ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และ
แนวปฏิบัติ (Certification Practice Statement)
ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)
พ.ศ. ๒๕๕๒

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีความน่าเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวทางในการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

อาศัยอำนาจตามความในมาตรา ๒๘ (๖) มาตรา ๒๙ (๗) และมาตรา ๓๗ (๔) แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) จัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ตามแนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) ท้ายประกาศนี้

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๘ ตุลาคม พ.ศ. ๒๕๕๒
ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และ
แนวปฏิบัติ (Certification Practice Statement)
ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

๑. บทนำ

ในการนำใบรับรองอิเล็กทรอนิกส์ (Electronic Certificate) ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) เพื่อให้ผู้ใช้บริการสามารถนำไปใช้ในการรับรองตัวบุคคลผู้ถือใบรับรองสำหรับใช้ในการสร้างลายมือชื่อดิจิทัล (Digital Signature) อันเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ประเภทหนึ่ง หรือสำหรับการรับรองความมีตัวตนของนิติบุคคล หรือรับรองเครื่องให้บริการหรือเซิร์ฟเวอร์ (Server) หรือเอนทิตี (Entity) อื่นใดก็ตาม ด้วยการประยุกต์ใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure หรือเทคโนโลยี PKI) นั้น ความน่าเชื่อถือของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ นับว่ามีส่วนสำคัญยิ่งต่อการใช้บริการและก่อให้เกิดผลผูกพันทางกฎหมายในธุรกรรมต่างๆ ที่ทำขึ้นโดยมีการนำใบรับรองอิเล็กทรอนิกส์ไปใช้ยืนยันหรือรับรองตัวบุคคล นิติบุคคล เครื่องให้บริการหรือเซิร์ฟเวอร์ หรือเอนทิตีใดก็ตาม ในการทำธุรกรรมแต่ละครั้ง

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มีความน่าเชื่อถือ หน่วยงานที่ชื่อว่า Internet Engineering Task Force หรือ IETF ซึ่งทำการพัฒนาสถาปัตยกรรมทางอินเทอร์เน็ต (Internet Architecture) จึงได้กำหนดกรอบหรือแนวทางในการทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขึ้น เรียกว่า Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) อันเป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล จึงได้นำมาใช้เป็นแนวทางในการจัดทำประกาศฉบับนี้สำหรับใช้ปฏิบัติในการจัดทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในประเทศไทย เพื่อให้สอดคล้องตามมาตรฐานสากล

๒. คำนิยาม (Definition) และคำย่อ (Acronym)

ในส่วนนี้แสดงถึงคำนิยามและคำย่อเพื่อให้ความหมายกับคำที่ถูกใช้ในเอกสารนี้อย่างเข้าใจได้ถูกต้องตรงกัน

คำ/คำย่อ	คำนิยาม
RFC	“The Internet Request For Comments” เป็นชุดเอกสารที่เขียนเพื่อนิยามหรือบรรยายตามความเป็นจริงปัจจุบันและแนะนำแนวปฏิบัติเกี่ยวกับเกณฑ์วิธี (Protocol) และนโยบายของอินเทอร์เน็ต เป็นต้น

คำ/คำย่อ	คำนิยาม
บุคคล	บุคคลธรรมดา หรือนิติบุคคล
เอนทิตี	บุคคลและรวมถึงเครื่องให้บริการ (Server) หรือเว็บไซต์ หรือหน่วยปฏิบัติงาน (Operating Unit/Site) หรือเครื่องมืออื่นใด (Device) ที่อยู่ภายใต้การควบคุมของบุคคล
Certificate Revocation List (CRL)	รายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ คือ รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนการใช้งาน
Online Certificate Status Protocol (OCSP)	เกณฑ์วิธี (Protocol) สำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง หรือวันเวลาที่เริ่มต้นและสิ้นสุดการใช้ใบรับรอง
Object Identifier (OID)	ค่าสัมพันธ์ซึ่งบ่งบอกถึงข้อมูลสารสนเทศของวัตถุ (Information Object) ใดๆ โดยเป็นค่าที่สามารถบ่งชี้ได้ถึงความเป็นหนึ่งเดียวของ Object นั้นๆ
กุญแจสาธารณะ Public Key	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น
กุญแจส่วนตัว Private Key	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้
คู่กุญแจ Key Pair	กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการที่ทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้

คำ/คำย่อ	คำนิยาม
เจ้าหน้าที่รับลงทะเบียน Registration Authority (RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ แจ้งเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ใช้บริการให้ไว้
พฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล (Compromise)	หมายถึง การที่ข้อมูลสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์ของการเก็บรักษาข้อมูลนั้น รวมทั้งกรณีที่มีเหตุอันควรสงสัยว่าจะมีพฤติการณ์ดังกล่าว

๓. หัวข้อที่ต้องกำหนดไว้ในแนวนโยบาย และ แนวปฏิบัติ

บทที่ ๑ บทนำ (Introduction)

บทที่ ๒ ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

บทที่ ๓ การระบุและการยืนยันตัวบุคคล (Identification and Authentication)

บทที่ ๔ ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operation Requirements)

บทที่ ๕ การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)

บทที่ ๖ การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

บทที่ ๗ การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)

บทที่ ๘ การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่างๆ และการประเมินความเสี่ยงอื่นๆ (Compliance Audit and Other Assessment)

บทที่ ๙ ข้อกำหนดอื่นๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

๔. เนื้อหาที่ต้องกำหนดไว้ในแนวนโยบาย และแนวปฏิบัติ

บทที่ ๑ บทนำ (Introduction)

เนื้อหาในบทนี้ จะกล่าวถึงประเภทของบุคคลหรือเอนทิตีที่เกี่ยวข้องและการนำแนวนโยบายหรือแนวปฏิบัติไปใช้งาน

๑. ข้อมูลเบื้องต้นทั่วไป (Overview)

สาระสำคัญของเนื้อหาในข้อนี้ คือ การกล่าวถึงแนวนโยบายและแนวปฏิบัติ โดยทั่วๆ ไป และการนำแนวนโยบายและแนวปฏิบัติที่จัดทำขึ้นไปปรับใช้เมื่อมีการประยุกต์ใช้ PKI เช่น กรณีที่มีการกำหนดระดับความน่าเชื่อถือของใบรับรองอิเล็กทรอนิกส์ที่แตกต่างกัน ใบรับรองซึ่งแตกต่างกันนั้นอาจมีความซับซ้อนหรืออาจมีการกำหนดขอบเขตการใช้ PKI ที่แตกต่างกัน ดังนั้น การแสดงข้อมูลเกี่ยวกับโครงสร้างของ PKI จึงมีประโยชน์ต่อการทำความเข้าใจเนื้อหาในส่วนนี้

๒. ชื่อเอกสาร (Document Name and Identification)

เนื้อหาในส่วนนี้จะกำหนดเกี่ยวกับ “ชื่อ” สำหรับใช้เรียกแนวนโยบายและแนวปฏิบัติ หรือเรียกสิ่งหนึ่งสิ่งใด (Other Identifier) ทั้งนี้ รวมถึงการเรียกชื่อเอกสารหรือสิ่งที่ระบุถึงเช่นว่านั้นในทางเทคนิคด้วย กล่าวคือ จำเป็นต้องมีการจดทะเบียนเลข OID ซึ่งมีชื่อเรียกอย่างเป็นทางการว่า “ASN.1 Object Identifier ” ในทางปฏิบัติการกำหนดเลข OID ของแนวนโยบายและแนวปฏิบัติ หรือสิ่งหนึ่งสิ่งใดนั้นก็เพื่อให้สามารถตรวจสอบได้ว่าแนวนโยบายและแนวปฏิบัติ หรือสิ่งอื่นที่ถูกระบุถึงและกำกับด้วยเลข OID นั้น มีอยู่จริง เนื่องจากเลข OID จะเป็นตัวเลขซึ่งมีความสัมพันธ์หรือเชื่อมโยงถึง Information Object ใดๆ ลักษณะการกำหนดเลข OID จะมีการจัดเรียงลำดับตัวเลขกันและคั่นตัวเลขด้วยจุด โดยมีหน่วยงานรับจดทะเบียนเลข OID จำนวนหลายหน่วยงานด้วยกัน ได้แก่ American National Standard Institute (ANSI) สหรัฐอเมริกา, ISO เป็นต้น

