แนวนโยบายและแนวปฏิบัติการให้บริการ

ใบรับรองอิเล็กทรอนิกส์

(Certificate Policy/Certification Practice Statement)

Version 2.0

การปรับปรุงเอกสาร

เวอร์ชั่น	ปรับปรุงเมื่อ
1.0	พฤษภาคม 2546
2.0	พฤษภาคม 2561

สารบัญ

1.บทนำ (INTRODUCTION)

1.1. ข้อมูลเบื้องต้นทั่วไป (Overview)

บริษัท ทีโอที จำกัด (มหาชน) เป็นบริษัทสื่อสารโทรคมนาคม ซึ่งให้บริการแก่องค์กรภาครัฐ เอกชนและบุคคลทั่วไป โดยมีธุรกิจบริการที่สำคัญ ได้แก่ บริการโทรศัพท์พื้นฐาน บริการโทรศัพท์สาธารณะ บริการโทรศัพท์เคลื่อนที่ บริการโทรศัพท์ระหว่างประเทศ บริการสื่อสารข้อมูล รวมทั้ง บริการเสริมพิเศษต่าง ๆ นอกจากนั้น ยังเป็นผู้ให้บริการโครงข่ายโทรคมนาคมที่มีความแข็งแกร่งสูงสุดในประเทศด้วยเครือข่ายเชื่อมโยงระหว่างประเทศครอบคลุมภาคพื้นเอเชียแปซิฟิก และภูมิภาคอื่น ๆ ของโลก สามารถให้บริการโทรคมนาคมครบวงจรทั้งในประเทศและระหว่างประเทศ

บริษัท ทีโอที จำกัด (มหาชน) ได้มุ่งเข้าสู่ธุรกิจพาณิชย์อิเล็กทรอนิกส์ (e-Business) เพื่อตอบสนองต่อความต้องการของประชาชนและความสำเร็จของธุรกิจยุคดิจิตอล โดยให้เปิดให้บริการต่าง ๆ ที่รองรับการเติบโตของธุรกิจพาณิชย์อิเล็กทรอนิกส์ อาทิ บริการรับชำระค่าบริการโทรศัพท์ผ่านอินเทอร์เน็ต บริการศูนย์พาณิชย์อิเล็กทรอนิกส์ (e-Business Center) การจัดการระบบการจัดซื้อจัดหาผ่านอินเทอร์เน็ต (e-Procurement) และการเปิดให้บริการออกใบรับรองอิเล็กทรอนิกส์ (TOT Certification Authority: TOT CA) ซึ่งจะเรียกว่า “TOT CA”

บริษัท ทีโอที จำกัด (มหาชน) ทำหน้าที่ให้บริการเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งแบ่งใบรับรองออกเป็น 2 ประเภท ได้แก่

1) ใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล โดยใบรับรองดังกล่าวเป็นข้อมูลในรูปอิเล็กทรอนิกส์ที่เชื่อมโยงกับบุคคล ซึ่งปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์นั้น เพื่อยืนยันและรับรองว่ากุญแจสาธารณะเป็นของบุคคลนั้น

2) ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บ โดยใบรับรองดังกล่าวเป็นข้อความในรูปอิเล็กทรอนิกส์ที่เชื่อมโยงกับเว็บไซต์ ซึ่งปรากฏชื่ออยู่ในใบรับรองนั้น เพื่อยืนยันและรับรองว่ากุญแจสาธารณะเป็นของเว็บไซต์นั้น

เอกสารฉบับนี้เรียกว่า "แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement)" หรือเรียกว่า “CP/CPS” ถูกจัดทำขึ้นตามมาตรฐาน Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy และ Certification Practices Framework [RFC3647] โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ เพื่อให้รับทราบถึง ข้อความระบุในเอกสาร ตลอดจนทำความเข้าใจและเป็นแนวทางในการประยุกต์ใช้งานใบรับรอง นอกจากนี้ยังใช้เป็นเอกสารที่ผูกพันทางกฎหมาย ระหว่างคู่กรณีทุกฝ่ายอีกด้วย ทั้งนี้แนวทางในการดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์แต่ละประเภทสามารถดูได้จากเอกสารคำชี้แจงทางปฏิบัติในการประกอบการรับรองอิเล็กทรอนิกส์จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (TOT Certification Authority:TOT CA) โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หรือ TOT CA ได้ยึดตามข้อปฏิบัติตามมาตรฐาน ของ Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published ที่ถูกประกาศเป็น Version ล่าสุดอยู่ใน http://www.cabforum.org หากเอกสารฉบับนี้มีข้อปฏิบัติใดผิดไปจาก ข้อปฏิบัติตามมาตรฐาน Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published ขอให้ยึดตามข้อปฏิบัติตามมาตรฐานฯ

โครงสร้างพื้นฐานกุญแจสาธารณะ(Public Key Infrastructure : PKI) จะประกอบด้วย

1. ผู้ใช้บริการ (End Entity) เป็นผู้ซึ่งประสงค์จะขอใช้บริการใบรับรองอิเล็กทรอนิกส์ โดยยื่นคำขอผ่านทางเจ้าหน้าที่รับลงทะเบียน

2. เจ้าหน้าที่รับลงทะเบียน (Registration Authority) เป็นผู้ซึ่งทำหน้าที่รับลงทะเบียน เมื่อมีการยื่นขอใบรับรองอิเล็กทรอนิกส์ แจ้งเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ใช้บริการให้ไว้ตามแบบคำขอที่ผู้ให้บริการกำหนดขึ้น

3. ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) เป็นองค์กรซึ่งทำหน้าที่ในการให้บริการเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ เพื่อรับรองตัวตนที่แท้จริงของบุคคล นิติบุคคล หรือเอ็นทิตี้ใดๆ

4. ที่บันทึกข้อมูล (Repository) เป็นระบบคอมพิวเตอร์ที่เปิดให้บุคคลอื่นสามารถสืบค้นใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการเพื่อใช้ในการติดต่อสื่อสารอย่างปลอดภัย

1.2. **ชื่อเอกสาร** (Document Name and Identification)

เอกสารฉบับนี้เรียกว่า “แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement)” ซึ่งเรียกว่า “CP/CPS” โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ เพื่อให้ทราบถึงข้อความที่ระบุในเอกสารตลอดจนความเข้าใจและเป็นแนวทางในการดำเนินการเกี่ยวกับใบรับรอง นอกจากนี้ยังใช้เป็นเอกสารที่มีผลผูกพันทางกฎหมายระหว่างคู่กรณีทุกฝ่ายอีกด้วย

เอกสารแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ฉบับนี้ เป็นเอกสารที่อธิบายถึงการประยุกต์ใช้งานใบรับรองอิเล็กทรอนิกส์ประเภทต่าง ๆ ที่ TOT มีให้บริการ โดยอ้างอิงตามมาตรฐาน RFC 3647 ซึ่งเป็นมาตรฐานสากล และสอดคล้องกับกฎหมายและระเบียบต่าง ๆ ที่มีการประกาศใช้งาน

ทั้งนี้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้กำหนด Object Identifier (OID) สำหรับแนวนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์ฉบับนี้คือ

1.3.6.1.4.1.16350.200.1.1

ซึ่งแต่ละหมายเลขของ OID มีความหมายดังนี้

ISO assigned	1
ISO Identified Organization	3
US Department of Defense	6
Internet	1
Private	4
ANA registered private enterprises	1
TOT Public Company Limited	16350
TOT CA Service	200
Security Objects	1
Certificate Policy	1

1.3. **บุคคลที่เกี่ยวข้อง** (PKI participants)

1.3.1 **ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์** (Certification Authority : TOT CA)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หมายความว่า ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่ง สร้างและออกใบรับรองอิเล็กทรอนิกส์ เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List หรือมีชื่อย่อว่า CRL) ตามความถี่ที่เหมาะสม

1.3.2. **หน่วยรับลงทะเบียน**(Registration Authorities : TOT RA)

หน่วยรับลงทะเบียน (Registration Authorities : TOT RA) คือ ผู้ซึ่งทำหน้าที่รับลงทะเบียน เมื่อมีการยื่นคำขอใช้บริการ คำขอเพิกถอนใบรับรอง หรือต่ออายุใบรับรอง โดยการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ของข้อมูลที่ผู้ใช้บริการให้ไว้ตามแบบคำขอที่ผู้ให้บริการกำหนดขึ้น

1.3.3. **ผู้ใช้บริการ** (Subscribers)

ผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์ (End Entities) หมายความว่า ผู้ที่ได้ใช้บริการใบรับรองอิเล็กทรอนิกส์จากผู้ให้บริการ โดยมีชื่อปรากฏในใบรับรองอิเล็กทรอนิกส์ และเป็นเจ้าของกุญแจส่วนตัวและกุญแจสาธารณะที่ปรากฏในใบรับรองอิเล็กทรอนิกส์นั้น

1) บุคคลธรรมดา ได้แก่

- บุคคลทั่วไปที่ยื่นคำขอใช้บริการใบรับรองแก่ผู้ให้บริการ เมื่อมีการออกใบรับรองจะมีการระบุชื่อผู้ใช้บริการไว้ในใบรับรอง
- บุคคลทั่วไปที่ยื่นคำขอใช้บริการใบรับรองสำหรับเครื่องบริการเว็บแก่ผู้ให้บริการ เมื่อมีการออกใบรับรองจะมีการระบุชื่อเว็บไซต์ของเครื่องบริการเว็บไว้ในใบรับรอง

2) นิติบุคคล ได้แก่

- นิติบุคคลที่ยื่นคำขอใช้บริการใบรับรองแก่ผู้ให้บริการ เมื่อมีการออกใบรับรองจะมีการระบุชื่อนิติบุคคลของผู้ใช้บริการไว้ในใบรับรอง
- นิติบุคคลที่ยื่นคำขอใช้บริการใบรับรองสำหรับเครื่องบริการเว็บแก่ผู้ให้บริการ เมื่อมีการออกใบรับรองจะมีการระบุชื่อเว็บไซต์ของเครื่องบริการเว็บไว้ในใบรับรอง

1.3.4. **คู่กรณีที่เกี่ยวข้อง** (Relying Parties)

คู่กรณีที่เกี่ยวข้อง (Relying Party) คือ ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใด ๆ เพราะเชื่อถือใบรับรองหรือลายมือชื่อดิจิตอล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองไปใช้ในการตรวจสอบตัวตน ของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิตอล และมีชื่อปรากฏอยู่ในใบรับรอง

1.3.5. **บุคคลซึ่งเกี่ยวข้องอื่น ๆ** (Other Participants)

ไม่มี

1.4.**การใช้ใบรับรองอิเล็กทรอนิกส์** (Certificate Usage)

1.4.1. **การใช้ใบรับรองอิเล็กทรอนิกส์ที่เหมาะสม** (Appropriate Certificate Uses)

ใบรับรองที่ผู้ให้บริการออกให้แก่ผู้ใช้บริการนั้นได้มีการจำกัดการใช้งานสำหรับใบรับรองแต่ละประเภทดังนี้

1. Personal Certificate คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้บุคคลหรือ ประชาชนทั่วไป เพื่อรักษาความ มั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์ จะมีอายุการใช้งานตั้งแต่ 1 ปี 2 ปีและ 3 ปี

2. Enterprise Certificate คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้กับนิติบุคคล ที่มีความต้องการใช้งานใบรับรองอิเล็กทรอนิกส์เพื่อรักษาความมั่นคงปลอดภัย ให้กับธุรกรรมอิเล็กทรอนิกส์โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้ จะมีอายุการใช้งานตั้งแต่ 1 ปี 2 ปีและ 3 ปี

3. Computer/Equipment Certificate คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ ใช้ในการติดต่อสื่อสารทางเครือข่าย เช่น เราท์เตอร์ (Router) เพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรม อิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้ จะมีอายุการใช้งานตั้งแต่ 1 ปี 2 ปีและ 3 ปี

4. Web Server Certificate (SSL Certificate) คือ ใบรับรองอิเล็กทรอนิกส์ที่ใช้ยืนยันตัวตนของ Web Server โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้ จะมีอายุการใช้งานตั้งแต่ 1 ปี 2 ปีและ 3 ปี

1.4.2. **ข้อจำกัดในการใช้ใบรับรองอิเล็กทรอนิกส์** (Prohibited Certificate Uses)

ใบรับรองอิเล็กทรอนิกส์ที่ TOT CA ออกให้แก่ผู้ใช้งาน ไม่อนุญาตให้นำไปใช้ในการอื่นใดที่นอกเหนือจากข้อ 1.4.1 ทั้งนี้ ให้เป็นไปตามข้อกำหนดของผู้มีอำนาจในการกำกับดูแลการให้บริการออกใบรับรองอิเล็กทรอนิกส์

1.5. **การบริหารจัดการเกี่ยวกับแนวนโยบาย** (Policy Administration)

1.5.1. **หน่วยงานที่ทำหน้าที่บริหารจัดการเอกสารฉบับนี้** (Organization Administering the Document)

หน่วยงานที่บริหารจัดการเอกสารฉบับนี้ คือ บริษัท ทีโอที จำกัด (มหาชน)

1.5.2. **ข้อมูลสำหรับติดต่อหน่วยงาน** (Contact person)

แนวนโยบายและแนวปฏิบัติการให้บริการ ใบรับรองอิเล็กทรอนิกส์ นี้ออกโดย บริษัท ทีโอที จำกัด (มหาชน) สอบถามหรือการติดต่อใด ๆ อันเกี่ยวกับเอกสารนี้ ให้ติดต่อที่ :

ศูนย์บริการพาณิชย์อิเล็กทรอนิกส์

บริษัท ทีโอที จำกัด (มหาชน)

เลขที่ 89/2 หมู่ 3 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง

เขตหลักสี่ กรุงเทพฯ 10210 ประเทศไทย

โทรศัพท์ 02 574 8912, 02 575 5221

โทรสาร 02 574 8913

Website: http://www.ca.tot.co.th

Email Address: info@ca.tot.co.th

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

ผู้ให้บริการ มีหน้าที่ต้องยื่นเอกสาร แนวนโยบายและแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ ไปยังสำนักงานพัฒนาธุรกรรมทางอิเล็กทรนิกส์ (องค์การมหาชน) ตั้งอยู่ ณ อาคารเดอะไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310 มีอำนาจในการกำกับดูแลการให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อดำเนินการตรวจสอบและรับรอง

1.5.4. **กระบวนการอนุมัติแนวนโยบาย/แนวปฏิบัติ** (CPS Approval Procedures)

การสร้างหรือเปลี่ยนแปลงเอกสารฉบับนี้ จะต้องได้รับอนุมัติจาก บริษัท ทีโอที จำกัด (มหาชน)ทั้งนี้ โดยอยู่ภายใต้กฎเกณฑ์หรือข้อกำหนดทางกฎหมาย หากมี

1.6. **คำนิยามและคำย่อ** (Definitions and Acronyms)

คำนิยาม (Definitions)

คำศัพท์	ความหมาย
RFC	“The Internet Request For Comments” เป็นชุดเอกสารที่เขียนเพื่อนิยามหรือบรรยายตามความเป็นจริงปัจจุบันและแนะนำแนวปฏิบัติเกี่ยวกับเกณฑ์วิธี (Protocol) และนโยบายของอินเทอร์เน็ต เป็นต้น
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	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิตอล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้
คู่กุญแจ Key Pair	กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิตอลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้
เจ้าหน้าที่รับลงทะเบียน Registration Authority (RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ แจ้งเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ใช้บริการให้ไว้
พฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล (Compromise)	หมายถึง การที่ข้อมูลสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์ของการเก็บรักษาข้อมูลนั้น รวมทั้งกรณีที่มีเหตุอันควรสงสัยว่าจะมีพฤติการณ์ดังกล่าว

คำย่อ (Definitions)

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. การเผยแพร่ข้อมูลและความรับผิดชอบในการเก็บรักษาข้อมูล(Publication and Repository Responsibilities)

