Thai Digital ID CA G3

แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์

(Certificate Policy/Certification Practice Statement)

ประวัติการปรับปรุงเอกสาร

Doc. Version	Status	Date of Issue	Issued By	Comments	Date of PA Approval
1.0	Published	11-07-16	TDID PCA	The first version for TDID CA G3	29-Jul-16
1.1	Published	28-03-17	TDID PCA	(1) Specify applicable standards used to develop this CP/CPS (secion 1.1) (2) Update CPS Approval Procedures 1.5.4 (3) Update Certificate Authority Authorization (CAA) 4.2.4 (4) Update suspension process time (4.9.15) (5) Update Limited period of Suspension(4.9.16) (6) Review backup off-site backup (5.1.8) (7) Classify Events Recorded (5.5.1) (8) Review Public Key Archival (6.3.1) (9) Review Certificate operational periods and key pair usage periods (6.3.2)	21-Apr-17
1.2	Published	26/06/2017	TDID PCA	(1) Update CRL and OCSP link in section (4.9.6), (4.9.9) and (4.10.1) (2) Add organizationIdentifier in Name Forms (7.1.4)	26/06/2017
1.3	Published	18/10/2018	TDID PCA	(1) Update certificate validity to be upto 2 years (1.4) (2) Update company address (1.5, 4.1.2)	18/10/2018

1.4	Published	09/09/2019	TDID PCA	(1) Update Notification to Subscriber by the CA of Issuance of Certificate (4.3.2) (2) Update Certificate Acceptance (4.4.1,4.4.3)	09/09/2019
1.5	Published	31/10/2019	TDID PCA	(1) Update 4.2.4 CAA record “thaidigitalid.com” (2) Change 4.9.7 to CRL Issuance Frequency (3) Change 4.9.8 to Maximum Latency for CRLs (4) Update 5.4.3 Retention Period for Audit Log to 10 years	07/11/2019

หมายเหตุ :

TDID PCA = TDID Policy Creation Authority

สารบัญ

1 บทนำ (Introduction)

1.1 ข้อมูลเบื้องต้นทั่วไป (Overview)

เอกสารฉบับนี้เรียกว่า "แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement)" หรือเรียกว่า "CP/CPS" ถูกจัดทำขึ้นตามมาตราฐาน Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy และ Certification Practices Framework [RFC3647] โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Thai Digital ID Certification Authority:TDID CA)

โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือ TDID CA ได้ยึดตามข้อปฏิบัติตามมาตราฐานของ Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published ที่ถูกประกาศเป็น Version ล่าสุดอยู่ใน http://www.cabforum.org หากเอกฉบับนี้มีข้อปฏิบัติใดผิดไปจาก ข้อปฏิบัติตามมาตราฐาน Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published ขอให้ยึดตามข้อปฏิบัติตามมาตราฐานฯ

1.2 ชื่อเอกสาร (Document Name and Identification)

เอกสารฉบับนี้เรียกว่า “แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement)” หรือเรียกว่า “CP/CPS” ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ เพื่อให้ทราบและเข้าใจถึงข้อความที่ระบุในเอกสารที่ใช้เป็นแนวทางในการดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์

1.3 บุคคลที่เกี่ยวข้อง (PKI Participants)

1.3.1 ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authorities): TDID CA

คือ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งสร้างและออกใบรับรองอิเล็กทรอนิกส์เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List หรือมีชื่อย่อว่า CRL)

1.3.2 หน่วยงานรับลงทะเบียน (Registration Authorities): TDID RA

คือ ผู้ซึ่งทำหน้าที่รับลงทะเบียน เมื่อมีการยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์ คำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ ของข้อมูลที่ผู้ใช้บริการให้ไว้ตามแบบคำขอที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์กำหนดขึ้น

1.3.3 **ผู้ใช้บริการ** (Subscribers)

คือ บุคคล นิติบุคคล หรือ เอนทิตี้อื่นใด ที่ได้รับใบรับรองอิเล็กทรอนิกส์ จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

1.3.4 **คู่กรณีที่เกี่ยวข้อง** (Relying Parties)

คือ บุคคล นิติบุคคล หรือ เอนทิตี้อื่นใด ที่เชื่อถือลายมือชื่อดิจิทัล อันเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง หรือ เชื่อถือใบรับรองอิเล็กทรอนิกส์ ดังนั้น คู่กรณีที่เกี่ยวข้องอาจเป็นผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือ อาจไม่ใช่ผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ก็ได้ แต่เป็นผู้ซึ่งกระทำการหรืองดเว้นกระทำการใด ๆ เพราะเชื่อถือลายมือชื่อดิจิทัลหรือใบรับรองอิเล็กทรอนิกส์ โดยการใช้กุญแจสาธารณะที่อยู่ในใบรับรองอิเล็กทรอนิกส์นั้นในการตรวจสอบตัวตนที่แท้จริงของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัล และมีชื่อปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์

1.3.5 **บุคคลอื่นที่เกี่ยวของ** (Other Participants)

คือ บุคคล นิติบุคคล หรือ เอนทิตี้อื่นใด นอกจากที่กล่าวถึงข้างต้น เช่น ผู้ให้บริการในการเก็บรักษาข้อมูล (Providers of Repository Services) หรือ ผู้ได้รับการว่าจ้างโดยการ Outsource ให้เป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นต้น

1.4 **การใช้ใบรับรองอิเล็กทรอนิกส์** (Certificate Usage)

ชนิดของใบรับรองอิเล็กทรอนิกส์ที่ออกโดย ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ประกอบด้วย ใบรับรองอิเล็กทรอนิกส์ 4 ชนิด คือ

Personal Certificate คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้บุคคลหรือ ประชาชนทั่วไป เพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้มีอายุการใช้งานทั้งแบบ 1 ปี และ 2 ปี

Enterprise Certificate คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้กับนิติบุคคล ซึ่งอาจเป็น หน่วยงาน หรือ องค์กร ภาครัฐ และเอกชน ที่มีความต้องการใช้งานใบรับรองอิเล็กทรอนิกส์เพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้มีอายุการใช้งานทั้งแบบ 1 ปี และ 2 ปี

Computer/Equipment Certificate คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการติดต่อสื่อสารทางเครือข่าย เช่น เราท์เตอร์(Router) เพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้มีอายุการใช้งานทั้งแบบ 1 ปี และ 2 ปี

Web Server Certificate (SSL Certificate) คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกสำหรับใช้ยืนยันตัวตนของ Web Server โดยใบรับรองอิเล็กทรอนิกส์ประเภทนี้มีอายุการใช้งานทั้งแบบ 1 ปี และ 2 ปี

1.4.1 **การใช้ใบรับรองอิเล็กทรอนิกส์ที่ถูกต้อง** (Appropriate Certificate Uses)

การใช้ใบรับรองอิเล็กทรอนิกส์ที่ถูกต้อง จะต้องปฏิบัติตามเงื่อนไขการใช้ใบรับรองอิเล็กทรอนิกส์อย่างเคร่งครัด

1.4.2 **ข้อห้ามเกี่ยวกับการใช้ใบรับรองอิเล็กทรอนิกส์** (Prohibited Certificate Uses)

ใบรับรองอิเล็กทรอนิกส์ที่ออกโดย ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ซึ่ง ออกให้แก่บุคคลหรือนิติบุคคล ตามประเภทของการใช้งานใบรับรองอิเล็กทรอนิกส์ที่ระบุไว้ในข้อ 1.4 เท่านั้น ห้ามใช้งานใบรับรองอิเล็กทรอนิกส์ นอกเหนือจากวัตถุประสงค์ของการใช้งานดังกล่าว

1.5 **นโยบายการจัดการ** (Policy Administration)

หน่วยงาน Policy Creation Authority หรือ PCA ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

รายละเอียดที่อยู่ของหน่วยงาน PCA ที่ทำหน้าที่ในการดูแลและปรับปรุงเอกสารแนวนโยบาย/แนวปฏิบัติ ใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) นี้

Name:	Thai Digital ID CA
Company Registration No.:	0105543112679
Trading as:	TDID CA
Postal Address:	319 25th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok , 10330 Thailand
Phone:	+66-2029-0312
Domain Name:	www.thaidigitalid.com
Email Address:	support@thaidigitalid.com
Contact:	Policy Creation Authority, Thai Digital ID Co., Ltd. 319 25th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok , 10330

1.5.1 หน่วยงานที่ทำหน้าที่ในการบริหารดูแลแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Organization Administering the Document)

หน่วยงาน Policy Creation Authority ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

1.5.2 บุคคลที่ติดต่อ (Contact Person)

หน่วยงาน Policy Creation Authority ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

1.5.3 ผู้รับผิดชอบในการตรวจสอบความถูกต้องของแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Person Determining CPS Suitability for Policy)

หน่วยงาน Policy Creation Authority ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รวมถึง ผู้ตรวจสอบภายใน (Internal Auditor) และ ผู้ตรวจสอบภายนอก (External Auditor)

1.5.4 ขั้นตอนในการอนุมัติแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (CPS Approval Procedures)

ในกรณีที่ที่มีการเปลี่ยนแปลงข้อความใดๆ ในแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์(Certificate Policy/Certification Practice Statement) เล่มนี้ ให้ทีมงาน PCA ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นผู้พิจารณาความเหมาะสม ในการปรับปรุงเปลี่ยนแปลง

ในกรณีที่ PCA เห็นชอบให้มีการเปลี่ยนแปลง ให้ทีม PCA เป็นผู้แก้ไขปรับปรุงผ่าน Change Control Procedure โดยนำเสนอกรรมการผู้จัดการเพื่อลงนามอนุมัติ เมื่อ PA อนุมัติเรียบร้อยแล้วให้ปรับปรุงเวอร์ชั่นของแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ในส่วนของ ประวัติปรับปรุงเอกสาร แล้วจึง เผยแพร่ขึ้นสู่เว็บไซต์ของบริษัท

โดยปกติ แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) จะถูกทบทวนอย่างน้อยปีละ 1 ครั้ง โดย PCA จะเป็นผู้ทบทวน และขออนุมัติต่อกรรมการผู้จัดการเพื่อลงบันทึกทวนสอบ (ผ่าน Change Control) ในส่วนของประวัติปรับปรุงเอกสาร แล้วจึงเผยแพร่ขึ้นสู่เว็บไซต์บริษัทที่ www.thaidigitalid.com

1.6 คำนิยามและคำย่อ (Definitions and Acronyms)