๓. บุคคลที่เกี่ยวข้อง (PKI Participants)

เนื้อหาในบทนี้ควรจะกำหนดลักษณะ (Identity) ประเภทของบุคคลหรือเอนทิตี (Entity) ที่เกี่ยวข้อง รวมทั้งกำหนดบทบาทและหน้าที่ของบุคคลหรือเอนทิตีเหล่านั้นด้วย

๓.๑ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

คือ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งสร้างและออกใบรับรองอิเล็กทรอนิกส์เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ

๓.๒ เจ้าหน้าที่รับลงทะเบียน (Registration Authority)

คือ บุคคลหรือเอนทิตี ที่ทำหน้าที่ในการตรวจสอบตัวบุคคลผู้สมัครขอใช้บริการ ทั้งในขั้นตอนที่มีการะบุตัวบุคคลผู้สมัครขอใช้บริการ (Identification) ว่าผู้สมัครขอใช้บริการเป็นใคร หรือเอนทิตีใดและขั้นตอนการยืนยันหรือพิสูจน์ตัวบุคคล (Authentication) ว่า ผู้สมัครขอใช้บริการหรือเอนทีตีอื่นใด

เป็นบุคคลหรือเอนทิตีนั้นจริง นอกจากนั้นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเจ้าหน้าที่รับลงทะเบียน จะทำหน้าที่ทำนองเดียวกันในการเพิกถอนใบรับรอง หรือต่ออายุใบรับรอง โดยทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้สมัครขอใช้บริการได้ให้ไว้ในขั้นตอนต่างๆ หลังจากตรวจสอบความถูกต้องของข้อมูลผู้สมัครขอใช้บริการเรียบร้อยแล้ว จึงแจ้งให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ออกใบรับรองให้กับผู้สมัครขอใช้บริการต่อไป ทั้งนี้เจ้าหน้าที่รับลงทะเบียน อาจเป็นบุคลากรของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรืออาจเป็นบุคลากรของผู้สมัครขอใช้บริการ หรืออาจเป็นหน่วยงานหรือเอนทิตีอื่นที่ได้ทำข้อตกลงกับเจ้าหน้าที่รับลงทะเบียน เพื่อทำหน้าที่ดังกล่าว

๓.๓ ผู้ใช้บริการ (Subscriber)

คือ บุคคล หรือเอนทิตีใดๆ ที่ได้รับใบรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

๓.๔ คู่กรณีที่เกี่ยวข้อง (Relying Party)

คือ บุคคล หรือเอนทิตีอื่นใดที่เชื่อถือลายมือชื่อดิจิทัล อันเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง หรือเชื่อถือใบรับรองอิเล็กทรอนิกส์ ดังนั้น คู่กรณีที่เกี่ยวข้องอาจเป็นผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรืออาจไม่ใช่ผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ก็ได้ แต่เป็นผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองอิเล็กทรอนิกส์หรือลายมือชื่อดิจิทัล โดยการใช้กุญแจสาธารณะที่อยู่ในใบรับรองนั้นในการตรวจสอบตัวตนที่แท้จริงของผู้ขอใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัลและมีชื่อปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์

๓.๕ บุคคลซึ่งเกี่ยวข้องอื่นๆ (Other Participants)

คือ บุคคล หรือเอนทิตีอื่น นอกจากที่กล่าวถึงข้างต้น เช่น ผู้ให้บริการในการเก็บรักษาข้อมูล (Providers of Repository Services) หรือผู้ได้รับการว่าจ้างโดยการ Outsource ให้เป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๓.๖ การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)

เนื้อหาในส่วนนี้ควรกำหนดเกี่ยวกับลักษณะหรือประเภทของใบรับรองอิเล็กทรอนิกส์ที่มีการนำไปใช้ในทางปฏิบัติ เช่น ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองตัวบุคคล ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองตัวนิติบุคคล ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองเว็บไซต์ ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองเครื่องให้บริการหรือเซิร์ฟเวอร์ ใบรับรองอิเล็กทรอนิกส์เพื่อใช้กับจดหมายอิเล็กทรอนิกส์หรืออีเมล์ ใบรับรองอิเล็กทรอนิกส์สำหรับใช้กับสัญญาหรือการทำข้อตกลง เป็นต้น

ทั้งนี้ ในกรณีที่มีข้อจำกัดการใช้งาน หรือกรณีที่มีการจัดระดับความน่าเชื่อถือของใบรับรองอิเล็กทรอนิกส์ ก็ควรระบุไว้ให้ชัดเจนด้วย และหากลักษณะการใช้งานหรือชนิดของใบรับรองอิเล็กทรอนิกส์มีความแตกต่างกันจนจำเป็นต้องจัดทำแนวนโยบายหรือแนวปฏิบัติสำหรับการใช้งานแต่ละลักษณะหรือตามชนิดของใบรับรอง ก็จำเป็นต้องให้ข้อมูลในเรื่องดังกล่าวเอาไว้ชัดเจนด้วยเช่นกัน

๓.๗ การบริหารจัดการเกี่ยวกับแนวนโยบายและแนวปฏิบัติ (Policy Administration)

เนื้อหาในส่วนนี้ควรกล่าวถึงชื่อ ที่อยู่ของหน่วยงานที่ยกร่าง จดทะเบียน ดูแลและปรับปรุงเอกสารแนวนโยบายและแนวปฏิบัติ นอกจากนั้นยังรวมถึง ชื่อ ที่อยู่ของจดหมายอิเล็กทรอนิกส์ หมายเลขโทรศัพท์ หมายเลขโทรสารของผู้ที่สามารถติดต่อได้ ทั้งนี้ โดยอาจกำหนดเป็นตำแหน่งที่รับผิดชอบในการตอบข้อซักถามหรือติดต่อกับผู้ใช้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ก็ได้

นอกจากนั้น เพื่อสร้างความน่าเชื่อถือให้กับการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เอง ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้จัดทำแนวนโยบายและแนวปฏิบัติ ตามแนวทางที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนดแล้ว ควรระบุถึงคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และที่อยู่ของหน่วยงานธุรการของคณะกรรมการไว้ในข้อนี้ด้วย

๓.๘ คำนิยามและคำย่อ (Definitions and Acronyms)

โดยที่ในการจัดทำแนวนโยบายและแนวปฏิบัติ จำเป็นต้องมีการกล่าวถึงคำศัพท์ และคำย่อเป็นจำนวนมาก ดังนั้น ในบทนี้จึงควรมีการให้ความหมายของคำศัพท์หรือคำย่อเหล่านั้นไว้ด้วย เช่น การให้ความหมายของคำว่าผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียนผู้ใช้บริการ แนวนโยบายและแนวปฏิบัติ ลายมือชื่อดิจิทัล ใบรับรองอิเล็กทรอนิกส์ คู่กุญแจ กุญแจส่วนตัว กุญแจสาธารณะ เอนทิตี เป็นต้น เพื่อเป็นข้อมูลให้กับผู้ใช้บริการต่อไป

บทที่ ๒ ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

สำหรับเนื้อหาในส่วนนี้ ควรจะต้องระบุเกี่ยวกับบุคคลซึ่งทำหน้าที่ในการเก็บรักษาข้อมูล (Repository) ในการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ไม่ว่าผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะทำหน้าที่ดังกล่าวนั้นเอง หรือเป็นการใช้บริการจากผู้ให้บริการรายอื่น และความรับผิดชอบของบุคคลหรือหน่วยงานที่ทำหน้าที่ในการเผยแพร่ข้อมูลเกี่ยวกับแนวนโยบาย และแนวปฏิบัติ รวมทั้งเนื้อหาที่จะมีการเผยแพร่ เช่น การควบคุมมาตรการในการรักษาความมั่นคงปลอดภัย (Security Controls) การรักษาความลับทางการค้า (Trade Secret) สำหรับข้อมูลสำคัญที่มีความอ่อนไหว เป็นต้น