2.1. ที่บันทึกข้อมูล (Repositories)

ผู้ให้บริการมีแหล่งเก็บข้อมูล 3 แห่ง ได้แก่

1) ไดเรกทอรี(Directory) ซึ่งเป็นระบบฐานข้อมูลสำหรับบันทึกใบรับรอง และรายการเพิกถอนใบรับรอง

2) ฐานข้อมูล (Database) ซึ่งเป็นที่สำหรับเก็บข้อมูลของผู้ใช้บริการ

3) เว็บไซต์ (Website) ซึ่งเป็นที่สำหรับเก็บหรือประกาศข้อมูลเพื่อเผยแพร่ เช่น แนวนโยบายและแนวปฏิบัติสู่สาธารณะ

2.2. การเผยแพร่ข้อมูลของผู้ใช้บริการ (Publication of Certification Information)

ผู้ให้บริการมีหน้าที่เผยแพร่ข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์และรายการเพิกถอนใบรับรองผ่านเว็บไซต์ของ TOT CA เพื่อให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบข้อมูลที่เกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือ ข้อมูลสถานะต่างๆ ของใบรับรองอิเล็กทรอนิกส์ได้ และเผยแพร่โดยผ่านทาง X.500 Directory หรือ LDAP repository

2.3. เวลาและความถี่ในการเผยแพร่ข้อมูล (Time or Frequency of Publication)

- ข้อมูลใบรับรองอิเล็กทรอนิกส์ข้อมูลอันได้แก่ ใบรับรองอิเล็กทรอนิกส์ รายการใบเพิกถอนใบรับรอง แนวนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์ (CP) และแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์(CPS) มีการเผยแพร่ทางเว็บไซต์ของผู้ให้บริการ (http://www.ca.tot.co.th) ในลักษณะดังต่อไปนี้และรายการเพิกถอนใบรับรองจะได้รับการเผยแพร่โดยเร็ว โดยผู้ให้บริการ จะนำใบรับรองอิเล็กทรอนิกส์และรายการเพิกถอนใบรับรองไปบันทึกไว้ในไดเรกทอรี หลังจากมีการสร้างรายการเหล่านั้น

- ผู้ให้บริการจะทำการเผยแพร่สำเนาของแนวนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์ (CP) และแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (CPS) เวอร์ชั่นล่าสุดผ่านทางเว็บไซต์ของผู้ให้บริการ

- ข้อมูลที่ได้ประกาศและเผยแพร่ทางเว็บไซต์ของผู้ให้บริการ จะถูกคงไว้เพื่อให้มีการเข้าถึงข้อมูลเหล่านี้ได้จนกระทั่งมีการเปลี่ยนแปลงแก้ไขหรือมีการทำเวอร์ชั่น (Version) ใหม่ของข้อมูลดังกล่าว

2.4. การควบคุมการเข้าถึงที่บันทึกข้อมูล (Access Controls on Repositories)

ในกรณีที่เห็นว่าเหมาะสม ผู้ให้บริการอาจกำหนดการควบคุมการเข้าถึงข้อมูลที่ถูกเผยแพร่บางประเภท เพื่อให้สิทธิแก่ผู้ใช้บริการและนายทะเบียนเท่านั้นในการเข้าถึงข้อมูลดังกล่าว ผู้ใช้บริการอาจกำหนดมาตรการเกี่ยวกับความมั่นคงและปลอดภัยในการกำหนดให้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้นในการสร้าง แก้ไข และนำข้อมูลไปใส่ในเว็บไซต์สำหรับเผยแพร่

3. **การระบุและยืนยันตัวบุคคล** (Identification and Authentication (I&A))

3.1. **การกำหนดรูปแบบของชื่อ** (Naming)

3.1.1. **ลักษณะของชื่อ** (Types of Names)

ชื่อที่ปรากฏในใบรับรองของผู้ใช้บริการแต่ละรายจะมีลักษณะเป็นชื่อเฉพาะ (Distinguished Name: DN) และไม่ซ้ำกัน เพื่อให้รับรองได้ว่าสามารถเชื่อมโยงใบรับรองเข้ากับผู้ใช้บริการ ผู้ให้บริการ หรือเครื่องให้บริการได้ ทั้งนี้อ้างอิงตาม ISO/IEC 9594-1/ITU-T Recommendation X.500 The Directory: Overview of Concepts, Models, and Services

3.1.2. **ความหมายของชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์** (Need for Names to be Meaningful)

ชื่อที่ปรากฏในใบรับรองจะต้องสื่อถึงความหมาย ซึ่งเชื่อมโยงไปยังการระบุตัวตนของผู้ใช้บริการที่มีชื่อปรากฏในใบรับรองอิเล็กทรอนิกส์ เช่น ชื่อของนิติบุคคล (Organization Unit: OU) จะเป็นชื่อของนิติบุคคลที่ขอใช้บริการเป็นต้น

3.1.3. **การกำหนดชื่อของผู้ให้บริการ ในกรณีที่มีการใช้ชื่อนิรนามหรือนามแฝงหรือปิดบังชื่อที่แท้จริง** (Anonymity or Pseudonymity of Subscribers)

ไม่มี

3.1.4. **กฎในการแปลงชื่อในรูปแบบต่าง ๆ** (Rules for Interpreting Various Name Forms)

ไม่มี

3.1.5. **ความเป็นเอกภาพของชื่อ** (Uniqueness of Names)

ชื่อเฉพาะที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ จะไม่ซ้ำกัน และ ไม่คลุมเครือ

3.1.6. Recognition, Authentication, and Role of Trademarks

จะต้องไม่ใช้ชื่อในการสมัครที่ฝ่าฝืนสิทธิตามกฎหมายทรัพย์สินทางปัญญา

3.2. **ความสมบูรณ์ในการระบุตัวตน** (Initial Identity Validation)

3.2.1. **วิธีการในการพิสูจน์การครอบครองกุญแจส่วนตัว** (Method to Prove Possession of Private Key)

ผู้ใช้บริการจะต้องแสดงวิธีการที่มีความมั่นคงปลอดภัยเพื่อให้มั่นใจได้ว่าได้เป็นเจ้าของกุญแจส่วนตัวซึ่งสัมพันธ์กับกุญแจสาธารณะที่ปรากฏในข้อมูลซีเอสอาร์ (CSR: Certificate Signing Request) ที่ส่งมายังผู้ให้บริการ สำหรับการขอใบรับรองอิเล็กทรอนิกส์ หรือจากใบสมัครขอใบรับรองอิเล็กทรอนิกส์ ซึ่งประกอบไปด้วยชื่อ เลขที่บัตรประจำตัวประชาชน หรือ พาสปอร์ต ลายเซ็นต์ของผู้ใช้บริการเอง และสำเนาบัตรประชาชน

3.2.2. **การยืนยันความมีตัวตนขององค์กร** (Authentication of Organization Identity)

การตรวจสอบยืนยันความมีตัวตนของนิติบุคคลเพื่อออกใบรับรองนั้น เป็นหน้าที่ของเจ้าหน้าที่รับลงทะเบียน โดยผู้ใช้บริการต้องกรอกแบบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์สำหรับนิติบุคคล เพื่อขอใช้ใบรับรองพร้อมทั้งแนบหลักฐานที่ใช้ในการสมัครขอใช้บริการซึ่งเจ้าหน้าที่รับลงทะเบียน จะตรวจสอบหนังสือรับรองนิติบุคคลซึ่งจะต้องมี อายุไม่เกินหกเดือนจากวันที่ออกและมีลายเซ็นต์ของกรรมการผู้มีอำนาจที่ถูกต้องและ ครบถ้วน หรือพระราชบัญญัติจัดตั้งนิติบุคคล

3.2.3. **การยืนยันความมีตัวตนของบุคคล** (Authentication of Individual Identity)

การตรวจสอบและยืนยันความมีตัวตนของบุคคลธรรมดาเพื่อออกใบรับรองนั้น เป็นหน้าที่ของเจ้าหน้าที่รับลงทะเบียน โดยผู้ใช้บริการต้องกรอกแบบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์สำหรับบุคคลธรรมดา เพื่อขอใช้ใบรับรองพร้อมทั้งแนบหลักฐานที่ใช้ในการสมัครขอใช้บริการแก่เจ้าหน้าที่รับลงทะเบียนด้วย ได้แก่ สำเนาบัตรประจำตัวข้าราชการ หรือสำเนาบัตรประจำตัวประชาชนและหรือ พาสปอร์ต สำเนาทะเบียนบ้าน เป็นต้น

3.2.4. **ข้อมูลของผู้ใช้งานที่ไม่ต้องผ่านการตรวจสอบ** (Non-Verified Subscriber Information)

ไม่มี

3.2.5. **การตรวจสอบผู้มีอำนาจ** (Validation of Authority)

เจ้าหน้าที่รับลงทะเบียน จะตรวจสอบ และเก็บหนังสือมอบอำนาจที่แนบมาพร้อมกับใบคำขอใบรับรองอิเล็กทรอนิกส์เพื่อยืนยันว่าผู้ใช้บริการนั้นได้รับมอบอำนาจมาจากนิติบุคคลและสามารถขอใบรับรองอิเล็กทรอนิกส์ในนามของนิติบุคคลได้

3.2.6. **เกณฑ์การร่วมมือกันระหว่างกัน** (Criteria for Interoperation)

ไม่มี

3.3. **การระบุยืนยันตัวตนเมื่อมีการขอออกใบรับรองอิเล็กทรอนิกส์ใหม่** (I&A for Re-key Requests)

3.3.1. **การขอออกกุญแจใหม่** (Identification and Authentication for Routine Re-key)

โดยปกติแล้ว การขอออกกุญแจใหม่จะเกิดขึ้นเมื่อใบรับรองอิเล็กทรอนิกส์ใบเดิมได้หมดอายุแล้ว เพื่อให้ผู้ใช้บริการสามารถดำเนินการขอออกกุญแจใหม่ได้ ทั้งนี้ เจ้าหน้าที่รับทะเบียนกำหนดให้ผู้ใช้บริการกรอกใบสมัครใบรับรองอิเล็กทรอนิกส์สำหรับบุคคลธรรมดาหรือนิติบุคคล ส่งให้กับเจ้าหน้าที่รับลงทะเบียน โดยดำเนินการตามหัวข้อ 4.1 ต่อไป

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

กรณีที่ใบรับรองอิเล็กทรอนิกส์ถูกเพิกถอนแล้ว ผู้ใช้บริการสามารถดำเนินการขอออกกุญแจใหม่ ทั้งนี้ เจ้าหน้าที่รับทะเบียนกำหนดให้ผู้ใช้บริการกรอกใบสมัครใบรับรองอิเล็กทรอนิกส์สำหรับบุคคลธรรมดาหรือนิติบุคคล ส่งให้กับเจ้าหน้าที่รับลงทะเบียน โดยดำเนินการตามหัวข้อ 4.1 ต่อไป

3.4. **การระบุและยืนยันตัวตนเมื่อมีการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์** (I&A for Revocation Requests)

ผู้ใช้บริการที่ต้องการเพิกถอนใบรับรองอิเล็กทรอนิกส์ ต้องแจ้งต่อผู้ให้บริการโดยตรง เมื่อผู้ให้บริการได้รับแจ้งความต้องการเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดยตรวจสอบใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐานประกอบตามขั้นตอนแล้ว จะดำเนินการเพิกถอนใบรับรองอิเล็กทรอนิกส์ตามที่แจ้งไว้และประกาศในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดยรายละเอียดอยู่ในหัวข้อ 4.9

4. ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์
(Certificate Life-Cycle Operational Requirements)

4.1. การยื่นคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Application)

4.1.1 **ผู้ที่สามารถขอใช้บริการใบรับรองอิเล็กทรอนิกส์ได้**(Who Can Submit a Certificate Application?)

บุคคลที่สมัครขอใบรับรองอิเล็กทรอนิกส์สามารถเป็นได้ทั้งบุคคลที่ขอใบรับรองอิเล็กทรอนิกส์ในนามบุคคลธรรมดา และบุคคลที่ได้รับมอบหมายจากนิติบุคคลให้ดำเนินการสมัครขอใบรับรองอิเล็กทรอนิกส์ในนามนิติบุคคล เพื่อใช้รักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์

4.1.2 **กระบวนการยื่นคำขอใบรับรองอิเล็กทรอนิกส์** (Enrollment Process and Responsibilities)

ผู้ใช้บริการควรปฏิบัติตามขั้นตอนต่อไปนี้

กรณีการขอใบรับรองอิเล็กทรอนิกส์ประเภท Personal Certificate

ขั้นตอนดำเนินการ

1. กรอกใบคำขอใบรับรองอิเล็กทรอนิกส์
2. ยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์พร้อมหลักฐานที่

   หน่วยงานรับลงทะเบียน บริษัท ทีโอที จำกัด (มหาชน)

   โทรศัพท์ 0-2574-8912, 0-2575-5221, 0-2505-6168 โทรสาร 0-2574-8913
3. เจ้าหน้าที่รับลงทะเบียนตรวจสอบใบคำขอใบรับรองอิเล็กทรอนิกส์และหลักฐานประกอบ
4. เจ้าหน้าที่รับลงทะเบียนจัดส่งใบรับรองอิเล็กทรอนิกส์ให้ผู้ใช้บริการ
5. ผู้ใช้บริการชำระค่าบริการ

หลักฐานประกอบ

1. สำเนาบัตรประชาชนของผู้ใช้บริการพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
2. สำเนาทะเบียนบ้านของผู้ใช้บริการพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสืออนุญาตให้ทำงานในประเทศไทย (Work Permit) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

กรณีการขอใบรับรองอิเล็กทรอนิกส์ประเภท Enterprise Certificate

ขั้นตอนดำเนินการ

1. กรอกใบคำขอใบรับรองอิเล็กทรอนิกส์
2. ยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์พร้อมหลักฐานที่

   หน่วยงานรับลงทะเบียน บริษัท ทีโอที จำกัด (มหาชน)

   โทรศัพท์ 0-2574-8912, 0-2575-5221, 0-2505-6168 โทรสาร 0-2574-8913

3. เจ้าหน้าที่รับลงทะเบียนตรวจสอบใบคำขอใบรับรองอิเล็กทรอนิกส์ และหลักฐานประกอบ

4. เจ้าหน้าที่รับลงทะเบียนจัดส่งใบรับรองอิเล็กทรอนิกส์ ให้ผู้ใช้บริการ

5. ผู้ใช้บริการชำระค่าบริการ

หลักฐานประกอบ

1. สำเนาหนังสือรับรองการเป็นนิติบุคคลที่มีอายุไม่เกิน 90 วัน (3 เดือน) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้องโดยกรรมการผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท (ถ้ามี)

2. สำเนาบัตรประชาชนของกรรมการผู้มีอำนาจ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

3. กรณีกรรมการผู้มีอำนาจมอบอำนาจให้ผู้อื่นดำเนินการแทน ให้เพิ่ม

    3.1 หนังสือมอบอำนาจ พร้อมปิดอากรแสตมป์ 30 บาทตามจำนวนผู้รับมอบอำนาจ

    3.2 สำเนาบัตรประชาชนของผู้รับมอบอำนาจพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

กรณีการขอใบรับรองอิเล็กทรอนิกส์ประเภท SSL Certificate

ขั้นตอนดำเนินการ

1. กรอกใบคำขอใบรับรองอิเล็กทรอนิกส์

2. ยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์พร้อมหลักฐานที่

    หน่วยงานรับลงทะเบียน บริษัท ทีโอที จำกัด (มหาชน)