คำศัพท์	ความหมาย
ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority : TDID CA)	บริษัท ไทยดิจิทัล ไอดี จำกัด ภายใต้ TDID CA Service ทำหน้าที่ให้บริการเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
หน่วยงานรับลงทะเบียน (Registration Authority : TDID RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใบรับรองอิเล็กทรอนิกส์ คำขอพักใช้ใบรับรองอิเล็กทรอนิกส์ หรือคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดยตรวจสอบและยืนยันความถูกต้องสมบูรณ์ของข้อมูลตามที่ผู้ใช้บริการให้ไว้
ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)	เอกสารอิเล็กทรอนิกส์ที่เป็นองค์ประกอบส่วนหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะของผู้ใช้บริการ ซึ่งอาจหมายถึงบุคคลธรรมดา นิติบุคคล หรือ เครื่องมืออุปกรณ์ ซึ่งเอกสารอิเล็กทรอนิกส์ดังกล่าวสอดคล้องตามมาตรฐาน X.509 Version 3 Certificate โดยมีรายการอย่างน้อย ดังนี้ — เวอร์ชั่นของใบรับรองอิเล็กทรอนิกส์ — หมายเลขของใบรับรองอิเล็กทรอนิกส์ — วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลของผู้ถือใบรับรองอิเล็กทรอนิกส์ — ชื่อของผู้ให้บริการ — วัน เวลาที่เริ่มต้นและสิ้นสุดของการใช้ใบรับรองอิเล็กทรอนิกส์ — ชื่อของผู้ถือใบรับรองอิเล็กทรอนิกส์ — กุญแจสาธารณะของผู้ถือใบรับรองอิเล็กทรอนิกส์และวิธีการที่ใช้ในการสร้าง
ผู้ใช้บริการ (Subscriber)	บุคคลหรือนิติบุคคลที่ยื่นสมัครขอใช้บริการใบรับรองอิเล็กทรอนิกส์กับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์จะมีการระบุชื่อบุคคลหรือนิติบุคคลของผู้ใช้บริการไว้ในใบรับรองอิเล็กทรอนิกส์

คำศัพท์	ความหมาย
กุญแจ (Key)	สัญลักษณ์หรือลำดับของสัญลักษณ์ หรือสัญญาณไฟฟ้าที่เกี่ยวเนื่องกับสัญลักษณ์ที่นำมาเข้ารหัสข้อมูลหรือถอดรหัสข้อมูล
กุญแจส่วนตัว (Private Key)	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการ ถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ และ กุญแจส่วนตัวนี้จะนำไปใช้สร้าง ลายมือชื่อดิจิทัล
กุญแจสาธารณะ (Public Key)	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษา ความลับของข้อมูลอิเล็กทรอนิกส์นั้น และ กุญแจสาธารณะนี้จะนำไปใช้ตรวจสอบลายมือชื่อดิจิทัล
กุญแจคู่ (Key Pair)	กุญแจส่วนตัวและกุญแจสาธารณะ ในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะ โดยที่สามารถใช้กุญแจสาธารณะตรวจสอบว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้
ลายมือชื่อดิจิทัล (Digital Signature)	ลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่งที่สร้างขึ้นโดยการนำข้อมูลอิเล็กทรอนิกส์มาแปลงเป็นตัวเลขและใช้กับระบบกุญแจคู่ โดยนำไปคำนวณร่วมกับกุญแจส่วนตัวของเจ้าของลายมือชื่อ โดยที่สามารถใช้กุญแจสาธารณะของเจ้าของลายมือชื่อมาตรวจสอบได้ว่าเป็นลายมือชื่อดิจิทัลที่ได้สร้างขึ้นโดยกุญแจส่วนตัวของเจ้าของลายมือชื่อดิจิทัลนั้นหรือไม่ และข้อมูลอิเล็กทรอนิกส์ที่ได้มีการลง

คำศัพท์	ความหมาย
	ลายมือชื่อดิจิทัลนั้นได้มีการแก้ไขเปลี่ยนแปลงภายหลังการลงลายมือชื่อหรือไม่
การเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation)	การทำให้ใบรับรองอิเล็กทรอนิกส์ไม่สามารถใช้ได้อีกต่อไปหลังจากการเพิกถอนใบรับรอง ซึ่งส่งผลให้กุญแจส่วนตัวของผู้ใช้บริการนั้นไม่สามารถใช้ในการสร้างลายมือชื่อดิจิทัลหรือถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ได้ ทั้งนี้ไม่มีผลกระทบกับใบรับรองหรือกุญแจสาธารณะ ซึ่งยังคงสามารถใช้ในการตรวจสอบลายมือชื่อดิจิทัลที่สร้างขึ้นก่อนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้
รายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List : CRL)	รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนการใช้งาน
คู่กรณีที่เกี่ยวข้อง (Relying Party)	ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองอิเล็กทรอนิกส์หรือลายมือชื่อดิจิทัล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองไปใช้ในการตรวจสอบตัวตนของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัล และมีชื่อปรากฏอยู่ในใบรับรอง
ไดเรกทอรี (Directory)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดการเพื่อให้สามารถสืบค้นข้อมูลได้อย่างรวดเร็วและเป็นตามมาตรฐานไดเรกทอรี (X.500 หรือ LDAP)
ฐานข้อมูล (Database)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดเก็บแบบที่เอื้อให้โปรแกรมคอมพิวเตอร์สามารถเข้าถึง จัดการและปรับเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว

2 ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

2.1 การจัดเก็บข้อมูล (Repositories)

ข้อมูลที่เกี่ยวข้องกับการขอใบรับรองอิเล็กทรอนิกส์จะถูกจัดเก็บลงฐานข้อมูลและลงลายมือชื่อโดยเจ้าหน้าที่ของหน่วยงานรับลงทะเบียน ในขณะที่ใบรับรองอิเล็กทรอนิกส์ จะถูกจัดเก็บลง X.500 Directory

2.2 การเผยแพร่ข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ (Publication of Certificate Information)

ใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะถูกเผยแพร่ที่ X.500 Directory

2.3 ความสม่ำเสมอในการเผยแพร่ข้อมูล (Time or Frequency of Publication)

ใบรับรองอิเล็กทรอนิกส์ จะถูกเผยแพร่ลง X.500 Directory ทันทีเมื่อมีการออกใบรับรองอิเล็กทรอนิกส์

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะปรับปรุงแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์(Certificate Policy/Certification Practice Statement) ให้ทันสมัยอยู่เสมอ โดยจะประกาศทางเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (www.thaidigitalid.com) เพื่อใช้สำหรับการอ้างอิงแก่ผู้ใช้บริการ และบุคคลทั่วไป

2.4 การควบคุมการเข้าถึง (Access Controls on Repositories)

การเข้าถึงใบรับรองอิเล็กทรอนิกส์ สามารถเข้าถึงผ่าน LDAP protocol เอกสารแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) สามารถดาวน์โหลดผ่านทางเว็บไซต์ www.thaidigitalid.com ได้

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

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 ชื่อที่ระบุในใบรับรองอิเล็กทรอนิกส์ (Need for Names to be Meaningful)

ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์แต่ละใบ จะมีความหมายที่ใช้สื่อถึงเจ้าของใบรับรองอิเล็กทรอนิกส์นั้นๆได้ เพื่อประโยชน์ในการสืบค้นกลับไปยังเจ้าของใบรับรองอิเล็กทรอนิกส์ได้

3.1.3 นามสมมุติหรือนามแฝง (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)

ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์แต่ละใบ จะมีความแตกต่างกัน ภายใต้ CA เดียวกัน เพื่อใช้ในการสืบค้นกลับไปยังเจ้าของใบรับรองอิเล็กทรอนิกส์ได้

3.1.6 การจดจำ รับรอง และ บทบาทหน้าที่ของเครื่องหมายการค้า (Recognition, Authentication, and Role of Trademarks)

ไม่มีข้อกำหนด

3.2 การตรวจสอบตัวบุคคลเมื่อมีการขอใช้บริการครั้งแรก (Initial Identity Validation)

การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเพื่อออกใบรับรองอิเล็กทรอนิกส์นั้น เป็นหน้าที่ของหน่วยงานรับลงทะเบียนโดยผู้ใช้บริการต้องกรอกใบคำขอใบรับรองอิเล็กทรอนิกส์ เพื่อสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์พร้อมทั้งแนบหลักฐานที่ใช้ในการสมัครขอใช้บริการ ให้แก่หน่วยงานรับลงทะเบียน โดยรายละเอียดอยู่ในหัวข้อ 4.1 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอออกใบรับรองอิเล็กทรอนิกส์ใหม่

3.2.1 วิธีพิสูจน์ผู้เป็นเจ้าของกุญแจส่วนตัว (Method to Prove Possession of Private Key)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบข้อมูลของผู้ถือกุญแจจาก ใบคำขอใบรับรองอิเล็กทรอนิกส์ที่ส่งมา ซึ่งประกอบไปด้วยชื่อ เลขที่บัตรประจำตัวประชาชน หรือพาสปอร์ต ลายเซ็นต์ของผู้ใช้บริการเอง และสำเนาบัตรประชาชน

3.2.2 ตรวจสอบความน่าเชื่อถือขององค์กร (Authentication of Organization Identity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบหนังสือรับรองบริษัทซึ่งจะต้องมีอายุไม่เกินสามเดือนจากวันที่ออกและมีลายเซนต์ของกรรมการผู้มีอำนาจที่ถูกต้องและครบถ้วน หรือพระราชบัญญัติจัดตั้งองค์กร

3.2.3 ตรวจสอบความน่าเชื่อถือรายบุคคล (Authentication of Individual Identity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบความน่าเชื่อถือจากลายเซ็นต์ในใบคำขอใบรับรองอิเล็กทรอนิกส์รวมถึงสำเนาบัตรประชาชนหรือพาสปอร์ตที่แนบมากับใบคำขอใบรับรองอิเล็กทรอนิกส์เพื่อเป็นการยืนยันว่าผู้ใช้บริการนั้นมีอยู่จริง

3.2.4 ข้อมูลของผู้ใช้บริการยังไม่ได้ยืนยันตนเอง (Non-verified Subscriber Information)

ใบรับรองอิเล็กทรอนิกส์ที่ออก จะต้องมีการยืนยันและตรวจสอบจากเอกสารที่ระบุไว้ในใบคำขอใบรับรองอิเล็กทรอนิกส์เสมอ ดังนั้นจะไม่มีการออกใบรับรองอิเล็กทรอนิกส์ให้แก่ผู้ใช้บริการที่ไม่ได้ส่งเอกสารครบถ้วนเพื่อยืนยันตัวตน

3.2.5 การตรวจสอบผู้มีอำนาจ (Validation of Authority)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบ และเก็บหนังสือมอบอำนาจที่แนบมาพร้อมกับใบคำขอใบรับรองอิเล็กทรอนิกส์เพื่อยืนยันว่าผู้ใช้บริการนั้นได้รับมอบอำนาจมาจากกรรมการบริษัทจริงและสามารถขอใบรับรองอิเล็กทรอนิกส์ในนามขององค์กรได้

3.2.6 เกณฑ์ในการเชื่อมโยงการปฏิบัติงาน (Criteria for Interoperation)

ไม่มีข้อกำหนด

3.3 การระบุและยืนยันตัวบุคคลเมื่อมีการขอใบรับรองอิเล็กทรอนิกส์ในครั้งถัดไป (I&A for Re-Key Requests)

3.3.1 การยืนยันตัวบุคคลในการขอกุญแจใหม่(Identification and Authentication for Routine Re-key)

ผู้ใช้บริการต้องกรอกใบคำขอใบรับรองอิเล็กทรอนิกส์ใหม่ และส่งหลักฐานให้กับหน่วยงานรับลงทะเบียน โดยรายละเอียดอยู่ในหัวข้อ 4.1 และ 4.3

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

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะตรวจสอบข้อมูลของผู้ถือกุญแจจากใบคำขอใบรับรองอิเล็กทรอนิกส์และหลักฐานที่ส่งมาถึงผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งประกอบไปด้วยชื่อ เลขที่บัตรประจำตัวประชาชน หรือ พาสปอร์ต และลายเซ็นต์ของผู้สมัครเอง

3.4 การระบุและยืนยันตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ (I&A for Revocation Requests)

ผู้ใช้บริการที่ต้องการเพิกถอนใบรับรองอิเล็กทรอนิกส์ ต้องแจ้งต่อผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยตรง เมื่อผู้ให้บริการการออกใบรับรองอิเล็กทรอนิกส์ได้รับแจ้งความต้องการเพิกถอนใบรับรองอิเล็กทรอนิกส์และตรวจสอบตามขั้นตอนแล้ว จะดำเนินการเพิกถอนใบรับรองอิเล็กทรอนิกส์ตามที่แจ้งไว้และประกาศในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดยรายละเอียดอยู่ในหัวข้อ 4.9

4 ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operational Requirements)

4.1 การยื่นขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application)

4.1.1 ผู้ที่สามารถสมัครขอใบรับรองอิเล็กทรอนิกส์ได้(Who Can Submit a Certificate Application?)

