แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์
(Certificate Policy/Certification Practice Statement)

Version 1.0

ส่วนเทคโนโลยีดิจิทัลและสารสนเทศ
ฝ่ายบริหารทรัพยากรองค์กรและบุคคล

ประวัติการแก้ไขเอกสาร

ครั้งที่	วันที่สร้าง	เวอร์ชัน	รายละเอียดการแก้ไข	ผู้รับผิดชอบ
1	11/3/2567	1.0	สร้างเอกสาร	นายสนธิ นราเขมอนันต์

สารบัญ

1. บทนำ (Introduction)

1.1. ข้อมูลเบื้องต้นทั่วไป (Overview)

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa) เป็นหน่วยงานของรัฐ จัดตั้งขึ้นตามพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 มีอำนาจหน้าที่ในการดำเนินการตามมาตรา 34 และ 35 ประกอบด้วย

- จัดทำแผนยุทธศาสตร์การส่งเสริมเศรษฐกิจดิจิทัลให้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม
- ส่งเสริมและสนับสนุนการลงทุนหรือประกอบกิจการเกี่ยวกับอุตสาหกรรมหรือนวัตกรรมดิจิทัล
- ส่งเสริม สนับสนุน และร่วมมือกับบุคคลอื่นในการพัฒนาอุตสาหกรรมหรือนวัตกรรมดิจิทัล
- ส่งเสริม สนับสนุน และดำเนินการเกี่ยวกับการพัฒนาบุคลากรด้านอุตสาหกรรมและนวัตกรรมดิจิทัล
- เสนอแนะ เร่งรัด และติดตามการปรับปรุงแก้ไขกฎหมายหรือกฎระเบียบหรือมาตรการเกี่ยวกับการคุ้มครองทรัพย์สินทางปัญญาของอุตสาหกรรมหรือนวัตกรรมดิจิทัลต่อหน่วยงานที่เกี่ยวข้อง
- ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการ คณะกรรมการเฉพาะด้าน หรือคณะกรรมการกำกับสำนักงานส่งเสริมเศรษฐกิจดิจิทัลมอบหมาย หรือตามที่กฎหมายกำหนด

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa) มีการดำเนินงานในการออกใบรับรองอิเล็กทรอนิกส์สำหรับใช้กับงานบริการและงานบริหารจัดการต่างๆ ของสำนักงาน ในรูปแบบอิเล็กทรอนิกส์ที่เชื่อมโยงกับบุคคล ซึ่งปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์นั้น เพื่อยืนยันและรับรองว่ากุญแจสาธารณะเป็นของบุคคลนั้น

เอกสารฉบับนี้เรียกว่า “แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certificate Practice Statement)” หรือเรียกว่า “CP/CPS” ถูกจัดทำขึ้นโดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (depa Certification Authority: depa CA)

1.2. ชื่อเอกสาร (Document Name and Identification)

เอกสารฉบับนี้ เรียกว่า “แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement)” ซึ่งเรียกว่า “CP/CPS” โดยมีวัตถุประสงค์ในการชี้แจงบุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ เพื่อให้ทราบถึงข้อความที่ระบุในเอกสารตลอดจนความเข้าใจและเป็นแนวทางในการดำเนินการเกี่ยวกับใบรับรอง นอกจากนี้ยังใช้เป็นเอกสารที่มีผลผูกพันทางกฎหมายระหว่างคู่กรณีทุกฝ่ายอีกด้วย

1.3. บุคคลที่เกี่ยวข้อง (PKI Participants)

1.3.1. ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: depa CA)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: depa CA) คือ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งสร้างและออกใบรับรองอิเล็กทรอนิกส์ เพื่อรับรอง

กุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List หรือมีชื่อย่อว่า CRL) ตามความถี่ที่เหมาะสม

1.3.2. หน่วยรับลงทะเบียน (Registration Authority: depa RA)

หน่วยรับลงทะเบียน (Registration Authority: depa RA) คือ ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ คำขอเพิกถอนใบรับรอง หรือต่ออายุใบรับรอง โดยการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ของข้อมูลที่ผู้ใช้บริการให้ไว้ตามแบบคำขอที่ผู้ให้บริการกำหนดขึ้น

1.3.3. ผู้ใช้บริการ (Subscriber)

ผู้ใช้บริการ (Subscriber) คือ ผู้ที่ได้ใช้บริการใบรับรองอิเล็กทรอนิกส์จากผู้ให้บริการ โดยมีชื่อปรากฏในใบรับรองอิเล็กทรอนิกส์ และเป็นเจ้าของกุญแจส่วนตัวและกุญแจสาธารณะที่ปรากฏในใบรับรองอิเล็กทรอนิกส์นั้น ประกอบด้วย

- บุคคลทั่วไปที่ยื่นคำขอใช้บริการใบรับรองแก่ผู้ให้บริการ โดยเมื่อมีการออกใบรับรองจะมีการระบุชื่อผู้ใช้บริการไว้ในใบรับรอง
- นิติบุคคลที่ยื่นคำขอใช้บริการใบรับรองแก่ผู้ให้บริการ โดยเมื่อมีการออกใบรับรองจะมีการะบุชื่อนิติบุคคลของผู้ใช้บริการไว้ในใบรับรอง

1.3.4. คู่กรณีที่เกี่ยวข้อง (Relying Party)

คู่กรณีที่เกี่ยวข้อง (Relying Party) คือ ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองอิเล็กทรอนิกส์ หรือลายมือชื่อดิจิทัล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองไปใช้ในการตรวจสอบตัวตนที่แท้จริงของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัล และมีชื่อปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์

1.3.5. บุคคลซึ่งเกี่ยวข้องอื่นๆ (Other Participant)

บุคคลซึ่งเกี่ยวข้องอื่นๆ (Other Participant) คือ บุคคล นิติบุคคล หรือเอนทิตี้อื่นใดนอกจากที่กล่าวข้างต้น เช่น ผู้ให้บริการในการเก็บรักษาข้อมูล (Providers of Repository Services) หรือผู้ได้รับการว่างจ้างโดยการ Outsource ให้เป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นต้น

1.4. การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)

1.4.1. การใช้ใบรับรองอิเล็กทรอนิกส์ที่เหมาะสม (Appropriate Certificate Uses)

ชนิดของใบรับรองอิเล็กทรอนิกส์ที่ออกให้แก่ผู้ใช้บริการนั้น เป็นใบรับรองอิเล็กทรอนิกส์ประเภท Personal Certificate หรือใบรับรองอิเล็กทรอนิกส์ที่ออกให้บุคคล หรือประชาชนทั่วไปเพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้มีอายุการใช้งานแบบ 1 ปี 2 ปี และ 3 ปี

1.4.2. ข้อจำกัดในการใช้ใบรับรองอิเล็กทรอนิกส์ (Prohibited Certificate Uses)

ใบรับรองอิเล็กทรอนิกส์ที่ออกโดยสำนักงานส่งเสริมเศรษฐกิจดิจิทัล ซึ่งออกให้แก่บุคคล หรือประชาชนทั่วไป ให้ใช้เฉพาะตามวัตถุประสงค์ที่ระบุไว้ในข้อ 1.4.1 เท่านั้น และโดยเฉพาะอย่างยิ่งให้ใช้เฉพาะในขอบเขตการใช้งานที่สอดคล้องกับกฎหมายที่บังคับใช้เท่านั้น

1.5. การบริหารจัดการเกี่ยวกับแนวนโยบาย (Policy Administration)

1.5.1. หน่วยงานที่ทำหน้าที่บริหารจัดการเอกสารฉบับนี้ (Organization Administering the Document)

หน่วยงานที่บริหารจัดการเอกสารฉบับนี้ คือ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

1.5.2. ข้อมูลสำหรับติดต่อหน่วยงาน (Contact Person)

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
80 ถนนลาดพร้าว ซอยลาดพร้าว 4 แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900
โทรศัพท์: 02 026 2333
เว็บไซต์: www.depa.or.th
อีเมล์: support@depa.or.th

1.5.3. ผู้มีหน้าที่พิจารณาความเหมาะสมของแนวนโยบาย/แนวปฏิบัติ (Person Determining CPS Suitability for the Policy)

คณะกรรมการเทคโนโลยีดิจิทัลและสารสนเทศ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล รวมถึงส่วนเทคโนโลยีดิจิทัลและสารสนเทศ และส่วนกฎหมาย

1.5.4. กระบวนการอนุมัติแนวนโยบาย/แนวปฏิบัติ (CPS Approval Procedures)

การสร้างหรือเปลี่ยนแปลงเอกสารฉบับนี้ ได้รับอนุมัติจากสำนักงานส่งเสริมเศรษฐกิจดิจิทัล ทั้งนี้โดยอยู่ภายใต้กฎเกณฑ์หรือข้อกำหนดทางกฎหมาย (หากมี) ซึ่งแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ที่ถูกสร้าง ทบทวน หรือมีการเปลี่ยนแปลง จะถูกลงบันทึกทบทวนในส่วนของประวัติปรับปรุงเอกสาร แล้วนำเผยแพร่ผ่านกระบวนการทำงานที่เกี่ยวข้อง

1.6. คำนิยาม (Definition) และคำย่อ (Acronym)

คำศัพท์	ความหมาย
ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: depa CA)	สำนักงานส่งเสริมเศรษฐกิจดิจิทัล ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการที่เกี่ยวกับการขอรับบริการ/ขอรับการส่งเสริมของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
หน่วยงานรับลงทะเบียน (Registration Authority: depa RA)	บุคคล และเอนทิตี้ ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใบรับรองอิเล็กทรอนิกส์ คำขอพักใช้ใบรับรองอิเล็กทรอนิกส์ หรือคำขอเพิกถอน

คำศัพท์	ความหมาย
	ใบรับรองอิเล็กทรอนิกส์ โดยตรวจสอบและยืนยันความถูกต้องสมบูรณ์ของข้อมูลตามที่ผู้ใช้บริการให้ไว้
เอนทิตี้ (Entity)	บุคคล และรวมถึงเครื่องให้บริการ (Server) หรือเว็บไซต์ หรือหน่วยปฏิบัติงาน (Operating Unit) หรือเครื่องมืออื่นใด (Device) ที่อยู่ภายใต้การควบคุมของบุคคล
ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)	เอกสารอิเล็กทรอนิกส์ที่เป็นองค์ประกอบส่วนหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะของผู้ใช้บริการ ซึ่งอาจหมายถึงบุคคลธรรมดา นิติบุคคล หรือเครื่องมืออุปกรณ์ ซึ่งเอกสารอิเล็กทรอนิกส์ดังกล่าวสอดคล้องตามมาตรฐาน X.509 Version 3 Certificate โดยมีรายการอย่างน้อย ดังนี้ - เวอร์ชั่นของใบรับรองอิเล็กทรอนิกส์ - หมายเลขของใบรับรองอิเล็กทรอนิกส์ - วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลของผู้ถือใบรับรองอิเล็กทรอนิกส์ - ชื่อของผู้ให้บริการ - วัน เวลาที่เริ่มต้นและสิ้นสุดของการใช้ใบรับรองอิเล็กทรอนิกส์ - ชื่อของผู้ถือใบรับรองอิเล็กทรอนิกส์ - กุญแจสาธารณะของผู้ถือใบรับรองอิเล็กทรอนิกส์และวิธีการที่ใช้ในการสร้าง
ผู้ใช้บริการ (Subscriber)	บุคคล นิติบุคคล คู่สัญญา หรือผู้ขอบริการ/ขอรับการส่งเสริมกับสำนักงานส่งเสริมเศรษฐกิจดิจิทัล ที่ยื่นสมัครขอใช้บริการใบรับรองอิเล็กทรอนิกส์กับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์จะมีการระบุชื่อบุคคล หรือนิติบุคคลของผู้ใช้บริการไว้ในใบรับรองอิเล็กทรอนิกส์
กุญแจ (Key)	สัญลักษณ์ หรือลำดับของสัญลักษณ์ หรือสัญญาณไฟฟ้าที่เกี่ยวเนื่องกับสัญลักษณ์ที่นำมาเข้ารหัสข้อมูลหรือถอดรหัสข้อมูล
กุญแจส่วนตัว (Private Key)	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ และกุญแจส่วนตัวนี้จะนำไปใช้สร้างลายมือชื่อดิจิทัล
กุญแจสาธารณะ (Public Key)	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น และกุญแจสาธารณะนี้จะนำไปใช้ตรวจสอบลายมือชื่อดิจิทัล
กุญแจคู่ (Key Pari)	กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะ โดยที่สามารถใช้กุญแจสาธารณะตรวจสอบว่า ลายมือ

คำศัพท์	ความหมาย
	ชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับขอบข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้
ลายมือชื่อดิจิทัล (Digital Signature)	ลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่งที่สร้างขึ้นโดยการนำข้อมูลอิเล็กทรอนิกส์มาแปลงเป็นตัวเลขและใช้กับระบบกุญแจคู่ โดยนำไปคำนวณร่วมกับกุญแจส่วนตัวของเจ้าของลายมือชื่อ โดยที่สามารถใช้กุญแจสาธารณะของเจ้าของลายมือชื่อมาตรวจสอบได้ว่าเป็นลายมือชื่อดิจิทัลที่ได้สร้างขึ้นโดยกุญแจส่วนตัวของเจ้าของลายมือชื่อดิจิทัลนั้นหรือไม่ และข้อมูลอิเล็กทรอนิกส์ที่ได้มีการลงลายมือชื่อดิจิทัลนั้นได้มีการแก้ไขเปลี่ยนแปลงภายหลังการลงลายมือชื่อหรือไม่
การเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation)	การทำให้ใบรับรองอิเล็กทรอนิกส์ไม่สามารถใช้ได้อีกต่อไปหลังจากการเพิกถอนใบรับรอง ซึ่งส่งผลให้กุญแจส่วนตัวของผู้ใช้บริการนั้นไม่สามารถใช้ในการสร้างลายมือชื่อดิจิทัลหรือถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ได้ ทั้งนี้ไม่มีผลกระทบกับใบรับรองหรือกุญแจสาธารณะ ซึ่งยังคงสามารถใช้ในการตรวจสอบลายมือชื่อดิจิทัลที่สร้างขึ้นก่อนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้
รายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List: CRL)	รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนการใช้งาน
คู่กรณีที่เกี่ยวข้อง (Relying Party)	ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองอิเล็กทรอนิกส์หรือลายมือชื่อดิจิทัล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองไปใช้ในการตรวจสอบตัวตนของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัล และมีชื่อปรากฏอยู่ในใบรับรอง
ไดเรกทอรี่ (Directory)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดการเพื่อให้สามารถสืบค้นข้อมูลได้อย่างรวดเร็ว และเป็นตามมาตรฐานไดเรกทอรี (X.500 หรือ LDAP)
ฐานข้อมูล (Database)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดเก็บให้โปรแกรมคอมพิวเตอร์สามารถเข้าถึง จัดการ และปรับเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว

คำย่อ	คำศัพท์
CA	Certification Authority
CN	Common Name
CP	Certification Practice
CRL	Certificate Revocation List
DN	Distinguished Name
ITU-T	ITU Telecommunication Standardization sector
LDAP	Lightweight Directory Access Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
OU	Organization Unit
X.500	The ITU-T standard for Directory: overview of concepts, models, and services
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

2.1. ที่บันทึกจัดเก็บข้อมูล (Repositories)

ข้อมูลที่เกี่ยวข้องกับการขอใบรับรองอิเล็กทรอนิกส์ จะถูกจัดเก็บลงฐานข้อมูล ด้วยการเข้ารหัสจัดเก็บตามรูปแบบของข้อมูลระบบคอมพิวเตอร์ของหน่วยงานรับลงทะเบียน ในขณะที่ใบรับรองอิเล็กทรอนิกส์จะถูกจัดเก็บลง X.500 Directory

2.2. การเผยแพร่ข้อมูลของผู้ใช้บริการ (Publication of Certification Information)

ใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะถูกเผยแพร่ที่ X.500 Directory

2.3. เวลาและความถี่ในการเผยแพร่ข้อมูล (Time or Frequency of Publication)

- ข้อมูลใบรับรองอิเล็กทรอนิกส์ จะถูกเผยแพร่ลง X.500 Directory ทันทีเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์
- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ประกาศรายการใบเพิกถอนใบรับรอง แนวนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์ (CP) และแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (CPS) มีการเผยแพร่ทางเว็บไซต์ของผู้ให้บริการ (contract.depa.or.th) เพื่อใช้สำหรับการอ้างอิงแก่ผู้ใช้บริการ

2.4. การควบคุมการเข้าถึงที่บันทึกข้อมูล (Access Controls on Repositories)

ผู้ให้บริการกำหนดการควบคุมการเข้าถึงข้อมูลที่ถูกเผยแพร่บางประเภท เพื่อให้สิทธิแก่ผู้ใช้บริการและนายทะเบียนเท่านั้นในการเข้าถึงข้อมูลดังกล่าว ผู้ใช้บริการกำหนดมาตรการเกี่ยวกับความมั่นคงและ

ปลอดภัยในการกำหนดให้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้นในการสร้าง แก้ไข และนำข้อมูลไปใส่ในเว็บไซต์ที่ใช้สำหรับเผยแพร่

3. การระบุและการยืนยันตัวบุคคล (Identification and Authentication)

3.1. การกำหนดรูปแบบของชื่อ (Naming)

3.1.1. ชนิดของชื่อ (Type of Names)

ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการแต่ละรายจะมีลักษณะเป็นชื่อเฉพาะ (Distinguished Name: DN) และไม่ซ้ำกัน เพื่อให้รับรองได้ว่าสามารถเชื่อมโยงใบรับรองอิเล็กทรอนิกส์เข้ากับผู้ใช้บริการ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเครื่องที่ให้บริการได้ ทั้งนี้ อ้างอิงตาม ISO/IEC 9594-1/ITU-T Recommendation X.500 The Directory: Overview of Concepts, Models, and Services

3.1.2. ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (Need for Names to be Meaningful)

ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์จะต้องสื่อถึงความหมาย ซึ่งเชื่อมโยงไปยังการระบุตัวตนของผู้ใช้บริการที่มีชื่อปรากฏในใบรับรองอิเล็กทรอนิกส์นั้นๆ ได้ เพื่อประโยชน์ในการสืบค้นกลับไปยังเจ้าของใบรับรองอิเล็กทรอนิกส์ได้ เช่น ชื่อของนิติบุคคล (Organization Unit: OU) จะเป็นชื่อของนิติบุคคลที่ขอใช้บริการ เป็นต้น

3.1.3. นามสมมติหรือนามแฝง (Anonymity or Pseudonymity of Subscribers)

การกำหนดชื่อในส่วนของ Common Name: CN อาจกำหนดโดยความต้องการของผู้ใช้บริการเองได้

3.1.4. กฎเกณฑ์ในการสื่อความหมายสำหรับผู้ใช้บริการ (Rules for Interpreting Various Name Forms)

ไม่มีข้อกำหนด

3.1.5. เอกลักษณ์ของชื่อ (Uniqueness of Names)

ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์แต่ละใบจะมีความแตกต่างกัน ไม่ซ้ำกัน และไม่คลุมเครือ ภายใต้ CA เดียวกัน เพื่อใช้สืบค้นกลับไปยังเจ้าของใบรับรองอิเล็กทรอนิกส์ได้

3.1.6. การจดจำ รับรอง และบทบาทหน้าที่ของเครื่องหมายการค้า (Recognition, Authentication, and Role of Trademarks)

ต้องไม่ใช้ชื่อในการสมัครที่ฝ่าฝืนสิทธิตากฎหมายทรัพย์สินทางปัญญา

3.2. ความสมบูรณ์ในการระบุตัวบุคคล (Initial Identity Validation)

3.2.1. วิธีการพิสูจน์ผู้เป็นเจ้าของกุญแจส่วนตัว (Method to Prove Possession of Private Key)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบข้อมูลของผู้ถือกุญแจส่วนตัวซึ่งสัมพันธ์กับกุญแจสาธารณะจากใบสมัครขอใบรับรองอิเล็กทรอนิกส์ หรือข้อมูลการสมัคร/ยืนยัน

ผู้ใช้บริการในการจัดทำใบรับรองอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสำนักงาน ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ชื่อนิติบุคคล (กรณีเป็นนิติบุคคล) ลายเซ็นของผู้ใช้บริการเอง และ username/password

3.2.2. การยืนยันความมีตัวตนขององค์กร (Authentication of Organization Identity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบหนังสือรับรองนิติบุคคล ซึ่งจะต้องมีอายุไม่เกินหกเดือนจากวันที่ออกและมีลายเซ็นต์ของกรรมผู้มีอำนาจที่ถูกต้องและครบถ้วน หรือพระราชบัญญัติจัดตั้งองค์กร โดยสำนักงานจะดำเนินการร่วมกันส่วนงานที่เกี่ยวข้องภายในสำนักงาน

3.2.3. การยืนยันความมีตัวตนของบุคคล (Authentication of Individual Identity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบตัวตนของบุคคลจากลายเซ็นต์ในใบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ หรือข้อมูลการสมัคร/ยืนยันผู้ใช้บริการในการจัดทำใบรับรองอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสำนักงาน

3.2.4. ข้อมูลของผู้ใช้บริการยังไม่ได้ผ่านการตรวจสอบ (Non-verified Subscriber Information)

ใบรับรองอิเล็กทรอนิกส์ที่ออกจะต้องมีการยืนยันและตรวจสอบจากเอกสารที่ระบุไว้ในใบคำขอใบรับรองอิเล็กทรอนิกส์ หรือข้อมูลการสมัคร/ยืนยันผู้ใช้บริการในการจัดทำใบรับรองอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสำนักงาน ดังนั้น จะไม่มีการออกใบรับรองอิเล็กทรอนิกส์ให้แก่ผู้ใช้บริการที่ไม่ได้ยื่นคำขอใช้บริการเพื่อยืนยันตัวตน

3.2.5. การตรวจสอบผู้มีอำนาจ (Validation of Authority)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะมีกระบวนการตรวจสอบหนังสือมอบอำนาจสำหรับประกอบการสร้างข้อมูลใบคำขอใบรับรองอิเล็กทรอนิกส์เพื่อยืนยันว่า ผู้ใช้บริการนั้นได้รับมอบอำนาจมาจากกรรมการบริษัทจริง และสามารถขอใบรับรองอิเล็กทรอนิกส์ในนามขององค์กรได้

3.2.6. เกณฑ์ในการเชื่อมโยงการปฏิบัติงาน (Criteria for Interoperation)
ไม่มีข้อกำหนด

3.3. การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอใบรับรองอิเล็กทรอนิกส์ในครั้งถัดไป (Identification and Authentication for Re-key Requests)

3.3.1. การยืนยันตัวบุคคลในการขอกุญแจใหม่ (Identification and Authentication for Routine Re-key)
ผู้ใช้บริการต้องกรอกใบคำขอใบรับรองอิเล็กทรอนิกส์ใหม่ หรือข้อมูลการสมัคร/ยืนยันผู้ใช้บริการในการจัดทำใบรับรองอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสำนักงานใหม่ โดยรายละเอียดอยู่ในหัวข้อ “การยื่นคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Application)” และ “การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)”

3.3.2. การยืนยันตัวบุคคลและขอกุญแจใหม่หลังจากที่ได้เพิกถอนไปแล้ว (Identification and Authentication for Re-key after Revocation)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบข้อมูลของผู้ถือกุญแจจากใบคำขอใบรับรองอิเล็กทรอนิกส์ หรือข้อมูลการสมัคร/ยืนยันผู้ใช้บริการในการจัดทำใบรับรองอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสำนักงาน ซึ่งประกอบด้วย ชื่อ-นามสกุล ชื่อนิติบุคคล (กรณีเป็นนิติบุคคล) ลายเซ็นของผู้ใช้บริการเอง และ username/password

3.4. การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Identification and Authentication for Revocation Requests)

ผู้ใช้บริการที่ต้องการเพิกถอนใบรับรองอิเล็กทรอนิกส์ ต้องแจ้งต่อผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยตรง เมื่อผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้รับแจ้งความต้องการเพิกถอนใบรับรองอิเล็กทรอนิกส์และตรวจสอบตามขั้นตอนแล้ว จะดำเนินการเพิกถอนใบรับรองอิเล็กทรอนิกส์ตามที่แจ้งไว้ และประกาศในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดยรายละเอียดอยู่ในหัวข้อ “การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension”

4. ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operation Requirements)

4.1. การยื่นขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application)

4.1.1. ผู้ที่สามารถสมัครขอใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Submit a Certificate Application?)

ผู้ใช้บริการที่มีการดำเนินธุรกรรมทางอิเล็กทรอนิกส์กับสำนักงาน ต้องสมัครขอใบรับรองอิเล็กทรอนิกส์ โดยบุคคลที่สมัครขอใบรับรองอิเล็กทรอนิกส์สามารถเป็นได้ทั้งบุคคลที่ขอใบรับรองอิเล็กทรอนิกส์ในนามบุคคล และบุคคลที่ได้รับมอบหมายจากองค์กรให้ดำเนินการสมัครขอใบรับรองอิเล็กทรอนิกส์ในนามองค์กร เพื่อใช้รักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์

4.1.2. ขั้นตอนในการลงทะเบียนและความรับผิดชอบ (Enrollment Process and Responsibilities)

สำนักงานกำหนดขั้นตอนการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ ต้องลงทะเบียนเพื่อขอมีใบรับรองอิเล็กทรอนิกส์ตามขั้นตอนต่อไปนี้

1) สำนักงานตรวจสอบคุณสมบัติและการมีตัวตนข้อมูลผู้ใช้บริการ พร้อมหลักฐานต่างๆ ผ่านส่วนงานภายในที่เกี่ยวข้อง
2) ผู้ใช้บริการกรอกข้อมูลเพื่อลงทะเบียนสร้างใบรับรองอิเล็กทรอนิกส์ผ่านลิงค์ที่สำนักงานกำหนด โดยสำนักงานจะทำการส่งลิงค์ไปทางอีเมล์ที่ผู้ใช้บริการแจ้งไว้กับสำนักงาน พร้อมกับวิธีการในการสร้างและลงทะเบียนใบรับรองอิเล็กทรอนิกส์
3) หน่วยงานรับลงทะเบียนตรวจสอบข้อมูลการสร้างใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

4) หน่วยงานรับลงทะเบียนจัดส่งใบรับรองอิเล็กทรอนิกส์ให้กับผู้ใช้บริการ โดยมีการจัดเก็บอยู่ในระบบสารสนเทศ ซึ่งผู้ใช้บริการจะสามารถเข้าถึงผ่าน username/password ที่ดำเนินการไว้กับสำนักงาน

4.2. การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)

4.2.1. การใช้ฟังก์ชันยืนยันและรับรองตัวบุคคล (Performing Identification and Authentication Functions)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะตรวจสอบการสมัครและหลักฐานการสมัครก่อนออกใบรับรองอิเล็กทรอนิกส์ โดยจะแจ้งให้ผู้ใช้บริการรับทราบ หากข้อมูลในการสมัครผิดพลาด หรือหลักฐานไม่ครบถ้วน

4.2.2. การพิจารณาอนุมัติหรือปฏิเสธการสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ (Approval or Rejection of Certificate Applications)

หน่วนงานรับลงทะเบียนจะพิจารณาข้อมูลการสมัคร โดยตรวจสอบความครบถ้วนและถูกต้องตามความเป็นจริง จึงจะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ให้กับผู้ใช้บริการ โดยหากส่วนหนึ่งส่วนใดหรือทั้งหมดของข้อมูลการสมัครใบรับรองอิเล็กทรอนิกส์ไม่ครบถ้วน ไม่ถูกต้อง จะแจ้งให้ผู้ใช้บริการทราบ

4.2.3. เวลาที่ใช้ในการดำเนินการสำหรับการออกใบรับรองอิเล็กทรอนิกส์ (Time to Process Certificate Applications)

หน่วยงานรับลงทะเบียนจะตรวจสอบข้อมูลการสมัครขอใบรับรองอิเล็กทรอนิกส์ หลังจากได้รับคำขอใบรับรองอิเล็กทรอนิกส์ในระบบแล้ว และจะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ให้ภายในวันที่ส่งข้อมูลในระบบ หรือภายในวันทำการถัดไป

4.3. การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)

4.3.1. การทำงานของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในช่วงของการออกใบรับรองอิเล็กทรอนิกส์ (CA Actions During Certificate Issuance)