    โทรศัพท์ 0-2574-8912, 0-2575-5221, 0-2505-6168 โทรสาร 0-2574-8913

3. เจ้าหน้าที่รับลงทะเบียนตรวจสอบใบคำขอใบรับรองอิเล็กทรอนิกส์ และหลักฐานประกอบ

4. เจ้าหน้าที่รับลงทะเบียนจัดส่งใบรับรองอิเล็กทรอนิกส์ ให้ผู้ใช้บริการ

5. ผู้ใช้บริการชำระค่าบริการ

หลักฐานประกอบ

กรณีจดทะเบียน Domain Name **ในนามบุคคล**

1. สำเนาบัตรประชาชนของผู้ใช้บริการ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

2. สำเนาทะเบียนบ้านของผู้ใช้บริการ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสืออนุญาตให้ทำงานในประเทศไทย (Work Permit) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

3. สำเนาหนังสือรับรองการจดทะเบียน Domain Name พร้อมลงลายมือชื่อรับรองสำเนาถูกต้องโดยผู้ใช้บริการ

กรณีจดทะเบียน Domain Name ในนามองค์กร

1. สำเนาหนังสือรับรองการเป็นนิติบุคคลที่มีอายุไม่เกิน 90 วัน (3 เดือน) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้องโดยกรรมการผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท (ถ้ามี)
2. สำเนาหนังสือรับรองการจดทะเบียน Domain Name พร้อมลงลายมือชื่อรับรองสำเนาถูกต้องโดยกรรมการผู้มีอำนาจ
3. สำเนาบัตรประชาชนของกรรมการผู้มีอำนาจ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
4. กรณีกรรมการผู้มีอำนาจมอบอำนาจให้ผู้อื่นดำเนินการแทน ให้เพิ่ม
    4.1 หนังสือมอบอำนาจ พร้อมปิดอากรแสตมป์ 30 บาทตามจำนวนผู้รับมอบอำนาจ
    4.2 สำเนาบัตรประชาชนของผู้รับมอบอำนาจพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

4.2. การพิจารณาคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)

4.2.1. การใช้ฟังก์ชั่นยืนยันและรับรองตัวบุคคล (Performing Identification and Authentication Functions)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะตรวจสอบใบสมัครและหลักฐานการสมัครก่อนออกใบรับรองอิเล็กทรอนิกส์ โดยจะแจ้งให้ผู้ใช้บริการรับทราบ หากข้อมูลในใบสมัครผิดพลาดหรือ เอกสารหลักฐานไม่ครบถ้วน

4.2.2. การพิจารณาอนุมัติหรือปฏิเสธการสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ (Approval or Rejection of Certificate Applications)

เจ้าหน้าที่รับลงทะเบียนจะพิจารณาใบสมัครขอใบรับรองอิเล็กทรอนิกส์ และหลักฐานต่างๆที่ใช้ประกอบการพิจารณา ต้องมีความครบถ้วนและถูกต้อง จึงจะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ให้กับผู้ใช้บริการ โดยหากส่วนหนึ่งส่วนใดหรือทั้งหมดของใบสมัครใบรับรองอิเล็กทรอนิกส์ และ/หรือหลักฐานประกอบการสมัครใบรับรองอิเล็กทรอนิกส์ ไม่ครบถ้วน ไม่ถูกต้อง ก็จะส่งเอกสารคืนให้แก่ผู้ใช้บริการ

4.2.3. เวลาที่ใช้ในการดำเนินการสำหรับการออกใบรับรองอิเล็กทรอนิกส์ (Time to Process Certificate Applications)

เจ้าหน้าที่รับลงทะเบียนจะดำเนินการตรวจสอบหลักฐานและพิจารณาใบสมัครใบรับรองอิเล็กทรอนิกส์ หากหลักฐานเอกสารครบถ้วน จะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ให้ภายในวันเวลาทำการ เวลา 8.30 – 16.30 น.

4.3. **การออกใบรับรองอิเล็กทรอนิกส์** (Certificate Issuance)

4.3.1. **การทำงานของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ในช่วงของการออกใบรับรองอิเล็กทรอนิกส์** (CA Actions During Certificate Issuance)

1. เจ้าหน้าที่รับลงทะเบียนตรวจสอบเอกสารหลักฐาน และ CSR file(ถ้ามี) ที่ได้รับจากผู้ใช้บริการ โดยต้องมีความถูกต้องตรงกัน หากพบว่าข้อมูลไม่ตรงกันให้แจ้งผู้ใช้บริการ

2. เมื่อตรวจสอบพบข้อมูลถูกต้องแล้ว เจ้าหน้าที่รับลงทะเบียนจะบันทึกข้อมูลตามใบสมัครใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการ และออกใบรับรองอิเล็กทรอนิกส์

3. เจ้าหน้าที่รับลงทะเบียนจะตรวจสอบความถูกต้องของข้อมูลในใบรับรองอิเล็กทรอนิกส์และใบรับรองอิเล็กทรอนิกส์ที่ออกให้

4. เจ้าหน้าที่รับลงทะเบียนส่งใบรับรองอิเล็กทรอนิกส์ ถึงผู้ใช้บริการผ่านช่องทางที่เหมาะสม

4.3.2. **การแจ้งผลการพิจารณา สมัครบริการใบรับรองอิเล็กทรอนิกส์** (Notification to Subscriber by the CA of Issuance of Certificate)

ผู้ให้บริการจะดำเนินการแจ้งแก่ผู้ใช้บริการด้วยวิธีการที่เหมาะสม เมื่อมีการออกใบรับรองอิเล็กทรอนิกส์แล้ว

4.4. **การยอมรับใบรับรองอิเล็กทรอนิกส์** (Certificate Acceptance)

4.4.1. **หลักปฏิบัติในการยอมรับใบรับรองอิเล็กทรอนิกส์** (Conduct Constituting Certificate Acceptance)

เมื่อได้รับใบรับรองที่ออกให้โดยผู้ให้บริการแล้ว ผู้ใช้บริการต้องตรวจข้อมูลที่ปรากฏในใบรับรองและยืนยันความถูกต้องของข้อมูลอันเป็นสาระสำคัญซึ่งแสดงในใบรับรอง ตลอดอายุของใบรับรอง และต้องแจ้งให้ผู้ใช้บริการทราบโดยมิชักช้า เมื่อมีการเปลี่ยนแปลงข้อมูลหรือมีการเพิ่มเติมข้อมูลดังกล่าว เมื่อได้ตรวจสอบและยืนยันความถูกต้องของข้อมูลดังกล่าว และมิได้แจ้งปฏิเสธหรือไม่ยอมรับข้อมูล ตามที่ปรากฏในเวลา 15 วัน ให้ถือว่าเป็นการยอมรับใบรับรอง

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

ผู้ให้บริการ จะดำเนินการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการที่ได้สร้างขึ้นไว้ใน Directory ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

4.4.3. **การแจ้งให้หน่วยงานอื่นทราบถึงการออกใบรับรองอิเล็กทรอนิกส์** (Notification of Certificate Issuance by the CA to Other Entities)

การแจ้งให้บุคคลอื่นทราบถึงใบรับรองอิเล็กทรอนิกส์ที่ได้ออกให้ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ เช่น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจส่งใบรับรองอิเล็กทรอนิกส์ที่ออกให้ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ แก่เจ้าหน้าที่รับลงทะเบียน เป็นต้น

4.5. **การใช้กุญแจคู่และใบรับรองอิเล็กทรอนิกส์** (Key Pair and Certificate Usage)

4.5.1. **การใช้กุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ** (Entities Private Key and Certificate Usage)

การใช้กุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์จะมีความผูกพันเมื่อผู้ใช้บริการได้ยอมรับข้อตกลงในการใช้งานใบรับรองอิเล็กทรอนิกส์ และยอมรับใบรับรองอิเล็กทรอนิกส์แล้ว ทั้งนี้การใช้ใบรับรองอิเล็กทรอนิกส์จะต้องสัมพันธ์กับค่าที่ระบุไว้ในฟิลด์ Key Usage ในใบรับรองอิเล็กทรอนิกส์ รวมทั้งผู้ใช้งานจะต้องปกป้องกุญแจส่วนตัวจากการเข้าถึงโดยไม่ได้รับอนุญาต และจะต้องยุติการใช้กุญแจส่วนตัวในทันทีที่ใบรับรองอิเล็กทรอนิกส์ใบนั้นหมดอายุหรือถูกเพิกถอน

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

คู่กรณีที่เกี่ยวข้องจะต้องปฏิบัติตามข้อตกลงในการใช้งานใบรับรองอิเล็กทรอนิกส์สำหรับคู่กรณีที่เกี่ยวข้องที่ระบุไว้ในเอกสารฉบับนี้ ซึ่งจะต้องตรวจสอบเงื่อนไขบางประการก่อนที่จะใช้ใบรับรองอิเล็กทรอนิกส์ใบนั้น หากเงื่อนไขระบุว่าจะจัดหาข้อมูลเพิ่มเติมคู่กรณีเกี่ยวข้องก็จำเป็นต้องดำเนินการอย่างเหมาะสม ก่อนที่จะใช้ใบรับรองอิเล็กทรอนิกส์ คู่กรณีที่เกี่ยวข้องจำเป็นต้องประเมินดังนี้

- ความเหมาะสมในการใช้ใบรับรองอิเล็กทรอนิกส์ ซึ่งสอดคล้องกับที่ได้ระบุไว้ในฟิลด์ Key Usage ในใบรับรองอิเล็กทรอนิกส์ และจะต้องไม่ขัดต่อข้อจำกัดในการใช้ใบรับรองอิเล็กทรอนิกส์ที่ระบุไว้ในเอกสารฉบับนี้
- สถานะของใบรับรองอิเล็กทรอนิกส์ที่กำลังตรวจสอบ หากใบรับรองอิเล็กทรอนิกส์ถูกเพิกถอน คู่กรณีเกี่ยวข้องจะต้องปฏิเสธการใช้ใบรับรองอิเล็กทรอนิกส์ใบนั้นทันที

4.6. **การต่ออายุใบรับรองอิเล็กทรอนิกส์** (Certificate Renewal)

4.6.1. **กรณีในการขอต่ออายุใบรับรองอิเล็กทรอนิกส์** (Circumstance for Certificate Renewal)

ปัจจุบันผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีนโยบายในการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการโดยไม่มีการเปลี่ยนแปลงกุญแจสาธารณะของผู้ใช้บริการ หรือข้อมูลอื่นใดที่ปรากฏในใบรับรองอิเล็กทรอนิกส์

หากมีใบรับรองอิเล็กทรอนิกส์ที่กำลังจะหมดอายุลงใน 30 วันข้างหน้า ระบบจะส่งจดหมายอิเล็กทรอนิกส์แจ้งเตือนไปยังผู้ใช้บริการให้รับทราบ เพื่อให้ผู้ใช้บริการดำเนินการขอใบรับรองใหม่แทนใบรับรองเดิมที่ใกล้หมดอายุ ตามข้อ 4.1

4.6.2. **ผู้ที่สามารถขอต่อใบรับรองอิเล็กทรอนิกส์** (Who May Request Renewal)

ไม่มีบริการ

4.6.3. **กระบวนการขอต่อใบรับรองอิเล็กทรอนิกส์** (Processing Certificate Renewal Request)

ไม่มีบริการ

4.6.4. **วิธีการแจ้งต่อใบรับรองอิเล็กทรอนิกส์กับ** Subordinate CA (Notification of New Certificate Issuance to Subscriber)

ไม่มีบริการ

4.6.5. **วิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ได้มีการต่ออายุ** (Conduct Constituting Acceptance of a Renewal Certificate)

ไม่มีบริการ

4.6.6.**การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้มีการต่ออายุ** (Publication of the Renewal Certificate by the CA)

ไม่มีบริการ

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

ไม่มีบริการ

4.7. **การรับรองกุญแจคู่ใหม่** (Certificate Re-Key)

4.7.1. **กรณีที่อนุญาตให้มีการรับรองกุญแจคู่ใหม่** (Circumstance for Certificate Re-Key)

ก่อนที่ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการใบเดิมจะหมดอายุ ผู้ใช้บริการหรือผู้มีอำนาจแทนผู้ใช้งานสามารถติดต่อผู้ให้บริการ โดยมีกระบวนการเช่นเดียวกับการยื่นขอใบรับรองอิเล็กทรอนิกส์ใหม่ ตามข้อ 4.1

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

อ้างอิงตามข้อ 4.1

4.7.3. **กระบวนการขอรับรองกุญแจคู่ใหม่** (Processing Certificate Re-keying Requests)

อ้างอิงตามข้อ 4.1

4.7.4. **วิธีการแจ้งเตือนการออกใบรับรองอิเล็กทรอนิกส์ใหม่แก่ผู้ใช้บริการ** (Notification of New Certificate Issuance to Subscriber)

อ้างอิงตามข้อ 4.3 และ 4.4

4.7.5. **การยอมรับใบรับรองอิเล็กทรอนิกส์ที่ได้มีการรับรองกุญแจคู่ใหม่** (Conduct Constituting Acceptance of a Re-keyed Certificate)

อ้างอิงตามข้อ 4.3 และ 4.4

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

อ้างอิงตามข้อ 4.3 และ 4.4

4.7.7. **การแจ้งไปยังหน่วยงานที่เกี่ยวข้องเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์ที่ได้มีการรับรองกุญแจคู่ใหม่โดยผู้ให้บริการออกใบรับรอง** (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** (Circumstance for Certificate Modification)

การเปลี่ยนแปลงข้อมูลใบรับรองอิเล็กทรอนิกส์เป็นการออกใบรับรองอิเล็กทรอนิกส์ใบใหม่ เนื่องจากมีการเปลี่ยนแปลงข้อมูลในใบรับรองอิเล็กทรอนิกส์ ทั้งนี้ต้องทำการยื่นเอกสารเพื่อขอยกเลิกใบเดิม 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

4.8.7. **การแจ้งเตือนไปยังหน่วยงานที่เกี่ยวข้องโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์** (Notification of Certificate Issuance by the CA to Other Entities)

อ้างอิงตามข้อ 4.3 และ 4.4

4.9. **การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์** (Certificate Revocation and Suspension)

สำหรับบริการการเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์นั้น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะดำเนินการก็ต่อเมื่อได้รับคำขอยกเลิกหรือพักใช้ใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการ และเจ้าหน้าที่ได้ตรวจสอบเอกสารดังกล่าวเรียบร้อยแล้ว หรือได้รับคำสั่งโดยชอบด้วยกฎหมายให้ดำเนินการดังกล่าว

4.9.1. **เหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์** (Circumstances for Revocation)

การเพิกถอนใบรับรองให้ทำได้ดังกรณีต่อไปนี้

- การเพิกถอนโดยผู้ใช้บริการ

ผู้ใช้บริการจะต้องขอเพิกถอนใบรับรองทันทีเมื่อมีเหตุการณ์ดังต่อไปนี้

1) มีผู้อื่นล่วงรู้กุญแจส่วนตัวของผู้ใช้บริการหรือผู้อื่นสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ใช้บริการไปใช้งาน
2) มีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ใช้บริการ
3) อุปกรณ์ที่ใช้ในการเก็บกุญแจส่วนตัวสูญหายหรือไม่สามารถใช้งานได้
4) มีเหตุอื่นใดที่อาจจะทำให้ผู้อื่นนำใบรับรองไปใช้โดยไม่มีสิทธิ
5) ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลที่อยู่ในใบรับรอง เช่น ชื่อหรือนามสกุล เป็นต้น
6) ผู้ใช้บริการระงับหรือยกเลิกการใช้บริการ

- การเพิกถอนโดยผู้ให้บริการ

1) ผู้ใช้บริการไม่ได้ชำระค่าบริการ
2) ผู้ใช้บริการไม่ปฏิบัติตามนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์ และแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ หรือไม่ปฏิบัติตามกฎระเบียบของหน่วยงานของผู้ให้บริการ
3) มีผู้อื่นล่วงรู้กุญแจส่วนตัวของผู้ให้บริการ
4) มีคำสั่งของศาลหรือต้องดำเนินการตามกฎหมาย
5) ผู้ให้บริการ ระงับหรือยกเลิกการให้บริการ
6) กรณีอื่น ๆ ที่ผู้ให้บริการ พิจารณาแล้วว่าจะมีผลกระทบต่อความมั่นคงปลอดภัยของการให้บริการใบรับรอง

