับมาเกี่ยวกับนวัตกรรมนับว่าเหมาะสมกับตัวเขาทั้งในสภาพปัจจุบันและในอนาคตหรือไม่อย่างไร บุคคลจะมีการพัฒนาแนวคิดเชิงประเมินเกี่ยวกับนวัตกรรมนั้นเป็นการพิจารณาคุณค่าของนวัตกรรมว่าเมื่อรับมาใช้จะมีผลผลิตตามมาด้านใด เป็นประโยชน์หรือเป็นโทษต่อสภาพการทำงานของบุคคลนั้น ถ้าบุคคลพิจารณาเห็นว่าเป็นประโยชน์จะพัฒนาความรู้สึกในทางบวกต่อนวัตกรรม ขั้นการจูงใจเป็นขั้นตอนของกระบวนการตัดสินใจ ในการ

ยอมรับนวัตกรรมที่เกิดขึ้น เมื่อบุคคลต้องการเปลี่ยนแปลงสภาพเดิมที่มีอยู่แต่ยังมีความไม่แน่ใจในนวัตกรรมและอาจมีความรู้สึกเกี่ยวกับนวัตกรรมนั้นเป็นผลมาจากการรับรู้คุณค่าของนวัตกรรม ดังนั้นขั้นจูงใจจึงสอดคล้องกับขั้นการประเมินหรือพิจารณาทางเลือกในขั้นตอนกระบวนการตัดสินใจทั่วไป

3. ขั้นการตัดสินใจ การตัดสินใจยอมรับหรือไม่ยอมรับนวัตกรรมนั้นขึ้นอยู่กับ 2 ขั้นตอนที่ผ่านมาคือ ขั้นความรู้ และ ขั้นการจูงใจ ถ้าบุคคลมีความรู้เกี่ยวกับนวัตกรรม มีความรู้สึกชอบและเห็นประโยชน์ของวัตกรรมนั้นบุคคลก็มีแนวโน้มที่จะตัดสินใจยอมรับนวัตกรรมนั้น ขั้นการตัดสินใจเป็นขั้นตอนที่มีความสำคัญมาก การที่บุคคลจะเลือกทางเลือกใดเป็นผลมาจากขั้นความรู้และขั้นการ จูงใจและการพิจารณาลักษณะนวัตกรรมว่าสอดคล้องกับฐานะเศรษฐกิจ สถานภาพทางสังคมและขนมธรรมเนียมประเพณี

4. ขั้นการนำไปใช้ ในขั้นตอนต้นๆเป็นเรื่องของความรู้ ความคิดแต่การนำไปใช้เป็นเรื่องของการปฏิบัติ เมื่อบุคคลตัดสินใจที่จะยอมรับนวัตกรรมนั้นไปใช้ เขาต้องรู้ว่าเขาสามารถได้นวัตกรรมนั้นมาจากไหน นวัตกรรมนั้นใช้อย่างไร เมื่อนำไปใช้จะประสบปัญหาอย่างไรและสามารถแก้ปัญหานั้นได้อย่างไร ขั้นการนำไปใช้จะสิ้นสุดลงเมื่อใดขึ้นอยู่กับลักษณะของนวัตกรรมแต่ละชนิด เมื่อนวัตกรรมได้ถูกนำไปใช้และกลายเป็นส่วนหนึ่งของบุคคลในการดำเนินงานขั้นตอนนี้ก็สิ้นสุดลงและจบสิ้นกระบวนการตัดสินใจยอมรับนวัตกรรม แต่ในหลายกรณีนั้นการนำไปใช้จะนำไปสู่ขั้นตอนที่ 5 คือขั้นการยืนยันต่อไป