นอกจากนั้น ควรให้ข้อมูลเกี่ยวกับความถี่หรือความบ่อยในการเผยแพร่ข้อมูล การควบคุมการเข้าถึงข้อมูลที่มีการเผยแพร่นั้น (Access Control) รวมทั้งแนวนโยบายและแนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ หรือสถานะของใบรับรองอิเล็กทรอนิกส์ รวมทั้งการเพิกถอนใบรับรองอิเล็กทรอนิกส์

บทที่ ๓ การระบุและการยืนยันตัวบุคคล ((Identification and Authentication (I&A))

สำหรับเนื้อหาในบทนี้ควรให้ข้อมูลเกี่ยวกับขั้นตอนในการยืนยันหรือพิสูจน์ตัวบุคคล หรือเอนทิตีของผู้สมัครขอใช้บริการกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเจ้าหน้าที่รับลงทะเบียนก่อนที่จะมีการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งกำหนดขั้นตอนในการยืนยันหรือพิสูจน์บุคคลของ

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเจ้าหน้าที่รับลงทะเบียน หรือเอนทิตีที่เกี่ยวข้องกับการให้บริการหรือร่วมให้บริการกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ นอกจากนั้น อาจให้ข้อมูลเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ใหม่ การต่ออายุใบรับรองอิเล็กทรอนิกส์ หรือการเพิกถอนใบรับรองอิเล็กทรอนิกส์ไปพร้อมกันด้วย อย่างไรก็ตาม เนื้อหาที่พึงกำหนดไว้ในบทนี้นอกจากที่กล่าวถึงข้างต้น มีดังต่อไปนี้

๑. การกำหนดรูปแบบของชื่อ (Naming)

สำหรับการกำหนดรูปแบบของชื่อที่ใช้ (Naming Convention) เพื่อระบุถึงผู้ใช้บริการนั้น ควรกำหนด ดังนี้

๑.๑ รูปแบบของชื่อ เช่น X.500 Distinguished Name หรือ RFC 822 Names สำหรับจดหมายอิเล็กทรอนิกส์หรืออีเมล์ (e-mail) และ X.400 สำหรับชื่อ

๑.๒ ชื่อนั้น จะมีความหมายหรือไม่มีก็ได้

๑.๓ การกำหนดชื่อของผู้ใช้บริการในกรณีที่มีการใช้ชื่อนิรนามหรือนามแฝงหรือปิดบังชื่อที่แท้จริง (Anonymous or Pseudonymous)

๑.๔ กฎในการแปลงชื่อในรูปแบบต่างๆ เช่น มาตรฐาน X.500 และ RFC 822 เป็นต้น

๑.๕ ชื่อนั้นจะต้องมีลักษณะเฉพาะ (Unique Name)

๒. ความสมบูรณ์ในการระบุตัวบุคคล (Initial Identity Validation)

ข้อมูลในส่วนนี้ ควรจะกำหนดเกี่ยวกับวิธีการระบุตัวบุคคล (Identification) และยืนยันหรือพิสูจน์ตัวบุคคล (Authentication) เมื่อแรกเริ่มลงทะเบียนกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ หรือคู่กรณีที่เกี่ยวข้องอื่นๆ ทั้งนี้ โดย

๒.๑ การยืนยันหรือพิสูจน์ความสัมพันธ์ของกุญแจส่วนตัวกับกุญแจสาธารณะที่ถือหรือครอบครองอยู่โดยผู้ใช้บริการ เช่น การใช้ในการพิสูจน์ลายมือชื่อดิจิทัลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ด้วยการใช้ลายมือชื่อดิจิทัลในการส่ง Certificate Request Message มายังผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๒.๒ การยืนยันหรือพิสูจน์เงื่อนไขสำหรับการตรวจสอบความมีอยู่ขององค์กรหรือหน่วยงาน เช่น การตรวจสอบจากหนังสือรับรองของบริษัทหรือนิติบุคคลที่ออกโดยกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ เป็นต้น

๒.๓ การยืนยันหรือพิสูจน์เงื่อนไขสำหรับการตรวจสอบข้อมูลของบุคคลซึ่งกระทำการในนามขององค์กรหรือหน่วยงาน เช่น การตรวจสอบจากหนังสือมอบอำนาจ เป็นต้น

๓. การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอออกกุญแจใหม่ (Identification and Authentication for Re-key Requests)

สำหรับขั้นตอนนี้ จะครอบคลุมทั้งในขั้นตอนที่ใบรับรองอิเล็กทรอนิกส์หมดอายุลงและกรณีมีการเพิกถอนการใช้ใบรับรองอิเล็กทรอนิกส์ ดังนั้น จึงควรจะเป็นขั้นตอนที่มีรูปแบบการทำงานทำนองเดียวกันกับการระบุและยืนยันหรือพิสูจน์ตัวบุคคลเหมือนกับขั้นตอนแรกที่ได้มีการขอใช้บริการ

๔. การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Identification and Authentication for Revocation Requests)

เพื่อระบุประเภทของบุคคลที่สามารถทำการร้องขอเพิกถอนใบรับรองอิเล็กทรอนิกส์และขั้นตอนในการยืนยันหรือพิสูจน์ข้อมูลที่แสดงตัวตนของบุคคลดังกล่าวรวมทั้งสิทธิของบุคคลนั้น

บทที่ ๔ ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operation Requirements)

ข้อมูลในส่วนนี้ใช้ในการระบุข้อกำหนดในการดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์สำหรับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ และบุคคลที่เกี่ยวข้องอื่นๆ ให้สอดคล้องกับบทบาทและหน้าที่ของตน

๑. การยื่นคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application)

ส่วนนี้ควรระบุข้อกำหนดเกี่ยวกับการสมัครขอใบรับรองอิเล็กทรอนิกส์ดังต่อไปนี้

๑.๑ บุคคลที่สามารถสมัครขอใบรับรองอิเล็กทรอนิกส์ได้ เช่น ผู้ที่จะมีชื่อในใบรับรองอิเล็กทรอนิกส์ (Certificate Subject) หรือ RA เป็นต้น

๑.๒ กระบวนการยื่นคำขอใบรับรองอิเล็กทรอนิกส์ และภาระหน้าที่ที่เกี่ยวข้อง ตัวอย่างของกระบวนการยื่นขอใบรับรองอิเล็กทรอนิกส์ อาจเป็นดังต่อไปนี้

(๑) ผู้ส่งคำขอใบรับรองสร้างคู่กุญแจและส่งคำขอใบรับรองอิเล็กทรอนิกส์ให้เจ้าหน้าที่รับลงทะเบียน โดยผู้ส่งคำขอใบรับรองต้องให้ข้อมูลที่ครบถ้วนและถูกต้องตามระเบียบการขอใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

(๒) เจ้าหน้าที่รับลงทะเบียนตรวจคำขอ และลงลายมือชื่อกำกับคำขอที่ผ่านการตรวจสอบแล้วไปให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน และผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ต้องกำหนดหลักการและวิธีการขอใบรับรองอิเล็กทรอนิกส์

๒. การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับกระบวนการพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ ตัวอย่างกระบวนการ เช่น

๒.๑ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียนจะดำเนินการตรวจสอบความถูกต้องของผู้สมัคร เพื่อการระบุและยืนยันตัวบุคคล

๒.๒ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียนจะพิจารณาว่าจะอนุมัติหรือไม่อนุมัติการสมัครขอใช้บริการใบรับรองอิเล็กทรอนิกส์