4.9.2. **ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้** (Who can Request Revocation)

ผู้มีอำนาจหรือผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ ทั้งนี้ผู้ให้บริการสามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้เช่นกัน หากตรงตามเงื่อนไขที่ระบุไว้ในข้อ 4.9.1

4.9.3. **ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์** (Procedure for Revocation Request)

1. ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์กรอกใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์ พร้อมทั้งลงลายมือชื่อกำกับ

2. ส่งใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐานประกอบให้เจ้าหน้าที่รับลงทะเบียน โดยหลักฐานมีดังต่อไปนี้

- กรณีสมัครในนามบุคคล ใช้สำเนาบัตรประชาชนของผู้ใช้บริการ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

- กรณีสมัครในนามนิติบุคคล ใช้สำเนาหนังสือรับรองการเป็นนิติบุคคล ที่มีอายุไม่เกิน 90 วัน พร้อมลงลายมือชื่อรับรองสำเนาถูกต้องโดยกรรมการผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท (ถ้ามี) และสำเนาบัตรประชาชนของกรรมการผู้มีอำนาจ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

- กรณีกรรมการผู้มีอำนาจมอบอำนาจให้ผู้อื่นมาดำเนินการแทน ให้กรอกชื่อผู้รับมอบอำนาจลงในใบคำขอ พร้อมปิดอากรแสตมป์ 10 บาท และเพิ่มสำเนาบัตรประชาชนของผู้รับมอบอำนาจ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

3. เจ้าหน้าที่รับลงทะเบียนตรวจสอบใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐาน

4. หลังจากเจ้าหน้าที่รับลงทะเบียนตรวจสอบใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐานเรียบร้อย เจ้าหน้าที่รับลงทะเบียนจึงจะเพิกถอนใบรับรองอิเล็กทรอนิกส์

4.9.4. **ระยะเวลาที่ใช้ในการเพิกถอนใบรับรองอิเล็กทรอนิกส์** (Revocation Request Grace Period)

หลังจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้รับใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์ และได้ตรวจสอบความถูกต้องของใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์ และเอกสารประกอบแล้ว โดยปกติผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะเพิกถอนใบรับรองอิเล็กทรอนิกส์ในทันที

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

อ้างอิงตามข้อ 4.9.4

4.9.6. **ตรวจสถานะเพิกถอนของใบรับรองอิเล็กทรอนิกส์ โดยหน่วยงานที่เกี่ยวข้อง** (Revocation Checking Requirement for Relying Parties)

ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าไปตรวจสอบ CRL ได้ที่

http://crl.ca.tot.co.th/totca.crl

4.9.7. **ความถี่ในการอัพเดตรายการเพิกถอนใบรับรอง** (CRL Issuance Frequency)

ผู้ให้บริการจะทำการอัพเดตรายการเพิกถอนใบรับรองทุก 1 ชั่วโมง หรือเมื่อมีการเพิกถอนใบรับรอง

4.9.8. **ระยะเวลาที่ใช้ในขั้นตอนการประกาศรายการเพิกถอนใบรับรอง** (Maximum Latency for CRLs)

ผู้ให้บริการจะทำการเพิกถอนใบรับรอง ประกาศไว้ในที่เว็บไซต์ของผู้ให้บริการโดยเร็วหลังจากที่ได้สร้างรายการ

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

ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าไปตรวจสอบ OCSP ได้ที่

http://ocsp.ca.tot.co.th:8080/ejbca/publicweb/status/ocsp

4.9.10. **ความต้องการตรวจสอบการเพิกถอนใบรับรองอิเล็กทรอนิกส์แบบออนไลน์** (On-line Revocation Checking Requirements)

อ้างอิงตามข้อ 4.9.9

4.9.11. **การประกาศสถานะการเพิกถอนใบรับรองอิเล็กทรอนิกส์ในรูปแบบอื่น** (Other Forms of Revocation Advertisements Available)

ระบบให้บริการของ ผู้ให้บริการ ไม่รองรับการประกาศรายการเพิกถอนใบรับรองในรูปแบบอื่น นอกเหนือจากการประกาศไว้ในรายการเพิกถอนใบรับรอง ซึ่งปรากฏอยู่ในเว็บไซต์ของผู้ให้บริการ

4.9.12. **ความต้องการพิเศษกรณีที่มีการขอให้รับรองกุญแจคู่ใหม่เมื่อกุญแจเสียหาย** (Special Requirements Regarding Key Compromise)

หากผู้ใช้บริการตรวจพบว่ากุญแจส่วนตัวได้ถูกโจรกรรม ถูกล่วงรู้ ถูกเข้าถึงหรือไม่สามารถใช้งานได้ ให้ผู้ใช้บริการดำเนินการเพื่อขอเพิกถอนใบรับรองตามกระบวนการดังกล่าวแล้วข้างต้น การเพิกถอนใบรับรองดังกล่าวให้ถือว่าเป็นการยกเลิกการใช้งานกุญแจคู่นั้นด้วย

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/หรือ คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้ทางเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือสามารถโทรมาสอบถามได้ที่หน่วยงานรับลงทะเบียน

4.10.1. **ลักษณะของบริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์** (Operational Characteristics)

ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าไปตรวจสอบ CRL ได้ที่ http://crl.ca.tot.co.th/totca.crl

และสามารถเข้าไปตรวจสอบ OCSP ได้ที่ http://ocsp.ca.tot.co.th:8080/ejbca/publicweb/status/ocsp

4.10.2. **สภาพพร้อมใช้งานของระบบบริการ** (Service Availability)

บริการเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์จะสามารถใช้บริการได้อย่างต่อเนื่องตลอด 24x7 อย่างน้อย 99% ยกเว้นในกรณีที่มีการปรับปรุงระบบให้บริการ หรือเมื่อระบบมีปัญหา จะมีการแจ้งผ่านหน้าเว็บไซต์/แจ้งผู้ใช้บริการที่สอบถามโดยตรง และมีการสำรองข้อมูล (Backup) ไว้แล้ว พร้อมนำข้อมูลที่สำรองไว้มาใช้เมื่อระบบขัดข้อง

4.10.3. **ความสามารถอื่น ๆ** (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 การบริหารจัดการและดำเนินงาน** (Facility, Management, and Operational Controls)

5.1. **การควบคุมความปลอดภัยด้านกายภาพ** (Physical Controls)

5.1.1. **สถานที่ตั้ง** (Site Location and Construction)

สถานที่ตั้งของหน่วยงานออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรอง อิเล็กทรอนิกส์ตั้งอยู่ที่ บริษัท ทีโอที จำกัด (มหาชน) เลขที่ 89/2 หมู่ 3 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กทม. 10210 ซึ่งมีการปฏิบัติงานในสิ่งแวดล้อมที่มีความปลอดภัยตามมาตรฐาน ISO27001 (Information Security Management System : ISMS) เพื่อประโยชน์ ในการรักษาความปลอดภัยทางด้านกายภาพของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ผู้ ให้บริการใบรับรองอิเล็กทรอนิกส์จึงได้ติดตั้งอุปกรณ์รักษาความปลอดภัย ณ สถานที่ตั้งของ ระบบให้บริการใบรับรองอิเล็กทรอนิกส์ดังนี้

การรักษาความมั่นคงและปลอดภัยทางด้านกายภาพของระบบผู้ให้บริการได้ติดตั้งอุปกรณ์รักษาความมั่นคงและปลอดภัย ณ สถานที่ตั้งของระบบให้บริการ ดังนี้

1) โทรทัศน์วงจรปิด เพื่อประโยชน์ในการบันทึกภาพเหตุการณ์ภายในสถานที่ตั้ง
2) Door Hold Open Sounder ซึ่งจะส่งเสียงร้อนเตือนมีการเปิดประตูทิ้งค้างไว้เพื่อความมั่นคงและปลอดภัยของสถานที่ตั้ง
3) ระบบ Motion Detection เพื่อตรวจจับความเคลื่อนไหวเมื่อมีการบุกรุกหรือลักลอบเข้าในระบบ
4) ระบบ Smart Card Access Control ซึ่งเป็นระบบการควบคุมการเปิดใช้ประตูด้วยบัตร Smart Card พร้อมกำหนดรหัสผ่าน
5) ระบบ Smoke Detector เพื่อตรวจจับควันไฟ
6) อุปกรณ์ดับเพลิงแบบ FM-200 ซึ่งมี (ก๊าซ) สารดับเพลิงที่ไม่ก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์
7) อุปกรณ์ตรวจสอบความถี่ เพื่อส่งสัญญาณเตือนภัยเมื่อกระจกประตูหรือหน้าต่างแตก

5.1.2. **การเข้าถึงทางกายภาพ** (Physical Access)

การเข้าถึงหรือเข้าออกพื้นที่ซึ่งติดตั้งระบบให้บริการใบรับรองนั้นเฉพาะเจ้าหน้าที่ของผู้ให้บริการหรือเจ้าหน้าที่ที่ได้รับมอบหมายจาก ผู้ให้บริการเท่านั้น ที่มีสิทธิเข้าถึงหรือเข้าออกบริเวณพื้นที่ซึ่งติดตั้งระบบ โดยควบคุมการเข้าถึงหรือเข้าออกด้วยอุปกรณ์อ่านสมาร์ตการ์ด (Smart Card Access Control) พร้อมการใช้รหัสผ่านด้วย

5.1.3. **ระบบไฟฟ้าและระบบปรับอากาศ** (Power and Air Conditioning)

ผู้ให้บริการ จัดให้มีเครื่องจ่ายไฟฟ้าที่ไม่ขาดตอนและเครื่องกำเนิดไฟฟ้าสำรอง เพื่อป้องกันการทำงานของระบบที่ไม่เป็นไปตามปกติในกรณีที่เกิดไฟฟ้าขัดข้อง พื้นที่ต่าง ๆ มีระบบการปรับอากาศเพื่อควบคุมความร้อนและความชื้นของห้องให้คงที่ โดยแยกออกมาจากระบบการปรับอากาศในอาคาร

5.1.4. **การป้องกันภัยจากน้ำ** (Water Exposures)

ผู้ให้บริการ จัดให้มีสภาพแวดล้อมที่เหมาะสมเพื่อป้องกันภัยจากน้ำอันก่อให้เกิดความเสียหายกับระบบให้บริการ

5.1.5. **การป้องกันภัยอัคคีภัย** (Fire Prevention and Protection)

บริเวณพื้นที่ซึ่งติดตั้งและจัดวางอุปกรณ์ระบบการให้บริการใบรับรอง ได้มีการติดตั้งระบบดับเพลิงอัตโนมัติโดยใช้สารประเภท FM-200 ซึ่งมีคุณสมบัติพิเศษในการดับเพลิงได้อย่างรวดเร็วและมีประสิทธิภาพโดยไม่ก่อให้เกิดความเสียหายกับอุปกรณ์ประเภทไฟฟ้า อิเล็กทรอนิกส์หรือคอมพิวเตอร์ สารประเภท FM-200 จะทำงานเมื่ออุปกรณ์ตรวจจับควันไฟ (Smoke Detector) ตรวจพบควันไฟหรือพบอุณหภูมิสูงเกินกว่าปกติ

5.1.6. **การเก็บรักษาสื่อที่ใช้เก็บข้อมูล** (Media Storage)

สื่อแม่เหล็กหรือสื่ออื่นซึ่งใช้ในการบันทึกข้อมูลและสำรองข้อมูลจะถูกจัดเก็บไว้อย่างปลอดภัย

5.1.7. **การกำจัดสิ่งที่ไม่ใช้** (Waste Disposal)

สื่อแม่เหล็กหรือสื่ออื่นซึ่งใช้ในการบันทึกหรือเก็บข้อมูลที่ไม่ใช้อีกต่อไป จะถูกกำจัดหรือ ทำลาย เพื่อไม่ให้มีการนำสื่อข้างต้นกลับมาใช้หรือเรียกค้นข้อมูลได้อีก ทั้งนี้ การทำลายสื่อแม่เหล็ก หมายถึงรวมถึงการเขียนข้อมูลใหม่ทับ (Overwrite) การทำลายด้วยสนามแม่เหล็ก (Degauss) หรือการทำลายทิ้ง (Destruct) ด้วย

5.1.8. **การสำรองข้อมูลไว้ที่อื่น** (Off-site backup)

ได้สำรองข้อมูลที่สำคัญไว้ภายนอกสถานที่ปฏิบัติงานตามปกติ ซึ่งสำรองข้อมูลที่ Information Data Center ที่ บริษัท ทีโอที จำกัด(มหาชน) สาขากรุงเกษม เพื่อป้องกันการสูญหายของข้อมูลต่าง ๆ ที่สำคัญในกรณีที่เกิดเหตุฉุกเฉิน ซึ่งมีการรักษาความมั่นคงและปลอดภัยทางด้านกายภาพ ตรงตามข้อ 5.1.1

5.2.**การควบคุมความปลอดภัยในการดำเนินงาน** (Procedural Controls)

5.2.1. **บทบาทที่น่าเชื่อถือ** (Trusted Roles)

ความไว้วางใจได้รับการกำหนดขึ้นโดยผู้ให้บริการ เพื่อรักษาการแบ่งแยกหน้าที่ต่าง ๆ ให้มีอยู่เพื่อรับประกันว่าไม่มีบุคคลใดที่สามารถทำการแก้ไขดัดแปลงและบันทึกเรื่องราวต่าง ๆ ของ ผู้ให้บริการ

บทบาทต่อไปนี้ได้กำหนดขึ้นสำหรับการดำเนินงานเกี่ยวกับโครงสร้างของ ผู้ให้บริการ:

- พนักงาน CA Operations
- เจ้าหน้าที่รักษาความมั่นคงและปลอดภัยในสถานที่
- ผู้จัดการด้านการรักษาความมั่นคงและปลอดภัยในส่วนของเทคโนโลยีสารสนเทศ

วิธีการดำเนินการเพื่อรักษาการแบ่งแยกหน้าที่ต่าง ๆ ให้มีอยู่นั้น ได้มีการให้คำจำกัดความไว้ในแผนการรักษาความมั่นคงและปลอดภัยของผู้ให้บริการ ซึ่งไม่มีการนำมาเปิดเผยต่อสาธารณะ

5.2.2. **จำนวนบุคลากรที่ใช้ในการดำเนินงานที่ต้องการความมั่นคงปลอดภัยสูง** (Number of Persons Required Per Task)

ในแต่ละบทบาทหน้าที่ที่ระบุไว้ข้างต้นจะได้รับการดำเนินงานโดยแต่ละบุคคลที่แยกกัน เพื่อให้การรักษาความมั่นคงและปลอดภัยในระดับสูงสุด งานใด ๆ ที่เกี่ยวกับการแก้ไของค์ประกอบทางอิเล็กทรอนิกส์หรือทางกายภาพของโครงสร้างผู้ให้บริการนั้น จะต้องมีบุคลากรที่ได้รับความเชื่อถือ 2 ราย ในกรณีที่มีบุคลากรเพียง 1 คนที่กำลังปฏิบัติงานตามจริง อีกคนหนึ่งจะรับหน้าที่ในการตรวจสอบติดตามความคืบหน้า

5.2.3. **การระบุและพิสูจน์ความเป็นตัวตนแท้จริงของเจ้าหน้าที่ในแต่ละบทบาท** (Identification and Authentication for Each Role)

ผู้ให้บริการ และ เจ้าหน้าที่รับลงทะเบียน จะระบุตัวบุคคลอย่างเป็นทางการที่จะปฏิบัติหน้าที่ในบทบาทที่ได้รับ

5.2.4. **บทบาทที่ต้องการแบ่งแยกหน้าที่ความรับผิดชอบ** (Roles Requiring Separation of Duties)