5. ขั้นการยืนยัน ขั้นตอนนี้เกิดขึ้นเป็นขั้นตอนสุดท้ายของกระบวนการตัดสินใจยอมรับนวัตกรรมในบุคคลส่วนใหญ่ กล่าวคือเมื่อบุคคลได้ตัดสินใจที่ยอมรับหรือไม่ยอมรับนวัตกรรมไปแล้ว บุคคลจะแสวงหาข่าวสารข้อมูลแรงเสริมเพื่อสนับสนุนการตัดสินใจของเขา ผลจากการแสวงหาข่าวสารข้อมูลเป็นผลให้บุคคลเปลี่ยนแปลงการตัดสินใจของตนเมื่อได้รับข่าวสารที่ขัดแย้งกับข้อมูลเดิมที่ได้รับมาบุคคลพยายามที่จะหลีกเลี่ยงความขัดแย้งหรือลดความขัดแย้งลงการได้รับการศึกษาอบรมเพิ่มเติมการให้คำปรึกษาหารือของเจ้าหน้าที่การได้รับข่าวสารจากสื่อสารมวลชนการได้รับคำแนะนำจากเพื่อนบ้าน ตลอดจนการเห็นผลสำเร็จของนวัตกรรมนั้นจะมีอิทธิพลต่อขั้นการยืนยันมาก คุณลักษณะของนวัตกรรมที่มีผลต่อระดับการยอมรับนวัตกรรมแบ่งได้ 5 ประการด้วยกันได้แก่

1. ประโยชน์ในเชิงเปรียบเทียบ (Relative Advantage) ได้แก่ ผลโดยเปรียบเทียบระหว่างคุณและโทษที่จะบังเกิดจากนวัตกรรมนั้น หากผู้ใช้เห็นว่านวัตกรรมนั้นมีประโยชน์หรือคุณค่ามากกว่า การยอมรับก็จะสูงตามไปด้วย

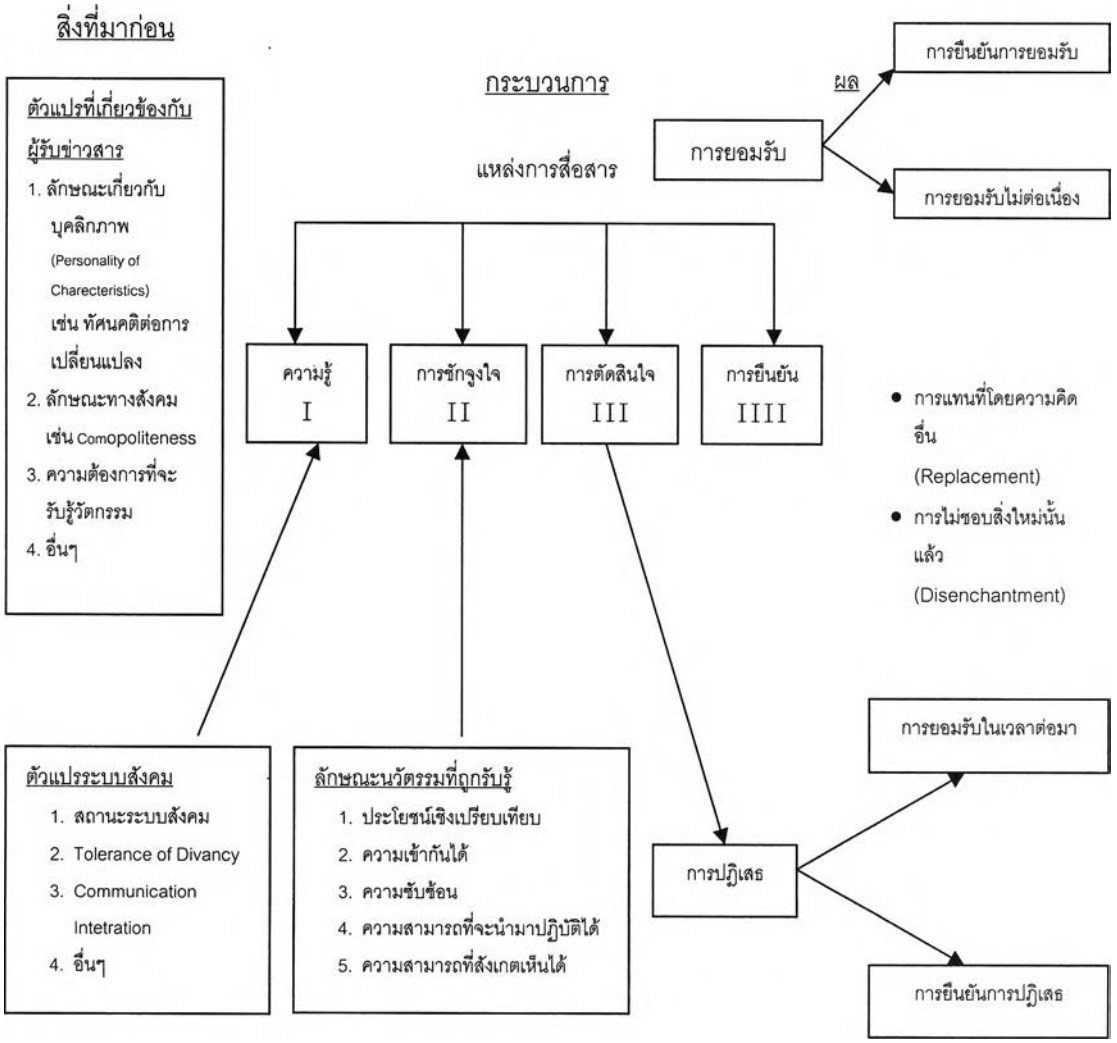
2. ความสอดคล้องต้องกัน (Compatibility) หรือความเข้าใจกันได้ระหว่างความเชื่อทางสังคมและวัฒนธรรมของผู้ใช้ซึ่งทำให้เกิดการยอมรับได้เร็วกว่านวัตกรรมที่มีความขัดแย้งกัน