๒.๓ การกำหนดระยะเวลาที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และเจ้าหน้าที่รับลงทะเบียนใช้ในการพิจารณาการยื่นคำขอใบรับรองอิเล็กทรอนิกส์

๓. การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับกระบวนการออกใบรับรองอิเล็กทรอนิกส์ในประเด็นต่างๆ ดังต่อไปนี้

๓.๑ ข้อปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ในการออกใบรับรองอิเล็กทรอนิกส์ เช่น การตรวจลายมือชื่อและอำนาจกระทำการของ เจ้าหน้าที่รับลงทะเบียน ตลอดจนการสร้างใบรับรองอิเล็กทรอนิกส์

๓.๒ วิธีการแจ้งผลการออกใบรับรองอิเล็กทรอนิกส์แก่ผู้ใช้บริการ เช่น การแจ้งทางจดหมายอิเล็กทรอนิกส์

๔. การยอมรับใบรับรองอิเล็กทรอนิกส์ (Certificate Acceptance)

๔.๑ ข้อปฏิบัติของผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ที่ถือเป็นการยอมรับใบรับรองอิเล็กทรอนิกส์ เช่น ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ออกให้ในกรณีที่

(๑) ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มิได้รับการแจ้งการใดๆ จากผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ภายในเวลาที่กำหนด

(๒) ผู้ใช้บริการลงลายมือชื่อกำกับข้อความแจ้งการยอมรับหรือไม่ยอมรับใบรับรองอิเล็กทรอนิกส์

๔.๒ การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้ยอมรับโดยผู้สมัครขอใบรับรองอิเล็กทรอนิกส์แล้ว ซึ่งอาจเผยแพร่โดยผ่านทาง X.500 Directory หรือ LDAP repository

๔.๓ การแจ้งให้บุคคลอื่นทราบถึงใบรับรองอิเล็กทรอนิกส์ที่ได้ออกให้ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ เช่น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจส่งใบรับรองอิเล็กทรอนิกส์ที่ออกให้ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ แก่เจ้าหน้าที่รับลงทะเบียน เป็นต้น

๕. การใช้คู่กุญแจ และใบรับรองอิเล็กทรอนิกส์ (Key Pair and Certificate Usage)

๕.๑ ความรับผิดชอบของผู้ใช้บริการในการใช้คู่กุญแจและใบรับรองอิเล็กทรอนิกส์ เช่น ผู้ใช้บริการจะต้องใช้กุญแจส่วนตัว (Private Key) และใบรับรองอิเล็กทรอนิกส์ตามนโยบายที่กำหนดในแนวนโยบาย และสัญญาระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์กับผู้ใช้บริการ โดยผู้ใช้บริการสามารถใช้กุญแจส่วนตัวหลังจากที่ผู้ใช้บริการได้ยอมรับใบรับรองอิเล็กทรอนิกส์นั้นแล้ว และไม่สามารถใช้งานกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ได้หลังจากใบรับรองอิเล็กทรอนิกส์ดังกล่าวหมดอายุลงหรือถูกเพิกถอน

๕.๒ ความรับผิดชอบของคู่กรณีที่เกี่ยวข้องในการใช้กุญแจสาธารณะ หรือใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ เช่น คู่กรณีที่เกี่ยวข้องจะต้องใช้ใบรับรองอิเล็กทรอนิกส์ตามนโยบายที่กำหนดในแนวนโยบาย และต้องตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ตามวิธีที่ระบุใน แนวนโยบายภายใต้เงื่อนไขเกี่ยวกับคู่กรณีที่เกี่ยวข้อง

๖. การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal)

การต่ออายุใบรับรองอิเล็กทรอนิกส์ หมายถึง การออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการโดยไม่มีการเปลี่ยนแปลงกุญแจสาธารณะของผู้ใช้บริการ หรือข้อมูลอื่นใดที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ การต่ออายุใบรับรองอิเล็กทรอนิกส์ควรคำนึงถึงประเด็นต่าง ๆ ดังต่อไปนี้

๖.๑ กรณีต่าง ๆ ที่อนุญาตให้มีการต่ออายุใบรับรองอิเล็กทรอนิกส์ เช่น ใบรับรองอิเล็กทรอนิกส์หมดอายุแต่นโยบายอนุญาตให้ใช้คู่กุญแจเดิมต่อไปได้ ให้สามารถต่ออายุใบรับรองอิเล็กทรอนิกส์ได้

๖.๒ บุคคลที่สามารถขอต่ออายุใบรับรองอิเล็กทรอนิกส์ได้ เช่น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจอนุญาตให้เจ้าหน้าที่รับลงทะเบียน ขอต่ออายุแทนผู้ใช้บริการได้ หรือผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจต่ออายุใบรับรองอิเล็กทรอนิกส์ให้ผู้ใช้บริการโดยอัตโนมัติเมื่อใบรับรองดังกล่าวหมดอายุลง

๖.๓ ควรมีการระบุกระบวนการในการขอต่ออายุใบรับรองอิเล็กทรอนิกส์ที่ชัดเจน เช่น การใช้รหัสผ่าน (Password) ในการยืนยันตัวบุคคลอีกครั้งก่อนการต่ออายุใบรับรองอิเล็กทรอนิกส์

๖.๔ ควรมีวิธีการแจ้งว่าได้ต่ออายุใบรับรองอิเล็กทรอนิกส์ให้ผู้ใช้บริการแล้ว

๖.๕ ควรระบุวิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต่ออายุให้แก่ผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์

๖.๖ ควรอธิบายเกี่ยวกับการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ตลอดจนวิธีการแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงการต่ออายุใบรับรองอิเล็กทรอนิกส์

๗. การรับรองคู่กุญแจใหม่ (Certificate Re-key)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับการสร้างคู่กุญแจใหม่ รวมถึงการออกใบรับรองอิเล็กทรอนิกส์ใหม่เพื่อรองรับคู่กุญแจใหม่ โดยผู้ใช้บริการหรือบุคคลอื่น

๗.๑ กรณีต่างๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์สามารถหรือต้องสร้างคู่กุญแจ และออกใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่นี้ เช่น กรณีของการเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือการหมดอายุการใช้งานของคู่กุญแจ

๗.๒ การกำหนดให้บุคคลใดสามารถขอใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่

๗.๓ ควรมีวิธีการแจ้งการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการทราบ

๗.๔ ควรระบุวิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่

๗.๕ ควรอธิบายเกี่ยวกับการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ตลอดจนวิธีการแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงการออกใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่

๘. การแก้ไขเปลี่ยนแปลงใบรับรองอิเล็กทรอนิกส์ (Certificate Modification)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ใหม่อันเนื่องมาจากการแก้ไขเปลี่ยนแปลงข้อมูลในใบรับรองอิเล็กทรอนิกส์ที่ไม่ใช่กุญแจสาธารณะของผู้ใช้บริการ เช่น

๘.๑ กรณีต่างๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์อนุญาตให้ผู้ใช้บริการสามารถแก้ไขเปลี่ยนแปลงข้อมูลในใบรับรองอิเล็กทรอนิกส์ได้ เช่น การเปลี่ยนชื่อ การเปลี่ยนแปลง Distinguished Name และการเปลี่ยนบทบาทภาระหน้าที่ในที่ทำงาน

๘.๒ การกำหนดให้บุคคลใดสามารถขอแก้ไขเปลี่ยนแปลงใบรับรองอิเล็กทรอนิกส์ได้ เช่น ผู้ใช้บริการ เจ้าหน้าที่ฝ่ายบุคคล หรือเจ้าหน้าที่รับลงทะเบียน เป็นต้น

๘.๓ ควรมีวิธีการแจ้งการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการทราบ

๘.๔ ควรระบุวิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกให้ใหม่

๘.๕ ควรอธิบายเกี่ยวกับการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ตลอดจนวิธีการแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงการออกใบรับรองอิเล็กทรอนิกส์ใหม่

๙. การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับการเพิกถอนและการพักใช้ใบรับรองอิเล็กทรอนิกส์