บทบาทที่ต้องการการแบ่งแยกหน้าที่ความรับผิดชอบ ประกอบด้วย

- เจ้าหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ มีหน้าที่หลัก ในการดูแลบริหารจัดการระบบให้บริการใบรับรองอิเล็กทรอนิกส์ และ ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้อง ได้แก่ Database, Firewall, LDAP และการสำรองข้อมูลระบบ

- เจ้าหน้าที่รับลงทะเบียน มีหน้าที่หลักในการตรวจสอบความถูกต้องของใบคำขอใบรับรองอิเล็กทรอนิกส์ และพิจารณาตรวจสอบเอกสารหลักฐานประกอบการขอใบรับรองอิเล็กทรอนิกส์และดำเนินการออกใบรับรองอิเล็กทรอนิกส์ รวมถึงดำเนินการ พักใช้ใบรับรองอิเล็กทรอนิกส์และ เพิกถอนใบรับรองอิเล็กทรอนิกส์

5.3. **การควบคุมความปลอดภัยทางด้านบุคลากร** (Personnel Controls)

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

ผู้ให้บริการ และบุคลากรของผู้ให้บริการ จะคัดเลือกพนักงานที่มีความรู้ความสามารถ มีความเหมาะสมในการปฏิบัติงานที่เกี่ยวข้อง จะต้องมีคุณสมบัติ ประสบการณ์และข้อกำหนดประวัติเพื่อปฏิบัติหน้าที่ต่าง ๆ ที่จะดำเนินการตามนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์นี้

5.3.2. **กระบวนการตรวจสอบประวัติ** (Background Check Procedures)

ฝ่ายทรัพยากรบุคคลจะทำการตรวจสอบประวัติ เช่น บัตรประจำตัวประชาชน ทะเบียนบ้านประกาศนียบัตรการศึกษาสูงสุด ประวัติอาชญากรรม ใบรับรองวิชาชีพ (ถ้ามี) หนังสือรับรองการทำงานก่อนหน้านี้ เพื่อการรักษาความมั่นคงและปลอดภัย ทั้งนี้เพื่อรับประกันถึงความถูกต้องและความสามารถของพวกเขาในการดำเนินบทบาทหน้าที่ที่ได้รับความเชื่อถือภายในโครงสร้างของผู้ให้บริการ การตรวจสอบประวัติความเป็นมาเหล่านี้จะมีการดำเนินการโดยบุคคลที่สามที่มีความเชี่ยวชาญในงานดังกล่าว

5.3.3. **การฝึกอบรมบุคลากร** (Training Requirements)

เจ้าหน้าที่ของผู้ให้บริการ จะได้รับการฝึกอบรมอย่างเหมาะสมและเพียงพอเกี่ยวกับการบริหารจัดการระบบบริการใบรับรองอิเล็กทรอนิกส์ ซึ่งมีเนื้อหาหลักสูตรดังนี้

1) ความรู้เกี่ยวกับเทคโนโลยี PKI
2) การใช้งานระบบบริการใบรับรองอิเล็กทรอนิกส์
3) การตระหนักถึงการรักษาความมั่นคงและปลอดภัยของระบบคอมพิวเตอร์และวิธีการต่าง ๆ
4) ความสามารถในการทำให้ระบบสามารถทำงานได้อย่างต่อเนื่อง การสำรองข้อมูลและการเรียกคืนข้อมูล
5) ความรู้เกี่ยวกับการใช้งาน hardware และ software ที่เกี่ยวข้องในระบบ
6) ความหมายและประสิทธิภาพของแนวนโยบายการให้บริการใบรับรองอิเล็กทรอนิกส์และแนว ปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์

5.3.4. **ความถี่ในการฝึกอบรมบุคลากร** (Retraining Frequency and Requirements)

เจ้าหน้าที่จะได้รับการอบรมเกี่ยวกับการเปลี่ยนแปลง หน้าที่ ความรับผิดชอบ ต่าง ๆ เป็นประจำทุกปี และอบรมเพิ่มเติม เมื่อมีเทคโนโลยีใหม่ๆ ที่เกี่ยวข้องกับการทำงาน

5.3.5. **ความถี่ในการโอนย้ายหน้าที่** (Job Rotation Frequency and Sequence)

บุคลากรฝ่ายดำเนินงานของผู้ให้บริการทุกคนจะเข้าร่วมโครงการการจัดอบรมซึ่งกันและกัน เพื่อให้พนักงานสามารถปฏิบัติหน้าที่แทนพนักงานที่ลาออกจากผู้ให้บริการ หรือไม่มาปฏิบัติงานด้วยเหตุผลใด ๆ ก็ตามได้

5.3.6. **บทลงโทษสำหรับการละเมิดสิทธิ์** (Sanction for Unauthorized Action)

บุคคลที่ดำเนินการโดยไม่ได้รับอนุญาตจะเป็นไปตามกระบวนการทางวินัยหรือทางกฎหมาย โดยการดำเนินการของผู้ให้บริการ ในกรณีที่มีความร้ายแรง ผู้กระทำผิดจะถูกดำเนินคดีสำหรับการกระทำของพวกเขา

5.3.7. **ผู้รับดำเนินการภายนอก** (Independent Contractor Requirements)

ในบ้างครั้ง ผู้รับดำเนินการภายนอกหรือที่ปรึกษาภายนอกอาจได้รับสิทธิ์ให้ดำเนินการในตำแหน่งซึ่งต้องการความน่าเชื่อถือ อย่างไรก็ตาม บุคคลดังกล่าวจะอยู่ภายใต้บรรทัดฐานด้านความมั่นคงปลอดภัยเทียบเท่ากับเจ้าหน้าที่ของผู้ให้บริการ ส่วนผู้รับดำเนินการภายนอกหรือที่ปรึกษาภายนอกที่ยังไม่ผ่านเกณฑ์การตรวจสอบประวัติตามข้อ 5.3.2 จะได้รับอนุญาตให้เข้าถึงระบบการให้บริการใบรับรองอิเล็กทรอนิกส์ ได้เฉพาะขอบเขตที่กำหนดและจำเป็นต้องมีเจ้าหน้าที่คอยติดตามขณะปฏิบัติงานด้วย

5.3.8. **เอกสารประกอบสำหรับบุคลากร** (Documentation Supplied to Personnel)

บุคลากรของผู้ให้บริการ สามารถเรียกดูเอกสารประกอบต่าง ๆ เกี่ยวกับระบบให้บริการ อุปกรณ์ ฮาร์ดแวร์ ซอฟแวร์ และคู่มือการใช้ระบบงานต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติงาน สำหรับผู้ใช้บริการนั้น สามารถเรียกดูคู่มือการใช้งานสำหรับผู้ใช้บริการได้ ทั้งนี้ขึ้นอยู่กับประเภทของบริการและข้อตกลงการใช้บริการด้วย

5.4. **กระบวนการบันทึกเหตุการณ์** (Audit Logging Procedures)

5.4.1. **ข้อมูลที่เก็บบันทึก** (Types of Events Recorded)

TOT CA จะทำการบันทึกเหตุการณ์ต่าง ๆ แบบอัตโนมัติหรือโดยบุคคลตามความสำคัญของเหตุการณ์ ดังนี้

1) การบันทึกเหตุการณ์เกี่ยวกับวงจรการใช้งานกุญแจของ TOT CA
   - การสร้างกุญแจ การสำรอง การจัดเก็บ การกู้คืน การบันทึกข้อมูล และการทำลาย
   - การจัดการอุปกรณ์การเข้ารหัสลับ
2) การบันทึกเหตุการณ์ของกุญแจผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ ผู้ขอใช้ใบรับรองอิเล็กทรอนิกส์
   - แบบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ แบบคำขอต่ออายุใบรับรองอิเล็กทรอนิกส์ แบบคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์
   - การอนุมัติหรือไม่อนุมัติแบบคำขอ
   - การออกใบรับรองอิเล็กทรอนิกส์และรายการเพิกถอนใบรับรอง
3) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
   - การเข้าถึงระบบ TOT CA ที่สำเร็จและไม่สำเร็จ
   - กิจกรรมเกี่ยวกับความมั่นคงปลอดภัยที่กระทำโดยเจ้าหน้าที่ TOT CA
   - การอ่าน – เขียน – ลบ ไฟล์ที่มีความสำคัญ
   - การเปลี่ยนแปลงการตั้งค่าความมั่นคงปลอดภัยของระบบ
   - ปัญหาของระบบ อุปกรณ์ฮาร์ดแวร์ และความผิดปกติอื่น ๆ
   - การทำงานของอุปกรณ์เครือข่ายและไฟร์วอลล์
   - การเยี่ยมชมระบบโดยบุคคลภายนอก

บันทึกเหตุการณ์แต่ละรายการ ประกอบด้วยข้อมูลดังกล่าว

- วันที่และเวลาของแต่ละรายการ
- ลำดับรายการ โดยบันทึกอัตโนมัติ

- ผู้ดำเนินการ
- ประเภทของเหตุการณ์

5.4.2. **ความถี่ในการประมวลผลข้อมูลการลงบันทึกเหตุการณ์** (Frequency of Processing Log)

เจ้าหน้าที่ดูแลระบบจะเข้ามาตรวจสอบข้อมูลการลงบันทึกเหตุการณ์อย่างสม่ำเสมอ อย่างน้อยวันละ 1 ครั้ง

5.4.3. **ระยะเวลาที่จะเก็บข้อมูลการลงบันทึกเหตุการณ์** (Retention Period for Audit Log)

ข้อมูลการลงบันทึกเหตุการณ์ต่าง ๆ จะถูกเก็บไว้เป็นเวลาอย่างน้อย 6 เดือน หรือมากกว่านั้นหากเป็นไปตามกฎหมาย

5.4.4. **การป้องกันข้อมูลการลงบันทึกเหตุการณ์** (Protection of Audit Log)

การจัดเก็บข้อมูลการลงบันทึกเหตุการณ์ต่างๆ ไว้บนเครื่องให้บริการสำหรับบันทึกเหตุการณ์ (Log Server) ซึ่งจะมีแต่เจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงและอ่านข้อมูลได้

5.4.5. **ขั้นตอนการสำรองเก็บข้อมูลการลงบันทึกเหตุการณ์** (Audit Log Backup Procedure)

ข้อมูลการลงบันทึกเหตุการณ์ต่าง ๆ จะได้รับการบันทึกลงเทปในลักษณะการสำรองเพิ่มเติม (Incremental Backup) วันละ 1 ครั้ง และการสำรองแบบสมบูรณ์ (Full Backup) สัปดาห์ละ 1 ครั้ง และเดือนละ 1 ครั้ง

5.4.6. **ระบบการเก็บข้อมูลการลงบันทึกเหตุการณ์** (Audit Collection System (Internal VS External))

บันทึกเหตุการณ์ต่าง ๆ สามารถแบ่งได้เป็นแบบอัตโนมัติ (Automatic) และโดยบุคคล (Manual)

5.4.7. **การแจ้งไปยังบุคคลที่เกี่ยวข้อง** (Notification to Event-Causing Subject)

เจ้าหน้าที่ดูแลระบบ จะคอยตรวจสอบบันทึกเหตุการณ์ (Log Event) วันละ 1 ครั้ง เพื่อให้ทราบถึงเหตุการณ์ที่ไม่ปกติเกี่ยวกับความมั่นคงและปลอดภัยของระบบ ทำให้สามารถรองรับและแก้ไขสถานการณ์ได้ทันท่วงที ทั้งนี้หากเหตุการณ์ที่ไม่ปกติจากภายนอกระบบ จะมีการแจ้งไปยังบุคคลที่เกี่ยวข้องด้วย

5.4.8. **การตรวจประเมินช่องโหว่ของระบบ** (Vulnerability Assessments)

การประเมินช่องโหว่ของระบบเป็นการดำเนินการเพื่อหาจุดอ่อนหรือช่องโหว่ของ ซึ่งจะถูกดำเนินการแบบอัตโนมัติเดือนละครั้ง และโดยผู้ปฏิบัติงานจากภายนอกอย่างน้อยปีละครั้ง

5.5. **การเก็บบันทึกถาวรของข้อมูล** (Records Archival)

5.5.1. **ประเภทของข้อมูลที่ต้องการเก็บบันทึก** (Types of event recorded)

การเก็บบันทึกถาวรของข้อมูล มีดังนี้

- ข้อมูลการลงบันทึกเหตุการณ์ต่าง ๆ ตามข้อ 5.4
- ข้อมูลเกี่ยวกับการขอใบรับรองอิเล็กทรอนิกส์ และเอกสารต่าง ๆ ที่เกี่ยวข้อง
- ข้อมูลเกี่ยวกับวงจรการใช้ใบรับรองอิเล็กทรอนิกส์ ได้แก่ การเพิกถอนใบรับรองอิเล็กทรอนิกส์ การต่ออายุใบรับรองอิเล็กทรอนิกส์

5.5.2. **ช่วงเวลาในการเก็บรักษาข้อมูล** (Retention Period for Archive)

ข้อมูลต่าง ๆ จะถูกเก็บต่อไปอย่างน้อย อีก 5 ปี หลังจากที่ใบรับรองอิเล็กทรอนิกส์นั้นหมดอายุหรือถูกเพิกถอน

5.5.3. **การป้องกันบันทึกถาวรของข้อมูล** (Protection of Archive)

การป้องกันการเข้าถึงข้อมูลที่ได้ทำการสำรองไว้เพื่อให้บุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลนั้นได้ สำหรับข้อมูลในรูปแบบอิเล็กทรอนิกส์จะได้รับการบันทึกไว้บนเครื่องให้บริการและเทป โดยจะนำเทปดังกล่าวไปเก็บรักษาไว้ในสถานที่ที่ความปลอดภัยสูงและสามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น

ส่วนข้อมูลในรูปแบบเอกสารจะได้รับการจัดเก็บไว้ในสถานที่ที่มีความปลอดภัยสูงและสามารถเข้าถึงได้จากเฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้นเช่นกัน

5.5.4. **กระบวนการในการสำรองบันทึกถาวรของข้อมูล** (Archive Backup Procedure)

ในแต่ละวัน ข้อมูลต่าง ๆ ทุกรายการในข้อ 5.5.1 จะได้รับการสำรองข้อมูลลงเทปสำรองข้อมูล

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 ซึ่งทำหน้าที่โดยระบบปฏิบัติการของเครื่องให้บริการของผู้ให้บริการ โปรแกรมประยุกต์ของผู้ให้บริการ และเจ้าหน้าที่ที่ได้รับมอบหมายของผู้ให้บริการ

5.5.7. **กระบวนการได้รับและตรวจสอบข้อมูลที่บันทึกถาวร** (Procedures to obtain and verify Archive Information)

เจ้าหน้าที่ ที่ได้รับสิทธิ์เท่านั้น ที่สามารถเข้าถึงข้อมูลที่บันทึกถาวรนี้ได้ ซึ่งความถูกต้องครบถ้วนของข้อมูลจะถูกตรวจสอบเมื่อข้อมูลเหล่านั้นถูกเรียกใช้

5.6. **การเปลี่ยนแปลงกุญแจ** (Key changeover)

เมื่อใบรับรองอิเล็กทรอนิกส์ ของ Root CA, Sub CA ใกล้จะหมดอายุ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะออกใบรับรองอิเล็กทรอนิกส์ใหม่ ก่อนที่ใบรับรองอิเล็กทรอนิกส์เดิมจะหมดอายุ อย่างน้อย 60 วัน และจะต้องไม่มีผลกระทบกับ Application ของผู้ใช้บริการ

5.7. **การรั่วไหลของข้อมูล และ การกู้คืนจากภัยพิบัติ** (Compromise and Disaster Recovery)

5.7.1. **กระบวนการรับมือกับเหตุละเมิดและการรั่วไหลของข้อมูล** (Incident and Compromise Handling Procedures)