บุคคลที่สมัครขอใบรับรองอิเล็กทรอนิกส์สามารถเป็นได้ทั้งบุคคลที่ขอใบรับรองอิเล็กทรอนิกส์ในนามบุคคล และบุคคลที่ได้รับมอบหมายจากองค์กรให้ดำเนินการสมัครขอใบรับรองอิเล็กทรอนิกส์ในนามองค์กร เพื่อใช้รักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยสามารถสมัครขอใบรับรองอิเล็กทรอนิกส์ตามประเภทต่าง ๆ ที่กำหนดไว้ในหัวข้อ 1.4

4.1.2 ขั้นตอนในการลงทะเบียนและความรับผิดชอบ(Enrollment Process and Responsibilities)

ผู้ใช้บริการควรปฏิบัติตามขั้นตอนต่อไปนี้

กรณีการขอใบรับรองอิเล็กทรอนิกส์ประเภท Personal Certificate

ขั้นตอนดำเนินการ

1. กรอกใบคำขอใบรับรองอิเล็กทรอนิกส์
2. ยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์พร้อมหลักฐานที่
   หน่วยงานรับลงทะเบียน บริษัท ไทยดิจิทัล ไอดี จำกัด
   319 อาคารจัตุรัสจามจุรี ชั้น 25 ห้อง 10-11 ถนนพญาไท แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330
   โทรศัพท์. 02-029-0312
3. เจ้าหน้าที่รับลงทะเบียนตรวจสอบใบคำขอใบรับรองอิเล็กทรอนิกส์และหลักฐานประกอบ
4. เจ้าหน้าที่รับลงทะเบียนจัดส่งใบรับรองอิเล็กทรอนิกส์ให้ผู้ใช้บริการ
5. ผู้ใช้บริการชำระค่าบริการ

หลักฐานประกอบ

1. สำเนาบัตรประชาชนของผู้ใช้บริการพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

2. สำเนาทะเบียนบ้านของผู้ใช้บริการพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสืออนุญาตให้ทำงานในประเทศไทย (Work Permit) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

กรณีการขอใบรับรองอิเล็กทรอนิกส์ประเภท Enterprise Certificate

ขั้นตอนดำเนินการ

1. กรอกใบคำขอใบรับรองอิเล็กทรอนิกส์
2. ยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์พร้อมหลักฐานที่
   หน่วยงานรับลงทะเบียน บริษัท ไทยดิจิทัล ไอดี จำกัด
   319 อาคารจัตุรัสจามจุรี ชั้น 25 ห้อง 10-11 ถนนพญาไท แขวงปทุมวัน เขตปทุมวัน กรุงเทพฯ 10500
   โทรศัพท์. 02-029-0312
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 ไทยดิจิทัล ไอดี
   142 อาคารธนาคารกสิกรไทย ชั้น 4 ห้อง 2 ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพฯ 10500
   โทรศัพท์. 0-2237-6363 โทรสาร. 0-2237-6364
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 การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)

4.2.1 การใช้ฟังก์ชั่นยืนยันและรับรองตัวบุคคล(Performing Identification and Authentication Functions)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะตรวจสอบใบสมัครและหลักฐานการสมัครก่อนออกใบรับรองอิเล็กทรอนิกส์ โดยจะแจ้งให้ผู้ใช้บริการรับทราบ หากข้อมูลในใบสมัครผิดพลาดหรือ เอกสารหลักฐานไม่ครบถ้วน

4.2.2 การอนุมัติหรือปฏิเสธการสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ (Approval or Rejection of Certificate Applications)

หน่วยงานรับลงทะเบียนจะพิจารณาใบสมัคร โดยดูจากใบคำขอใบรับรองอิเล็กทรอนิกส์ และหลักฐานต่างๆที่ใช้ประกอบการพิจารณา ต้องมีความครบถ้วนและถูกต้องตามความเป็นจริง จึงจะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ ให้กับผู้ใช้บริการ โดยหากส่วนหนึ่งส่วนใดหรือทั้งหมดของใบคำขอใบรับรองอิเล็กทรอนิกส์ และ/หรือหลักฐานประกอบการขอใบรับรองอิเล็กทรอนิกส์ ไม่ครบถ้วน ไม่ถูกต้อง ก็จะส่งเอกสารคืนให้แก่ผู้ใช้บริการพร้อมทั้งแจ้งถึงความไม่ถูกต้องดังกล่าว

4.2.3 เวลาที่ใช้ในการดำเนินการสำหรับการออกใบรับรองอิเล็กทรอนิกส์(Time to Process Certificate Applications)

หลังจากได้รับใบคำขอใบรับรองอิเล็กทรอนิกส์แล้ว เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะตรวจสอบหลักฐาน ประกอบใบคำขอใบรับรองอิเล็กทรอนิกส์ หากหลักฐานเอกสารครบถ้วนจะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ให้ภายในวันทำการถัดไป

4.2.4 บริการตรวจสอบตัวตนสำหรับการออกใบรับรองอิเล็กทรอนิกส์จาก CAA Record ของผู้ขอใบรับรอง (Certificate Authority Authorization)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มีบริการตรวจสอบตัวตนจาก CAA Record ของลูกค้า โดยมีกำหนดค่าของ CAA Record คือ “thaidigitalid.com”

4.3 การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)

4.3.1 การทำงานของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในช่วงของการออกใบรับรองอิเล็กทรอนิกส์ (CA Actions During Certificate Issuance)

- เจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบเอกสารหลักฐาน และ CSR file(ถ้ามี) ที่ได้รับจากผู้ใช้บริการ โดยต้องมีความถูกต้องตรงกัน หากพบว่าข้อมูลไม่ตรงกันให้แจ้งผู้ใช้บริการ
- เมื่อตรวจสอบพบข้อมูลถูกต้องแล้ว เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะบันทึกข้อมูลตามใบคำขอใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการ และออกใบรับรองอิเล็กทรอนิกส์
- เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะตรวจสอบความถูกต้องของข้อมูลในใบรับรองอิเล็กทรอนิกส์และใบรับรองอิเล็กทรอนิกส์ที่ออกให้
- เจ้าหน้าที่หน่วยงานรับลงทะเบียนส่งใบรับรองอิเล็กทรอนิกส์ ถึงผู้ใช้บริการผ่านช่องทางที่เหมาะสม

4.3.2 การแจ้งผู้ใช้บริการ หลังจากที่มีการออกใบรับรองอิเล็กทรอนิกส์ (Notification to Subscriber by the CA of Issuance of Certificate)

เมื่อเจ้าหน้าที่รับลงทะเบียนออกใบรับรองอิเล็กทรอนิกส์แล้ว ระบบจะแจ้งข้อมูลของการออกใบรับรองอิเล็กทรอนิกส์ และส่งใบตอบรับใบรับรองอิเล็กทรอนิกส์ ไปให้ผู้ใช้บริการได้รับทราบผ่านทางจดหมายอิเล็กทรอนิกส์ พร้อมทั้งส่งรหัส ONE TIME PASSWORD(OTP) ผ่านทางโทรศัพท์มือถือของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการได้ดำเนินการตามขั้นตอนที่ถูกต้องต่อไป

4.4 การยอมรับใบรับรองอิเล็กทรอนิกส์ (Certificate Acceptance)

4.4.1 หลักปฏิบัติในการยอมรับใบรับรองอิเล็กทรอนิกส์ (Conduct Constituting Certificate Acceptance)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะถือว่าผู้ใช้บริการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ออกให้ก็ต่อเมื่อผู้ใช้บริการดำเนินการตามข้อ 1 หรือ ข้อ 2 ดังต่อไปนี้

1.ผู้ใช้บริการทำการเปิดใช้งานใบรับรองอิเล็กทรอนิกส์ ด้วยรหัส OTP” ผ่านทางหน้าเว็บไซต์

2.ผู้ใช้บริการลงนามในเอกสารใบตอบรับใบรับรองอิเล็กทรอ นิกส์ และส่งกลับมาที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

หากผู้ใช้บริการไม่ได้ทำการเปิดใช้งานใบรับรองอิเล็กทรอนิกส์ผ่านทางระบบ “เปิดใช้งาน(Activate)ใบรับรองอิเล็กทรอนิกส์ ด้วยรหัส OTP หรือ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่ได้รับใบตอบรับใบรับรองอิเล็กทรอกนิกส์ที่ผ่านการลงนามจากผู้ใช้บริการ หลังจากที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้ส่งใบรับรองอิเล็กทรอนิกส์ไปให้ผู้ใช้บริการแล้ว ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะไม่ดำเนินการ Activate ใบรับรองอิเล็กทรอนิกส์ในระบบให้กับผู้ใช้บริการ

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

ใบรับรองอิเล็กทรอนิกส์ที่ได้รับการยอมรับโดยผู้ใช้บริการ จะถูกเผยแพร่ผ่านทาง X.500 Directory ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

4.4.3 **การแจ้งผู้ที่เกี่ยวข้องต่าง ๆว่าด้วยเรื่องของใบรับรองอิเล็กทรอนิกส์ที่ออกโดย ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์** (Notification of Certificate Issuance by the CA to Other Entities)

เมื่อเจ้าหน้าที่รับลงทะเบียนออกใบรับรองอิเล็กทรอนิกส์แล้ว ระบบจะแจ้งข้อมูลของการออกใบรับรองอิเล็กทรอนิกส์ และส่งใบตอบรับใบรับรองอิเล็กทรอนิกส์ ไปให้ผู้ใช้บริการได้รับทราบผ่านทางจดหมายอิเล็กทรอนิกส์ พร้อมทั้งส่งรหัส ONE TIME PASSWORD(OTP) ผ่านทางโทรศัพท์มือถือของผู้ใช้บริการ

4.5 การใช้กุญแจคู่ และใบรับรองอิเล็กทรอนิกส์ (Key Pair and Certificate Usage)

4.5.1 **กุญแจส่วนตัวและการนำไปใช้งานของผู้ใช้บริการ** (Subscriber Private Key and Certificate Usage)

ใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ออกให้แก่ผู้ใช้บริการนั้น ได้มีการจำกัดการใช้งานเพื่อสนับสนุนการใช้ลายมือชื่อดิจิทัล (Digital Signature) และการเข้ารหัสลับข้อมูล (Data Encryption) สำหรับ โปรแกรมประยุกต์ต่างๆเท่านั้น และผู้ใช้บริการไม่สามารถใช้งานกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ได้หลังจากใบรับรองอิเล็กทรอนิกส์ดังกล่าวหมดอายุลงหรือถูกเพิกถอน

4.5.2 **กุญแจส่วนตัวและการนำไปใช้งานของผู้ที่มีส่วนเกี่ยวข้อง**(Relying Party Public Key and Certificate Usage)

ความรับผิดชอบของคู่กรณีที่เกี่ยวข้องในการใช้กุญแจสาธารณะหรือใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ ให้เป็นไปตามระเบียบและเงื่อนไขในการใช้ใบรับรอง

อิเล็กทรอนิกส์แต่ละประเภทที่กำหนดโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อย่างไรก็ตาม คู่กรณีที่เกี่ยวข้องต้องใช้ใบรับรองอิเล็กทรอนิกส์ตามแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) และ ต้องตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ตามที่กำหนดในแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement)

4.6 การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal)

4.6.1 กรณีในการขอต่ออายุใบรับรองอิเล็กทรอนิกส์ (Circumstance for Certificate Renewal)

ในปัจจุบันผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีนโยบายในการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการ โดยไม่มีการเปลี่ยนแปลงกุญแจสาธารณะของผู้ใช้บริการ หรือข้อมูลอื่นใดที่ปรากฏในใบรับรองอิเล็กทรอนิกส์

ในทุกๆวัน หากมีใบรับรองอิเล็กทรอนิกส์ที่กำลังจะหมดอายุลงในอีก 60 วัน หรือ 30 วันข้างหน้า ระบบจะส่งจดหมายอิเล็กทรอนิกส์ แจ้งเตือนไปยังผู้ใช้บริการให้รับทราบ เพื่อให้ผู้ใช้บริการดำเนินการขอใบรับรองใหม่แทนใบรับรองเดิมที่ใกล้หมดอายุ ตามข้อ 4.1

4.6.2 ผู้ที่สามารถขอต่ออายุใบรับรองอิเล็กทรอนิกส์ (Who may Request Renewal)

ไม่มีบริการ

4.6.3 การดำเนินการขอต่ออายุใบรับรองอิเล็กทรอนิกส์ (Processing Certificate Renewal Request)

ไม่มีบริการ

4.6.4 การแจ้งเตือนผู้ใช้บริการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ใหม่ (Notification of New Certificate Issuance to Subscriber)

ไม่มีบริการ

4.6.5 การดำเนินการเพื่อยอมรับใบรับรองอิเล็กทรอนิกส์ใหม่(Conduct Constituting Acceptance of a Renewal Certificate)

ไม่มีบริการ

4.6.6 การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ใหม่โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Publication of the Renewal Certificate by the CA)

ไม่มีบริการ

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

ไม่มีบริการ

4.7 การรับรองกุญแจคู่ใหม่ (Certificate Re-key)

4.7.1 กรณีการขอใบรับรองอิเล็กทรอนิกส์ใบใหม่(Circumstance for Certificate Re-Key)

ผู้ใช้บริการสามารถยื่นใบคำขอใบรับรองอิเล็กทรอนิกส์ และเอกสารประกอบ เพื่อขอใบรับรองอิเล็กทรอนิกส์ใหม่ โดยมีกระบวนการเช่นเดียวกับการยื่นขอใบรับรองอิเล็กทรอนิกส์ใหม่ตามข้อ 4.1

4.7.2 ผู้ที่สามารถขอกุญแจสาธารณะใหม่(Who may Request Certificate of a New Public Key)

อ้างอิงตามข้อ 4.1

4.7.3 ขั้นตอนในการขอกุญแจสาธารณะใหม่(Processing Certificate Re-Keying Requests)

อ้างอิงตามข้อ 4.1

4.7.4 การแจ้งเตือนผู้ใช้บริการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ใหม่ (Notification of New Certificate Issuance to Subscriber)

อ้างอิงตามข้อ 4.3 และ 4.4

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

อ้างอิงตามข้อ 4.3 และ 4.4

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

อ้างอิงตามข้อ 4.3 และ 4.4

4.7.7 การแจ้งเตือนไปยังหน่วยงานที่เกี่ยวข้องโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (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 Certificate Modification)

ในกรณีที่ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลใบรับรองอิเล็กทรอนิกส์ที่ได้ออกไปแล้วนั้น จะต้องยื่นเอกสารเพื่อขอยกเลิกใบรับรองอิเล็กทรอนิกส์ใบเดิม พร้อมทั้งเอกสารเพื่อขอสมัครใหม่เท่านั้น

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 ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะดำเนินการก็ต่อเมื่อได้รับคำขอยกเลิกหรือพักใช้ใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการและเจ้าหน้าที่ได้ตรวจสอบเอกสารดังกล่าวเรียบร้อยแล้ว หรือได้รับคำสั่งโดยชอบด้วยกฎหมายให้ดำเนินการดังกล่าว

4.9.1 **เหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์** (Circumstances for Revocation)

การเพิกถอนใบรับรองอิเล็กทรอนิกส์ คือ การทำให้ใบรับรองอิเล็กทรอนิกส์ไม่สามารถนำมาใช้ได้อีกต่อไป โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หรือผู้ใช้บริการสามารถเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ในกรณีดังต่อไปนี้

- มีผู้อื่นล่วงรู้กุญแจส่วนตัว หรือมีผู้อื่นสามารถเข้าถึง หรือนำกุญแจส่วนตัวของผู้ใช้บริการไปใช้งาน
- มีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ผู้ใช้บริการ
- อุปกรณ์ที่ใช้ในการเก็บกุญแจส่วนตัวสูญหาย หรือไม่สามารถใช้งานได้
- องค์กรของผู้ใช้บริการได้เลิกกิจการ
- ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลที่อยู่ในใบรับรองอิเล็กทรอนิกส์ เช□น ชื่อ-นามสกุล เป็นต้น
- ผู้ใช้บริการไม่ปฏิบัติตามระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ของ ผู้ให้บริการ หรือ แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) หรือ ข้อตกลงการใช้บริการ
- มีคำสั่งของศาลหรือต้องดำเนินการตามกฎหมาย
- มีผู้อื่นที่ล่วงรู้กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ระงับหรือยกเลิกการให้บริการ
- กรณีอื่นๆที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์พิจารณาแล้วว่าจะมีผลกระทบต่อความมั่นคงปลอดภัยของการให้บริการออกใบรับรองอิเล็กทรอนิกส์

4.9.2 **ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้** (Who Can Request Revocation)

- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียน
- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์

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

1. ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์กรอกใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์ พร้อมทั้งลงลายมือชื่อกำกับ
2. ส่งใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐานประกอบให้เจ้าหน้าที่หน่วยงานรับลงทะเบียน โดยหลักฐานมีดังต่อไปนี้ คือ
   - กรณีสมัครมาในนามบุคคล ให้ใช้สำเนาบัตรประชาชนของผู้ใช้บริการ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง(Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
   - กรณีสมัครมาในนามองค์กร ให้ใช้สำเนาหนังสือรับรองการเป็นนิติบุคล ที่มีอายุไม่เกิน 90 วัน(3 เดือน) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยกรรมการ ผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท(ถ้ามี) และสำเนาบัตรประชาชนของกรรมการผู้มีอำนาจ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติ ให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
     - กรณีกรรมการผู้มีอำนาจมอบอำนาจให้ผู้อื่นดำเนินการแทน
       - ให้เพิ่มหนังสือมอบอำนาจ พร้อมปิดอากรแสตมป์ 30 บาทตามจำนวนผู้รับมอบอำนาจ
       - สำเนาบัตรประชาชนของผู้รับมอบอำนาจ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
3. เจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐาน
4. หลังจากเจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์และหลักฐานเรียบร้อย เจ้าหน้าที่หน่วยงานรับลงทะเบียนจึงจะเพิกถอนใบรับรองอิเล็กทรอนิกส์

<u>หมายเหตุ</u>

การเพิกถอนใบรับรองอิเล็กทรอนิกส์ ไม่ได้เป็นเพียงแค่การลบใบรับรองอิเล็กทรอนิกส์ออกไปจากฐานข้อมูล แต่ใบรับรองที่ถูกเพิกถอน จะมีสถานะยกเลิกอย่างถาวรในระบบ CA

4.9.4 **ระยะเวลาที่ใช้ในการเพิกถอน** (Revocation Request Grace Period)

หลังจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้รับใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์ และได้ตรวจสอบความถูกต้องของใบคำขอยกเลิกใบรับรองอิเล็กทรอนิกส์ และเอกสารประกอบแล้ว โดยปกติผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะเพิกถอนใบรับรองอิเล็กทรอนิกส์ในทันที แต่ไม่เกินภายในวันถัดไป

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)

ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าไปตรวจสอบ CRL ได้ที่

http://www.thaidigitalid.com/tdidcag3crl/certdist?cmd=crl&issuer=CN%3dThai+Digital+ID+CA+G3%2cO%3dThai+Digital+ID+Company+Limited%2cC%3dTH

4.9.7 **ความถี่ของการอัพเดต** CRL (CRL Issuance Frequency)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะอัพเดต CRL ทุก 20 นาที และหากในระหว่างนั้น มีการขอเพิกถอนใบรับรอง อิเล็กทรอนิกส์เพิ่มเติม ใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนนั้นจะไปอยู่ใน CRL รอบถัดไป

4.9.8 **ระยะเวลาในการเผยแพร่** CRL(Maximum Latency for CRLs)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะทำการเผยแพร่ CRL ไปยังหน้าเว็บไซต์ภายในระยะเวลาไม่เกิน 1 ชั่วโมง

4.9.9 **การตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์** (On-line Revocation/Status Checking Availability)

ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าไปตรวจสอบ OCSP ได้ที่

http://www.thaidigitalid.com/tdidcag3ocsp

4.9.10 **การตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์**(On-Line Revocation Checking Requirements)

อ้างอิงตามข้อ 4.9.9

4.9.11 **การเผยแพร่ข้อมูลสถานะใบรับรองอิเล็กทรอนิกส์แบบอื่น**(Other Form of Revocation Advertisements Available)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีบริการแจ้งข้อมูลใบรับรองอิเล็กทรอนิกส์ที่ถูกยกเลิก นอกเหนือไปจากบริการในรูปแบบของ CRL และ OCSP

4.9.12 **การออกกุญแจใหม่ให้เป็นกรณีพิเศษหากมีการรั่วไหลของกุญแจเดิม**(Special Requirements Re-Key Compromise)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีนโยบายในการจัดการกับการรั่วไหลของข้อมูลสำคัญ และความต่อเนื่องของการให้บริการ โดยถ้ามีการรั่วไหลของข้อมูลสำคัญที่เกี่ยวข้องกับกุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หรือผู้ใช้บริการ จะมีการแจ้งให้ผู้ใช้บริการทราบและเพิกถอนหรือพักใช้ใบรับรองอิเล็กทรอนิกส์ที่เกี่ยวข้องดังกล่าว