๙.๑ กรณีต่างๆผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ให้มีการพักใช้หรือเพิกถอนใบรับรองอิเล็กทรอนิกส์ เช่น การเลิกจ้างงานผู้ใช้บริการ การสูญหายของอุปกรณ์เข้ารหัสลับ หรือมีเหตุอันควรสงสัยว่ามีการล่วงรู้กุญแจส่วนตัวโดยมิชอบ เป็นต้น

๙.๒ การกำหนดให้บุคคลใดสามารถขอเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการได้ เช่น ผู้ใช้บริการ และเจ้าหน้าที่รับลงทะเบียน เป็นต้น

๙.๓ ควรมีการระบุกระบวนการขอเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ เช่น การกำหนดให้เจ้าหน้าที่รับลงทะเบียน หรือผู้ใช้บริการต้องลงลายมือชื่อกำกับคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๙.๔ ควรมีการกำหนดระยะเวลาที่ผู้ใช้บริการสามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้

๙.๕ ควรมีการกำหนดวิธีการที่คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้

๙.๖ ในกรณีที่มีการใช้ Certificate Revocation List (CRL) ในการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้เพิกถอนและพักใช้ ควรมีการกำหนดความถี่ของการเผยแพร่ข้อมูลดังกล่าว ระยะเวลาระหว่างการสร้าง CRL และเวลาที่เผยแพร่ CRL ให้สาธารณะทราบ และถ้ามีการให้บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ ก็ควรแจ้งให้สาธารณะทราบถึงวิธีการใช้งาน เงื่อนไข และข้อกำหนดที่เกี่ยวข้องด้วย

๙.๗ ควรกำหนดระยะเวลาการพักใช้ใบรับรองอิเล็กทรอนิกส์

๑๐. บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)

ข้อมูลส่วนนี้กล่าวถึงบริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์สำหรับคู่กรณีที่เกี่ยวข้อง และควรมีประเด็นดังต่อไปนี้

๑๐.๑ ลักษณะของบริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ และสภาพพร้อมใช้งานของระบบบริการ รวมถึงนโยบายรองรับกรณีที่ระบบไม่สามารถให้บริการได้

๑๐.๒ ลักษณะของบริการอื่นที่เกี่ยวข้อง

๑๑. การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription)

ข้อมูลส่วนนี้กล่าวถึงขั้นตอนที่ผู้ใช้บริการปฏิบัติในการเลิกใช้ใบรับรองอิเล็กทรอนิกส์ซึ่งอาจมีสาเหตุมาจากการหมดอายุของใบรับรองอิเล็กทรอนิกส์ หรือการเลิกให้บริการโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

๑๒. การเก็บรักษาและการกู้คืนกุญแจ (Key Escrow and Recovery)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรระบุนโยบายเกี่ยวกับการเก็บรักษาและการกู้คืนกุญแจส่วนตัว และการป้องกัน Session Key (Session Key Encapsulation)

บทที่ ๕ การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)

สำหรับเนื้อหาในบทนี้จะครอบคลุมการควบคุมและการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต้องใช้ในการสร้างกุญแจ (Key Generation) การยืนยันตัวบุคคล (Subject Authentication) การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance) การเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation) การตรวจสอบระบบและเก็บรักษาข้อมูล (Auditing and Archiving) ให้มั่นคงปลอดภัย

ดังนั้น จึงควรมีการกำหนดวิธีการในการรักษาความมั่นคงปลอดภัยของบุคคลที่เกี่ยวข้อง เพื่อสร้างความเชื่อมั่นในการใช้งานใบรับรองอิเล็กทรอนิกส์ และป้องกันมิให้มีการบุกรุก หรือเข้าถึงระบบหรือล่วงรู้ข้อมูลในระบบการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งป้องกันมิให้เกิดความผิดพลาดในข้อมูลที่ใช้ในการสร้างใบรับรองอิเล็กทรอนิกส์ หรือรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์กรณีที่มีการล่วงรู้กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยมิชอบ

ทั้งนี้ ความมั่นคงปลอดภัยทางกายภาพ (Physical Security Controls) นั้น ครอบคลุมในเรื่องดังต่อไปนี้

๑. สถานที่ตั้งหรือการก่อสร้างสำนักงานในการให้บริการ (Site Location and Construction)

เนื้อหาในส่วนนี้ควรมีการกำหนดพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยเป็นพิเศษ (High Security Zone) หรือการใช้ห้องและตู้นิรภัย การติดตั้งระบบโทรทัศน์วงจรปิด และระบบตรวจจับการบุกรุกทางกายภาพ เป็นต้น

๒. การเข้าถึงทางกายภาพ (Physical Access)

ควรกำหนดเกี่ยวกับการเข้าออกระหว่างพื้นที่สำนักงานกับพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยเป็นพิเศษ การเคลื่อนย้ายจากพื้นที่หนึ่งไปยังอีกพื้นที่หนึ่ง ให้มีการป้องกันการเข้าถึงทางกายภาพ เช่น การพิสูจน์ตัวบุคคลก่อนอนุญาตให้เข้าถึงระบบให้บริการได้ อาจทำได้โดยการใช้บัตรแถบแม่เหล็ก และการตรวจสอบลายนิ้วมือ เป็นต้น นอกจากนี้ ยังควรมีการคำนึงถึงการบริหารจัดการระบบไฟฟ้าและระบบปรับอากาศ การป้องกันภัยจากน้ำ การจัดเก็บ Backup Media ไว้ในสถานที่อื่น ที่ได้รับการป้องกันการเข้าถึง ป้องกันภัยจากไฟและน้ำ

๓. การควบคุมความมั่นคงปลอดภัยด้านกายภาพ (Physical Security Controls)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรบรรยายวิธีการควบคุมด้านกายภาพของสถานที่ประกอบการในหัวข้อดังต่อไปนี้

๓.๑ สถานที่ตั้งของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และการจัดแบ่งพื้นที่ตามระดับของความมั่นคงปลอดภัยที่ต้องการ

๓.๒ การควบคุมการเข้าถึงพื้นที่ที่ต้องการระดับความมั่นคงปลอดภัยที่ต่างกัน

๓.๓ การดูแลเรื่องพลังงานไฟฟ้า การไหลเวียนของน้ำ การควบคุมสภาพอากาศ อุณหภูมิและความชื้นสัมพัทธ์ การป้องกันการเกิดอัคคีภัย เพื่อป้องกันการหยุดชะงักของการให้บริการจากเหตุเหล่านี้

๓.๔ การเก็บรักษาสื่อที่ใช้เก็บข้อมูลของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ให้มั่นคงปลอดภัย ตลอดจนการกำหนดให้มีการสำรองข้อมูลนอกสถานที่ประกอบการเพื่อป้องกันการสูญเสีย หรือสูญหายของข้อมูล

๔. การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรมีการจัดบทบาทและหน้าที่ของบุคลากรในองค์กรให้เหมาะสม และกำหนดนโยบายเกี่ยวกับการทำงานของบุคลากรในแต่ละบทบาท เช่น วิธีการระบุและยืนยันตัวบุคคล หรือวิธีการเข้าถึงข้อมูลสำคัญโดยบุคคลในบทบาทต่าง ๆ โดยการแบ่งแยกหน้าที่ซึ่งไม่อนุญาตให้บุคคลหนึ่งรับหน้าที่ในหลายบทบาทด้วยเหตุผลด้านความมั่นคงปลอดภัยของข้อมูล

๕. การกู้คืนระบบอันเกิดจากพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลและภัยพิบัติอันเกิดแก่ระบบ (Compromise and Disaster Recovery)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรมีนโยบายในการกู้คืนระบบอันเกิดจากพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลและภัยพิบัติอันเกิดแก่ระบบ เช่น ข้อมูลถูกทำลายอันเนื่องมาจากอุบัติเหตุหรือสาเหตุอื่นใด เพื่อให้การให้บริการไม่หยุดชะงัก