ข้อมูลของระบบ จะได้รับการสำรองไว้ที่ศูนย์สำรองข้อมูล และจะถูกนำขึ้นมาใช้ ในกรณีเกิดเหตุฉุกเฉินหรือภัยพิบัติขึ้น

5.7.2. **ทรัพยากรที่ใช้ประมวลผล ซอฟต์แวร์ และ/หรือ ข้อมูลเกิดความผิดพลาด** (Computing Resources, Software, and/or Data Are Corrupted)

ในกรณีที่เกิดความผิดพลาดกับฮาร์ดแวร์ ซอฟต์แวร์ และ/หรือข้อมูล เหตุการณ์ดังกล่าวจะมีการรายงานไปยังผู้บริหาร ทีมงานหรือบุคคลที่เกี่ยวข้อง เพื่อรับมือกับเหตุการณ์ที่เกิดขึ้น โดยการประเมินสถานการณ์ การหาสาเหตุและเหตุละเมิด การตอบสนองต่อเหตุละเมิด การจัดทำแผนการกู้คืนระบบ และดำเนินการวางแผน

5.7.3. **กระบวนการจัดการเมื่อเกิดการรั่วไหลของกุญแจส่วนตัว** (Entity Private Key Compromise Procedures)

ในกรณีที่สงสัยหรือมีเหตุอันควรเชื่อว่ากุญแจส่วนตัวของผู้ให้บริการเกิดการรั่วไหล จะมีการนำกระบวนการรับมือเมื่อข้อมูลรั่วไหลมาใช้งาน และเหตุการณ์ดังกล่าวจะมีการรายงานไปยังผู้บริหาร ทีมงานหรือบุคคลที่เกี่ยวข้อง เพื่อรับมือกับเหตุการณ์ที่เกิดขึ้น โดยการประเมินสถานการณ์ การหาสาเหตุของเหตุละเมิด การตอบสนองของเหตุละเมิด การจัดทำแผนการกู้คืนระบบ และดำเนินการตามแผน หากเหตุละเมิดนั้นจำเป็นต้องมีการเพิกถอนใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ จะมีขั้นตอนการดำเนินการดังนี้

- สถานะของใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนจะได้รับการเผยแพร่ไปยังผู้ที่เกี่ยวข้องผ่านระบบไดเรกทอรีของผู้ให้บริการ
- จะมีการแจ้งไปยังผู้ที่ได้รับผลกระทบจากการเพิกถอนใบรับรองอิเล็กทรอนิกส์ให้รับทราบโดยเร็ว
- ผู้ให้บริการจะดำเนินการสร้างกุญแจคู่ใหม่ ยกเว้นในกรณีที่ผู้ให้บริการ จะยุติการให้บริการ

5.7.4. **ความต่อเนื่องของการให้บริการภายหลังจากเกิดภัยพิบัติ** (Business Continuity Capabilities after a Disaster)

ผู้ให้บริการได้จัดเตรียมแผนการดำเนินการกู้ระบบเมื่อเกิดภัยพิบัติ ซึ่งแผนดังกล่าวได้รับการทดสอบ ตรวจสอบและปรับปรุงอย่างต่อเนื่อง โดยเมื่อเกิดเหตุภัยพิบัติขึ้นกับระบบให้บริการหลักของผู้ให้บริการ แผนดังกล่าวจะต้องสามารถกู้คือข้อมูลอย่างเต็มรูปแบบได้ภายใน 15 วัน

ผู้ให้บริการได้เตรียมความพร้อมในการกู้คืนข้อมูลที่จำเป็นและสำคัญที่สุดให้ได้ภายใน 24 ชั่วโมง ซึ่งประกอบด้วยข้อมูลดังนี้

- ข้อมูลใบรับรองอิเล็กทรอนิกส์
- ข้อมูลใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน

5.8. **การยุติการให้บริการของผู้ให้บริการ** (CA or RA Termination)

เมื่อมีเหตุจำเป็นที่ทำให้ต้องมีการยุติการให้บริการของ บริการใบรับรองอิเล็กทรอนิกส์ จะมีการแจ้งเตือนผู้ใช้งานและผู้ที่เกี่ยวข้องทั้งหมด ซึ่งมีแผนการดำเนินการดังนี้

- แจ้งผู้ได้รับผลกระทบให้ทราบถึงสถานะของผู้ให้บริการ เช่น ผู้ใช้บริการ และผู้ที่เกี่ยวข้องทั้งหมด
- การเพิกถอนใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ
- การเก็บรักษาข้อมูลของผู้ใช้บริการตามช่วงเวลาที่เอกสารฉบับนี้กำหนด
- ความต่อเนื่องในการสนับสนุน/ตอบคำถามการให้บริการ
- ความต่อเนื่องในการบริการออกรายการเพิกถอนใบรับรอง
- การจัดการกับกุญแจส่วนตัวของผู้ให้บริการ และอุปกรณ์ฮาร์ดแวร์ที่เกี่ยวข้อง
- การดำเนินการเปลี่ยนผ่านบริการไปสู่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์รายใหม่

6. การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (TECHNICAL SECURITY CONTROLS)

6.1. การสร้างและติดตั้งกุญแจคู่ (Key Pair Generation and Installation)

6.1.1. การสร้างกุญแจคู่ (Key Pair Generation)

ผู้ให้บริการสร้างกุญแจคู่ของตน ขณะติดตั้งระบบให้บริการออกใบรับรอง โดยทำการสร้างและจัดเก็บกุญแจคู่ดังกล่าวไว้ใน Hardware Security Module (HSM) ซึ่งได้รับการรับรองตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 Level 3

6.1.2. การส่งกุญแจส่วนตัวไปให้ผู้ใช้บริการ (Private Key Delivery to Subscriber)

กุญแจส่วนตัวของผู้ใช้บริการจะถูกสร้างและจัดเก็บอยู่ในสื่ออิเล็กทรอนิกส์ USB Token หรือ Hardware Security Module (HSM) ซึ่งเป็นอุปกรณ์จัดเก็บรักษากุญแจส่วนตัวที่มีความปลอดภัยสูง ไม่สามารถคัดลอก กุญแจส่วนตัวและข้อมูลอื่นใดออกไปได้ โดยสื่ออิเล็กทรอนิกส์ดังกล่าว จะเก็บอยู่ที่ผู้ใช้บริการโดยตรง หรือ ในกรณีกุญแจส่วนตัวที่ถูกจัดเก็บในรูปของ File จะมีรหัสลับป้องกันการเข้าถึง

6.1.3. การส่งกุญแจสาธารณะให้กับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Public Key Delivery to Certificate Issuer)

กุญแจสาธารณะที่ถูกส่งมาให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์นั้น จะเป็นรูปแบบของไฟล์ PKCS#10 Certificate Signing Request (CSR) หรือถูกส่งมาทางเว็บไซต์ที่ได้มาตรฐานของ Secure Sockets Layer (SSL)

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

ในกรณีที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องประสงค์จะนำกุญแจสาธารณะของผู้ให้บริการ ซึ่งบันทึกไว้ในใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการ ไปใช้งาน สามารถเชื่อมต่อเข้าไปยังที่บันทึกข้อมูลของผู้ให้บริการ เพื่อนำกุญแจสาธารณะในใบรับรองอิเล็กทรอนิกส์ไปใช้งานได้

6.1.5. ขนาดของกุญแจ (Key Sizes)

ขนาดกุญแจของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะมีขนาด 4096 บิต ส่วนขนาดกุญแจของผู้ใช้บริการจะ มีขนาดอยู่ที่ 2048 บิต

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

ตัวแปรที่นำมาใช้เพื่อสร้างกุญแจสาธารณะนั้น ได้มีการกำหนดพารามิเตอร์ขึ้นโดยผู้ให้บริการ ซึ่งยึดตามมาตรฐาน X.509 Version 3 และคุณภาพของตัวแปรของกุญแจสาธารณะ จะถูกตรวจสอบโดยอัตโนมัติจากโปรแกรมในระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.1.7. **วัตถุประสงค์ของการนำกุญแจคู่ไปใช้** (Key Usage Purposes (As Per X.509 v3 Key Usage Field))

จุดประสงค์ของการใช้กุญแจได้ถูกอธิบายไว้ในหัวข้อ 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 ได้รับการรับรองตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 Level 3 ซึ่งเป็นมาตรฐานสากลในการสร้างและเก็บรักษากุญแจส่วนตัวขอระบบให้บริการใบรับรองอิเล็กทรอนิกส์

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

กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้มีการควบคุมการเข้าถึงแบบหลายบุคคล

6.2.3. **การกู้คืนกุญแจส่วนตัว** (Private Key Escrow)

ผู้ให้บริการไม่ได้จัดให้มีบริการสำหรับการกู้กุญแจส่วนตัวคืนเพื่อนำกับมาใช้ใหม่อีกครั้งเมื่อกุญแจส่วนตัวสูญหายหรือถูกล่วงรู้โดยวิธีการอื่นใด

6.2.4. **การสำรองกุญแจส่วนตัว** (Private Key Backup)

กุญแจส่วนตัวของผู้ให้บริการถูกบันทึกไว้ในอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความมั่นคงและปลอดภัยสูง

6.2.5. **การบันทึกถาวรกุญแจส่วนตัว** (Private Key Archival)

กุญแจส่วนตัวของผู้ให้บริการถูกบันทึกไว้ในอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความมั่นคงและปลอดภัยสูง

6.2.6. **การแปลงกุญแจส่วนตัวให้เป็น หรือ มาจากโมดูลการเข้ารหัส**(Private Key Transfer into or from a Cryptographic Module)

กุญแจส่วนตัวของ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้ถูกสร้างขึ้นภายในโมดูลที่มีรูปแบบของการเข้ารหัสและถอดรหัส ซึ่งได้รับการรับรองตามมาตรฐานสากล Federal Information Processing Standard (FIPS) 140-2 Level 3 และจะนำมาถอดรหัสก็ต่อเมื่อมีการตรวจสอบสิทธิ์ผ่านอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยสูงเช่นกัน และมีการใส่รหัสผ่านที่ถูกต้องโดยเจ้าหน้าที่ดูแลระบบให้บริการใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เท่านั้น

6.2.7. **การจัดเก็บกุญแจส่วนตัวลงบนโมดูลที่มีการเข้ารหัส** (Private Key Storage on Cryptographic Module)

กุญแจส่วนตัวของผู้ให้บริการ ถูกบันทึกไว้ในอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยสูง ในรูปแบบที่มีการเข้ารหัสลับไว้

6.2.8. **วิธีการใช้งานกุญแจส่วนตัว** (Method of Activating Private Key)

กุญแจส่วนตัวของ ผู้ให้บริการ จะถูกนำมาใช้งานได้เมื่อมีการตรวจสอบสิทธิผ่านอุปกรณ์จัดเก็บข้อมูลเป็นฮาร์ดแวร์ ที่มีมาตรฐานความมั่นคงและปลอดภัยสูงและมีการใส่รหัสผ่านที่ถูกต้องโดยเจ้าหน้าที่ดูแลระบบให้บริการใบรับรองของผู้ให้บริการ

6.2.9. **วิธีการยกเลิกการใช้งานกุญแจส่วนตัว** (Method of Deactivating Private Key)

กุญแจส่วนตัวจะเลิกใช้งานได้ก็ต่อเมื่อมีการร้องขอจากผู้ใช้บริการ ให้เพิกถอนการใช้งานกุญแจส่วนตัวนั้น โดยผู้ให้บริการจะตรวจสอบความถูกต้องของการร้องขอจากผู้ใช้บริการ จึงทำการเพิกถอนกุญแจส่วนตัวนั้นได้

6.2.10. **วิธีการทำลายกุญแจส่วนตัว** (Method of Destroying Private Key)

ในกรณีที่ผู้ใช้บริการต้องการทำลายกุญแจส่วนตัว ให้ใช้โปรแกรมประยุกต์ในการเขียนค่าทับกุญแจส่วนตัว (Overwriting the key) โดยผู้ให้บริการกระทำการเขียนค่าทับกุญแจส่วนตัวนั้น

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)

กุญแจสาธารณะจะถูกจัดเก็บบันทึกไว้ในใบรับรอง โดยใบรับรองได้ถูกจัดเก็บไว้ในฐานข้อมูลของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตลอดอายุของใบรับรอง

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

ระยะเวลาการใช้กุญแจส่วนตัวของผู้ให้บริการ คือ ยี่สิบ (20) ปี

ระยะเวลาการใช้กุญแจส่วนตัวของนายทะเบียน คือ สอง (2) ปี

6.4. ข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Activation Data)

6.4.1. การสร้างและการนำข้อมูลไปใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ (Activation Data Generation and Installation)

ข้อมูลที่ใช้ในการสร้างและติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ ถูกสร้างและจัดเก็บอย่างปลอดภัย และในกรณีที่ต้องการ activate การใช้งานใบรับรองอิเล็กทรอนิกส์ต้องติดต่อ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อตรวจสอบความเป็นเจ้าของของผู้ใช้ใบรับรอง หลังจากนั้นใบรับรองอิเล็กทรอนิกส์ดังกล่าวจึงจะถูก activate ผ่านระบบซอฟต์แวร์ CA และ update สถานะของใบรับรองอิเล็กทรอนิกส์ใน X.500 Directory

6.4.2. การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Activation Data Protection)

การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ จะเป็นไปตามกลไกการป้องกันข้อมูลด้วยอุปกรณ์ HSM ที่ได้มาตรฐาน FIPS 140-2 Level 3

6.4.3. ข้อมูลด้านอื่นที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ (Other Aspects of Activation Data)

ไม่มีข้อมูลอื่นใดนอกเหนือจากข้อมูลสำคัญที่ใช้ในการสมัครขอใบรับรองอิเล็กทรอนิกส์

6.5. การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)

6.5.1. ข้อกำหนดทางเทคนิคเกี่ยวกับการควบคุมความปลอดภัยของคอมพิวเตอร์ (Specific Computer Security Technical Requirements)

ผู้ให้บริการได้รวมข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน ISO 27001 (Information Security Management System : ISMS)

6.5.2. การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating)

ผู้ให้บริการได้แบ่งระดับในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน ISO 27001 (Information Security Management System : ISMS)

6.6. การควบคุมทางเทคนิคของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ (Lite Cycle Technical Controls)

6.6.1. การควบคุมการพัฒนาระบบ (System Development Controls)

การควบคุมและพัฒนาซอฟต์แวร์ที่นำมาใช้ในการพัฒนาซอฟต์แวร์ของผู้ให้บริการ ได้รับการพัฒนาตามหลักเกณฑ์ในการประเมินการรักษาความมั่นคงและปลอดภัยด้านข้อมูลตามข้อกำหนดของ Information Technology Security Evaluation Criteria Level E3 (ITSEC E3)

6.6.2. **การควบคุมการบริหารจัดการด้านความมั่นคงปลอดภัย** (Security Management Controls)

การจัดการในการรักษาความมั่นคงและปลอดภัยของระบบสำหรับผู้ให้บริการ และเจ้าหน้าที่รับลงทะเบียน นั้นจะถูกควบคุมให้เป็นไปตามข้อกำหนดมาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ ISO 27001 (Information Security Management System : ISMS)

6.6.3. **การควบคุมความมั่นคงปลอดภัยทางเทคนิค** (Life Cycle Security Controls)

ไม่มี

6.7. การควบคุมความปลอดภัยทางเครือข่าย (Network Security Controls)

ระบบการควบคุมทางเครือข่ายของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ได้ถูกออกแบบให้เป็นระบบเครือข่ายเฉพาะที่ใช้สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องเทานั้น โดยมิได้มีการเชื่อมต่อกับระบบเครือข่ายภายนอก และมีการติดตั้งทั้งฮาร์ดแวร์และซอฟต์แวร์ ไฟล์วอล (เจ้าหน้าที่ที่สามารถแก้ไข หรือ ตั้งค่าไฟล์วอลจะต้องเป็น IT Security Manager เท่านั้น) ในการป้องกันการบุกรุกจากการเข้าถึงภายนอก ระบบตรวจสอบและป้องกันผู้บุกรุก (Intrusion Protection System: IDS) และระบบป้องกันไวรัส (Anti-Virus)