- หน่วยงานรับลงทะเบียนตรวจสอบข้อมูล เอกสารหลักฐาน และ CSR file (ถ้ามี) ที่ได้รับจากผู้ใช้บริการ โดยต้องมีความถูกต้องตรงกัน หากพบข้อมูลไม่ตรงกันให้แจ้งผู้ใช้บริการ
- เมื่อตรวจสอบพบข้อมูลถูกต้องแล้ว หน่วยงานรับลงทะเบียนจะบันทึกข้อมูลตามคำขอใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการ และออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียนตรวจสอบความถูกต้องของข้อมูลในใบรับรองอิเล็กทรอนิกส์และใบรับรองอิเล็กทรอนิกส์ที่ออกให้
- หน่วยงานรับลงทะเบียนส่งใบรับรองอิเล็กทรอนิกส์ถึงผู้ใช้บริการผ่านช่องทางที่เหมาะสม

4.3.2. การแจ้งผู้ใช้บริการหลังจากที่มีการออกใบรับรองอิเล็กทรอนิกส์ (Notification to Subscriber by the CA of Issuance of Certificate)

เมื่อหน่วยงานรับลงทะเบียนออกใบรับรองอิเล็กทรอนิกส์แล้ว ระบบจะแจ้งข้อมูลของการออกใบรับรองอิเล็กทรอนิกส์ไปให้ผู้ใช้บริการได้รับทราบผ่านทางจดหมายอิเล็กทรอนิกส์ เพื่อให้ผู้ใช้บริการได้ดำเนินการตามขั้นตอนที่ถูกต้องต่อไป

4.4. การยอมรับใบรับรองอิเล็กทรอนิกส์ (Certificate Acceptance)

4.4.1. หลักปฏิบัติในการยอมรับใบรับรองอิเล็กทรอนิกส์ (Conduct Constituting Certificate Acceptance)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะถือว่าผู้ใช้บริการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ออกให้ ก็ต่อเมื่อผู้ใช้บริการลงนามในเอกสารตอบรับใบรับรองอิเล็กทรอนิกส์ และส่งกลับมาที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือลงทะเบียนผ่านระบบสารสนเทศของสำนักงานครบถ้วนเรียบร้อย ทั้งนี้ หากผู้ใช้บริการได้ตรวจสอบและยืนยันความถูกต้องของข้อมูลดังกล่าว และมิได้แจ้งปฏิเสธหรือไม่ยอมรับข้อมูลภายในเวลา 15 วัน ให้ถือว่าผู้ใช้บริการยอมรับใบรับรองอิเล็กทรอนิกส์นั้นเรียบร้อย

4.4.2. การเผยแพร่ใบรับรองอิเล็กทรอนิกส์โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Publication of the Certificate by the CA)

ข้อมูลใบรับรองอิเล็กทรอนิกส์ จะถูกจัดเก็บลง X.500 Directory ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และเผยแพร่ทางเว็บไซต์ของผู้ให้บริการ (contract.depa.or.th) เพื่อใช้สำหรับการอ้างอิงแก่ผู้ใช้บริการ

4.4.3. การแจ้งผู้ที่เกี่ยวข้องต่างๆ ว่าด้วยเรื่องของใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Notification of Certificate Issuance by the CA to Other Entities)

หน่วยงานรับลงทะเบียนออกใบรับรองอิเล็กทรอนิกส์ จะแจ้งข้อมูลของผู้ใช้บริการได้รับทราบผ่านทางเว็บไซต์ของผู้ให้บริการ (contract.depa.or.th)

4.5. การใช้กุญแจคู่ และใบรับรองอิเล็กทรอนิกส์ (Key Pair and Certificate Usage)

4.5.1. การใช้กุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Entities Private Key and Certificate Usage)

การใช้กุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์จะมีความผูกพันเมื่อผู้ใช้บริการได้ยอมรับข้อตกลงในการใช้งานใบรับรองอิเล็กทรอนิกส์ และยอมรับใบรับรองอิเล็กทรอนิกส์แล้ว ทั้งนี้ การใช้ใบรับรองอิเล็กทรอนิกส์จะต้องสัมพันธ์กับค่าที่ระบุไว้ในฟิลด์ Key Usage ในใบรับรองอิเล็กทรอนิกส์ รวมทั้งผู้ใช้งานจะต้องปกป้องกุญแจส่วนตัวจากการเข้าถึงโดยไม่ได้รับอนุญาต และจะต้องยุติการใช้กุญแจส่วนตัวในทันทีที่ใบรับรองอิเล็กทรอนิกส์ใบนั้นหมดอายุ หรือถูกเพิกถอน

4.5.2. การใช้กุญแจสาธารณะและใบรับรองอิเล็กทรอนิกส์ของคู่กรณีที่เกี่ยวข้อง (Relying Party Public Key and Certificate Usage)

คู่กรณีที่เกี่ยวข้องจะต้องปฏิบัติตามข้อตกลงในการใช้งานใบรับรองอิเล็กทรอนิกส์สำหรับคู่กรณีที่เกี่ยวข้องที่ระบุไว้ในเอกสารฉบับนี้ ซึ่งจะต้องตรวจสอบเงื่อนไขบางประการก่อนที่จะใช้ใบรับรองอิเล็กทรอนิกส์ใบนั้น หากเงื่อนไขระบุว่าจะจัดหาข้อมูลเพิ่มเติมคู่กรณีที่เกี่ยวข้องก็จำเป็นต้องดำเนินการอย่างเหมาะสมก่อนที่จะใช้ใบรับรองอิเล็กทรอนิกส์ คู่กรณีที่เกี่ยวข้องจำเป็นต้องประเมินดังนี้

- ความเหมาะสมในการใช้ใบรับรองอิเล็กทรอนิกส์ ซึ่งสอดคล้องกับที่ได้ระบุไว้ในฟิลด์ Key Usage ในใบรับรองอิเล็กทรอนิกส์ และจะต้องไม่ขัดต่อข้อจำกัดในการใช้ใบรับรองอิเล็กทรอนิกส์ที่ระบุไว้ในเอกสารฉบับนี้
- สถานะของใบรับรองอิเล็กทรอนิกส์ที่กำลังตรวจสอบ หากใบรับรองอิเล็กทรอนิกส์ถูกเพิกถอน คู่กรณีที่เกี่ยวข้องจะต้องปฏิเสธการใช้ใบรับรองอิเล็กทรอนิกส์ใบนั้นทันที

4.6. การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal)

4.6.1. กรณีในการขอต่ออายุใบรับรองอิเล็กทรอนิกส์ (Circumstance for Certificate Renewal)

ปัจจุบันผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีนโยบายในการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการ โดยไม่มีการเปลี่ยนแปลงกุญแจสาธารณะของผู้ใช้บริการหรือข้อมูลอื่นใดที่ปรากฏในใบรับรองอิเล็กทรอนิกส์

หากมีใบรับรองอิเล็กทรอนิกส์ที่กำลังจะหมดอายุลงในอีก 60 วัน หรือ 30 วันข้างหน้า ระบบจะส่งจดหมายอิเล็กทรอนิกส์แจ้งเตือนไปยังผู้ใช้บริการให้รับทราบ เพื่อให้ผู้ใช้บริการดำเนินการขอใบรับรองใหม่แทนใบรับรองเดิมที่ใกล้หมดอายุ ตามข้อ 4.1

4.6.2. ผู้ที่สามารถขอต่ออายุใบรับรองอิเล็กทรอนิกส์ (Who may Request Renewal)

ไม่มีบริการ

4.6.3. กระบวนการขอต่ออายุใบรับรองอิเล็กทรอนิกส์ (Processing Certificate Renewal Request)

ไม่มีบริการ

4.6.4. การแจ้งเตือนผู้ใช้บริการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ใหม่ (Notification of New Certificate Issuance to Subscriber)

ไม่มีบริการ

4.6.5. การดำเนินการเพื่อยอมรับใบรับรองอิเล็กทรอนิกส์ที่ได้มีการต่ออายุใหม่ (Conduct Constituting Acceptance of a Renewal Certificate)

ไม่มีบริการ

4.6.6. การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้มีการต่ออายุใหม่โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Publication of the Renewal Certificate by the CA)

ไม่มีบริการ

4.6.7. การแจ้งเตือนไปยังหน่วยงานที่เกี่ยวข้องเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์ที่ได้มีการต่ออายุ (Notification of Certificate Issuance by the CA to Other Entities)

ไม่มีบริการ

4.7. การรับรองกุญแจคู่ใหม่ (Certificate Re-key)

4.7.1. กรณีที่อนุญาตให้มีการรับรองคู่กุญแจใหม่ (Circumstance for Certificate Re-Key)

ก่อนที่ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการเดิมจะหมดอายุ ผู้ใช้บริการหรือผู้มีอำนาจแทนผู้ใช้งานสามารถติดต่อผู้ให้บริการ โดยมีกระบวนการเช่นเดียวกับการยื่นขอใบรับรองอิเล็กทรอนิกส์ใหม่ ตามข้อ 4.1

4.7.2. ผู้ที่สามารถขอกุญแจสาธารณะใหม่ (Who May Request Certification of a New Public Key)

อ้างอิงตามข้อ 4.1

4.7.3. กระบวนการขอรับรองคู่กุญแจใหม่ (Processing Certificate Re-Keying Requests)

อ้างอิงตามข้อ 4.1

4.7.4. การแจ้งเตือนการออกใบรับรองอิเล็กทรอนิกส์ใหม่แก่ผู้ใช้บริการ (Notification of New Certificate Issuance to Subscriber)

อ้างอิงตามข้อ 4.3 และ 4.4

4.7.5. การยอมรับใบรับรองอิเล็กทรอนิกส์ที่ได้มีการรับรองคู่กุญแจใหม่ (Conduct Constituting Acceptance of a Re-Keyed Certificate)

อ้างอิงตามข้อ 4.3 และ 4.4

4.7.6. การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้มีการรับรองคู่กุญแจใหม่ (Publication of the Re-Keyed Certificate by the CA)

อ้างอิงตามข้อ 4.3 และ 4.4

4.7.7. การแจ้งเตือนไปยังหน่วยงานที่เกี่ยวข้องเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์ที่ได้มีการรับรองคู่กุญแจใหม่โดยผู้ให้บริการออกใบรับรอง (Notification of Certificate Issuance by the CA to Other Entities)

อ้างอิงตามข้อ 4.3 และ 4.4

4.8. การเปลี่ยนแปลงข้อมูลใบรับรองอิเล็กทรอนิกส์ (Certificate Modification)

4.8.1. กรณีการขอแก้ไขเปลี่ยนแปลงข้อมูลใบรับรองอิเล็กทรอนิกส์ (Circumstances for Certification Modification)

ในกรณีที่ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลใบรับรองอิเล็กทรอนิกส์ที่ได้ออกไปแล้วนั้น ผู้ใช้บริการจะต้องยื่นคำร้องเพื่อขอยกเลิกใบรับรองอิเล็กทรอนิกส์ใบเดิม พร้อมทำการสมัครใบรับรองอิเล็กทรอนิกส์ใหม่

4.8.2. ผู้ที่สามารถขอแก้ไข (Who may Request Certificate Modification)

อ้างอิงตามข้อ 4.1

4.8.3. ขั้นตอนในการขอแก้ไขใบรับรองอิเล็กทรอนิกส์ (Processing Certificate Modification Request)

อ้างอิงตามข้อ 4.1

4.8.4. การแจ้งเตือนผู้ใช้บริการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ใหม่ (Notification of New Certificate Issuance to Subscriber)

อ้างอิงตามข้อ 4.3 และ 4.4

4.8.5. การดำเนินการเพื่อยอมรับใบรับรองอิเล็กทรอนิกส์ที่ถูกแก้ไข (Conduct Constituting Acceptance of Modified Certificate)

อ้างอิงตามข้อ 4.3 และ 4.4

4.8.6. การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ถูกแก้ไขโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Publication of the Modified Certificate by the CA)

อ้างอิงตามข้อ 4.3 และ 4.4

4.9. การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension)

สำหรับบริการเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์นั้น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะดำเนินการก็ต่อเมื่อได้รับคำขอยกเลิกหรือพักใช้ใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการ และได้รับการตรวจสอบเรียบร้อยแล้ว หรือได้รับคำสั่งโดยชอบด้วยกฎหมายให้ดำเนินการดังกล่าว

4.9.1. เหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension)

การเพิกถอนโดยผู้ใช้บริการ

- มีผู้อื่นล่วงรู้กุญแจส่วนตัวของผู้ใช้บริการ หรือผู้อื่นสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ใช้บริการไปใช้งาน
- มีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ใช้บริการ
- อุปกรณ์ที่ใช้ในการเก็บกุญแจส่วนตัวสูญหาย หรือไม่สามารถใช้งานได้
- มีเหตุอื่นใดที่อาจจะทำให้ผู้อื่นนำใบรับรองอิเล็กทรอนิกส์ไปใช้โดยไม่มีสิทธิ

- ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลที่อยู่ในใบรับรองอิเล็กทรอนิกส์ เช่น ชื่อหรือนามสกุล เป็นต้น
- ผู้ใช้บริการระงับหรือยกเลิกการใช้บริการ

การเพิกถอนโดยผู้ให้บริการ

- ผู้ใช้บริการไม่ปฏิบัติตามนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์ และแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ หรือไม่ปฏิบัติตามกฎระเบียบของหน่วยงานของผู้ให้บริการ
- ผู้ใช้บริการไม่มีข้อผูกพันทางสัญญา และ/หรือไม่มีความจำเป็นต้องดำเนินธุรกรรมใดๆ ของผู้ให้บริการ
- มีผู้อื่นล่วงรู้กุญแจส่วนตัวของผู้ให้บริการ
- มีคำสั่งของศาลหรือต้องการดำเนินการตามกฎหมาย
- ผู้ให้บริการระงับหรือยกเลิกการให้บริการ
- กรณีอื่นๆ ที่ผู้ให้บริการพิจารณาแล้วว่าจะมีผลกระทบต่อความมั่นคงปลอดภัยของการให้บริการใบรับรองอิเล็กทรอนิกส์

4.9.2. ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Revocation)

ผู้มีอำนาจหรือผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ ทั้งนี้ผู้ให้บริการสามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้เช่นกัน หากตรงตามเงื่อนไขที่ระบุไว้ในข้อ 4.9.1