๖. การเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียน (CA or RA Termination)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หรือเจ้าหน้าที่รับลงทะเบียนเลิกกิจการจะต้องมีการแจ้งให้บุคคลที่เกี่ยวข้องทราบ รวมถึงผู้ที่รับผิดชอบข้อมูลของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียนเพื่อให้เกิดผลกระทบต่อผู้ใช้บริการน้อยที่สุด

บทที่ ๖ การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

สำหรับเนื้อหาในส่วนนี้เป็นการกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยของกุญแจและข้อมูลสำหรับอนุญาตให้ใช้กุญแจ เช่น PIN และ Password และประเด็นต่าง ๆ ที่เกี่ยวกับการบริหารจัดการกุญแจ

๑. การสร้างและติดตั้งคู่กุญแจ (Key Pair Generation and Installation)

การสร้างและการติดตั้งคู่กุญแจมีประเด็นที่ต้องพิจารณาและกำหนดเป็นนโยบาย ดังต่อไปนี้

๑.๑ ใครเป็นผู้สร้างคู่กุญแจให้ผู้ใช้บริการ และสร้างโดยซอฟต์แวร์หรือฮาร์ดแวร์

๑.๒ วิธีการที่ผู้ใช้บริการจะได้รับกุญแจส่วนตัวของตนแบบมั่นคงปลอดภัยเป็นไปได้อย่างไรบ้าง

๑.๓ วิธีการที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะได้รับกุญแจสาธารณะของผู้ใช้บริการแบบมั่นคงปลอดภัยเป็นไปได้อย่างไรบ้าง

๑.๔ คู่กรณีที่เกี่ยวข้องจะได้รับกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แบบมั่นคงปลอดภัยเป็นไปได้อย่างไรบ้าง

๑.๕ ความยาวของคู่กุญแจเป็นเท่าใด เช่น กุญแจอาจมีความยาว 1,024 บิต RSA และ 1,024 บิต DSA

๑.๖ ใครเป็นผู้ที่กำหนดพารามิเตอร์ของกุญแจสาธารณะ และมีการตรวจสอบคุณภาพของพารามิเตอร์ระหว่างการสร้างกุญแจหรือไม่

๑.๗ วัตถุประสงค์ที่อาจจะนำคู่กุญแจไปใช้ หรือวัตถุประสงค์ที่ควรจำกัดการใช้คู่กุญแจคืออะไร สำหรับใบรับรองตาม X.509 นั้นวัตถุประสงค์เหล่านี้ควรจะสอดคล้องกับการใช้งานกุญแจตามมาตรฐาน X.509 เวอร์ชั่น 3

๒. การป้องกันกุญแจส่วนตัว (Private Key Protection) และการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Control)

ในส่วนนี้ควรกำหนดวิธีการป้องกันกุญแจส่วนตัวและการใช้งานชิ้นส่วนสำหรับการเข้ารหัสลับของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ และผู้ให้บริการเก็บข้อมูล โดยคำนึงถึงความมั่นคงปลอดภัยและความเสียหายอันเกิดจากการเก็บรักษากุญแจส่วนตัว การสำรองกุญแจส่วนตัว และการบันทึกถาวรกุญแจส่วนตัว ทั้งนี้ ให้พิจารณาคำถาม ดังต่อไปนี้

๒.๑ ถ้ามีการใช้งานชิ้นส่วนสำหรับการเข้ารหัสลับ (อาจเป็นซอฟต์แวร์ ฮาร์ดแวร์ และ หรือ เฟิร์มแวร์) ควรจะอ้างอิงตามมาตรฐานใด

๒.๒ จำเป็นต้องมีการควบคุมการเข้าถึงกุญแจส่วนตัว โดยผู้มีสิทธิมากกว่า ๑ คนหรือไม่ (แบบ m out of n)

๒.๓ มีนโยบายในการเก็บรักษากุญแจส่วนตัวหรือไม่ (Key Escrow)

๒.๔ มีนโยบายในการสำรองกุญแจส่วนตัวหรือไม่ (Private Key Backup)

๒.๕ มีนโยบายในการบันทึกถาวรกุญแจส่วนตัวหรือไม่ (Private Key Archival)

๒.๖ ในกรณีใดบ้างที่จะมีการถ่ายโอนกุญแจส่วนตัวเข้าไปในหรือออกจากชิ้นส่วนสำหรับเข้ารหัสลับ

๒.๗ การจัดเก็บกุญแจส่วนตัวในชิ้นส่วนสำหรับเข้ารหัสลับ (Private Key Storage in Cryptographic Module) จะทำด้วยวิธีใด เช่น เก็บในรูปแบบข้อมูลธรรมดาที่อ่านเข้าใจได้ (Plaintext) รูปแบบของข้อมูลที่มีการเข้ารหัสลับ (Encrypted) หรือการแยกกุญแจ (Split Key) เป็นต้น

๒.๘ ใครเป็นผู้ที่มีสิทธิในการใช้งานกุญแจส่วนตัว ด้วยวิธีอย่างไร

๒.๙ ใครเป็นผู้มีสิทธิในการยกเลิกการใช้งานกุญแจส่วนตัว ด้วยวิธีอย่างไร

๒.๑๐ ใครมีสิทธิทำลายกุญแจส่วนตัว ด้วยวิธีอย่างไร

๒.๑๑ รายละเอียดความสามารถของชิ้นส่วนสำหรับเข้ารหัสลับ เป็นอย่างไร (อาจอ้างถึงมาตรฐานที่เกี่ยวข้อง เช่น FIPS 140-1

๓. รายละเอียดอื่นเกี่ยวกับการจัดการและบริหารคู่กุญแจ (Other Aspects of Key Pair Management)

ในส่วนนี้ควรกำหนดวิธีการในการจัดการและบริหารคู่กุญแจของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ และผู้ให้บริการเก็บข้อมูล โดยพิจารณาคำถามดังต่อไปนี้

๓.๑ ควรมีการเก็บบันทึกถาวรของกุญแจสาธารณะ (Public Key Archival) หรือไม่ ถ้ามีใครจะเป็นผู้ทำหน้าที่เก็บบันทึกถาวร และการควบคุมความมั่นคงปลอดภัยของระบบเก็บบันทึกถาวร ทั้งในเรื่องความจำเป็นในการปกป้องซอฟต์แวร์ และฮาร์ดแวร์ที่เกี่ยวข้องกับการใช้งานกุญแจสาธารณะอยู่ตลอดเวลา

๓.๒ ระยะเวลาใช้งานของใบรับรองอิเล็กทรอนิกส์ และคู่กุญแจของผู้ใช้บริการเป็นเท่าใด

๔. ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data)

เนื้อหาในส่วนนี้ควรกำหนดวิธีการป้องกันข้อมูลที่จำเป็นต้องใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data) ซึ่งอาจหมายถึง รหัสอ้างอิง (Reference Code) และรหัสติดตั้ง (Installation Code) เพื่อใช้ในการยืนยันตัวผู้ใช้บริการในขั้นตอนการติดตั้งใบรับรอง ซึ่งเป็นข้อมูลที่ผู้ใช้บริการได้รับจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยตรงหรือจากเจ้าหน้าที่รับลงทะเบียน

๕. การควบคุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)

เนื้อหาในส่วนนี้ควรอธิบายการควบคุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ เพื่อให้เกิดความน่าเชื่อถือของระบบผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยมีการควบคุมการเข้าถึง (Access Control) มีการตรวจสอบ (Audit) ระบบของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ การยืนยันตัวบุคคล (Identification และ Authentication) การทดสอบระบบความมั่นคงปลอดภัย (Security testing) และทดสอบการบุกรุกระบบ (Penetration Testing) โดยที่ระบบการควบคุมความมั่นคงปลอดภัยนั้นต้องได้รับการประเมินตามมาตรฐานสากล เช่น The Trusted System Evaluation Criteria (TCSEC)