6.8. การบันทึกเวลารายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน (Time-stamping)

ข้อมูลใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน จะมีข้อมูลวันที่ และเวลา ที่ถูกเพิกถอนกำกับลงไปด้วย

7. การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอนใบรับรองอิเล็กทรอนิกส์และโปรโตคอล OCSP (CERTIFICATE, CRL AND OCSP PROFILES)

7.1. รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)

7.1.1. เวอร์ชัน (Version Number(s))

ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้มาตรฐาน X.509 Version 3 Certificate ซึ่งมีรายการดังต่อไปนี้

- Version 3 : รุ่นที่ 3
- Serial Number : หมายเลขของใบรับรองอิเล็กทรอนิกส์
- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัล
- Issuer : ชื่อของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- Validity : วันเวลาที่เริ่มและสิ้นสุดการใช้ใบรับรองอิเล็กทรอนิกส์
- Subject : เลขบัตรประจำตัวประชาชนหรือเลขประจำตัวผู้เสียภาษีขององค์กร
- Subject Public Key Information : กญแจสาธารณะของผู้ใช้บริการและวิธีการที่ใช้ในการสร้าง

7.1.2. ข้อมูลเพิ่มเติมของใบรับรองอิเล็กทรอนิกส์ (Certificate Extensions)

ผู้ให้บริการสนับสนุนการใช้ใบรับรอง X.509 เวอร์ชั่น 3 ซึ่งใช้ข้อมูลเพิ่มเติมที่เป็นมาตรฐานของใบรับรองอิเล็กทรอนิกส์ต่อไปนี้

- Authority Key Identifier เป็นกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัว ที่ผู้ให้บริการออกใบรับรอง ใช้ในการลงลายมือชื่อดิจิตอลกำกับใบรับรองอิเล็กทรอนิกส์ เพื่อช่วยในการตรวจสอบลายมือชื่อ ดิจิตอลในใบรับรอง กรณีที่ผู้ให้บริการออกใบรับรองกุญแจหลายคู่

- Subject Key Identifier เป็นกุญแจสาธารณะในใบรับรองอิเล็กทรอนิกส์ ในกรณีที่ผู้ใช้งานใบรับรอง มีการเปลี่ยนคู่กุญแจการใช้งาน

- Key Usage เป็นวัตถุประสงค์ในการนำกุญแจไปใช้งาน

- CRL Distribution Points ระบุตำแหน่งที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง โดยอาจระบุเป็น URL (HTTP หรือ LDAP) เป็นต้น

7.1.3. อัลกอริทึมสำหรับการสร้างกุญแจคู่ (Algorithm object identifiers)

Algorithm ที่ใช้ในการออกใบรับรองอิเล็กทรอนิกส์คือ SHA-512 RSA

7.1.4. รูปแบบของชื่อ (Name Forms)

ใบรับรองที่ออกให้โดยผู้ให้บริการจะมีชื่อผู้ออกใบรับรอง และชื่อของผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์ (Subject) ซึ่งจะใช้รูปแบบของ Distinguished Name ตามมาตรฐาน X.500

7.1.5. **ข้อจำกัดเกี่ยวกับชื่อ** (Name Constraints)

ชื่อที่มีการปิดบังและการใช้ชื่อปลอมนั้นไม่สนับสนุนให้นำมาใช้ในใบรับรองอิเล็กทรอนิกส์

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)

การสร้าง Policy จะต้องมีการแสดง extension field ดังต่อไปนี้

- Authority Key Identifier
- Key Usage
- CRL Distribution Points
- Basic Constraints
- Certificate Policies
- Subject Alternative Name
- Authority Info Access
- Enhanced Key Usage

ทั้งนี้ขึ้นอยู่กับ Certificate Policy ด้วยว่าจะถูกกำหนดให้มี extension felid ตัวไหนบ้าง

7.1.8 **นโยบายในการระบุรูปแบบและความหมาย** (Policy qualifiers syntax and semantics)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้ระบุนโยบายในการระบุรูปแบบและความหมายของใบรับรองอิเล็กทรอนิกส์ ในหน้า เว็บไซต์ของ TOTCA หัวข้อ Certificate Policy

7.1.9 **การดำเนินการในส่วนของความหมายสำหรับนโยบายเพิ่มเติมของใบรับรองอิเล็กทรอนิกส์** (Processing semantics for the critical Certificate Policies extension)

การระบุ Critical extension ไว้ 2 ฟิลด์คือ Basic Constraints และ Key Usage

7.2. **รูปแบบของรายการเพิกถอนใบรับรอง** (CRL Profile)

7.2.1. **เวอร์ชัน** (Version Number(s))

ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ ทำรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดยทำตามมาตรฐาน X.509 เวอร์ชั่น 2 ซึ่งมีรายการดังต่อไปนี้

- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- Issuer : ชื่อของผู้ให้บริการที่ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- Effective date : วันเวลาที่ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์

- Next update : วันเวลาที่จะทำการปรับปรุงรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ ครั้งถัดไป

- CRL Number : หมายเลขของรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์

- Revocation List : รายการของใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน

7.2.2. **รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนและส่วนขยาย** (CRL and CRL Entry Extensions)

รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนจะถูกประกาศที่เว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยผู้ใช้บริการสามารถเข้ามา Download นำไปใช้งานได้

7.3. **รูปแบบของโปรโตคอล** OCSP (OCSP Profile)

OCSP หรือ Online Certificate Status Protocol คือ การตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ (Online)

7.3.1 **เลขรุ่น**(Version number(s))

การตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ (Online) โดยผู้ใช้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้มาตรฐาน X.509 OCSP Version 1

7.3.2 **ส่วนขยายของ** OCSP (OCSP extensions)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะทำการยืนยันตัวตนของ OCSP ที่ส่งกลับ (OCSP Response) ด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ (OCSP Signer)

8. **การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่าง ๆ และประเมินความเสี่ยงอื่น ๆ** (Compliance Audit and Other Assessment)

8.1. **ความถี่ในการตรวจประเมิน** (Frequency or Circumstances of Assessment)

ผู้ให้บริการจะจัดให้มีการตรวจสอบระบบให้บริการ เพื่อให้เป็นไปตามข้อกำหนดโดยละเอียดตามที่กำหนดในแนวปฏิบัติการให้บริการใบรับรองอิเล็กทรอนิกส์ (CPS) อย่างน้อยปีละครั้งและตามมาตรฐานของ ISO 27001

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

บุคคลหรือนิติบุคคลที่มีความรู้ความชำนาญและมีประสบการณ์ที่เกี่ยวข้องกับระบบการให้บริการใบรับรองอิเล็กทรอนิกส์

8.3. **ความสัมพันธ์ของผู้ประเมินและผู้ถูกประเมิน** (Assessor's Relationship to Assessed Entity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อยู่ในฐานะผู้ว่าจ้าง และผู้รับการประเมินเท่านั้น

8.4. **หัวข้อในการประเมิน** (Topics Covered by Assessment)

หัวข้อการประเมินเป็นไปตามเกณฑ์ข้อกำหนดของมาตรฐาน ISO 27001

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

เมื่อการตรวจประเมินเสร็จสิ้น ข้อบกพร่อง (Non-conformity) ที่พบจะต้องได้รับการแก้ไข โดยผู้ให้บริการ จะกำหนดแผนการแก้ไขข้อบกพร่องดังกล่าว และดำเนินการตามแผน ซึ่งแผนดังกล่าวจะถูกส่งไปยังผู้ตรวจประเมินภายนอกสำหรับการวิเคราะห์เพื่อให้มั่นใจว่าระบบยังคงมีความมั่นคงปลอดภัย

8.6. **การแจ้งผลการประเมิน** (Communication of Results)

ผู้ให้บริการ จะรายงานผลการประเมิน อยู่ในรูปแบบของรายงานการตรวจสอบ (Compliance Report)

9. **ข้อกำหนดอื่น ๆ และประเด็นทางกฎหมาย** (Other Business and Legal Matters)

9.1. **ค่าธรรมเนียม** (Fees)

9.1.1. **ค่าธรรมเนียมในการออกใบรับรองอิเล็กทรอนิกส์หรือต่ออายุใบรับรองอิเล็กทรอนิกส์** (Certificate issuance or renewal fees)

ค่าธรรมเนียมในการออกใบรับรองอิเล็กทรอนิกส์ แบ่งตามรูปแบบการออกใบรับรองได้ 2 รูปแบบ คือ CD และ USB Token โดยให้เป็นไปตามประกาศเรื่องราคาและค่าธรรมเนียมของผู้ให้บริการ

9.1.2. **ค่าธรรมเนียมในการเรียกดูใบรับรองอิเล็กทรอนิกส์** (Certificate Access Fees)

ผู้ให้บริการ ไม่มีการคิดค่าธรรมเนียมในการที่ผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องเข้าถึงใบรับรองอิเล็กทรอนิกส์ผ่านที่บันทึกข้อมูลของผู้ให้บริการที่ได้กำหนดไว้ เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

9.1.3. **ค่าธรรมเนียมในการเรียกดูข้อมูลสถานะของใบรับรองอิเล็กทรอนิกส์** (Revocation or Status Information Access Fees)

ไม่มีค่าธรรมเนียมในการเรียกดูข้อมูลเกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือสถานะล่าสุดของใบรับรองอิเล็กทรอนิกส์

9.1.4. **ค่าใช้จ่ายอื่น ๆ** (Fees for Other Services)

ผู้ให้บริการไม่มีการคิดค่าธรรมเนียมในการเข้าถึงแนวนโยบายหรือแนวปฏิบัติในกรณีที่มีวัตถุประสงค์เพื่ออ่านเท่านั้น เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น อย่างไรก็ตาม หากหน่วยงานใดมีความประสงค์จะทำซ้ำ เพิ่มเติม หรือแก้ไขส่วนหนึ่งส่วนใดหรือทั้งหมดของเอกสารดังกล่าว จะต้องปฏิบัติตามข้อกำหนดที่เกี่ยวกับลิขสิทธิ์ของเอกสารฉบับนี้

9.1.5. **นโยบายในการคืนค่าธรรมเนียม** (Refund Policy)

ถ้าผู้ใช้บริการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ภายใน 15 วัน หลังจากที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปให้ผู้ใช้บริการแล้ว ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะไม่คิดค่าใบรับรองอิเล็กทรอนิกส์ดังกล่าว

9.2. **ความรับผิดชอบทางการเงิน** (Financial Responsibility)

9.2.1. **วงเงินประกันความเสียหายที่คุ้มครองความรับผิดชอบที่เกิดขึ้น** (Insurance Coverage)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มีประกันภัยเครื่องอุปกรณ์อิเล็กทรอนิกส์ ประกันภัยทรัพย์สินคุ้มครองภัยจากเหตุการณ์ความไม่สงบ และประกันภัยอัคคีภัยสำหรับสถานที่ติดตั้งระบบให้บริการใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.2.2. **สินทรัพย์อื่น ๆ** (Other Assets)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นนิติบุคคลจดทะเบียนตามกฎหมายไทย โดยสามารถตรวจสอบข้อมูลสินทรัพย์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ ในงบแสดงฐานะทางการเงิน ที่เว็บไซต์ของกรมพัฒนาธุรกิจกระทรวงพาณิชย์

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

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์รับประกันความถูกต้องของข้อมูลที่ปรากฏบนใบรับรองอิเล็กทรอนิกส์ หากมีความผิดพลาดเกิดขึ้นอันเกี่ยวเนื่องมาจากความผิดพลาดของข้อมูลดังกล่าว โดยความผิดพลาดนั้นมาจากหน่วยงานรับลงทะเบียน หรือ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เอง ผู้ใช้บริการจะต้องแจ้งให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ทราบภายใน 15 วัน นับจากวันที่ออกใบรับรองอิเล็กทรอนิกส์ และ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะออกใบรับรองอิเล็กทรอนิกส์ให้ใหม่ โดยไม่คิดค่าใช้จ่าย

9.3. **การรักษาความลับของข้อมูลทางธุรกิจ** (Confidentiality of Business Information)

9.3.1. **ขอบเขตของข้อมูลที่เป็นความลับ** (Scope of Confidential Information)

ผู้ให้บริการ กำหนดให้ข้อมูลดังต่อไปนี้เป็นข้อมูลที่เป็นความลับ อันได้แก่

- รายการแบบคำขอสมัครใช้บริการใบระบบรองอิเล็กทรอนิกส์ ทั้งในกรณีที่แบบคำขอได้รับหรือไม่ได้รับอนุมัติ
- รายการกิจกรรมที่เกิดขึ้นระหว่าง ผู้ให้บริการ และผู้ใช้บริการ ซึ่งรวมถึงรายการที่สมบูรณ์ และบันทึกเหตุการณ์ (Audit Trail) ของรายการดังกล่าว
- บันทึกเหตุการณ์ที่เกิดขึ้น ที่บันทึกในระบบของผู้ให้บริการ
- รายการผลการตรวจสอบระบบ ทั้งที่ถูกสร้างโดยผู้ให้บริการ หรือผู้ตรวจประเมินจากภายนอก
- แผนปฏิบัติการฉุกเฉิน (Contingency Plan) หรือแผนการกู้ระบบในกรณีฉุกเฉิน (Disaster Recovery Plan)
- การควบคุมด้านความมั่นคงปลอดภัยต่าง ๆ ของผู้ให้บริการ ทั้งด้านฮาร์ดแวร์ ซอฟต์แวร์ และการบริหารจัดการเกี่ยวกับการให้บริการใบรับรองอิเล็กทรอนิกส์

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

ภายใต้กฎหมายทรัพย์สินทางปัญญา ข้อมูลดังต่อไปนี้ ไม่ถือว่าเป็นข้อมูลที่เป็นความลับ เช่น ใบรับรองอิเล็กทรอนิกส์ เอกสารแนวนโยบาย/แนวปฏิบัติ ข้อมูลภายในใบรับรอง รายการเพิกถอนใบรับรอง และข้อมูลเกี่ยวกับสถานะของใบรับรองอิเล็กทรอนิกส์

9.3.3. **ความรับผิดชอบในการป้องกันข้อมูลลับ** (Responsibility to Protect Confidential Information)

ผู้ให้บริการ ต้องกำหนดวิธีปฏิบัติเกี่ยวกับการป้องกันข้อมูลลับตาม ข้อ 9.3.1 รวมทั้งข้อมูลทางธุรกิจที่เป็นความลับนอกจากนั้น ยังต้องกำหนดความรับผิดชอบในการรักษาข้อมูลมิได้ถูกล่วงรู้ งดเว้นที่ใช้ข้อมูลและรวมถึงไม่เปิดเผยข้อมูลดังกล่าวแก่บุคคลภายนอก

9.4. **นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนตัวบุคคล** (Privacy of Personal Information)

9.4.1. **แผนการรักษาความเป็นส่วนตัว** (Privacy Plan)

ผู้ให้บริการ ได้ดำเนินการตามแผนการรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยได้กำหนดวิธีปฏิบัติไว้ที่เว็บไซต์ของผู้ให้บริการ

9.4.2. **ข้อมูลที่จัดให้เป็นข้อมูลส่วนบุคคล** (Information Treated As Private)

ข้อมูลที่เกี่ยวกับผู้ใช้บริการที่ไม่ได้เผยแพร่ผ่านที่บันทึกข้อมูลผู้ให้บริการ ที่สามารถเข้าถึงได้จากสาธารณะ จะถือว่าเป็นข้อมูลส่วนบุคคลทั้งสิ้น

9.4.3. **ข้อมูลที่ไม่ถือว่าเป็นข้อมูลส่วนบุคคล** (Information Not Deemed Private)

ข้อมูลต่าง ๆ ที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ ไม่ถือว่าเป็นข้อมูลส่วนบุคคล