4.9.3. ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Procedure for Revocation Request)

- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์กรอกคำร้องผ่านระบบสารสนเทศของสำนักงานที่กำหนด หรือส่งคำร้องผ่านจดหมายอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียนตรวจสอบข้อมูลคำร้องขอยกเลิกใบรับรองอิเล็กทรอนิกส์
- หลังจากหน่วยงานรับลงทะเบียนตรวจสอบคำร้องขอยกเลิกใบรับรองอิเล็กทรอนิกส์เรียบร้อย จึงจะเพิกถอนใบรับรองอิเล็กทรอนิกส์ต่อไป

4.9.4. ระยะเวลาที่ใช้ในการเพิกถอน (Revocation Request Grace Period)

หลังจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้รับคำร้องขอยกเลิกใบรับรองอิเล็กทรอนิกส์ และได้ตรวจสอบความถูกต้องของคำร้องเรียบร้อย ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะเพิกถอนใบรับรองอิเล็กทรอนิกส์ในทันที

4.9.5. ระยะเวลาที่ใช้ในการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Time within Which CA Must Process the Revocation Request)

อ้างอิงตามข้อ 4.9.4

4.9.6. ตรวจสถานะเพิกถอนของใบรับรองอิเล็กทรอนิกส์ โดยหน่วยงานที่เกี่ยวข้อง (Revocation Checking Requirements for Relying Parties)

ผู้ใช้บริการสามารถเข้าไปตรวจสอบ CRL ได้ที่เว็บไซต์ หรือระบบสารสนเทศของสำนักงานที่กำหนด

4.9.7. ความถี่ในการอัพเดตรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (CRL Issuance Frequency)

ผู้ให้บริการจะทำการอัพเดตรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ เมื่อมีการเพิกถอนใบรับรองอิเล็กทรอนิกส์เกิดขึ้น

4.9.8. ระยะเวลาที่ใช้ในขั้นตอนการประกาศรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Maximum Latency for CRLs)

ผู้ให้บริการจะทำการเพิกถอนใบรับรอง ประกาศไว้ในที่เว็บไซต์ หรือระบบสารสนเทศของสำนักงานที่กำหนด หลังจากที่ได้สร้างรายการเรียบร้อย

4.9.9. การตรวจสอบสถานะการเพิกถอนใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ (On-line Revocation/Status Checking Availability)

ผู้ใช้บริการของสำนักงานเท่านั้น ที่สามารถเข้าตรวจสอบ OCSP (Online Certificate Status Protocol) ได้ที่เว็บไซต์ หรือระบบสารสนเทศของสำนักงานที่กำหนด

4.9.10. ความต้องการการตรวจสอบการเพิกถอนใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ (On-line Revocation Checking Requirements)

อ้างอิงตามข้อ 4.9.9

4.9.11. การประกาศสถานการณ์เพิกถอนใบรับรองอิเล็กทรอนิกส์ในรูปแบบอื่น (Other Forms of Revocation Advertisements Available)

ระบบให้บริการของผู้ให้บริการไม่รองรับการประกาศรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ในรูปแบบอื่น นอกเหนือจากการประกาศไว้ในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ ซึ่งปรากฏอยู่บนเว็บไซต์ หรือระบบสารสนเทศของสำนักงานที่กำหนด

4.9.12. ความต้องการพิเศษกรณีที่มีการขอให้รับรองคู่กุญแจใหม่เมื่อกุญแจเสียหาย (Special Requirements Regarding Key Compromise)

หากผู้ใช้บริการตรวจพบว่ากุญแจส่วนตัวได้ถูกโจรกรรม ถูกล่วงรู้ ถูกเข้าถึง หรือไม่สามารถใช้งานได้ ให้ผู้ใช้บริการดำเนินการเพื่อขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ตามกระบวนการดังกล่าวข้างต้น การเพิกถอนใบรับรองอิเล็กทรอนิกส์ดังกล่าวให้ถือว่าเป็นการยกเลิกการใช้งานคู่กุญแจนั้นด้วย

4.9.13. กรณีที่อนุญาตให้มีการพักใช้ใบรับรองอิเล็กทรอนิกส์ (Circumstances for Suspension)

ไม่มีให้บริการการพักใช้งานใบรับรองอิเล็กทรอนิกส์

4.9.14. ผู้ที่สามารถขอพักใช้ใบรับรองอิเล็กทรอนิกส์ (Who can Request Suspension)

ไม่มีให้บริการการพักใช้งานใบรับรองอิเล็กทรอนิกส์

4.9.15. กระบวนการขอพักใบรับรองอิเล็กทรอนิกส์ (Procedure for Suspension Request)

ไม่มีให้บริการการพักใช้งานใบรับรองอิเล็กทรอนิกส์

4.9.16. ขอบเขตระยะเวลาในการพักใช้ใบรับรองอิเล็กทรอนิกส์ (Limits on Suspension Period)

ไม่มีให้บริการการพักใช้งานใบรับรองอิเล็กทรอนิกส์

4.10. บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)

ผู้ใช้บริการ และ/หรือคู่กรณีที่เกี่ยวข้องสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้บนเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือระบบสารสนเทศของสำนักงานที่กำหนด

4.10.1. ลักษณะของบริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Operational Characteristics)

ผู้ใช้บริการของสำนักงานเท่านั้น ที่สามารถเข้าตรวจสอบได้ที่เว็บไซต์ หรือระบบสารสนเทศของสำนักงานที่กำหนด

4.10.2. สภาพพร้อมใช้งานของระบบบริการ (Service Availability)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ให้บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ผ่านทางเว็บไซต์ หรือระบบสารสนเทศของสำนักงานที่กำหนด ตลอด 24 ชั่วโมง

4.10.3. ความสามารถอื่นๆ (Optional Features)

ไม่มี

4.11. การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription)

ผู้ใช้บริการสามารถเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ได้ โดยดำเนินการเพิกถอนใบรับรองอิเล็กทรอนิกส์ตามข้อ 4.9.3

4.12. การเก็บรักษาและการกู้คืนกุญแจ (Key Escrow and Recovery)

4.12.1. แนวนโยบายและแนวปฏิบัติเกี่ยวกับการเก็บรักษาและการกู้คืนกุญแจ (Key Escrow and Recovery Policy and Practices)

ไม่มีให้บริการ

4.12.2. การป้องกัน Session Key รวมทั้งแนวนโยบายและแนวปฏิบัติในการกู้คืนกุญแจ (Session Key Encapsulation and Recovery Policy and Practices)

ไม่มีให้บริการ

5. การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)

5.1. การควบคุมความปลอดภัยด้านกายภาพ (Physical Controls)

5.1.1. สถานที่ตั้ง (Site Location and Construction)

สถานที่ตั้งของหน่วยงานออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตั้งอยู่ที่ 80 ถนนลาดพร้าว ซอยลาดพร้าว 4 แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900 ซึ่งมีการดำเนินงานตามแผนงานด้านโครงสร้างพื้นฐานดิจิทัลที่มีประสิทธิภาพเชื่อมโยงถึงกัน และการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ด้วยระบบคอมพิวเตอร์แบบคลาวด์ (Cloud Computing) ตามมาตรฐานด้านความปลอดภัยต่างๆ ที่ได้รับการรับรองการควบคุมคุณภาพการให้บริการตามมาตรฐานสากล ISO/IEC 27001, 20000-1 และ CSA STAR Certification

5.1.2. การเข้าถึงทางกายภาพ (Physical Access)

การเข้าถึงพื้นที่ซึ่งติดตั้งระบบให้บริการใบรับรองอิเล็กทรอนิกส์จะอนุญาตให้สามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ของผู้ให้บริการหรือเจ้าหน้าที่ได้รับมอบหมายจากผู้ให้บริการเท่านั้น โดยควบคุมการเข้าถึงระบบให้บริการใบรับรองอิเล็กทรอนิกส์ด้วยการใช้รหัสผ่าน พร้อมระบบการพิสูจน์และยืนยันตัวตน

5.1.3. ระบบไฟฟ้าและระบบปรับอากาศ (Power and Air Conditioning)

สำนักงานดำเนินงานตามแผนงานด้านโครงสร้างพื้นฐานดิจิทัลที่มีประสิทธิภาพเชื่อมโยงถึงกัน และการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ด้วยระบบคอมพิวเตอร์แบบคลาวด์ (Cloud Computing) ตามมาตรฐานด้านความปลอดภัยต่างๆ ได้แก่ ด้านระบบไฟฟ้าและระบบปรับอากาศ ด้านระบบป้องกันภัยจากน้ำท่วม และระบบป้องกันภัยจากอัคคีภัย

5.1.4. การป้องกันภัยจากน้ำ (Water Exposures)

สำนักงานดำเนินงานตามแผนงานด้านโครงสร้างพื้นฐานดิจิทัลที่มีประสิทธิภาพเชื่อมโยงถึงกัน และการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ด้วยระบบคอมพิวเตอร์แบบคลาวด์ (Cloud Computing) ตามมาตรฐานด้านความปลอดภัยต่างๆ ได้แก่ ด้านระบบไฟฟ้าและระบบปรับอากาศ ด้านระบบป้องกันภัยจากน้ำท่วม และระบบป้องกันภัยจากอัคคีภัย

5.1.5. การป้องกันภัยอัคคีภัย (Fire Prevention and Protection)

สำนักงานดำเนินงานตามแผนงานด้านโครงสร้างพื้นฐานดิจิทัลที่มีประสิทธิภาพเชื่อมโยงถึงกัน และการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ด้วยระบบคอมพิวเตอร์แบบคลาวด์ (Cloud Computing) ตามมาตรฐานด้านความปลอดภัยต่างๆ ได้แก่ ด้านระบบไฟฟ้าและระบบปรับอากาศ ด้านระบบป้องกันภัยจากน้ำท่วม และระบบป้องกันภัยจากอัคคีภัย

5.1.6. การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage)

สื่อที่ใช้ในการจัดเก็บ บันทึก และสำรองข้อมูลที่ใช้ในระบบงานจะถูกจัดเก็บไว้อย่างปลอดภัย

5.1.7. การกำจัดสิ่งที่ไม่ใช้ (Waste Disposal)

สื่อต่างๆ ที่ใช้ในการบันทึกหรือเก็บข้อมูลที่ไม่ใช้อีกต่อไป จะถูกกำจัด หรือทำลาย เพื่อไม่ใช้มีการนำสื่อดังกล่าวข้างต้นกลับมาใช้ หรือเรียกค้นข้อมูลได้อีก ทั้งนี้ การทำลายสื่อแม่เหล็ก หมายรวมถึงการเขียนข้อมูลใหม่ทับ (Overwrite) การทำลายด้วยสนามแม่เหล็ก (Degauss) หรือการทำลายทิ้ง (Destruct) ด้วย

5.1.8. การสำรองข้อมูลไว้ที่อื่น (Off-Site Backup)

ดำเนินการตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนบริหารความต่อเนื่อง และนโยบาย มาตรฐาน แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

5.2. การควบคุมความปลอดภัยในการดำเนินงาน (Procedural Controls)

5.2.1. บทบาทที่น่าเชื่อถือ (Trusted Roles)

บทบาทที่น่าเชื่อถือได้รับการกำหนดขึ้นโดยผู้ให้บริการ เพื่อรักษาการแบ่งแยกหน้าที่ต่างๆ ให้มีอยู่เพื่อรับประกันว่าไม่มีบุคคลใดที่สามารถทำการดัดแปลงแก้ไขและบันทึกเรื่องราวต่างๆ ของผู้ให้บริการ โดยมีบทบาทที่ถูกกำหนดขึ้นสำหรับการดำเนินงาน ประกอบด้วย

- เจ้าหน้าที่ส่วนเทคโนโลยีดิจิทัลและสารสนเทศ ที่ทำหน้าที่เสมือน CA Operation
- เจ้าหน้าที่ส่วนเทคโนโลยีดิจิทัลและสารสนเทศ ที่ทำหน้าที่ด้านรักษาความมั่นคงและปลอดภัย
- ผู้จัดการส่วนเทคโนโลยีดิจิทัลและสารสนเทศ ที่ทำหน้าที่กำกับ ตรวจสอบ และรักษาความมั่นคงและปลอดภัย

วิธีการดำเนินการเพื่อปฏิบัติหน้าที่ต่างๆ สำหรับการดำเนินงานด้านใบรับรองอิเล็กทรอนิกส์เป็นหน้าที่ที่ต้องปฏิบัติของเจ้าหน้าที่ของสำนักงาน ซึ่งไม่มีการนำมาเปิดเผยต่อสาธารณะ

5.2.2. จำนวนบุคลากรที่ต้องการต่องาน (Number of Persons Required Per Task)

ในแต่ละบทบาทหน้าที่ที่ระบุไว้ข้างต้นจะปฏิบัติงานตามที่กำหนด เพื่อการรักษาความมั่นคงและปลอดภัยในระดับสูงสุด งานใดๆ ที่เกี่ยวกับการแก้ไของค์ประกอบทางอิเล็กทรอนิกส์หรือทางกายภาพของโครงสร้างผู้ให้บริการนั้น จะได้รับความเห็นชอบผ่านคณะกรรมการเทคโนโลยีดิจิทัลและสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัลอย่างเหมาะสม

5.2.3. การระบุและพิสูจน์ความเป็นตัวตนแท้จริงของเจ้าหน้าที่ในแต่ละบทบาท (Identification and Authentication for Each Role)

ผู้ให้บริการ และเจ้าหน้าที่รับลงทะเบียน เป็นบุคลากรของสำนักงานส่งเสริมเศรษฐกิจดิจิทัลที่จะปฏิบัติหน้าที่ในบทบาทที่ได้รับ

5.2.4. บทบาที่ต้องการแบ่งแยกหน้าที่ความรับผิดชอบ (Roles Requiring Separation of Duties)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ กำหนดและแบ่งแยกบทบาทหน้าที่ความรับผิดชอบประกอบด้วย