๖. การควบคุมทางเทคนิคของระบบให้บริการ (Life Cycle Technical Controls)

เนื้อหาในส่วนนี้ควรจะกล่าวถึงการควบคุมการพัฒนาระบบและการควบคุมการบริหารจัดการด้านความมั่นคงปลอดภัย การควบคุมการพัฒนาระบบนั้นรวมความถึงความมั่นคงปลอดภัยของสภาพแวดล้อมในการพัฒนาระบบ บุคลากรที่พัฒนาระบบ และการออกแบบระบบ เป็นต้น

การควบคุมการบริหารจัดการด้านความมั่นคงปลอดภัย หมายความถึง การใช้เครื่องมืออุปกรณ์ (Tools) และกระบวนการ (procedure) เพื่อให้เกิดความมั่นใจด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ (Operational Systems) และระบบเครือข่าย (Networks)

๗. การควบคุมความมั่นคงปลอดภัยทางเครือข่าย (Network Security Controls)

เนื้อหาในส่วนนี้ระบุการควบคุมความมั่นคงปลอดภัยทางเครือข่ายของระบบผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยป้องกันมิให้เข้าถึงระบบได้โดยมิชอบด้วยกลไกของอุปกรณ์รักษาความมั่นคงปลอดภัยหลายส่วนหลายลำดับชั้น ได้แก่ อุปกรณ์เลือกเส้นทาง (Router) ตัวป้องกันการบุกรุก (Firewall) ระบบตรวจสอบผู้บุกรุก (Intrusion Detection System: IDS)

๘. ข้อกำหนดสำหรับการประทับเวลาในบันทึกต่าง ๆ (Time-stamping)

หากกำหนดให้มีการประทับเวลาในบันทึกต่างๆ ควรระบุไว้ในส่วนนี้ และกล่าวถึงแหล่งที่มาของเวลาและความน่าเชื่อถือประกอบด้วย

บทที่ ๗ การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)

๑. รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)

เนื้อหาในส่วนนี้กำหนดรายละเอียดเกี่ยวกับประเด็นดังต่อไปนี้ (อ้างอิงตาม IETF RFC 3280)

๑.๑ เวอร์ชั่นของใบรับรองอิเล็กทรอนิกส์ที่สนับสนุน

๑.๒ ข้อมูลใน Certificate Extensions และความสำคัญ (Criticality) ของข้อมูลดังกล่าว OID ของขั้นตอนวิธีการเข้ารหัสลับ (Cryptographic Algorithm Object Identifiers)

๑.๓ รูปแบบชื่อของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน และผู้ใช้บริการ

๑.๔ OID ของแนวนโยบายที่เกี่ยวข้อง

๒. รูปแบบรายการเพิกถอนใบรับรอง (Certification Revocation List Profile)

๒.๑ เนื้อหาในส่วนนี้กำหนดรายละเอียดเกี่ยวกับประเด็นดังต่อไปนี้ (อ้างอิงตาม IETF RFC 3280) เวอร์ชั่นของรายการเพิกถอนใบรับรองที่สนับสนุน และ

๒.๒ รายการเพิกถอนใบรับรอง และข้อมูลใน CRL Entry Extensions และความสำคัญของข้อมูลดังกล่าว (Criticality)

๓. รูปแบบโปรโตคอล OCSP (OCSP Profile)

ในส่วนนี้แสดงถึงเนื้อหาและรูปแบบของข้อมูลที่ใช้ในการตรวจสอบสถานะของใบรับรองโดยใช้โปรโตคอล OCSP (Online Certificate Status Protocol) รวมทั้งข้อมูลอื่นๆ เช่น เวอรชั่นของ OCSP และข้อมูลเพิ่มเติมที่สามารถระบุลงไปใน OCSP (อ้างอิงตาม IETF RFC 2560)

บทที่ ๘ การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่าง ๆ และการประเมินความเสี่ยงอื่น ๆ (Compliance Audit and Other Assessment)

สำหรับเนื้อหาในส่วนนี้จะต้องกำหนดเกี่ยวกับรายการที่ต้องมีการประเมินความเสี่ยง หรือระเบียบวิธี (Methodology) ที่ใช้ในการประเมินความเสี่ยง เช่น การประเมินความเสี่ยงตามแนวทางของ WebTrust เป็นต้น

นอกจากนั้น ก็อาจกำหนดความถี่ของการตรวจสอบหรือประเมินความเสี่ยง ทั้งนี้ ในการประเมินนั้น ก็ต้องประเมินตามแนวนโยบายและแนวปฏิบัติ และประเมินทั้งก่อนมีการให้บริการ เมื่อมีการให้บริการ และการตรวจสอบกรณีมีความเป็นไปได้ที่จะมีการล่วงรู้โดยมิชอบอันเป็นการกระทบถึงความมั่นคงปลอดภัย

ทั้งนี้ จำเป็นต้องระบุคุณสมบัติของบุคลากรที่ทำหน้าที่ตรวจสอบและประเมินความเสี่ยง การดำเนินการเกี่ยวกับผลการประเมิน เช่น การระงับการดำเนินการชั่วคราว หรือการเพิกถอนใบรับรองที่ออก เป็นต้น

บทที่ ๙ ข้อกำหนดอื่น ๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

สำหรับเนื้อหาในส่วนนี้ จะกำหนดเกี่ยวกับการจัดเก็บค่าธรรมเนียม (Fees) ความรับผิดชอบทางการเงิน (Financial Responsibility) ทั้งในส่วนที่เกี่ยวกับการดำเนินการหรือกรณีมีการเรียกร้องค่าเสียหายจากการให้บริการเกิดขึ้น รวมทั้งประเด็นข้อกฎหมายต่าง ๆ

อย่างไรก็ตาม ในการจัดทำแนวนโยบายและแนวปฏิบัติ นั้น หากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ต้องการให้เอกสารฉบับดังกล่าวถือเป็นสัญญาฉบับหนึ่งหรือเป็นส่วนหนึ่งของสัญญาในการให้บริการ ก็อาจจำเป็นต้องพิจารณาเพิ่มเติมเนื้อหาเกี่ยวกับข้อจำกัดความรับผิด (Limitation of Liability) ไว้ในแนวนโยบายหรือแนวปฏิบัติ ด้วย แต่หากไม่ประสงค์ให้แนวนโยบายและแนวปฏิบัติเป็นสัญญาหรือส่วนหนึ่งของสัญญาในการให้บริการ ก็อาจจำเป็นต้องมีการจัดทำสัญญาในการให้บริการผู้ใช้บริการ หรือคู่กรณีที่เกี่ยวข้องซึ่งมีข้อความกำหนดเกี่ยวกับข้อจำกัดความรับผิดของบุคคลดังกล่าวในการให้บริการเอาไว้ด้วย

๑. ค่าธรรมเนียม (Fees)

สำหรับค่าธรรมเนียมในการให้บริการนั้น อาจกำหนดให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ซึ่งให้บริการออกใบรับรองอิเล็กทรอนิกส์ ผู้ให้บริการเก็บรักษาข้อมูล หรือผู้ให้บริการในฐานะเจ้าหน้าที่รับลงทะเบียน จัดเก็บค่าธรรมเนียมได้จากกรณีที่มีการออกใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองดังกล่าว (Certificate Issuance or Renewal Fees) ค่าธรรมเนียมในการเข้าถึงใบรับรอง (Certificate Access Fees) การเข้าถึงข้อมูลเกี่ยวกับการเพิกถอนหรือสถานะล่าสุดของใบรับรองอิเล็กทรอนิกส์ ค่าธรรมเนียมสำหรับบริการอื่น ๆ เช่น การเข้าถึงแนวนโยบายหรือแนวปฏิบัติ ทั้งนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจจัดทำนโยบายในการคืนค่าธรรมเนียม (Refund Policy) ไว้ด้วย

๒. ความรับผิดชอบทางการเงิน (Financial Responsibility)