9.4.4. **ความรับผิดชอบในการป้องกันข้อมูลส่วนบุคคล** (Responsibility to Protect Private Information)

กำหนดวิธีปฏิบัติอย่างเหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดความเสียหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งกำหนดความรับผิดชอบในการรักษาข้อมูลมิให้ถูกล่วงรู้ งดเว้นที่จะใช้ข้อมูล และรวมถึงไม่เปิดเผยข้อมูลดังกล่าวแก่บุคคลภายนอกด้วย

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

อ้างอิงตามนโยบายการรักษาความลับของข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลจะไม่ถูกเปิดเผยจนกว่าจะได้รับความยินยอมจากเจ้าของข้อมูลนั้น

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

ผู้ให้บริการ จำเป็นต้องเปิดเผยข้อมูลบุคคลเมื่อได้รับคำสั่งทางกฎหมาย ดังนี้

- เมื่อจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลตามหมายเรียก หมายค้น
- เมื่อจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งศาล หรือคำสั่งทางปกครอง

9.4.7. **กรณีอื่นใดที่ต้องเปิดเผยข้อมูลส่วนบุคคล** (Other Information Disclosure Circumstances)

กรณีมีเหตุอันควรที่จำเป็นต้องเปิดเผยข้อมูลส่วนตัวของผู้ใช้บริการนอกเหนือจากข้อ 9.4.6 ผู้ให้บริการจะต้องได้รับความยินยอมจากผู้ใช้บริการนั้น เป็นลายลักษณ์อักษรเสียก่อน

9.5. **ทรัพย์สินทางปัญญา** (Intellectual Property Rights)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ กำหนดให้เอกสารแนวนโยบาย / แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) ฉบับนี้ ถือเป็นสิทธิ์ในทรัพย์สินทางปัญญาของผู้ให้บริการแต่เพียงผู้เดียว หรือที่กำหนดไว้ในข้อตกลงใดๆกับบุคคลที่เกี่ยวข้อง

9.6. **คำรับรอง** (Representations and Warranties)

9.6.1. **คำรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์** (CA Representations and Warranties)

ผู้ให้บริการ ให้คำรับรองว่า

- ข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออกโดยผู้ให้บริการ จะไม่มีข้อผิดพลาดเกิดขึ้นอันเกิดจากความบกพร่องของผู้ให้บริการ ในการออกใบรับรองอิเล็กทรอนิกส์
- ใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออกโดยผู้ให้บริการ ได้ผ่านกระบวนการตามที่ปรากฏในเอกสารแนวนโยบาย/แนวปฏิบัตินี้
- ข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์และข้อมูลเกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ที่ปรากฏในที่บันทึกข้อมูล ได้ผ่านกระบวนการสร้างตามที่ปรากฏในเอกสารแนวนโยบาย/แนวปฏิบัตินี้

9.6.2. **คำรับรองของหน่วยงานรับลงทะเบียน** (RA Representations and Warranties)

หน่วยงานรับลงทะเบียน ให้คำรับรองว่า

- ข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออก จะไม่มีข้อผิดพลาดเกิดขึ้นอันเกิดจากความบกพร่องของหน่วยงานรับลงทะเบียน ในขั้นตอนการตรวจสอบแบบคำขอสมัครใช้ใบรับรองอิเล็กทรอนิกส์
- ใบรับรองอิเล็กทรอนิกส์ทุกใบที่ออก ได้ผ่านกระบวนการตามที่ปรากฏในเอกสารแนวนโยบาย/แนวปฏิบัตินี้
- ข้อมูลที่ปรากฏในที่บันทึกข้อมูล และข้อมูลเกี่ยวกับการเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ผ่านกระบวนการตามที่ปรากฏในเอกสารแนวนโยบาย/แนวปฏิบัตินี้

9.6.3. **คำรับรองของผู้ใช้บริการ** (Subscriber Representations and Warranties)

ผู้ใช้บริการให้คำรับรองว่า

- ลายมือชื่อดิจิทัลทุกรายการที่ถูกสร้างโดยกุญแจส่วนตัวซึ่งเป็นคู่กับกุญแจสาธารณะที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ เป็นลายมือชื่อดิจิทัลของผู้ใช้บริการ ซึ่งใบรับรองอิเล็กทรอนิกส์ยังคงสามารถใช้งานได้โดยไม่ถูกเพิกถอนหรือหมดอายุในขณะที่มีการสร้างลายมือชื่อ
- กุญแจส่วนตัวได้รับการป้องกันอย่างเหมาะสมและไม่สามารถเข้าถึงได้โดยไม่ได้รับอนุญาต
- ข้อมูลทั้งหมดที่ปรากฏในแบบคำขอสมัครใช้บริการใบรับรองอิเล็กทรอนิกส์เป็นข้อมูลที่ถูกต้องและเป็นความจริง
- ใบรับรองอิเล็กทรอนิกส์จะถูกใช้งานอย่างถูกต้องตามกฎหมาย กฎระเบียบต่าง ๆ ที่เกี่ยวข้อง โดยผู้ที่ได้รับอนุญาตเท่านั้น

9.6.4. **คำรับรองของคู่กรณีที่เกี่ยวข้อง** (Relying Party Representations and Warranties)

คู่กรณีที่เกี่ยวข้อง ขอรับรองว่าได้ยอมรับข้อตกลงที่เกี่ยวกับคู่กรณีที่เกี่ยวข้องแล้ว และได้ตรวจสอบใบรับรองอิเล็กทรอนิกส์อย่างเหมาะสมแล้ว ก่อนที่จะเชื่อถือข้อมูลในใบรับรองอิเล็กทรอนิกส์ใบนั้น และจะยอมรับข้อผิดพลาดอันเกิดจากความบกพร่องในการตรวจสอบใบรับรองอิเล็กทรอนิกส์เพียงผู้เดียว

9.6.5. **คำรับรองของบุคคลอื่น ๆ** (Representations and Warranties of Other Participants)

ไม่มี

9.7. **ข้อจำกัดของการรับประกัน** (Disclaimers of Warranties)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะไม่รับประกันใดๆ ไม่ว่าโดยชัดแจ้งหรือโดยปริยายนอกเหนือจากที่ระบุไว้ในแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) รวมถึงไม่รับประกันผลสัมฤทธิ์ในเชิงพาณิชย์ หรือในวัตถุประสงค์ใดโดยเฉพาะ

9.8. **ข้อจำกัดความรับผิด** (Limitations of Liability)

ผู้ให้บริการ ได้กำหนดขอบเขตความรับผิดชอบและรวมถึงข้อจำกัดความรับผิด โดยผู้ให้บริการจะรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการปฏิบัติผิดเงื่อนไขข้อกำหนดตามแนวนโยบาย/แนวปฏิบัติในการให้บริการออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการตามที่เกิดขึ้นจริง จำกัดไว้ไม่เกิน 30,000 บาทต่อกรณีที่เกิดความเสียหาย

ทั้งนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะไม่รับผิดชอบในความเสียหายใดๆ อันเนื่องมาจาก หรือเกี่ยวข้องกับการใช้ใบรับรองอิเล็กทรอนิกส์ที่ผิดกฎหมาย หรือนอกวัตถุประสงค์ที่ระบุไว้ในแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ฉบับนี้ หรือการละเมิดระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งไม่รับผิดในความเสียหายที่เป็นผลโดยอ้อม ความเสียหายที่เป็นผลสืบเนื่อง หรือความเสียหายอันเกิดจากพฤติการณ์พิเศษ หรือความสูญเสียรายได้ หรือผลกำไรในทางธุรกิจ

9.9. **ค่าสินไหมทดแทน** (Indemnities)

ค่าสินไหมทดแทนให้เป็นไปตามข้อตกลงระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการ ทั้งนี้ ในกรณีที่คู่กรณีที่เกี่ยวข้องไม่ตรวจสอบสถานะการเพิกถอนใบรับรองอิเล็กทรอนิกส์ หากมีความเสียหายเกิดขึ้น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขอสงวนสิทธิ์ไม่รับผิดชอบชดใช้ค่าสินไหมทดแทนในความเสียหายดังกล่าว

9.10. **เงื่อนไข และการยกเลิก** (Term and Termination)

9.10.1. **เงื่อนไข** (Term)

เงื่อนไขใดๆ ที่เกี่ยวข้องกับการใช้ใบรับรองอิเล็กทรอนิกส์ เป็นเงื่อนไขที่ระบุในเอกสารระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ ซึ่งเป็นเอกสารประกอบการสมัครใบรับรองอิเล็กทรอนิกส์

9.10.2. **การยกเลิก** (Termination)

การขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ ต้องกระทำการโดยผู้ใช้บริการหรือผู้มีอำนาจกระทำการแทน

9.10.3. **ผลของการยกเลิกใช้บริการ** (Effect of Termination and Survival)

การขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ ถือเป็นการสิ้นสุดความผูกพันระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และผู้ใช้บริการทันที

การยกเลิกสัญญานี้ไม่ว่าด้วยเหตุประการใดก็ตาม จะไม่ถือเป็นการลบล้างหรือทำให้เสื่อมเสียซึ่งสิทธิ หน้าที่ความรับผิดใดๆที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการมีอยู่ต่อกัน อันเนื่องมาจากการใดๆ อันได้กระทำไปตามเงื่อนไขและข้อตกลงตามเอกสารฉบับนี้ก่อนที่จะมีการเพิกถอนใบรับรองอิเล็กทรอนิกส์

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

ในกรณีที่ไม่ระบุเป็นการอื่น ผู้ให้บริการจะติดต่อกับผู้ที่เกี่ยวข้อง โดยวิธีการที่รวดเร็วและน่าเชื่อถือโดยพิจารณาความสำคัญของข้อมูลที่ต้องการติดต่อสื่อสารเป็นสำคัญ

9.12. **การแก้ไขปรับปรุง** (Amendments)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขอสงวนสิทธิ์ในการแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงใดๆ ในการให้บริการตามเอกสารฉบับนี้ได้

9.12.1. **กระบวนการแก้ไขปรับปรุง** (Procedure for Amendment)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต้องการแก้ไข เพิ่มเติม ยกเลิก หรือ เปลี่ยนแปลงข้อตกลงในการให้บริการตามเอกสารฉบับนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะต้องแจ้งให้ผู้ใช้บริการหรือ หน่วยงานรับลงทะเบียนทราบล่วงหน้าไม่น้อยกว่า 90 วัน ก่อนจะประกาศบังคับใช้ โดยแจ้งเป็นหนังสือ หรือ อีเมล์ หรือ บนเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.12.2. **วิธีการแจ้งและระยะเวลาแจ้ง** (Notification Mechanism and Period)

หากหน่วยงานรับลงทะเบียนหรือผู้ใช้บริการเห็นว่า การแก้ไข เพิ่มเติม ยกเลิก หรือ เปลี่ยนแปลงข้อตกลงดังกล่าวเป็นการลดสิทธิ หรือประโยชน์อันพึงได้รับโดยชอบด้วยกฎหมาย หน่วยงานรับลงทะเบียน หรือ ผู้ใช้บริการมีสิทธิยกเลิกการใช้บริการตามเอกสารนี้ได้ โดยแจ้งให้ผู้ให้บริการทราบล่วงหน้าไม่น้อยกว่า 30 วัน ก่อนวันให้มีผลสิ้นสุดการใช้บริการ ทั้งนี้เว้นแต่เป็นการแก้ไข เพิ่มเติม ยกเลิก หรือ เปลี่ยนแปลง ตามที่กฎหมายกำหนด

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

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่ระบุเหตุการณ์หรือกรณีที่จะมีการเปลี่ยน OID

9.13. **การระงับข้อพิพาท** (Dispute Resolution Procedures)

1. **ข้อโต้แย้งระหว่างผู้ให้บริการและผู้ใช้บริการ** (Disputes between TOT CA and Entities)

ในกรณีที่มีข้อพิพาท หรือในกรณีที่มีข้อความขัดแย้งในเอกสารแนวนโยบาย/แนวปฏิบัตินี้ ของผู้ให้บริการ และผู้ใช้บริการ จะต้องปฏิบัติตามคำวินิจฉัยของบริษัท ทีโอที จำกัด (มหาชน)

2. **ข้อโต้แย้งระหว่างผู้ให้บริการและคู่กรณีที่เกี่ยวข้อง** (Disputes between Subordinate CA and Relying Parties)

ในกรณีที่มีข้อพิพาท หรือในกรณีที่มีข้อความขัดแย้งในเอกสารแนวนโยบาย/แนวปฏิบัตินี้ ของผู้ให้บริการ และคู่กรณที่เกี่ยวข้อง จะต้องปฏิบัติตามคำวินิจฉัยของบริษัท ทีโอที จำกัด (มหาชน)

9.14. **กฎหมายที่ใช้บังคับ** (Governing Law)

ให้ใช้กฎหมายแห่งราชอาณาจักรไทยเป็นกฎหมายที่ใช้ในการระงับข้อพิพาท

9.15. **ความสอดคล้องกับกฎหมายที่เกี่ยวข้อง** (Compliance with Applicable Law)

การประกาศใช้แนวนโยบาย/แนวปฏิบัตินั้น จะต้องสอดคล้องกับกฎหมายอื่น ๆ ที่เกี่ยวข้อง

9.16. **ประเด็นอื่น ๆ ที่เกี่ยวข้อง** (Miscellaneous Provisions)

9.16.1. **ข้อตกลง** (Entire Agreement)

เอกสารแนวนโยบาย/แนวปฏิบัติ ถือเป็นส่วนหนึ่งของข้อตกลงอื่น ๆ ที่ทำขึ้นระหว่าง ผู้ให้บริการและผู้ใช้บริการ

9.16.2. **การโอนสิทธิ** (Assignment)

หากมีการโอนสิทธิของผู้ให้บริการ ผู้รับโอนสิทธิจะต้องดำเนินการตามนโยบาย/แนวปฏิบัติฉบับนี้และรวมถึงรับเอาข้อจำกัดความรับผิดที่ผู้ให้บริการ มีต่อผู้ใช้บริการไว้ด้วย

9.16.3 **กรณีส่วนหนึ่งส่วนใดของข้อตกลงเป็นโมฆะ** (Severability)

ในกรณีที่ข้อความส่วนใดส่วนหนึ่งของเอกสารนี้เป็นโมฆะ ไม่สมบูรณ์ หรือ ไม่มีผลใช้บังคับตามกฎหมาย ไม่มีผลกระทบกับข้อความอื่นๆ ในเอกสารฉบับนี้ที่สมบรณ์และบังคับได้ตามกฎหมาย

9.16.4 **ค่าใช้จ่ายที่เกิดขึ้นจากการผิดข้อตกลง** (Enforcement)

ผู้ให้บริการได้กำหนดขอบเขตความรับผิดชอบและรวมถึงข้อจำกัดความรับผิด โดยให้อยู่ในดุลพินิจของ บริษัท ทีโอที จำกัด (มหาชน)

9.16.5. **เหตุสุดวิสัย** (Force Majeure)

ในกรณีที่ฝ่ายใดฝ่ายหนึ่ง ไม่สามารถดำเนินการตามแนวนโยบาย/แนวปฏิบัตินี้ได้ด้วยเหตุสุดวิสัยฝ่ายนั้นอาจเรียกให้อีกฝ่ายหาทางออกร่วมกันอย่างเหมาะสม

เหตุสุดวิสัย หมายถึง เหตุการณ์ที่อยู่นอกเหนือการควบคุมของคู่กรณีและเหตุการณ์ดังกล่าวส่งผลให้การปฏิบัติหน้าที่ของฝ่ายนั้นไม่สามารถกระทำได้ หรือพ้นวิสัยที่จะปฏิบัติหน้าที่ตามข้อตกลงในเอกสารฉบับนี้ได้

9.17 **บทบัญญัติอื่น**(Other provisions)

ไม่มี