ในเรื่องดังกล่าว เช่นเดียวกับการที่ผู้ใช้มีประสบการณ์เดิมในด้านนวัตกรรมและนวัตกรรมนั้นตรงกับความต้องการแล้วผู้ใช้จะยอมรับได้ง่ายและรวดเร็วขึ้น

3. ความสลับซับซ้อน (Complexity) หรือความยุ่งยากของนวัตกรรมจะทำให้ผู้ใช้ยอมรับยากและช้า ตรงข้ามกับนวัตกรรมที่เข้าใจง่าย ใช้สะดวกการยอมรับก็จะเป็นไปโดยง่ายและรวดเร็วกว่า

4. ความสามารถที่จะทดลองได้ (Trialability) นวัตกรรมที่สามารถแยกส่วนไปทดลองใช้ได้จะช่วยให้ผู้รับมีความรู้สึกเสี่ยงน้อยลง การยอมรับจะมากกว่าที่ไม่อาจทดลองได้ในขอบเขตจำกัด

5. ความสามารถสังเกตได้ (Observability) นวัตกรรมที่ผู้ใช้เห็นผลได้ง่ายและผล นั้นแสดงออกชัดเจน เข้าใจง่าย ผู้ใช้จะยอมรับได้ง่ายและรวดเร็วกว่า



รูปที่ 2.9 แนวคิดของกระบวนการตัดสินใจยอมรับนวัตกรรม [19]

การที่ผู้บริหารระดับสูงขององค์กร จะยอมรับสิ่งใหม่ๆที่ไม่คุ้นเคยหรืออาจยังไม่มีความคิดในการที่จะทำการทดลองใช้งานนวัตกรรมใหม่ๆนั้นต้องอธิบายให้ผู้บริหารได้เข้าใจถึงการเปลี่ยนแปลงการดำเนินงานโดยมีการใช้เทคโนโลยีเข้ามาทดแทนซึ่งการเปลี่ยนแปลงนั้น [18],[19] สามารถอธิบายได้ดังนี้คือ

1. การเปลี่ยนแปลงที่เกิดขึ้นในสังคมหรือวัฒนธรรมเป็นไปอย่างรวดเร็ว สม่ำเสมอ

2. การเปลี่ยนแปลงนั้นไม่ได้เป็นไปอย่างชั่วครั้งชั่วคราวหรือการเปลี่ยนแปลงเฉพาะเรื่องนั้นๆโดยลำพังแต่การเปลี่ยนแปลงมีแนวโน้มที่จะขยายออกไปในอาณาบริเวณกว้างหรือแผ่ออกไปทั่วโลก

3. การเปลี่ยนแปลงอาจเกิดได้ทุกสถานที่และมีความสำคัญต่อสังคมและวัฒนธรรมนั้นๆ การเปลี่ยนแปลงที่เกิดขึ้นและผลของมันมีความสัมพันธ์กัน คือก่อให้เกิดการเปลี่ยนแปลงอื่นๆตามมาอีก