- เจ้าหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ มีหน้าที่หลักในการดูแลบริหารจัดการระบบให้บริการใบรับรองอิเล็กทรอนิกส์ และซอฟต์แวร์ต่างๆ ที่เกี่ยวข้อง ได้แก่ Database, Firewall, LDAP และการสำรองข้อมูลระบบ
- เจ้าหน้าที่รับลงทะเบียน มีหน้าที่หลักในการตรวจสอบความถูกต้องของข้อมูลการสมัครขอใบรับรองอิเล็กทรอนิกส์ และดำเนินการออกใบรับรองอิเล็กทรอนิกส์ รวมถึงดำเนินการพักใช้ใบรับรองอิเล็กทรอนิกส์ และเพิกถอนใบรับรองอิเล็กทรอนิกส์

5.3. การควบคุมความปลอดภัยทางด้านบุคลากร (Personnel Controls)

5.3.1. คุณสมบัติ ประสบการณ์ และประวัติของบุคลากรผู้ปฏิบัติงาน (Qualifications, Experience, and Clearance Requirements)

บุคลากรสำหรับการดำเนินงานในระบบให้บริการใบรับรองอิเล็กทรอนิกส์ จำเป็นต้องปฏิบัติตามกฎระเบียบ ข้อบังคับ ที่ผ่านการดำเนินงานของส่วนบริหารและพัฒนาบุคคล ฝ่ายทรัพยากรองค์กรและบุคคล เพื่อการรักษาความมั่นคงและปลอดภัย อันเป็นการรับประกันถึงความถูกต้องและความสามารถในการดำเนินงานในบทบาทหน้าที่ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

5.3.2. กระบวนการตรวจสอบประวัติ (Background Check Procedures)

บุคลากรสำหรับการดำเนินงานในระบบให้บริการใบรับรองอิเล็กทรอนิกส์ จำเป็นต้องปฏิบัติตามกฎระเบียบ ข้อบังคับ ที่ผ่านการดำเนินงานของส่วนบริหารและพัฒนาบุคคล ฝ่ายทรัพยากรองค์กรและบุคคล เพื่อการรักษาความมั่นคงและปลอดภัย อันเป็นการรับประกันถึงความถูกต้องและความสามารถในการดำเนินงานในบทบาทหน้าที่ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

5.3.3. การฝึกอบรมบุคลากร (Training Requirements)

ดำเนินการตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนบริหารความต่อเนื่อง และนโยบาย มาตรฐาน แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล และปฏิบัติตามแผนงานด้านการบริหารทรัพยากรบุคคล โดยมีเนื้อหาอย่างเหมาะสมและเพียงพอสำหรับงานบริหารจัดการระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ได้แก่ ความรู้เกี่ยวกับเทคโนโลยี PKI, การใช้งานระบบบริการใบรับรองอิเล็กทรอนิกส์, การตระหนักการรักษาความมั่นคงและปลอดภัยของระบบคอมพิวเตอร์ และความรู้เกี่ยวกับแนวนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์และแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์

5.3.4. ความถี่ในการฝึกอบรมบุคลากร (Retraining Frequency and Requirements)

ดำเนินการตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนบริหารความต่อเนื่อง และนโยบาย มาตรฐาน แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล และปฏิบัติตามแผนงานด้านการบริหารทรัพยากรบุคคล

5.3.5. ความถี่ในการโอนย้ายหน้าที่ (Job Rotation Frequency and Sequence)

บุคลากรที่ดำเนินงานของผู้ให้บริการโดยหลักจะเป็นเจ้าหน้าที่ของส่วนเทคโนโลยีดิจิทัลและสารสนเทศ ซึ่งมีกระบวนการทำงานและปฏิบัติหน้าที่ตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนบริหารความต่อเนื่อง และนโยบาย มาตรฐาน แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล พร้อมกับการดำเนินงานตามแผนงานด้านการบริหารทรัพยากรบุคคล

5.3.6. บทลงโทษสำหรับการละเมิดสิทธิ์ (Sanction for Unauthorized Action)

บุคคลที่ดำเนินการโดยไม่ได้รับอนุญาตจะเป็นไปตามกระบวนการทางวินัยหรือทางกฎหมาย โดยการดำเนินการของผู้ให้บริการ ในกรณีที่มีความร้ายแรง ผู้กระทำผิดจะถูกดำเนินคดีจากการกระทำต่อไป

5.3.7. ผู้รับดำเนินการภายนอก (Independent Contractor Requirements)

ผู้ให้บริการ อาจมีการจ้างผู้รับดำเนินการภายนอกหรือที่ปรึกษาภายนอกมาดำเนินงานตามที่ได้รับมอบหมาย ทั้งนี้ ผู้ให้บริการจะกำหนดสิทธิ์ให้ดำเนินการ โดยจะอยู่ภายใต้บรรทัดฐานด้านความมั่นคงปลอดภัยเทียบเท่ากับเจ้าหน้าที่ของผู้ให้บริการ และจะมีเจ้าหน้าที่ของผู้ให้บริการคอยติดตามขณะปฏิบัติงานด้วย

5.3.8. เอกสารประกอบสำหรับบุคลากร (Documentation Supplied to Personnel)

บุคลากรของผู้ให้บริการ สามารถเรียกดูเอกสารประกอบต่างๆ เกี่ยวกับระบบให้บริการ อุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ และคู่มือการใช้ระบบงานต่างๆ ที่เกี่ยวข้องกับการปฏิบัติงานสำหรับผู้ใช้บริการนั้น สามารถเรียกดูคู่มือการใช้งานสำหรับผู้ใช้บริการได้ ทั้งนี้ ขึ้นอยู่กับประเภทของบริการและข้อตกลงการใช้บริการด้วย

5.4. กระบวนการบันทึกเหตุการณ์ (Audit Logging Procedures)

5.4.1. ข้อมูลที่เก็บบันทึก (Types of Events Recorded)

depa CA จะทำการบันทึกเหตุการณ์ต่างๆ แบบอัตโนมัติ หรือโดยบุคคลตามความสำคัญของเหตุการณ์ ดังนี้

1) การบันทึกเหตุการณ์เกี่ยวกับวงจรการใช้งานกุญแจของ depa CA
   - การสร้างกุญแจ การสำรอง การจัดเก็บ การกู้คืน การบันทึกข้อมูล และการทำลาย
   - การจัดการอุปกรณ์การเข้ารหัสลับ

2) การบันทึกเหตุการณ์ของกุญแจผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และผู้ขอใช้ใบรับรองอิเล็กทรอนิกส์
   - คำขอสมัครใช้บริการใบรับรองอิเล็กทรอนิกส์ คำขอสมัครต่ออายุใบรับรองอิเล็กทรอนิกส์ คำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์
   - การอนุมัติหรือไม่อนุมัติคำขอ
   - การออกใบรับรองอิเล็กทรอนิกส์ และรายการเพิกถอนใบรับรอง

3) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

- การเข้าถึงระบบ depa CA ที่สำเร็จและไม่สำเร็จ
- กิจกรรมเกี่ยวกับความมั่นคงปลอดภัยที่กระทำโดยเจ้าหน้าที่ depa CA
- การอ่าน/เขียน/ลบ ไฟล์ที่มีความสำคัญ
- การเปลี่ยนแปลงการตั้งค่าความมั่นคงปลอดภัยของระบบ
- ปัญหาของระบบ อุปกรณ์ฮาร์ดแวร์ และความผิดปกติอื่นๆ
- การทำงานของอุปกรณ์เครือข่ายและไฟร์วอลล์
- การเยี่ยมชมระบบโดยบุคคลภายนอก

การบันทึกเหตุการณ์แต่ละรายการ ประกอบด้วยข้อมูล ดังต่อไปนี้

- วันที่และเวลาของแต่ละรายการ
- ลำดับรายการ โดยบันทึกอัตโนมัติ
- ผู้ดำเนินการ
- ประเภทของเหตุการณ์

5.4.2. ความถี่ในการประมวลผลข้อมูลการลงบันทึกเหตุการณ์ (Frequency of Processing Log)

เจ้าหน้าที่ดูแลระบบจะตรวจสอบข้อมูลการลงบันทึกเหตุการณ์อย่างสม่ำเสมอ อย่างน้อยวันละ 1 ครั้ง โดยการตรวจสอบนั้น จะตรวจสอบด้วย log และเอกสารประกอบที่เกี่ยวข้อง

5.4.3. ระยะเวลาที่จะเก็บข้อมูลการลงบันทึกเหตุการณ์ (Retention Period for Audit Log)

ข้อมูลการลงบันทึกเหตุการณ์ต่างๆ จะถูกเก็บไว้เป็นวลาอย่างน้อย 90 วัน หรือมากกว่านั้นตามที่กำหนด

5.4.4. การป้องกันข้อมูลการลงบันทึกเหตุการณ์ (Protection of Audit Log)

การจัดเก็บข้อมูลการลงบันทึกเหตุการณ์ต่างๆ ไว้บนเครื่องแม่ข่ายให้บริการสำหรับบันทึกเหตุการณ์ ซึ่งจะมีแต่เจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงและอ่านข้อมูลได้

5.4.5. ขั้นตอนการสำรองเก็บข้อมูลการลงบันทึกเหตุการณ์ (Audit Log Backup Procedure)

ข้อมูลการลงบันทึกเหตุการณ์ต่างๆ จะได้รับการบันทึกการสำรองข้อมูล โดยอัตโนมัติและถูกเก็บไว้ทุกวันที่เครื่องแม่ข่าย

5.4.6. ระบบการเก็บข้อมูลการลงบันทึกเหตุการณ์ (Audit Collection System (Internal vs External))

บันทึกเหตุการณ์ต่างๆ สามารถแบ่งได้เป็นแบบอัตโนมัติ (Automatic) และโดยบุคคล (Manual)

5.4.7. การแจ้งไปยังบุคคลที่เกี่ยวข้อง (Notification to Event-Causing Subject)

เจ้าหน้าที่ดูแลระบบ จะตรวจสอบบันทึกเหตุการณ์ (Log Event) วันละ 1 ครั้ง เพื่อให้ทราบถึงเหตุการณ์ที่ไม่ปกติเกี่ยวกับความมั่นคงและปลอดภัยของระบบ ทั้งนี้หากเหตุการณ์ที่ไม่ปกติจากภายนอกระบบ จะมีการแจ้งไปยังบุคคลที่เกี่ยวข้องต่อไป

5.4.8. การตรวจประเมินช่องโหว่ของระบบ (Vulnerability Assessments)

การประเมินช่องโหว่ของระบบเป็นการดำเนินการเพื่อหาจุดอ่อนหรือช่องโหว่ ซึ่งจะถูกดำเนินการตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนบริหารความต่อเนื่อง และนโยบาย มาตรฐาน แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

5.5. การเก็บบันทึกถาวระของข้อมูล (Records Archival)

5.5.1. ประเภทของข้อมูลที่ต้องการเก็บบันทึก (Types of Event Recorded)

- ข้อมูลการลงบันทึกเหตุการณ์ต่างๆ ตามข้อ 5.4
- ข้อมูลเกี่ยวกับการขอใบรับรองอิเล็กทรอนิกส์ และเอกสารต่างๆ ที่เกี่ยวข้อง
- ข้อมูลเกี่ยวกับวงจรการใช้ใบรับรองอิเล็กทรอนิกส์ ได้แก่ การเพิกถอนใบรับรองอิเล็กทรอนิกส์ การต่ออายุใบรับรองอิเล็กทรอนิกส์ เป็นต้น

5.5.2. ช่วงเวลาในการเก็บรักษาข้อมูล (Retention Period for Archive)

ข้อมูลต่างๆ จะถูกเก็บต่อไปอย่างน้อยเป็นเวลา 3 ปี หลังจากที่ใบรับรองอิเล็กทรอนิกส์นั้นหมดอายุ หรือถูกเพิกถอน

5.5.3. การป้องกันบันทึกถาวระของข้อมล (Protection of Archive)

การป้องกันการเข้าถึงข้อมูลที่ได้ทำการสำรองไว้เพื่อให้บุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลนั้นได้ สำหรับข้อมูลในรูปแบบอิเล็กทรอนิกส์จะได้รับการบันทึกไว้บนเครื่องแม่ข่ายที่ให้บริการที่มีความปลอดภัยสูง และสามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น ส่วนข้อมูลในรูปแบบเอกสารที่มีการจัดเก็บ จะสามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้นเช่นเดียวกัน

5.5.4. กระบวนการในการสำรองบันทึกถาวรของข้อมูล (Archive Backup Procedure)

กระบวนการสำรองบันทึกข้อมูลจะดำเนินการบันทึกข้อมูลต่างๆ ทุกรายการในข้อ 5.5.1 เป็นประจำในแต่ละวัน

5.5.5. การลงเวลาข้อมูล (Requirements for Time-Stamping of Records)

ข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอนใบรับรอง และข้อมูลที่เกี่ยวข้องกับการเพิกถอนจะมีการบันทึกวันและเวลาไว้ด้วย

5.5.6. ระบบการจัดเก็บข้อมูล (ทั้งภายในและภายนอก) (Archive Collection System (Internal or External))

ระบบจัดเก็บข้อมูลจะมีทั้งแบบอัตโนมัติและโดยบุคคล ซึ่งทำหน้าที่โดยระบบปฏิบัติการของเครื่องแม่ข่ายที่ให้บริการ ด้วยโปรแกรมประยุกต์ของผู้ให้บริการ และเจ้าหน้าที่ที่ได้รับมอบหมาย

5.5.7. กระบวนการได้รับและตรวจสอบข้อมูลที่บันทึกถาวระ (Procedures to obtain and verify Archive Information)

เจ้าหน้าที่ที่ได้รับสิทธิ์เท่านั้น ที่สามารถเข้าถึงข้อมูลที่บันทึกถาวรนี้ได้ ซึ่งความถูกต้องครบถ้วนของข้อมูลจะถูกตรวจสอบเมื่อข้อมูลเหล่านั้นถูกเรียกใช้

5.6. การเปลี่ยนแปลงกุญแจ (Key Changeover)

เมื่อใบรับรองอิเล็กทรอนิกส์ของ depa Root CA, Sub CA ใกล้จะหมดอายุ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะออกใบรับรองอิเล็กทรอนิกส์ใหม่ ก่อนที่ใบรับรองอิเล็กทรอนิกส์เดิมจะหมดอายุอย่างน้อย 60 วัน และจะต้องไม่มีผลกระทบกับ Application ของผู้ใช้บริการ

5.7. การรั่วไหลของข้อมูล และการกู้คืนจากภัยพิบัติ (Compromise and Disaster Recovery)