4.9.13 **เหตุการณ์ที่ต้องขอพักใช้ใบรับรองอิเล็กทรอนิกส์ชั่วคราว** (Circumstances for Suspension)

การขอพักใช้ใบรับรองอิเล็กทรอนิกส์ชั่วคราว คือ การทำให้ไม่สามารถนำใบรับรองอิเล็กทรอนิกส์ มาใช้ได้ชั่วคราว โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือผู้ใช้บริการจะสามารถพักใช้ใบรับรองอิเล็กทรอนิกส์ ได้ในกรณีดังต่อไปนี้

- คาดว่าอาจจะมีผู้อื่นล่วงรู้กุญแจส่วนตัว หรือคาดว่าอาจจะมีผู้อื่นสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ใช้บริการไปใช้งาน
- คาดว่าอาจจะมีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ใช้บริการ
- ผู้ใช้บริการไม่ปฏิบัติตามระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ของ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือ แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) หรือข้อตกลงการใช้บริการ
- มีคำสั่งของศาลหรือต้องดำเนินการตามกฎหมาย

4.9.14 **ผู้ที่สามารถขอพักใช้ใบรับรองอิเล็กทรอนิกส์ชั่วคราว** (Who Can Request Suspension)

- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียน
- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์

4.9.15 **ขั้นตอนการขอพักใช้ใบรับรองอิเล็กทรอนิกส์ชั่วคราว** (Procedure for Suspension Request)

จะแบ่งเป็น 2 กรณีดังต่อไปนี้

- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์โทรศัพท์แจ้งขอพักใช้ใบรับรองอิเล็กทรอนิกส์ชั่วคราว (Suspension) ต่อหน่วยงานรับลงทะเบียนเจ้าหน้าที่ลงทะเบียน (RA Officer) จะดำเนินการ พักใช้ใบรับรองอิเล็กทรอนิกส์นั้นทันทีหลังจากยืนยันตัวตนของผู้ขอใบรับรองแล้ว

- กรณีผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์ส่งแบบฟอร์มพักใช้ใบรับรองอิเล็กทรอนิกส์ชั่วคราว (Suspension) แก่เจ้าหน้าที่รับลงทะเบียน เจ้าหน้าที่จะดำเนินการ พักใช้ใบรับรองอิเล็กทรอนิกส์ภายใน 1 วันทำการ หลังจากยืนยันตัวตนของผู้ขอใบรับรองแล้ว

4.9.16 **ความจำกัดของเวลาในการพักใช้ใบรับรองอิเล็กทรอนิกส์**(Limits on Suspension Period)

การขอพักใช้งานแต่ละครั้งสามารถกระทำได้ในระยะเวลา 45 วันเท่านั้น

4.10 บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)

ผู้ใช้บริการ และ/หรือ คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้ทางเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือสามารถโทรมาสอบถามได้ที่หน่วยงานรับลงทะเบียน

4.10.1 **ลักษณะของการกระทำการ** (Operational Characteristics)

ผู้ที่มีส่วนเกี่ยวข้องสามารถเข้าใช้และตรวจสอบ CRL ได้ที่

http://www.thaidigitalid.com/tdidcag3crl/certdist?cmd=crl&issuer=CN%3dThai+Digital+ID+CA+G3%2cO%3dThai+Digital+ID+Company+Limited%2cC%3dTH

และสามารถเข้าใช้และตรวจสอบ OCSP ได้ที่

http://www.thaidigitalid.com/tdidcag3ocsp

4.10.2 **ช่วงเวลาในการให้บริการ** (Service Availability)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ให้บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ผ่านทางเว็บไซต์ ตลอด 24 ชั่วโมง

4.10.3 **การบริการเพิ่มเติม** (Optional Features)

ไม่มีบริการ

4.11 การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription)

ผู้ใช้บริการสามารถเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ได้ โดยดำเนินการตามข้อ 4.9.3 ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์

4.12 การเก็บรักษาและการกู้คืนกุญแจ(Key Escrow and Recovery)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ไม่มีนโยบายการเก็บรักษากุญแจส่วนตัวของผู้ใช้บริการ ดังนั้นผู้ใช้บริการมีหน้าที่ในการจัดเก็บรักษากุญแจส่วนตัว ให้มีความปลอดภัย และ กุญแจส่วนตัวที่ออกให้โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์นั้น จะต้องนำมาใช้งานให้เหมาะสมกับประเภทของใบรับรองอิเล็กทรอนิกส์ที่ออกให้เท่านั้น

4.12.1 **นโยบายในการเก็บรักษาและกู้คืนกุญแจ**(Key Escrow and Recovery Policy and Practices)

อ้างอิงตามข้อ 4.12

4.12.2 **แนวทางในการเก็บรักษาและกู้คืนกุญแจ**(Session Key Encapsulation and Recovery Policy and Practices)

อ้างอิงตามข้อ 4.12

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

5.1 การควบคุมความมั่นคงปลอดภัยทางกายภาพ (Physical Controls)

5.1.1 สถานที่ตั้งและการก่อสร้าง (Site Location and Construction)

สถานที่ตั้งของหน่วยงานออกใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตั้งอยู่ที่319 อาคารจัตุรัสจามจุรี ชั้น 25 ห้อง 10-11 ถนนพญาไท แขวงปทุมวัน เขตปทุมวัน กรุงเทพฯ 10330 ซึ่งมีการปฏิบัติงานในสิ่งแวดล้อมที่มีความปลอดภัยตามมาตรฐาน ISO27001 (Information Security Management System : ISMS) และมาตรฐาน WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) เพื่อประโยชน์ในการรักษาความปลอดภัยทางด้านกายภาพของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์จึงได้ติดตั้งอุปกรณ์รักษาความปลอดภัย ณ สถานที่ตั้งของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ดังนี้

1) โทรทัศน์วงจรปิด เพื่อประโยชน์ในการบันทึกภาพเหตุการณ์ภายในสถานที่ตั้ง

2) Door Hold Open Sounder ซึ่งจะส่งเสียงร้องเตือนเมื่อมีการเปิดประตูทิ้งค้างไว้เพื่อความปลอดภัยของสถานที่ตั้ง

4) ระบบ Smoke Detector เพื่อตรวจจับควันไฟ

5) อุปกรณ์ดับเพลิงแบบ FM-200 ซึ่งมี (ก๊าซ) สารดับเพลิงที่ไม่ก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์

6) เสริมเหล็กทุกด้านของห้องที่ติดตั้งระบบให้บริการใบรับรองอิเล็กทรอนิกส์เพื่อป้องกันการทุบ ขุด หรือเจาะผนัง เพดาน หรือพื้น

5.1.2 การเข้าถึงทางกายภาพ (Physical Access)

การเข้าถึงพื้นที่ของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ จะอนุญาตให้สามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ผู้มีสิทธิ หรือ ผู้มาเยือนภายใต้การดูแลจากเจ้าหน้าที่ผู้มีสิทธิเท่านั้น โดยในการที่จะเข้าถึงพื้นที่ของระบบได้นั้นเจ้าหน้าที่จำเป็นต้องใช้รหัสผ่าน บัตรประจำตัวพนักงาน (RFID) และต้องผ่านการสแกนลายนิ้วมือ (Fingerprint Scan) ทั้งนี้ ได้กำหนดจำนวนเจ้าหน้าที่ ผู้มีสิทธิให้มีจำนวนน้อยที่สุด พร้อมทั้งจัดเก็บข้อมูลบันทึกการเข้าออกในพื้นที่บริการทั้งหมดด้วย

สถานที่ตั้งของผู้ให้บริการมีการควบคุมการเข้าถึงและการจัดแบ่งพื้นที่ตามระดับความปลอดภัย และอนุญาตให้สามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ผู้มีสิทธิ หรือ ผู้มาเยือนภายใต้การดูแลจากเจ้าหน้าที่ผู้มีสิทธิเท่านั้น

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

ระบบบริการทั้งหมดจะใช้ระบบไฟฟ้าจากแหล่งจ่ายไฟฟ้าแบบมาตรฐาน พร้อมทั้งยังมีเครื่องกำเนิดไฟฟ้าแบบส่วนตัวและเครื่องกำเนิดไฟฟ้าแบบต่อเนื่อง (UPS) เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง ในระบบบริการจะมีระบบปรับอากาศเพื่อควบคุมอุณหภูมิและความชื้นให้คงที่ โดยระบบปรับอากาศในส่วนนี้ จะเป็นอิสระจากระบบปรับอากาศของอาคารที่ตั้ง

5.1.4 **การป้องกันภัยจากน้ำ** (Water Exposures)

ในส่วนพื้นที่ของการปฏิบัติงานได้มีการป้องกันภัยจากน้ำโดยจัดให้พื้นที่บริการอยู่สูงกว่าระดับน้ำและอาคารที่ตั้งไม่ใช่บริเวณที่เกิดน้ำท่วม และตัวอาคารยังได้ออกแบบให้อยู่สูงกว่าบริเวณโดยรอบอีก 6 นิ้ว

5.1.5 **การป้องกันอัคคีภัย** (Fire Prevention and Protection)

ระบบป้องกันอัคคีภัยได้มีการใช้สารประเภท FM-200 ในการดับเพลิง โดยที่ไม่ก่อให้เกิดความเสียหายกับอุปกรณ์ประเภทไฟฟ้าอิเล็กทรอนิกส์หรือคอมพิวเตอร์ ซึ่งจะทำงานร่วมกับอุปกรณ์ตรวจจับควันไฟ (Smoke Detector) ด้วย

5.1.6 **การเก็บรักษาสื่อที่ใช้เก็บข้อมูล** (Media Storage)

สื่อที่ใช้สำรองข้อมูลทุกประเภทจะถูกเก็บรักษาไว้ในห้องที่มีความปลอดภัยในหลายๆ สถานที่

5.1.7 **การกำจัดขยะและอุปกรณ์ที่ไม่ได้นำมาใช้งานแล้ว**(Waste disposal)

การกำจัดขยะ และอุปกรณ์ที่ไม่ได้ใช้งาน จะมีกระบวนการควบคุมในการกำจัดข้อมูลที่ไม่ใช้งาน โดยเป็นไปตามมาตรฐาน ISO 27001

5.1.8 **การสำรองข้อมูลไปไว้ยังสถานที่อื่น** (Off-site backup)

การสำรองข้อมูลจะเป็นการ สำรองข้อมูลจากศูนย์ปฏิบัติงานหลัก ไปที่ ศูนย์ปฏิบัติงานสำรอง ด้วยโปรแกรมอัตโนมัติ โดยกระบวนการสำรองข้อมูลจะเกิดขึ้นทุกวัน

5.2 การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls)

5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles)

จากการที่มีการใช้ระบบควบคุมการเข้าถึงและการบริหารจัดการกุญแจ ทำให้บุคคลเพียงคนเดียวไม่สามารถเข้าถึงระบบได้ทั้งหมด จึงต้องแบ่งบทบาทหน้าที่เพื่อให้เป็นไปตามนโยบายความปลอดภัย โดยเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวทำให้อย่างน้อยจะต้องมีบทบาทดังต่อไปนี้