4. การเปลี่ยนแปลงปัจจุบันเป็นผลมาจากการวางแผนเอาไว้หรือเป็นผลที่เกิดจากการประดิษฐ์สิ่งต่างๆมากกว่าสมัยก่อน

5. ความรู้ในทางเทคนิคและนโยบายต่างๆในสังคมแผ่ออกไปอย่างรวดเร็วและมีมากขึ้น ในขณะเดียวกันการเลิกใช้กระบวนการบางอย่างก็เกิดขึ้นอย่างรวดเร็วด้วยเช่นกัน

6. การเปลี่ยนแปลงมีผลกระทบกระเทือนถึงประสพการณ์ของปัจเจกบุคคล และสังคมอย่างกว้างขวาง ทุกคนย่อมประสบกับการเปลี่ยนแปลงอยู่เสมอ ปัจจัยที่มีอิทธิพลต่อการเปลี่ยนแปลงขององค์กรนั้นเกิดจากสาเหตุด้วยกันสองประการคือ ประการแรกการเปลี่ยนแปลงที่เกิดจากแรงผลักดันหรือพลังจากภายนอกองค์กร (External Forces) ประการที่สองการเปลี่ยนแปลงที่เกิดจากแรงผลักดันหรือพลังจากภายในองค์กร (Internal Forces) โดยที่รูปแบบความเปลี่ยนแปลงแบ่งออกได้เป็น 3 ประการคือ

6.1 เป็นการเปลี่ยนแปลงแบบค่อยเป็นค่อยไป (Incremental Change) หรือการเปลี่ยนแปลงแบบวิวัฒนาการ (Evolution Change)

6.2 เป็นการเปลี่ยนแปลงแบบปฏิวัติ (Evolution Change) หรือการเปลี่ยนแปลงแบบรุนแรง (Radical Change)

6.3 เป็นการเปลียนแปลงโดยการวางแผน (Planned Change)

บทบาทของผู้นำการเปลี่ยนแปลง

ในกระบวนการยอมรับของ โรเจอร์ นั้นก็ยังมีข้อจำกัดที่ควรคำนึงถึงดังนี้ [19]

1. กระบวนการยอมรับมักจบลงด้วยการตัดสินใจยอมรับ ขณะที่ความจริงนั้นอาจมีการปฏิเสธเกิดขึ้น ดังนั้น กระบวนการยอมรับจึงอาจเกิดการยอมรับหรือการปฏิเสธก็ได้

2. กระบวนการยอมรับทั้ง 5 ขั้น ไม่จำเป็นต้องเกิดขึ้นเรียงลำดับ โดยเฉพาะขั้นทดลอง จริงๆแล้วการประเมินเกิดขึ้นตลอดทั้งกระบวนการมากกว่าที่จะเกิดขึ้นเพียง 1 ครั้งใน 5 ขั้นข้างต้น

3. กระบวนการยอมรับไม่ได้จบลงด้วยการยอมรับ คน (Individual) อาจมีการค้นหาข้อมูลเพิ่มเติมเพื่อเสริมการตัดสินใจและอาจเปลี่ยนจากการยอมรับเป็นปฏิเสธก็ได้

จะเห็นได้ว่าในการที่จะทำให้ผู้บริหารยอมรับ ในนวัตกรรมใหม่ๆนั้นไม่ใช่เรื่องง่ายนัก เพราะว่าโดยปกตินั้นเรื่องความปลอดภัยเป็นสิ่งจะต้องมีความเข้าใจพื้นฐานหรือขั้นตอนในการปฏิบัติซึ่งอาจไม่อำนวยความสะดวกให้ในระดับผู้บริหารเท่าไหร่นักจะแต่ก็มีกระบวนการในการที่จะทำให้ผู้บริหารยอมรับใน นวัตกรรมแต่ทั้งนั้นการยอมรับก็มีทั้งการยอมรับและการปฏิเสธ ในบทที่ 3 จะเป็นขั้นตอนการวิจัยที่จะนำมาตรฐานต่างๆแยกแยะเป็นขั้นตอนในการปฏิบัติงานโดยใช้สภาพแวดล้อมของจุฬาลงกรณ์มหาวิทยาลัย