เนื้อหาในส่วนนี้ควรกำหนดขึ้นเกี่ยวกับความรับผิดในการดำเนินการที่เกิดขึ้น (Operational PKI Responsibilities) การรักษาสถานะของผู้ให้บริการให้สามารถชำระหนี้และจ่ายค่าเสียหายในกรณีที่ต้องรับผิดได้ (to Remain Solvent and Pay Damages) ทั้งนี้ อาจมีการเพิ่มเติมเนื้อหาที่เกี่ยวกับวงเงินประกันความเสียหายที่คุ้มครองความรับผิดที่เกิดขึ้น (Insurance Coverage for Liabilities) และความรับผิดในอนาคต (Contingencies) สินทรัพย์ที่ปรากฏในงบดุล (Assets on The Balance Sheet) หนังสือค้ำประกัน (Surety Bond) เล็ตเตอร์ อ๊อฟ เครดิต (Letter of Credit) ค่าสินไหมทดแทน (Indemnity) และอาจให้ความคุ้มครองเพิ่มเติมด้วยการกำหนดเกี่ยวกับการประกันภัย (Insurance) หรือการให้คำรับรอง (Warranty)

๓. การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)

ด้วยข้อมูลบางประเภทเป็นความลับทางธุรกิจที่จำเป็นต้องเก็บไว้เป็นความลับ เช่น แผนทางธุรกิจ (Business Plan) ข้อมูลการขาย (Sales Information) ความลับทางการค้า (Trade Secrets) และข้อมูลที่ได้จากบุคคลที่สามภายใต้ข้อตกลงไม่เปิดเผยความลับ (Nondisclosure Agreement) จึงจำเป็นต้องกำหนดขอบเขตในการรักษาความลับ ข้อมูลที่อยู่นอกเหนือจากข้อตกลงว่าด้วยการรักษาความลับ และความรับผิดของบุคคลที่เกี่ยวข้องซึ่งได้รับข้อมูลลับนั้น ทั้งนี้ อาจต้องมีกลไกทำให้เกิดความเชื่อมั่นว่าจะมีการปกป้องมิให้เกิดพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล (Compromise)

๔. นโยบายในการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)

ในการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน หรือบุคคลอื่นๆ ซึ่งให้บริการที่เกี่ยวข้องนั้น จำเป็นต้องให้ความสำคัญสำหรับการรักษาความเป็นส่วนตัวหรือเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการไว้เป็นความลับ จะเปิดเผยได้เพียงข้อมูลบางอย่างเท่านั้น เช่น ข้อมูลที่ต้องเผยแพร่โดยการบันทึกไว้ในใบรับรองอิเล็กทรอนิกส์ ได้แก่ ชื่อ ชื่อสกุล ของผู้ใช้บริการ เป็นต้น

ดังนั้น การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลจึงต้องดำเนินการตามกฎหมายว่าด้วยการนั้น หรือกรณีที่ยังไม่มีการใช้บังคับกฎหมายเช่นว่านั้น ก็อาจจำเป็นต้องดำเนินการตามหลักเกณฑ์ในการให้ความคุ้มครองในเรื่องดังกล่าวตามมาตรฐานสากล เช่น ตามแนวทางของ OECD Guidelines

ด้วยเหตุนี้ ในการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จึงควรได้รับความยินยอมจากผู้ใช้บริการ ก่อนจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้ จะต้องกำหนดข้อยกเว้นกรณีที่จำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลในกรณีที่ต้องดำเนินการตามกฎหมายฉบับต่างๆ หรือเมื่อมีคำสั่งศาล หรือเมื่อมีคำสั่งทางปกครอง เป็นต้น ไว้ด้วย

๕. ทรัพย์สินทางปัญญา (Intellectual Property Rights)

ให้กำหนดเรื่องทรัพย์สินทางปัญญา อันได้แก่ ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า หรือความลับทางการค้าซึ่งบุคคลที่เกี่ยวข้องอาจมีหรือใช้สิทธิเรียกร้องตามที่กำหนดไว้ในแนวนโยบาย

แนวปฏิบัติ ใบรับรองอิเล็กทรอนิกส์ ชื่อ กุญแจ หรือภายใต้การอนุญาตหรือที่กำหนดไว้ในข้อตกลงใดๆ กับบุคคลที่เกี่ยวข้อง

๖. คำรับรอง (Representations and Warranties)

ในส่วนนี้จะกำหนดให้บุคคลที่เกี่ยวข้องทำคำรับรองในเรื่องต่างๆ ที่กำหนดไว้ในแนวนโยบายหรือแนวปฏิบัติ เช่น การกำหนดให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ต้องให้การรับรองว่า ข้อมูลหรือข้อเท็จจริงที่บันทึกไว้ในใบรับรองอิเล็กทรอนิกส์นั้นถูกต้อง ตามที่ได้มีการกำหนดให้แนวปฏิบัติเป็นข้อตกลงในการให้บริการ รวมทั้งกรณีมีการกำหนดให้มีการให้คำรับรองที่กำหนดไว้ในสัญญาหรือข้อตกลงอื่นๆ เช่น ข้อตกลงในการให้บริการกับผู้ใช้บริการ (Subscriber Agreement) และข้อตกลงในการให้บริการกับคู่กรณีที่เกี่ยวข้อง (Relying Party Agreement)

๗. การปฏิเสธความรับผิดตามคำรับรอง (Disclaimers of Warranties)

ในเนื้อหาของแนวนโยบายหรือแนวปฏิบัตินั้น ให้มีการกำหนดเกี่ยวกับการปฏิเสธความรับผิดตามคำรับรองหรือกำหนดเนื้อหาเกี่ยวกับเรื่องดังกล่าวไว้ในสัญญาในการให้บริการฉบับต่าง ๆ

๘. ข้อจำกัดความรับผิด (Limitations of Liability)

ในการให้บริการนั้น อาจมีการกำหนดเกี่ยวกับข้อจำกัดความรับผิดไว้ด้วยก็ได้ โดยอาจพิจารณาจากลักษณะของการจำกัดความรับผิด และจำนวนเงินค่าเสียหายที่จำกัดความรับผิด เช่น ค่าเสียหายอันเนื่องมาจากการผิดสัญญา (Incidental Damages) ค่าเสียหายจากการสูญเสียกำไรในอนาคต (Consequential Damages)

๙. ค่าสินไหมทดแทน (Indemnities)

สำหรับการชดใช้ค่าสินไหมทดแทนนั้น อาจมีการกำหนดให้คู่สัญญาฝ่ายใดต้องรับผิด ทั้งนี้โดยอาจมีการกำหนดไว้ในแนวนโยบาย แนวปฏิบัติ หรือสัญญา หรือข้อตกลงต่างๆ เช่น การกำหนดให้ผู้ใช้บริการต้องรับผิดในการชดใช้ค่าสินไหมทดแทนกรณีที่ผู้ใช้บริการได้แถลงข้อมูลหรือข้อเท็จจริงของตนที่ต้องบันทึกไว้ในใบรับรองอิเล็กทรอนิกส์เป็นเท็จหรือไม่ตรงกับความจริง หรือกรณีที่คู่กรณีที่เกี่ยวข้องต้องรับผิดชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในกรณีที่ไม่ตรวจสอบการเพิกถอนใบรับรองอิเล็กทรอนิกส์

สำหรับในบทที่ ๙ นี้ นอกจากหัวข้อข้างต้นแล้ว อาจมีการกำหนดเนื้อหาเกี่ยวกับการเลิกสัญญา การติดต่อสื่อสารระหว่างผู้ให้บริการและผู้ใช้บริการ การแก้ไขปรับปรุงแนวนโยบาย หรือแนวปฏิบัติ การระงับข้อพิพาท กฎหมายที่ใช้บังคับ รวมทั้งเนื้อหาอื่นๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ประสงค์จะกำหนดเพิ่มเติมได้อีกด้วย

<u>เอกสารอ้างอิง</u>

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)