5.2.1.1 บทบาทของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Trusted Roles for Certification Authority)

แบ่งออกได้ ดังนี้

- ผู้จัดการฝ่าย CA Operation มีหน้าที่ดังนี้
    - บริหารจัดการกุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
    - กำหนดและดูแลนโยบายด้านความมั่นคงที่เกี่ยวข้องกับบริการใบรับรองอิเล็กทรอนิกส์
    - ตรวจสอบการทำงานของเจ้าหน้าที่ System Support และ System Administrator
- เจ้าหน้าที่ System Support มีหน้าที่ดังนี้
    - กำหนดค่าตัวแปรสำคัญต่างๆ ให้กับระบบที่เกี่ยวข้องกับระบบให้บริการใบรับรองอิเล็กทรอนิกส์
    - บริหารและจัดการอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับระบบให้บริการใบรับรองอิเล็กทรอนิกส์
    - กำหนดค่าตัวแปรสำคัญต่างๆ ให้กับอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับระบบให้บริการใบรับรองอิเล็กทรอนิกส์
- เจ้าหน้าที่ System Administrator มีหน้าที่ดังนี้
    - ปรับปรุงประสิทธิภาพการทำงาน (Performance Tuning) และปรับปรุงระบบรักษาความมั่นคง (Security Hardening) ให้กับเครื่องคอมพิวเตอร์
    - บริหารจัดการกุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
    - กำหนดและดูแลนโยบายด้านความมั่นคงที่เกี่ยวข้องกับบริการใบรับรอง
    - ตรวจสอบการทำงานของเจ้าหน้าที่ System Support และ CA Operator

- เจ้าหน้าที่ CA Operator มีหน้าที่ดังนี้
    - บริหารและจัดการเครื่องคอมพิวเตอร์สำหรับระบบให้บริการใบรับรองอิเล็กทรอนิกส์
    - ดูแลระบบปฏิบัติการ (Operating System) ของเครื่องคอมพิวเตอร์
    - บริหารและจัดการระบบจัดเก็บข้อมูลของระบบให้บริการใบรับรองอิเล็กทรอนิกส์

5.2.1.2 บทบาทของเจ้าหน้าที่รับลงทะเบียน (Trusted Roles for Registration Authority)

แบ่งออกได้ ดังนี้

- เจ้าหน้าที่ RA Operator มีหน้าที่ดังนี้
    - รับใบคำขอใบรับรองอิเล็กทรอนิกส์
    - พิสูจน์ความแท้จริงและตัวตนของผู้ใช้บริการ
    - ออกใบรับรองอิเล็กทรอนิกส์ให้กับผู้ใช้บริการ
    - รับคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์
    - เพิกถอนใบรับรองอิเล็กทรอนิกส์ตามคำร้องขอของผู้ใช้บริการ
    - ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์

- เจ้าหน้าที่ RA Auditor มีหน้าที่ดังนี้
    - ตรวจสอบการทำงานของ RA Operator

5.2.2 **จำนวนบุคคลที่ต้องการต่องาน** (Number of Persons Required Per Task)

การแบ่งบทบาทหน้าที่จะถูกแบ่งออกตามที่ได้กล่าวไว้แล้วข้างต้น ซึ่งจะทำให้มีความสมดุลในการปฏิบัติงาน พร้อมกับมีความปลอดภัยสูงสุด และสามารถตรวจสอบได้ โดยหลักการสำคัญสำหรับการแบ่งแยกหน้าที่ คือ

1. CA Operator จะต้องแยกจากการทำหน้าที่ System Administrator เพื่อให้เกิดความเป็นอิสระจากการตรวจสอบบันทึกข้อมูล (audit log)
2. งานใดๆ ก็ตามที่จะต้องมีความเกี่ยวของกับการเปิดระบบ CA รวมทั้งการเข้าถึงระบบฐานข้อมูลจะต้องมีอย่างน้อย 2 บุคคลในการปฏิบัติงาน โดยคนหนึ่งต้องเป็นผู้ปฏิบัติงาน ส่วนอีกคนหนึ่งจะเป็นผู้ตรวจสอบ

5.2.3 **การระบุและพิสูจน์ความมีตัวตนแท้จริงของเจ้าหน้าที่ปฏิบัติงาน** (Identification and Authentication for each Role)

บุคคลากรที่จะมาปฏิบัติงานจะต้องผ่านการคัดเลือกตามกระบวนการมาตรฐานอย่างเป็นทางการเพื่อแสดงถึง “การเป็นบุคคลที่ไว้วางใจได้”

5.2.4 **การแบ่งแยกบทบาทหน้าที่ของผู้ปฏิบัติงาน** (Roles Requiring Separation of Duties)

มีการแยกบทบาทหน้าที่การปฏิบัติงานของเจ้าหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ และ เจ้าหน้าที่รับลงทะเบียน ออกจากกัน

- เจ้าหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ มีหน้าที่หลัก ในการดูแลบริหารจัดการระบบให้บริการใบรับรองอิเล็กทรอนิกส์ และ ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้อง ได้แก่ Database, Firewall, LDAP และการสำรองข้อมูลระบบ
- เจ้าหน้าที่รับลงทะเบียน มีหน้าที่หลักในการตรวจสอบความถูกต้องของใบคำขอใบรับรองอิเล็กทรอนิกส์ และพิจารณาตรวจสอบเอกสารหลักฐานประกอบการขอใบรับรองอิเล็กทรอนิกส์และดำเนินการออกใบรับรองอิเล็กทรอนิกส์ รวมถึงดำเนินการ พักใช้ใบรับรองอิเล็กทรอนิกส์และ เพิกถอนใบรับรองอิเล็กทรอนิกส์

5.3 **การควบคุมดูแลบุคลากร** (Personnel Controls)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะคัดเลือกพนักงานที่มีความน่าเชื่อถือ จากความรู้ความสามารถ ที่มีความเหมาะสมในการปฏิบัติงานที่เกี่ยวข้อง และการคัดเลือกบุคคลเข้าปฏิบัติหน้าที่จะมีการตรวจสอบประวัติอาชญากรรม และเมื่อรับเข้าปฏิบัติหน้าที่แล้วจะมีการตรวจสอบประวัติอาชญากรรมอย่างน้อยทุกๆ 5 ปี

5.3.1 **คุณสมบัติ ประสบการณ์ และ สิทธิในการเข้าถึงข้อมูล** (Qualifications, Experience, and Clearance Requirements)

จบการศึกษาขั้นต่ำในระดับปริญญาตรี ทางด้าน Computer Science, Information Technology, Computer Engineering, หรือสาขาที่เกี่ยวข้อง

5.3.2 **ขั้นตอนในการตรวจสอบประวัติ** (Background Check Procedures)

เมื่อมีการพิจารณาจัดรับพนักงานในเบื้องต้น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะส่งประวัติพนักงานที่จัดรับในขั้นต้นเพื่อตรวจสอบกับทะเบียนประวัติที่สำนักงานตำรวจแห่งชาติ กองตรวจสอบประวัติ หากไม่พบข้อมูลประวัติอาชญากรรม จึงจะพิจารณาบรรจุ หลังผ่านการทดลองงาน 3 เดือน

5.3.3 **การฝึกอบรม** (Training Requirements)

สำหรับพนักงานใหม่ มีหัวข้อที่จะต้องอบรม ดังนี้

- Basic PKI Concept
- Job responsibilities
- Operational policies and procedures
- มาตรฐาน ISO27001
- มาตรฐาน WebTrust for CA

- BCP and DRP plan

5.3.4 **ความถี่ในการฝึกอบรมซ้ำหรือฝึกอบรมเพิ่มเติม** (Retraining Frequency and Requirements)

มีการจัดอบรบทบทวนความรู้เกี่ยวกับหน้าที่ ความรับผิดชอบ ในการปฏิบัติงาน ให้กับเจ้าหน้าที่เป็นประจำทุกปี และอบรมเพิ่มเติม เมื่อมีเทคโนโลยีใหม่ๆ ที่เกี่ยวข้องกับการทำงาน

5.3.5 **การหมุนเวียนหน้าที่และความถี่ของวาระงาน** (Job Rotation Frequency and Sequence)

ทุก ๆ 2 ปี จะมีการประเมินประสิทธิภาพและผลการทำงานของเจ้าหน้าที่ และพิจารณาความเหมาะสมในการ หมุนเวียน หน้าที่ หรือ ปรับตำแหน่งงาน

5.3.6 **บทลงโทษสำหรับการกระทำที่ไม่ได้รับอนุญาต** (Sanctions for Unauthorized Actions)

บทลงโทษให้เป็นไปตามระเบียบ ข้อบังคับ ของบริษัทของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

5.3.7 **การว่าจ้างผู้รับเหมาอิสระ** (Independent Contractor Requirements)

การว่าจ้างผู้รับเหมาอิสระ ให้เป็นไปตามนโยบายของบริษัท และจะต้องมีการจัดทำสัญญาการว่าจ้างตามแต่ละกรณี

5.3.8 **เอกสารสำหรับบุคลากร** (Documentation Supplied to Personnel)

เจ้าหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ และ เจ้าหน้าที่รับลงทะเบียนจะมีคู่มือในการปฏิบัติงานคือ CA Operation Manual และ RA Operation Manual

5.4 ขั้นตอนการตรวจสอบ Audit Log (Audit logging Procedures)

5.4.1 ชนิดของเหตุการณ์ที่ถูกบันทึก (Types of Events Recorded)

เหตุการณ์ที่จะถูกบันทึกในระบบ มีดังนี้

CA Events Recorded

- CA key life cycle management events
- Key Generation, Backup, Storage,
- CA and Subscriber certificate life cycle management
- Certificate application, Renewal, Revocation
- Successful or unsuccessful processing of request

RA Events Recored

- RA Operation log
- Method used to validate identification document

Environment Events Recored

- Security-related events including
- Security profile changes
- System crashes, hardware failures
- Firewall and router activity
- Facility visitor entry/exit

5.4.2 ความถี่ในการบันทึก (Frequency of Processing Log)

Audit Log จะถูกตรวจสอบโดยเจ้าหน้าที่เป็นประจำทุกวัน และหากเกิดเหตุการณ์ที่ต้องสงสัย จะถูกพิจารณาเป็นพิเศษ

การตรวจสอบ Log นั้น ประกอบไปด้วยการตรวจสอบ log และเอกสารที่เกี่ยวข้องกับเหตุการณ์ที่ถูกบันทึกไว้ตาม Log

5.4.3 ระยะเวลาในการเก็บรักษา (Retention Period for Audit Log)

Audit log จะเก็บรักษาไว้ในระบบเป็นเวลา 10 ปี

5.4.4 การป้องกันข้อมูลที่ถูกบันทึก (Protection of Audit Log)

การเข้าถึงข้อมูลรายการของ Audit log จะสามารถเข้าถึงได้เฉพาะบุคคลที่มีสิทธิเท่านั้น

5.4.5 การสำรองข้อมูลที่ถูกบันทึก (Audit Log Backup Procedures)