5.7.1. กระบวนการรับมือกับเหตุละเมิดและการรั่วไหลของข้อมูล (Incident and Compromise Handling Procedures)

ในกรณีเกิดเหตุความผิดพลาดจากระบบ หรือความเสียหายใดจากระบบ ตลอดจนการเกิดภัยพิบัติต่างๆ ให้ปฏิบัติตามขั้นตอนตามแผนบริหารความต่อเนื่อง และแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

5.7.2. ทรัพยากรที่ใช้ประมวลผล ซอฟต์แวร์ และ/หรือ ข้อมูลเกิดความผิดพลาด (Computing Resources, Software, and/or Data are corrupted)

การจัดการดูแลทรัพยากรต่างๆ ดำเนินงานตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ

5.7.3. กระบวนการจัดการเมื่อเกิดการรั่วไหลของกุญแจส่วนตัว (Entity private key compromise procedures)

ในกรณีที่สงสัยหรือมีเหตุอันควรเชื่อว่ากุญแจส่วนตัวของผู้ให้บริการเกิดการรั่วไหล จะมีการนำกระบวนการรับมือเมื่อข้อมูลรั่วไหลมาใช้งานตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ และเหตุการณ์ดังกล่าวจะมีการรายงานไปยังผู้บริหารผ่านคณะกรรมการเทคโนโลยีดิจิทัลและสารสนเทศ ทีมงานหรือบุคคลที่เกี่ยวข้องรับมือเหตุการณ์ โดยการประเมินสถานการณ์ การหาสาเหตุของเหตุละเมิด การตอบสนองของเหตุละเมิด การจัดทำแผนการกู้คือระบบ หากเหตุละเมิดนั้นจำเป็นต้องมีการเพิกถอนใบรับรองอิเล็กทรอนิสก์ของผู้ให้บริการ จะมีขั้นตอนการดำเนินการดังนี้

- สถานะของใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนจะได้รับการเผยแพร่ไปยังผู้ที่เกี่ยวข้องผ่านระบบของผู้ให้บริการ
- แจ้งไปยังผู้ที่ได้รับผลกระทบจากการเพิกถอนใบรับรองอิเล็กทรอนิกส์ให้รับทราบโดยเร็ว
- ผู้ให้บริการจะดำเนินการสร้างกุญแจคู่ใหม่ ยกเว้นในกรณีที่ผู้ให้บริการยุติการให้บริการ

5.7.4. ความต่อเนื่องของการให้บริการภายหลังจากเกิดภัยพิบัติ (Business continuity capabilities after a disaster)

ผู้ให้บริการจะปฏิบัติตามตามแผนบริหารความต่อเนื่อง และแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล ซึ่งแผนดังกล่าวได้รับการทดสอบ ตรวจสอบ และปรับปรุงอย่างต่อเนื่อง

5.8. การยุติการให้บริการของผู้ให้บริการ (CA or RA Termination)

เมื่อมีเหตุจำเป็นที่ทำให้ต้องมีการยุติการให้บริการของบริการใบรับรองอิเล็กทรอนิกส์ จะมีการแจ้งเตือนผู้ใช้งานและผู้ที่เกี่ยวข้องทั้งหมด ซึ่งมีแผนการดำเนินการดังนี้

- แจ้งผู้ได้รบผลกระทบให้ทราบถึงสถานะของผู้ให้บริการ เช่น ผู้ใช้บริการ และผู้ที่เกี่ยวข้องทั้งหมด
- ดำเนินการเกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ
- ดำเนินการเกี่ยวกับการเก็บรักษาข้อมูลของผู้ใช้บริการตามช่วงเวลาที่เอกสารฉบับนี้กำหนด
- ดำเนินการในการให้การสนับสนุนเกี่ยวกับการให้บริการ
- ดำเนินการจัดการกุญแจส่วนตัวของผู้ให้บริการ และอุปกรณ์ฮาร์แวร์ที่เกี่ยวข้อง
- ดำเนินการเปลี่ยนผ่านบริการไปสู่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์รายใหม่

6. การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

6.1. การสร้างและติดตั้งกุญแจคู่ (Key Pair Generation and Installation)

6.1.1. การสร้างกุญแจคู่ (Key Pair Generation)

กุญแจคู่ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และผู้ใช้บริการ จะถูกสร้างและติดตั้งโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และถูกจัดเก็บอยู่ที่ระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.1.2. การส่งกุญแจส่วนตัวไปให้ผู้ใช้บริการ (Private Key Delivery to Subscriber)

กุญแจส่วนตัวของผู้ใช้บริการจะถูกสร้างและจัดเก็บอยู่บนระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้ โดยสำนักงานจะทำการส่งลิงค์ไปทางอีเมล์ที่ผู้ใช้บริการแจ้งไว้กับสำนักงาน พร้อมกับวิธีการในการสร้างและลงทะเบียนใบรับรองอิเล็กทรอนิกส์

6.1.3. การส่งกุญแจสาธารณะให้กับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Public Key Delivery to Certificate Issuer)

กุญแจสาธารณะที่ถูกส่งมาให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์นั้น จะเป็นรูปแบบของไฟล์ PCKS#12 Certificate Signing Request (CSR) (.p12) ซึ่งถูกสร้างและจัดเก็บอยู่บน

ระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.1.4. การจัดส่งกุญแจสาธารณะของผู้ให้บริการไปยังคู่กรณีที่เกี่ยวข้อง (depa CA Public Key Delivery to Relying Parties)

ในกรณีที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องประสงค์จะนำกุญแจสาธารณะของผู้ให้บริการ ซึ่งบันทึกไว้ในใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการไปใช้งาน ให้ผู้ใช้บริการแจ้งต่อผู้ให้บริการเพื่อดำเนินการอนุมัติต่อไป

6.1.5. ขนาดของกุญแจ (Key Sizes)

กระบวนการออกใบรับรองอิเล็กทรอนิกส์ดำเนินการสร้างกุญแจของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะมีขนาดตามมาตรฐานอย่างน้อย 4096 บิต ส่วนขนาดกุญแจของผู้ใช้บริการจะมีขนาดตามมาตรฐานอย่างน้อยอยู่ที่ 2048 บิต

6.1.6. การกำหนดพารามิเตอร์ของกุญแจสาธารณะ และการตรวจสอบคุณภาพของพารามิเตอร์ (Public Key Parameters Generation and Quality Checking)

ตัวแปรที่นำมาใช้เพื่อสร้างกุญแจสาธารณะนั้น ได้มีการกำหนดพารามิเตอร์ขึ้นโดยผู้ให้บริการซึ่งยึดตามมาตรฐาน X.509 และคุณภาพของตัวแปรกุญแจสาธารณะ จะถูกตรวจสอบโดยอัตโนมัติจากโปรแกรมในระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.1.7. วัตถุประสงค์ของการนำกุญแจคู่ไปใช้ (Key Usage Purposes)

วัตถุประสงค์ของการนำกุญแจคู่ไปใช้ได้ถูกอธิบายไว้ในหัวข้อ 1.4 การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)

6.2. การป้องกันกุญแจส่วนตัว และการควบคุมโมดูลสำหรับการเข้ารหัส (Private Key Protection and Cryptographic Module Engineering Controls)

6.2.1. มาตรฐานของโมดูลที่ใช้ในการเข้ารหัสลับ (Cryptographic Module Standards and Controls)

โมดูลที่ใช้ในการเข้ารหัสของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ได้ถูกสร้างขึ้นตามแนวมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 Level 3 ที่เป็นมาตรฐานสากลสำหรับใช้สร้างและเก็บรักษากุญแจส่วนตัวของระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.2.2. การควบคุมการเข้าถึงกุญแจส่วนตัว (Private Key (N out of M) Multi-Person Control)

กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้มีการควบคุมเข้าถึงแบบหลายบุคคล

6.2.3. การกู้คืนกุญแจส่วนตัว (Private Key Escrow)

ผู้ให้บริการไม่ได้จัดให้มีบริการสำหรับการกู้กุญแจส่วนตัวคืนเพื่อนำกลับมาใช้ใหม่อีกครั้งเมื่อกุญแจส่วนตัวสูญหาย หรือถูกล่วงรู้โดยวิธีการอื่นใด

6.2.4. การสำรองกุญแจส่วนตัว (Private Key Backup)

กุญแจส่วนตัวของผู้ให้บริการถูกบันทึกไว้ในอุปกรณ์จัดเก็บบนระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.2.5. การบันทึกถาวระกุญแจส่วนตัว (Private Key Archival)

กุญแจส่วนตัวของผู้ให้บริการถูกบันทึกไว้ในอุปกรณ์จัดเก็บบนระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.2.6. การแปลงกุญแจส่วนตัวให้เป็น หรือมาจากโมดูลการเข้ารหัส (Private Key Transfer into or from a Cryptographic Module)

กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้ถูกสร้างขึ้นตามแนวมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 Level 3 ที่เป็นมาตรฐานสากลสำหรับใช้สร้างและเก็บรักษากุญแจส่วนตัวของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ และมีระบบความปลอดภัยโดยเจ้าหน้าที่ดูแลระบบให้บริการใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เท่านั้น

6.2.7. การจัดเก็บกุญแจส่วนตัวลงบนโมดูลที่มีการเข้ารหัส (Private Key Storage on Cryptographic Module)

กุญแจส่วนตัวของผู้ให้บริการถูกบันทึกไว้ในอุปกรณ์จัดเก็บบนระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.2.8. วิธีการใช้งานกุญแจส่วนตัว (Method of Activating Private Key)

กุญแจส่วนตัวของผู้ให้บริการ จะถูกนำมาใช้บนระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.2.9. วิธีการยกเลิกการใช้งานกุญแจส่วนตัว (Method of Deactivating Private Key)

กุญแจส่วนตัวจะเลิกใช้งานได้ก็ต่อเมื่อมีการร้องขอจากผู้ใช้บริการ ให้เพิกถอนการใช้งานกุญแจส่วนตัวนั้น โดยผู้ให้บริการจะตรวจสอบความถูกต้องของการร้องขอจากผู้ใช้บริการ จึงทำการเพิกถอนกุญแจส่วนตัวนั้นได้

6.2.10. วิธีการทำลายกุญแจส่วนตัว (Method of Destroying Private Key)

ในกรณีที่ผู้ใช้บริการต้องการทำลายกุญแจส่วนตัว ให้แจ้งกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อดำเนินการต่อไป

6.2.11. ระดับของโมดูลที่มีการเข้ารหัส (Cryptographic Module Rating)

อ้างอิงตามข้อ 6.2.1

6.3. รายละเอียดอื่นเกี่ยวกับการจัดการกุญแจคู่ (Other Aspects of Key Pair Management)

6.3.1. การเก็บรักษากุญแจสาธารณะ (Public Key Archival)

กุญแจสาธารณะจะถูกจัดเก็บบันทึกไว้ในระบบการจัดทำใบรับรองอิเล็กทรอนิกส์ ภายใต้ระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้ เป็นระยะเวลา 3 ปี หรือตามที่ผู้ให้บริการกำหนด

6.3.2. ระยะเวลาใช้งานใบรับรองอิเล็กทรอนิกส์และกุญแจคู่ (Certificate Operational Periods and Key Pair Usage Periods)

ระยะเวลาใช้งานใบรับรองอิเล็กทรอนิกส์ และกุญแจคู่ ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ของแต่ละผู้ใช้บริการ คือ 3 ปี

6.4. ข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Activation Data)

6.4.1. การสร้างและการนำข้อมูลไปใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ (Activation Data Generation and Installation)

ข้อมูลที่ใช้ในการสร้างและติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ ถูกสร้างและจัดเก็บอย่างปลอดภัย และในกรณีที่ต้องการการใช้งานใบรับรองอิเล็กทรอนิกส์ ต้องติดต่อผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อตรวจสอบและดำเนินการตามกระบวนการที่กำหนดไว้ให้เกิดความปลอดภัยในการใช้บริการ ซึ่งการดำเนินการต่างๆ จะดำเนินการผ่านระบบการจัดทำใบรับรองอิเล็กทรอนิกส์ ภายใต้ระบบข้อมูลสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล บนระบบคลาวด์ (Cloud-Computing) ที่มีการตั้งและกำหนดสิทธิ์การใช้งานให้มีความปลอดภัยสำหรับการเข้าถึงได้

6.4.2. การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Activation Data Protection)

การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ดำเนินการสร้างขึ้นตามแนวมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 Level 3 ที่เป็นมาตรฐานสากลสำหรับใช้สร้างและเก็บรักษากุญแจส่วนตัวของระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.4.3. ข้อมูลด้านอื่นที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ (Other Aspects of Activation Data)

ไม่มีข้อมูลอื่นใดนอกเหนือจากข้อมูลสำคัญที่ใช้ในการสมัครและดำเนินการใช้บริการของสำนักงานส่งเสริมเศรษฐกิจดิจิทัลเกี่ยวกับระบบจัดทำใบรับรองอิเล็กทรอนิกส์

6.5. การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)

6.5.1. ข้อกำหนดทางเทคนิคเกี่ยวกับการควบคุมความปลอดภัยของคอมพิวเตอร์ (Specific Computer Security Technical Requirements)

ผู้ให้บริการดำเนินการจัดทำระบบออกใบรับรองอิเล็กทรอนิกส์ โดยปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์เป็นไปตามการให้บริการของระบบสารสนเทศบนระบบคลาวด์ภาครัฐ (Government Cloud Computing: GDCC) ซึ่งตัวระบบคลาวด์ภาครัฐ (Government Cloud Computing: GDCC) ดำเนินการตามข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของระบบคลาวด์ (Cloud Computing) ตามมาตรฐาน ISO 27001 (Information Security Management System: ISMS)

6.5.2. การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating)

ผู้ให้บริการได้แบ่งระดับในการรักษาความมั่นคงและปลอดภัยของระบบออกใบรับรองอิเล็กทรอนิกส์ โดยปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์เป็นไปตามการให้บริการของระบบสารสนเทศบนระบบคลาวด์ภาครัฐ (Government Cloud Computing: GDCC) ซึ่งตัวระบบคลาวด์ภาครัฐ (Government Cloud Computing: GDCC) มีการแบ่งระดับการรักษาความมั่นคงและปลอดภัยของระบบคลาวด์ (Cloud Computing) ตามมาตรฐาน ISO 27001 (Information Security Management System: ISMS)

6.6. การควบคุมทางเทคนิคของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ (Lite Cycle Technical Controls)

6.6.1. การควบคุมการพัฒนาระบบ (System Development Controls)

การควบคุมและพัฒนาซอฟต์แวร์ที่นำมาใช้ในการพัฒนาซอฟต์แวร์ของผู้ให้บริการได้พัฒนาให้สอดคล้องตามหลักเกณฑ์และมาตรฐานในการประเมินการรักษาความมั่นคงและปลอดภัยด้านข้อมูล

6.6.2. การควบคุมการบริหารจัดการด้านความมั่นคงปลอดภัย (Security Management Controls)

การจัดการในการรักษาความมั่นคงและปลอดภัยของระบบออกใบรับรองอิเล็กทรอนิกส์ จะถูกควบคุมให้เป็นไปตามข้อกำหนดตามแผนแม่บทด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนปฏิบัติการด้านเทคโนโลยีดิจิทัลและสารสนเทศ แผนบริหารความต่อเนื่อง และนโยบาย มาตรฐาน แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล และให้สอดคล้องกับมาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ ISO 27001 (Information Security Management System: ISMS)

6.6.3. การควบคุมความมั่นคงปลอดภัยทางเทคนิค (Life Cycle Security Controls)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ประเมินความเสี่ยงเกี่ยวกับความปลอดภัยสำหรับการปฏิบัติงานด้วยการนำระบบออกใบรับรองอิเล็กทรอนิกส์มาใช้ โดยได้มีการระบุและจัดการกับความเสี่ยวที่ระดับสูงและสูงมาก

6.7. การควบคุมความปลอดภัยทางเครือข่าย (Network Security Controls)

ระบบการควบคุมทางเครือข่ายของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ได้ถูกออกแบบให้เป็นระบบเครือข่ายเฉพาะเพื่อใช้ในการให้บริการใบรับรองอิเล็กทรอนิกส์บนระบบคลาวด์ภาครัฐ (Government Cloud Computing: GDCC) ซึ่งตัวระบบคลาวด์ (Cloud Computing) ติดตั้งทั้งฮาร์ดแวร์และซอฟต์แวร์ไฟล์วอลล์ตามมาตรฐานของระบบคลาวด์ (Cloud Computing) ในการป้องกันการบุกรุกจากการเข้าถึงภายนอก ระบบตรวจสอบและป้องกันผู้บุกรุก (Intrusion Protection System: IDS) และระบบป้องกันไวรัส (Antivirus) ของผู้ให้บริการคลาวด์ภาครัฐ

6.8. การบันทึกเวลารายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน (Time-stamping)

ข้อมูลใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน จะมีข้อมูลวันที่ และเวลาที่ถูกเพิกถอนกำกับลงไปในรายการใบรับรองอิเล็กทรอนิกส์ด้วย

7. การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)

7.1. รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)

7.1.1. เวอร์ชัน (Version Number(s))

ใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้มาตรฐาน X.509 Version 3 Certificate ประกอบด้วย

- หมายเลขของใบรับรองอิเล็กทรอนิกส์
- วิธีการที่ใช้ในการสร้างลายมือดิจิทัลของผู้ถือใบรับรองอิเล็กทรอนิกส์
- ชื่อของผู้ใช้บริการ
- วันเวลาเริ่มต้นและสิ้นสุดการใช้ใบรับรองอิเล็กทรอนิกส์
- ชื่อของผู้ถือใบรับรองอิเล็กทรอนิกส์
- กุญแจสาธารณะ

7.1.2. ข้อมูลเพิ่มเติมของใบรับรองอิเล็กทรอนิกส์ (Certificate Extensions)

ผู้ให้บริการสนับสนุนการใช้ใบรับรอง X.509 เวอร์ชัน 3 ซึ่งใช้ข้อมูลเพิ่มเติมที่เป็นมาตรฐานของใบรับรองอิเล็กทรอนิกส์

7.1.3. อัลกอริทึมสำหรับการสร้างกุญแจคู่ (Algorithm Object Identifiers)

อัลกอริทึมที่ใช้ในการออกใบรับรองอิเล็กทรอนิกส์ คือ SHA-1 RSA

7.1.4. รูปแบบของชื่อ (Name Forms)

ใบรับรองที่ออกให้โดยผู้ให้บริการจะมีชื่อผู้ออกใบรับรอง และชื่อของผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์ (Subject)

7.1.5. ข้อจำกัดเกี่ยวกับชื่อ (Name Constraints)

ชื่อที่มีการปิดบังและการใช้ชื่อปลอมนั้น ไม่สนับสนุนให้นำมาใช้ในใบรับรองอิเล็กทรอนิกส์

7.1.6. Object Identifier ของนโยบายใบรับรองอิเล็กทรอนิกส์ (Certificate Policy Object Identifier)

OID ของนโยบายใบรับรองอิเล็กทรอนิกส์นี้ ได้รับการดำเนินการในประเภทของการขยายผลที่มีมาตรฐานเกี่ยวกับใบรับรอง X.509 ที่ออกให้

7.1.7. นโยบายเรื่องข้อจำกัดของการใช้ส่วนขยาย (Usage of Policy Constraints Extension)

ไม่มีข้อกำหนด

7.1.8. นโยบายในการระบุรูปแบบและความหมาย (Policy Qualifiers Syntax and Semantics)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ระบุรูปแบบและความหมายของใบรับรองอิเล็กทรอนิกส์ในเว็บไซต์ของผู้ให้บริการ (contract.depa.or.th)

7.1.9. การดำเนินการในส่วนของความหมายสำหรับนโยบายเพิ่มเติมของใบรับรองอิเล็กทรอนิกส์ (Processing Semantics for the Critical Certificate Policies Extension)

ไม่มีข้อกำหนด

7.2. รูปแบบของรายการเพิกถอนใบรับรอง (CRL Profile)

7.2.1. เวอร์ชัน (Version Number(s))

ใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้มาตรฐาน X.509 Certificate ประกอบด้วย

- วิธีที่ใช้ในการสร้างลายมือชื่อดิจิทัลในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- ชื่อของผู้ให้บริการที่ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- วันเวลาที่ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- หมายเลขของรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- รายการของใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน

7.2.2. รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนและส่วนขยาย (CRL and CRL Entry Extensions)

รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนจะได้รับการเผยแพร่ไปยังผู้ที่เกี่ยวข้องผ่านระบบของผู้ให้บริการ

7.3. รูปแบบของโปรโตคอล OCSP (OCSP Profile)

OCSP หรือ Online Certificate Status Protocol คือ การตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ (Online)

7.3.1. เลขรุ่น (Version Number(s))

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ไม่มีบริการการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์

7.3.2. ส่วนขยายของ OCSP (OCSP Extensions)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ไม่มีบริการการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์

8. การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่างๆ และการประเมินความเสี่ยงอื่นๆ (Compliance Audit and Other Assessment)

8.1. ความถี่ในการตรวจประเมิน (Frequency or Circumstances of Assessment)

ผู้ให้บริการจะดำเนินการตรวจสอบระบบให้บริการ เพื่อให้เป็นไปตามข้อกำหนดโดยละเอียดตามที่กำหนดในแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (CPS) อย่างน้อยปีละครั้ง และจะดำเนินการระบบให้บริการออกใบรับรองอิเล็กทรอนิกส์มีการดำเนินงานสอดคล้องตามมาตรฐานของ ISO 27001 เพิ่มมากขึ้น

8.2. ผู้ประเมิน/คุณสมบัติของผู้ประเมิน (Identity/Qualification of Assessor)

ผู้ให้บริการกำหนดให้คณะกรรมการเทคโนโลยีดิจิทัลและสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัลเป็นผู้ประเมินและตรวจสอบการปฏิบัติงานต่างๆ ของระบบให้บริการออกใบรับรองอิเล็กทรอนิกส์

8.3. ความสัมพันธ์ของผู้ประเมินและผู้ถูกประเมิน (Assessor’s Relationship to Assessed Entity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ คือ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล ที่ดำเนินการโดยระบบสารสนเทศที่พัฒนาเพื่อให้บริการออกใบรับรองอิเล็กทรอนิกส์ อยู่ในฐานะผู้ว่าจ้าง และผู้รับการประเมินเท่านั้น

8.4. หัวข้อในการประเมิน (Topics Covered by Assessment)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะกำหนดข้อในการประเมินให้สอดคล้องและเป็นไปตามเกณฑ์ข้อกำหนดมาตรฐาน ISO 27001

8.5. การปฏิบัติเพื่อแก้ไขข้อบกพร่อง (Actions Taken As a Result of Deficiency)

เมื่อการตรวจประเมินเสร็จสิ้น ข้อบกพร่อง (Non-Conformity) ที่พบจะต้องได้รับการแก้ไข โดยผู้ให้บริการต้องกำหนดแผนการแก้ไขข้อบกพร่องดังกล่าว และดำเนินการตามแผน ซึ่งแผนดังกล่าวจะถูกเสนอและรายงานผ่านคณะกรรมการเทคโนโลยีดิจิทัลและสารสนเทศของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล เพื่อให้มั่นใจว่าระบบให้บริการยังคงมีความมั่นคงปลอดภัย

8.6. การแจ้งผลการประเมิน (Communication of Results)

ผู้ให้บริการจะรายงานผลการประเมินต่อคณะกรรมการเทคโนโลยีดิจิทัลและสารสนเทศ ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

9. ข้อกำหนดอื่นๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

9.1. ค่าธรรมเนียม (Fees)

9.1.1. ค่าธรรมเนียมในการออกใบรับรองอิเล็กทรอนิกส์หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance or Renewal Fees)

ผู้ให้บริการ ไม่มีการคิดค่าธรรมเนียมในการที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องขอเข้าถึงใบรับรองอิเล็กทรอนิกส์ผ่านระบบของผู้ให้บริการที่ได้กำหนดไว้ เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

9.1.2. ค่าธรรมเนียมในการเรียกดูใบรับรองอิเล็กทรอนิกส์ (Certificate Access Fees)

ผู้ให้บริการ ไม่มีการคิดค่าธรรมเนียมในการที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องขอเข้าถึงใบรับรองอิเล็กทรอนิกส์ผ่านระบบของผู้ให้บริการที่ได้กำหนดไว้ เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

9.1.3. ค่าธรรมเนียมในการเรียกดูข้อมูลสถานะของใบรับรองอิเล็กทรอนิกส์ (Revocation or Status Information Access Fees)

ผู้ให้บริการ ไม่มีการคิดค่าธรรมเนียมในการที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องขอเข้าถึงใบรับรองอิเล็กทรอนิกส์ผ่านระบบของผู้ให้บริการที่ได้กำหนดไว้ เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

9.1.4. ค่าใช้จ่ายอื่นๆ (Fees for Other Services)

ผู้ให้บริการ ไม่มีการคิดค่าธรรมเนียมในการที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องขอเข้าถึงแนวนโยบายหรือแนวปฏิบัติของใบรับรองอิเล็กทรอนิกส์ผ่านระบบของผู้ให้บริการที่ได้กำหนดไว้ เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

9.1.5. นโยบายในการคืนค่าธรรมเนียม (Refund Policy)

ผู้ให้บริการ ไม่มีการคิดค่าธรรมเนียมในการที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องในการขอคืนค่าธรรมเนียมใบรับรองอิเล็กทรอนิกส์ผ่านระบบของผู้ให้บริการที่ได้กำหนดไว้ เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

9.2. ความรับผิดชอบทางการเงิน (Financial Responsibility)

9.2.1. วงเงินประกันความเสียหายที่คุ้มครองความรับผิดชอบที่เกิดขึ้น (Insurance Coverage)

ในกรณีที่เกิดความเสียหายกับ CA จากการกระทำของผู้ใช้บริการหรือฝ่ายที่เกี่ยวข้องที่เกี่ยวข้อง CA ขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหาย

9.2.2. สินทรัพย์อื่นๆ (Other Assets)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ คือ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล เป็นหน่วยงานของรัฐ จัดตั้งขึ้นตามพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 มีอำนาจหน้าที่ในการดำเนินการตามมาตรา 34 และ 35

9.2.3. การทำประกันที่ครอบคลุมในส่วนของผู้ใช้บริการ (Insurance or Warranty Coverage for End-Entities)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์รับประกันความถูกต้องของข้อมูลที่ปรากฏบนใบรับรองอิเล็กทรอนิกส์ที่ออกให้โดยผู้ให้บริการ และใช้ในการขอรับบริการและทำธุรกรรมกับสำนักงานส่งเสริมเศรษฐกิจดิจิทัลเท่านั้น โดยหากเกิดความผิดพลาดที่เกิดมาจากผู้

ให้บริการออกใบรับรองอิเล็กทรอนิกส์นั้น ผู้ใช้บริการจะต้องแจ้งให้ผู้ให้บริการทราบ และดำเนินการออกใบรับรองอิเล็กทรอนิกส์ใหม่ โดยไม่คิดค่าใช้จ่าย

9.3. การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)

9.3.1. ขอบเขตของข้อมูลที่เป็นความลับ (Scope of Confidential Information)

ผู้ให้บริการ กำหนดให้ข้อมูลดังต่อไปนี้เป็นข้อมูลที่เป็นความลับของผู้ใช้บริการ ประกอบด้วย

- รายการคำขอสมัครใช้บริการใบรับรองอิเล็กทรอนิกส์
- รายการกิจกรรมที่เกิดขึ้นระหว่างผู้ให้บริการ และผู้ใช้บริการ
- บันทึกเหตุการณ์ที่เกิดขึ้นในระบบของผู้ให้บริการ
- รายการผลการตรวจสอบระบบ
- แผนปฏิบัติการฉุกเฉิน (Contingency Plan) หรือแผนการกู้ระบบในกรณีฉุกเฉิน (Disaster Recovery Plan)
- การควบคุมด้านความมั่นคงปลอดภัยต่างๆ ของผู้ให้บริการ และการบริหารจัดการเกี่ยวกับการให้บริการใบรับรองอิเล็กทรอนิกส์

9.3.2. ข้อมูลที่สามารถนำมาเผยแพร่ได้ (Information Not Within the Scope of Confidential Information)