การสำรองข้อมูลของ Audit log จะมีการสำรองโดยอัตโนมัติและถูกเก็บไว้ทุกวันที่เครื่อง Log Server

5.4.6 **ระบบจัดเก็บข้อมูลตรวจสอบ ภายใน และ ภายนอก** (Audit Collection System (Internal vs. External))

ผู้ให้บริการมีการจัดเก็บ Log ของ OS, Application, Firewall ไว้ที่ Local machine (ที่เครื่อง Log Server) และจัดเก็บข้อมูลดังกล่าวไว้ที่ ศูนย์ปฏิบัติงานสำรอง ด้วย

5.4.7 **การแจ้งเตือนเหตุการณ์** (Notification to Event-Causing Subject)

ในกรณีพบปัญหาจาก Audit log เจ้าหน้าที่ผู้ดูแลระบบมีหน้าที่ตรวจสอบ วิเคราะห์และแจ้งฝ่ายงานที่เกี่ยวข้องสำหรับแต่ละปัญหา

5.4.8 **การประเมินช่องโหว่ของระบบ และ การทดสอบเจาะระบบ** (Vulnerability Assessments & Penetration Testing)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีการประเมินช่องโหว่ของระบบเป็นประจำทุก 3 เดือน และการทดสอบความมั่นคงปลอดภัยโดยการทดสอบ เจาะระบบเป็นประจำทุก 1 ปี

5.5 การจัดเก็บข้อมูลบันทึก (Records Archival)

5.5.1 **ชนิดของข้อมูลบันทึกที่ถูกจัดเก็บ** (Types of Records Archived)

เหตุการณ์ที่จะถูกบันทึกในระบบ มีดังนี้

CA Events Recorded

- CA key life cycle management events
- Key Generation, Backup, Storage,
- CA and Subscriber certificate life cycle management
- Certificate application, Renewal, Revocation
- Successful or unsuccessful processing of request

RA Events Recored

- RA Operation log
- Method used to validate identification document

Environment Events Recored

- Security-related events including
- Security profile changes
- System crashes, hardware failures
- Firewall and router activity
- Facility visitor entry/exit

5.5.2 **ระยะเวลาที่ต้องเก็บรักษา** (Retention Period for Archive)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะจัดเก็บข้อมูลเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ เป็นเวลา 10 ปี และจัดเก็บข้อมูลระบบงานออกใบรับรองอิเล็กทรอนิกส์ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

5.5.3 **การป้องกันที่จัดเก็บบันทึก** (Protection of Archive)

ระบบจัดเก็บข้อมูลเกี่ยวกับใบรับรับรองอิเล็กทรอนิกส์ จะสามารถเข้าถึงได้โดยผู้ที่มีสิทธิเท่านั้น

5.5.4 **การสำรองข้อมูลที่ถูกจัดเก็บ** (Archive Backup Procedures)

การสำรองข้อมูล จะเป็นการสำรองข้อมูลจากศูนย์ปฏิบัติงานหลัก ไปศูนย์ปฏิบัติงานสำรอง เป็นประจำทุกวัน

5.5.5 **ความต้องการระบบบันทึกเวลา** (Requirements for Time-Stamping of Records)

ใบรับรองอิเล็กทรอนิกส์ และ CRLs ทุกใบจะมีวันที่ และเวลา กำกับอยู่ด้วยเสมอ

5.5.6 **ระบบการจัดเก็บเอกสารทั้งภายในและภายนอก** (Archive collection system (internal or external)

ข้อมูลในข้อ 5.5.1 จะถูกจัดเก็บทั้งในรูปแบบของ hard copy และ soft file โดยจัดเก็บไว้ที่ศูนย์ปฏิบัติงานหลัก และศูนย์ปฏิบัติงานสำรอง

5.5.7 **ขั้นตอนในการตรวจสอบความถูกต้องของข้อมูลที่ถูกจัดเก็บ** (Procedures to obtain and verify archive information)

มีเพียงผู้ที่ได้รับอนุญาติเท่านั้นถึงจะสามารถเข้าถึงข้อมูลที่ถูกจัดเก็บได้ ส่วนความถูกต้องสมบูรณ์ของข้อมูลนั้นจะถูกตรวจสอบหากมีการนำข้อมูลดังกล่าวมาใช้ใหม่

5.6 การเปลี่ยนแปลงกุญแจ (Key Changeover)

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

5.7 ความเสียหายและการกู้คืนหลังภัยพิบัติ (Compromise and Disaster Recovery)

5.7.1 **กระบวนการจัดการความผิดพลาดจากระบบ** (Incident and compromise handling procedures)

ในกรณีเกิดเหตุความผิดพลาดจากระบบ หรือความเสียหายใดจากระบบ ตลอดจนการเกิดภัยพิบัติ ต่างๆ ให้ปฏิบัติตามขั้นตอนในเอกสาร BCP/DRP

5.7.2 **การเสื่อมสภาพของทรัพยากรคอมพิวเตอร์ ซอฟต์แวร์ และ/หรือ ข้อมูล** (Computing resources, software, and/or data are corrupted)

การจัดการดูแลทรัพยากรต่างๆ จะมี การซ่อมบำรุง (MA plan) และการตรวจสอบอายุการใช้งาน ทั้งนี้หาก ทรัพยากรด้าน Hardware, Software หรือ ข้อมูลใด มีการเสื่อมสภาพ ก็จะถูกทำลาย และจัดการตามนโยบายความปลอดภัยของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

5.7.3 **การดำเนินการหลังการรั่วไหลของกุญแจส่วนตัว** (Entity private key compromise procedures)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนกส์มีนโยบายในการจัดการกับการรั่วไหลของข้อมูลสำคัญ และความต่อเนื่องของการให้บริการ โดยถ้ามีการรั่วไหลของข้อมูลสำคัญที่เกี่ยวข้องกับกุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนกส์หรือผู้ใช้บริการ โดยจะมีการแจ้งทาง NRCA และผู้ใช้งานใบรับรองที่เกี่ยวข้อง และทำการยกเลิกกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ที่เกี่ยวข้องดังกล่าวทันที หลังจากทราบว่ามีการรั่วไหลของกุญจส่วนตัว

5.7.4 **ความสามารถในการบริหารธุรกิจอย่างต่อเนื่องหลังเหตุภัยพิบัติ** (Business continuity capabilities after a disaster)

ในกรณีที่เกิดปัญหา หรือเหตุการณ์อันมีเหตุให้ระบบงานต้องหยุดชะงัก ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้จัดทำแผนสำรอง (Business Continuity Plan) และแผนฉุกเฉิน (Disaster Recovery Plan) เพื่อจัดการกับเหตุการณ์ดังกล่าว

5.8 การเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และหน่วยงานรับลงทะเบียน (CA or RA Termination)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือหน่วยงานรับลงทะเบียนมีความจำเป็นต้องเลิกกิจการ การให้บริการออกใบรับรองอิเล็กทรอนิกส์ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะแจ้งให้ทาง NRCA และผู้ใช้บริการทราบล่วงหน้าอย่างน้อย 60 วัน โดยในกรณีนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะเป็นผู้หาวิธีการในการโอนย้ายระบบ หรือ จัดหาระบบใหม่แทน หรือ มีมาตรการอื่นที่เหมาะสมสำหรับการแก้ไขผลกระทบในการยกเลิกระบบให้บริการใบรับรองอิเล็กทรอนิกส์ แก่ผู้ใช้บริการ

6 การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

6.1 การสร้างและติดตั้งคู่กุญแจ (Key Pair Generation and Installation)

6.1.1 การสร้างกุญแจคู่ (Key Pair Generation)

กุญแจคู่ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะถูกสร้างและติดตั้งโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และถูกจัดเก็บอยู่ใน Hardware Security Module (HSM) ส่วน กุญแจคู่ของผู้ใช้บริการ จะถูกสร้างและถูกติดตั้งในสื่ออิเล็กทรอนิกส์ Smartcard, USB Token หรือ HSM หรือถูกจัดเก็บในรูปของ File ซึ่งมีรหัสลับ และเก็บรักษาโดยผู้ใช้บริการเอง

การสร้างกุญแจคู่ของ CA จะถูกจัดการโดยอุปกรณ์ที่เรียกว่า Hardware Security Module ซึ่งสอดคล้องตามมาตรฐานสากล Federal Information Processing Standard (FIPS) 140-2 Level 3 ส่วนการสร้างกุญแจคู่ของผู้ใช้บริการ จะใช้อุปกรณ์ Smartcard, USB Token หรือ HSM ซึ่งสอดคล้องตามมาตรฐานสากล Federal Information Processing Standard (FIPS) 140-2 Level 2 หรือ Level 3

6.1.2 การส่งมอบกุญแจส่วนตัว (Private Key Delivery to subscriber)

กุญแจส่วนตัวของผู้ใช้บริการจะถูกสร้างและจัดเก็บอยู่ในสื่ออิเล็กทรอนิกส์ Smartcard, USB Token หรือ Hardware Security Module (HSM) ซึ่งเป็นอุปกรณ์จัดเก็บรักษากุญแจส่วนตัวที่มีความปลอดภัยสูง ไม่สามารถคัดลอก กุญแจส่วนตัวและข้อมูลอื่นใดออกไปได้โดยสื่ออิเล็กทรอนิกส์ดังกล่าว 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 การส่งมอบกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปยังคู่กรณีที่เกี่ยวข้อง (CA Public Key Delivery to relying Parties)

กุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะถูกส่งไปยังคู่กรณีที่เกี่ยวข้อง โดยอาจส่งไปพร้อมกับใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ หรือสามารถดาวน์โหลดได้จากเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

6.1.5 **ขนาดของกุญแจ** (Key Sizes)

ขนาดกุญแจของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะมีขนาด 4096 บิต ส่วนขนาดกุญแจของผู้ใช้บริการ จะ มีขนาดอยู่ที่ 2048 บิต

6.1.6 **การสร้างตัวแปรกุญแจสาธารณะ** (Public Key Parameters Generation & Quality Checking)

ตัวแปรที่ใช้ในการสร้างกุญแจสาธารณะจะถูกสร้างโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยยึดตามมาตรฐาน X.509 Version 3 และคุณภาพของตัวแปรของกุญแจสาธารณะ จะถูกตรวจสอบโดยอัตโนมัติจากโปรแกรมในระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.1.7 **จุดประสงค์ของการใช้กุญแจ** (Key Usage Purposes)

จุดประสงค์ของการใช้กุญแจได้ถูกอธิบายไว้ในหัวข้อ 1.4 การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)

6.2 การปกป้องกุญแจส่วนตัวและการควบคุมโมดูลสำหรับการเข้ารหัส (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 ซึ่งเป็นมาตรฐานสากลในการสร้างและเก็บรักษากุญแจส่วนตัวของระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.2.2 **การควบคุมกุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์** (Private Key (n out of m) Multi-Person Control)

กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้มีการควบคุมการเข้าถึงแบบหลายบุคคล

6.2.3 **การฝากกุญแจส่วนตัว** (Private Key Escrow)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีนโยบายในการรับฝากกุญแจส่วนตัว

6.2.4 **การสำรองกุญแจส่วนตัว** (Private Key Backup)