ใบรับรองอิเล็กทรอนิกส์ ใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ สามารถนำมาเปิดเผยได้ ส่วนรายการอื่นที่ยังไม่สามารถตีความได้ว่าเป็นความลับหรือไม่ จะถูกพิจารณาให้เป็นไปตามกฎหมายที่เหมาะสม

9.3.3. ความรับผิดชอบในการป้องกันข้อมูลลับ (Responsibility to Protect Confidential Information)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะไม่เปิดเผยข้อมูลซึ่งเป็นความลับของผู้ใช้บริการกับหน่วยงานที่ไม่เกี่ยวข้องโดยเด็ดขาด

9.4. นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)

9.4.1. แผนการรักษาความเป็นส่วนตัว (Privacy Plan)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.4.2. ข้อมูลที่จัดให้เป็นข้อมูลส่วนบุคคล (Information Treated as Private)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.4.3. ข้อมูลที่ไม่ถือว่าเป็นข้อมูลส่วนบุคคล (Information Not Deemed Private)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.4.4. ความรับผิดชอบในการป้องกันข้อมูลส่วนบุคคล (Responsibility to Protect Private Information)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.4.5. การบอกกล่าวและความยินยอมในการใช้ข้อมูลส่วนบุคคล (Notice and Consent to Use Private Information)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.4.6. การเปิดเผยข้อมูลส่วนบุคคลกรณีที่มีคำสั่งศาลหรือคำสั่งทางปกครอง (Disclosure Pursuant to Judicial or Administrative Process)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งทางกฎหมาย ดังนี้

- จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลตามหมายเรียก หมายค้น
- จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งศาล หรือคำสั่งทางปกครอง

9.4.7. กรณีอื่นใดที่ต้องเปิดเผยข้อมูลส่วนบุคคล (Other Information Disclosure Circumstances)

ผู้ให้บริการดำเนินการอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.5. ทรัพย์สินทางปัญญา (Intellectual Property Rights)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ กำหนดให้เอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ถือเป็นสิทธิ์ในทรัพย์สินทางปัญญาของผู้ให้บริการแต่เพียงผู้เดียว หรือที่กำหนดไว้ในข้อตกลงใดๆ กับบุคคลที่เกี่ยวข้อง

9.6. คำรับรอง (Representations and Warranties)

9.6.1. คำรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (CA Representations and Warranties)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รับรองว่า

- ข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออกโดยผู้ให้บริการ จะไม่มีข้อผิดพลาดเกิดขึ้นอันเกิดจากความบกพร่องของผู้ให้บริการในการออกใบรับรองอิเล็กทรอนิกส์
- ใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออกโดยผู้ให้บริการได้ผ่านกระบวนการตามที่ปรากฏในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้
- ข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์และข้อมูลเกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ที่ปรากฏได้ผ่านกระบวนการสร้างตามที่ปรากฏในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้

9.6.2. คำรับรองของหน่วยงานรับลงทะเบียน (RA Representations and Warranties)

หน่วยงานรับลงทะเบียนออกใบรับรองอิเล็กทรอนิกส์ รับรองว่า

- ข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออกให้ จะไม่มีข้อผิดพลาดเกิดขึ้นอันเกิดจากความบกพร่องของผู้ให้บริการในการออกใบรับรองอิเล็กทรอนิกส์
- ใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออกให้ ได้ผ่านกระบวนการตามที่ปรากฏในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้
- ข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์และข้อมูลเกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ที่ปรากฏได้ผ่านกระบวนการสร้างตามที่ปรากฏในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้

9.6.3. คำรับรองของผู้ใช้บริการ (Subscriber Representations and Warranties)

ผู้ใช้บริการให้คำรับรองว่า

- ลายมือชื่อดิจิทัลทุกรายการที่ถูกสร้างโดยกุญแจส่วนตัวซึ่งเป็นคู่กับกุญแจสาธารณะที่ปรากฏในระบบออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ เป็นลายมือชื่อดิจิทัลของผู้ใช้บริการ ซึ่งใบรับรองอิเล็กทรอนิกส์ยังคงสามารถใช้งานได้โดยไม่ถูกเพิกถอนหรือหมดอายุในขณะที่มีการสร้างลายมือชื่อ
- กุญแจส่วนตัวได้รับการป้องกันอย่างเหมาะสมและไม่สามารถเข้าถึงได้โดยไม่ได้รับอนุญาต
- ข้อมูลทั้งหมดที่ปรากฏในระบบออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ เป็นข้อมูลที่ถูกต้องและเป็นความจริง
- ใบรับรองอิเล็กทรอนิกส์จะถูกใช้งานอย่างถูกต้องตามกฎหมาย กฎระเบียบต่างๆ ที่เกี่ยวข้อง โดยผู้ที่ได้รับอนุญาตเท่านั้น

9.6.4. คำรับรองของคู่กรณีที่เกี่ยวข้อง (Relying Party Representations and Warranties)

คู่กรณีที่เกี่ยวข้อง ขอรับรองว่าได้ยอมรับข้อตกลงที่เกี่ยวกับคู่กรณีที่เกี่ยวข้องแล้ว และได้ตรวจสอบใบรับรองอิเล็กทรอนิกส์อย่างเหมาะสมแล้ว ก่อนที่จะเชื่อถือข้อมูลในใบรับรองอิเล็กทรอนิกส์ใบนั้น และจะยอมรับข้อผิดพลาดอันเกิดจากความบกพร่องในการตรวจสอบใบรับรองอิเล็กทรอนิกส์เพียงผู้เดียว

9.6.5. คำรับรองของบุคคลอื่นๆ (Representations and Warranties of Other Participants)

ไม่มี

9.7. ข้อจำกัดของการรับประกัน (Disclaimers of Warranties)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะไม่รับประกันใดๆ ไม่ว่าโดยชัดแจ้งหรือโดยปริยาย นอกเหนือจากที่ระบุไว้ในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ รวมถึงไม่รับประกันผลสัมฤทธิ์ในเชิงพาณิชย์ หรือในวัตถุประสงค์ใดโดยเฉพาะ

9.8. ข้อจำกัดความรับผิด (Limitations of Liability)

- ผู้ให้บริการ ได้กำหนดขอบเขตความรับผิดชอบและรวมถึงข้อจำกัดความรับผิดชอบ โดยผู้ให้บริการจะรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการปฏิบัติผิดเงื่อนไขข้อกำหนดตามเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ของผู้ให้บริการตามที่เกิดขึ้นจริง
- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะไม่รับผิดชอบในความเสียหายใดๆ อันเนื่องมาจาก หรือเกี่ยวข้องกับการใช้ใบรับรองอิเล็กทรอนิกส์ที่ผิดกฎหมาย หรือนอกวัตถุประสงค์ที่ระบุไว้เอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ หรือการละเมิดระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งไม่รับผิดในความเสียหายที่เป็นผลโดยอ้อม ความเสียหายที่เป็นผลสืบเนื่อง หรือความเสียหายอันเกิดจากพฤติการณ์พิเศษ หรือความสูญเสียรายได้ หรือผลกำไรในทางธุรกิจ

9.9. ค่าสินไหมทดแทน (Indemnities)

ในกรณีที่เกิดความเสียหายกับ CA จากการกระทำของผู้ใช้บริการหรือฝ่ายที่เกี่ยวข้องที่เกี่ยวข้อง CA ขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหาย

9.10. เงื่อนไข และการยกเลิก (Term and Termination)

9.10.1. เงื่อนไข (Term)

เงื่อนไขใดๆ ที่เกี่ยวข้องกับการใช้ใบรับรองอิเล็กทรอนิกส์ เป็นเงื่อนไขที่ระบุในเอกสารระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ ซึ่งเป็นเอกสารประกอบการสมัครขอใบรับรองอิเล็กทรอนิกส์

9.10.2. การยกเลิก (Termination)

การขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ ต้องกระทำการโดยผู้ใช้บริการหรือผู้มีอำนาจกระทำการแทน

9.10.3. ผลของการยกเลิกใช้บริการ (Effect of Termination and Survival)

- การขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ ถือเป็นการสิ้นสุดความผูกพันระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และผู้ใช้บริการทันที
- การยกเลิกสัญญานี้ไม่ว่าด้วยเหตุประการใดก็ตาม จะไม่ถือเป็นการลบล้างหรือทำให้เสื่อมเสียซึ่งสิทธิ หน้าที่ ความรับผิดชอบใดๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการมีอยู่ต่อกัน อันเนื่องมาจากการใดๆ อันได้กระทำไปตามเงื่อนไขและข้อตกลงตามเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ก่อนที่จะมีการเพิกถอนใบรับรองอิเล็กทรอนิกส์

9.11. การติดต่อสื่อสารระหว่างผู้ให้บริการ และผู้ที่เกี่ยวข้อง (Individual Notices and Communication with Participants)

ในกรณีที่ไม่ระบุเป็นการอื่น ผู้ให้บริการจะติดต่อกับผู้ที่เกี่ยวข้อง โดยวิธีการที่รวดเร็วและน่าเชื่อถือ โดยพิจารณาความสำคัญของข้อมูลที่ต้องการติดต่อสื่อสารเป็นสำคัญ

9.12. การแก้ไขปรับปรุง (Amendments)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขอสงวนสิทธิ์ในการแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงใดๆ ในการให้บริการตามเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ได้

9.12.1. กระบวนการแก้ไขปรับปรุง (Procedure for Amendment)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต้องการแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงในการให้บริการตามเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะต้องแจ้งให้ผู้ใช้บริการ หรือหน่วยงานรับลงทะเบียนทราบล่วงหน้าไม่น้อยกว่า 90 วัน ก่อนจะประกาศบังคับใช้ บนเว็บไซต์ระบบออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ

9.12.2. วิธีการแจ้งและระยะเวลาแจ้ง (Notification Mechanism and Period)

หากหน่วยงานรับลงทะเบียนหรือผู้ใช้บริการเห็นว่า การแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงดังกล่าวเป็นการลดสิทธิ หรือประโยชน์อันพึงได้รับโดยชอบด้วยกฎหมาย หน่วยงานรับลงทะเบียน หรือผู้ใช้บริการมีสิทธิยกเลิกการใช้บริการตามเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ โดยแจ้งให้ผู้ให้บริการทราบล่วงหน้าไม่น้อยกว่า 30 วัน ก่อนวันให้มีผลสิ้นสุดการใช้บริการ ทั้งนี้ เว้นแต่เป็นการแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงตามที่กฎหมายกำหนด

9.12.3. กรณีที่ต้องมีการเปลี่ยนแปลงหมายเลข OID (Circumstances under Which OID Must be Changed)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่ระบุเหตุการณ์หรือกรณีที่จะมีการเปลี่ยน OID

9.13. การระงับข้อพิพาท (Dispute Resolution Procedures)

9.13.1. ข้อโต้แย้งระหว่างผู้ให้บริการและผู้ใช้บริการ (Disputes between depa CA and Entities)

ในกรณีที่มีข้อพิพาท หรือในกรณีที่มีข้อความขัดแย้งในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ของผู้ให้บริการ และผู้ใช้บริการ จะต้องปฏิบัติตามคำวินิจฉัยของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

9.13.2. ข้อโต้แย้งระหว่างผู้ให้บริการและคู่กรณีที่เกี่ยวข้อง (Disputes between Subordinate CA and Relying Parties)

ในกรณีที่มีข้อพิพาท หรือในกรณีที่มีข้อความขัดแย้งในเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ของผู้ให้บริการ และคู่กรณีที่เกี่ยวข้อง จะต้องปฏิบัติตามคำวินิจฉัยของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

9.14. กฎหมายที่ใช้บังคับ (Governing Law)

กฎหมายแห่งราชอาณาจักรไทยเป็นกฎหมายที่ใช้ในการระงับข้อพิพาท

9.15. ความสอดคล้องกับกฎหมายที่เกี่ยวข้อง (Compliance with Applicable Law)

การประกาศใช้แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ จะต้องสอดคล้องกับกฎหมายอื่นๆ ที่เกี่ยวข้อง

9.16. ประเด็นอื่นๆ ที่เกี่ยวข้อง (Miscellaneous Provisions)

9.16.1. ข้อตกลง (Entire Agreement)

เอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ ถือเป็นส่วนหนึ่งของข้อตกลงอื่นๆ ที่ทำขึ้นระหว่าง ผู้ให้บริการและผู้ใช้บริการ

9.16.2. การโอนสิทธิ (Assignment)

หากมีการโอนสิทธิของผู้ให้บริการ ผู้รับโอนสิทธิจะต้องดำเนินการตามเอกสารแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ และรวมถึงรับเอาข้อจำกัดความรับผิดที่ผู้ให้บริการมีต่อผู้ใช้บริการไว้ด้วย

9.16.3. กรณีส่วนหนึ่งส่วนใดของข้อตกลงเป็นโมฆะ (Severability)

ในกรณีที่ข้อความส่วนใดส่วนหนึ่งของเอกสารฉบับนี้เป็นโมฆะ ไม่สมบูรณ์ หรือไม่มีผลบังคับใช้ตามกฎหมาย ไม่มีผลกระทบกับข้อความอื่นๆ ในเอกสารฉบับนี้ที่สมบูรณ์และบังคับได้ตามกฎหมาย

9.16.4. ค่าใช้จ่ายที่เกิดขึ้นจากการผิดข้อตกลง (Enforcement)

ผู้ให้บริการได้กำหนดขอบเขตความรับผิดชอบและรวมถึงข้อจำกัดความรับผิด โดยให้อยู่ในดุลพินิจของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

9.16.5. เหตุสุดวิสัย (Force Majeure)

- ในกรณีที่ฝ่ายใดฝ่ายหนึ่ง ไม่สามารถดำเนินการตามแนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้ได้ด้วยเหตุสุดวิสัย ฝ่ายนั้นอาจจะเรียกให้อีกฝ่ายหาทางออกร่วมกันอย่างเหมาะสม

- เหตุสุดวิสัย หมายถึง เหตุการณ์ที่อยู่นอกเหนือการควบคุมของคู่กรณีและเหตุการณ์ดังกล่าว ส่งผลให้การปฏิบัติหน้าที่ของฝ่ายนั้นไม่สามารถกระทำได้ หรือพ้นวิสัยที่จะปฏิบัติหน้าที่ตามข้อตกลงในเอกสารฉบับนี้ได้

9.17. บทบัญญัติอื่นๆ (Other Provisions)

ไม่มี