มีการสำรองกุญแจส่วนตัวเฉพาะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

6.2.5 **การบันทึกกุญแจส่วนตัวถาวร** (Private Key Archival)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีนโยบายในการการบันทึกถาวรกุญแจส่วนตัว

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 **การเก็บกุญแจส่วนตัวลงบนโมดูลที่มีการเข้ารหัส**(Private Key storage on cryptographic module)

กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ ของผู้ใช้บริการจะถูกจัดเก็บลงบน อุปกรณ์จัดเก็บที่ได้มาตรฐาน FIPS 140-2 Level 2 และ Level 3

6.2.8 **วิธีการนำกุญแจส่วนตัวมาใช้งาน** (Method of Activating Private Key)

กุญแจส่วนตัวของ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และของผู้ใช้บริการ จะถูกนำมาใช้งานได้เมื่อมีการตรวจสอบสิทธิผ่านอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยขั้นสูง และมีการใส่รหัสผ่านที่ถูกต้อง

6.2.9 **วิธีเลิกการใช้งานกุญแจส่วนตัว** (Method of Deactivating Private Key)

กุญแจส่วนตัวจะเลิกใช้งานได้ก็ต่อเมื่อมีการร้องขอจากผู้ใช้บริการ ให้เพิกถอนการใช้งานกุญแจส่วนตัวนั้น

6.2.10 **การทำลายกุญแจส่วนตัว** (Method of destroying private key)

ในกรณีที่ผู้ใช้บริการต้องการทำลายกุญแจส่วนตัว ให้ใช้โปรแกรมประยุกต์ในการเขียนค่าทับกุญแจส่วนตัว (Overwriting the key)

6.2.11 **ระดับของโมดูลที่มีการเข้ารหัส** (Cryptographic Module Rating)

กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ กุญแจส่วนตัวของผู้ใช้บริการ ถูกสร้างจากซอฟต์แวร์ที่ได้มาตรฐาน

6.3 รายละเอียดอื่นเกี่ยวกับการจัดการกุญแจคู่ (Other Aspects of Key Pair Management)

6.3.1 การเก็บรักษากุญแจสาธารณะ (Public Key Archival)

กุญแจสาธารณะจะถูกเก็บบันทึกไว้ในใบรับรอง โดยใบรับรองได้ถูกจัดเก็บไว้ในฐานข้อมูลของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตลอดอายุของใบรับรอง

6.3.2 ระยะเวลาใช้งานใบรับรองและกุญแจคู่ (Certificate operational periods and key pair usage periods)

ระยะเวลาใช้งานใบรับรองอิเล็กทรอนิกส์ และกุญแจคู่ ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ คือ 18 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 การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ (Activation Data Protection)

การป้องกันข้อมูลที่ที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ จะเป็นไปตามกลไกการป้องกันข้อมูลด้วยอุปกรณ์ HSM ที่ได้ตามมาตรฐาน FIPS 140-2 Level 2 หรือ Level 3 เช่น อาจมีการใช้รหัสลับ หรือ กระบวนการยืนยันตัวตนอื่นใดเพื่อใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์

6.4.3 ข้อมูลด้านอื่นที่ใช้ในการติดตั้งใบรับรองอิเล็กทรอนิกส์ (Other Aspects of Activation Data)

ไม่มีข้อมูลอื่นใดนอกเหนือจาก ข้อมูลสำคัญที่ใช้ในการสมัครขอใบรับรองอิเล็กทรอนิกส์

6.5 การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)

6.5.1 ข้อกำหนดทางเทคนิคที่มีลักษณะเฉพาะในการรักษาความปลอดภัยของคอมพิวเตอร์ (Specific Computer Security Technical Requirements)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้จัดตั้งแผนความปลอดภัยของระบบ ที่ได้รวมข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน ISO27001 (Information Security Management System : ISMS) และมาตรฐาน WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities)

6.5.2 การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้มีการจัดตั้งแผนความปลอดภัยของระบบ ที่ได้แบ่งระดับในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน ISO27001 (Information Security Management System : ISMS) และมาตรฐาน WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities)

6.6 การควบคุมวงจรทางเทคนิคของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ (Life Cycle Security Controls)

6.6.1 การควบคุมการพัฒนาระบบให้บริการใบรับรองอิเล็กทรอนิกส์(System Development Controls)

ซอฟต์แวร์ของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ ได้ถูกพัฒนาภายใต้การควบคุมที่มีคุณภาพอย่างเหมาะสม โดยเป็นไปตามข้อกำหนดของ Information Technology Security Evaluation Criteria Level E3 (ITSEC E3)

6.6.2 การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัย (Security Management Controls)

การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัยจะถูกควบคุมและบริหารภายใต้ระบบมาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ ISO27001 (Information Security Management System : ISMS) และมาตรฐาน WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) ทั้งในส่วนของ อุปกรณ์ (Tools) กระบวนการ (Procedure) และ บุคลากรซึ่งถูกควบคุมตามบทบาทหน้าที่ของเจ้าหน้าที่ผู้ดูแลระบบที่ได้กำหนดสิทธิไว้แล้ว ตามหัวข้อ 5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles)

6.6.3 การแบ่งระดับความปลอดภัยของวงจรทางเทคนิคของระบบให้บริการใบรับรองอิเล็กทรอนิกส์ (Life Cycle Security Ratings)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้มีการจัดสร้างเอกสารการประเมินความเสี่ยงเกี่ยวกับความปลอดภัย ซึ่งได้มีการระบุและจัดการกับความเสี่ยงที่ระดับสูงและสูงมากเกี่ยวกับความปลอดภัยของวงจรทางเทคนิคของระบบให้บริการใบรับรองอิเล็กทรอนิกส์

6.7 การควบคุมความปลอดภัยทางเครือข่าย (Network Security Controls)

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

6.8 การบันทึกเวลารายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน (Timestamping)

ใบรับรองอิเล็กทรอนิกส์ ที่ถูกเพิกถอนทุกใบ จะมีข้อมูลวันที่ และเวลา ที่ถูกเพิกถอนกำกับลงไปด้วย

7 รูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน และ OCSP (Certificate, CRL, and OCSP Profiles)

7.1 รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)

7.1.1 เลขรุ่น (Version number(s))

ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้มาตรฐาน X.509 Version 3 Certificate ซึ่งมีรายการดังต่อไปนี้

- Version 3 : รุ่นที่ 3
- Serial Number : หมายเลขของใบรับรองอิเล็กทรอนิกส์
- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลของ TDID CA
- Issuer : ชื่อของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- Validity : วันเวลาที่เริ่มและสิ้นสุดการใช้ใบรับรองอิเล็กทรอนิกส์
- Subject : เลขบัตรประจำตัวประชาชนหรือเลขประจำตัวผู้เสียภาษีขององค์กร
- Subject Public Key Information : กุญแจสาธารณะของผู้ใช้บริการและวิธีการที่ใช้ในการสร้าง

7.1.2 ข้อมูลเพิ่มเติมของใบรับรอง (Certificate Extension)

ข้อมูลเพิ่มเติมของใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้มาตรฐาน X.509 V.3 certificate extensions ซึ่งมีรายการอย่างน้อยดังต่อไปนี้

- Authority Key Identifier : ระบุถึงกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- Key Usage : วัตถุประสงค์ในการนำกุญแจไปใช้งาน
- Extended Key Usage : วัตถุประสงค์เพิ่มเติมในการนำกุญแจไปใช้งาน
- CRL Distribution Points : ระบุถึงที่อยู่ของรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ เพื่อใช้ตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์
- Basic Constraints : ระบุถึงประเภทของใบรับรองอิเล็กทรอนิกส์ว่าเป็นของผู้ใช้บริการหรือผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และจำนวนชั้นสูงสุดของห่วงโซ่ใบรับรองอิเล็กทรอนิกส์ (Certificate Chain) ที่ถูกทำการรับรองต่อกันเป็นทอดๆ
- Certificate Policies : ระบุถึงข้อมูลเพื่อใช้อ้างอิงไปยังเอกสารแนวนโยบายใบรับรองอิเล็กทรอนิกส์ โดยระบุในรูปของ Object Identifier (OID)

7.1.3 อัลกอริธึมสำหรับการสร้างคู่คีย์ (Algorithm object identifiers)

Algorithm ที่ใช้ในการออกใบรับรองอิเล็กทรอนิกส์คือ SHA-512RSA

7.1.4 **รูปแบบของชื่อ** (Name Forms)

รูปแบบของชื่อในส่วนของ Certificate Issuer และ Certificate Subject ที่ระบุในใบรับรองอิเล็กทรอนิกส์ที่ออกโดย ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ คือ ชื่อเฉพาะตามมาตรฐาน X.500

รูปแบบการตั้ง Distinguished Name (DN) ของ TDID CA จะใช้ข้อมูลดังนี้

C	=	TH
S	=	<State>
L	=	<Locality>
O	=	<Customer Corporate name in English>
organizationIdentifier	=	<Customer Corporate tax ID>
OU	=	<Department Name in English >
Title	=	<Position in organization>
Serial Number	=	<identification ID>
Givenname	=	<Customer First Name in Thai>
SN	=	<Customer Last Name in Thai>
CN	=	<Customer Name in English>
E	=	<Email>

ทั้งนี้ขึ้นอยู่กับ Certificate Policy ด้วยว่าจะถูกกำหนดให้มี DN เป็นตัวไหนบ้าง ซึ่ง Certificate Policy นั้นสามารถดูได้จากหน้าเวบไซต์ของ บริษัท ไทยดิจิทัล ไอดี จำกัด (http://www.thaidigitalid.com)

7.1.5 **ข้อจำกัดของชื่อ** (Name constraints)

ห้ามมีการใช้งานอักษรพิเศษ ลูกน้ำ (,) เนื่องจากทาง TDID ใช้ เครื่องหมายลูกน้ำ (,) เป็นตัวขั้นระหว่าง Distinguished Name (DN) แต่ละตัว

7.1.6 OID ของนโยบายใบรับรองอิเล็กทริกนิกส์ (Certificate policy object identifier)

2.16.764.1.1.2.1.10001.1 Enterprise Certificate

2.16.764.1.1.2.1.10002.1 Enterprise User ID Certificate

2.16.764.1.1.2.1.20001.1 Personal Certificate

2.16.764.1.1.2.1.30001.1 SSL Certificate

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 เป็นตัวไหนบ้าง ซึ่ง Certificate Policy นั้นสามารถดูได้จากหน้าเวบไซต์ของ บริษัท ไทยดิจิทัล ไอดี จำกัด (http://www.thaidigitalid.com)

7.1.8 นโยบายในการระบุรูปแบบและความหมาย (Policy qualifiers syntax and semantics)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้ระบุ นโยบายในการระบุรูปแบบและความหมายของใบรับรองอิเล็กทรอนิกส์ ในหน้า เวบไซต์ของ บริษัท ไทยดิจิทัล ไอดี จำกัด ในหัวข้อ Certificate Policy

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

มีการระบุ Critical extension ไว้ 2 ฟิลด์คือ Basic Constraints และ Key Usage

7.2 รูปแบบของรายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน (CRL Profile)

7.2.1 เลขรุ่น (Version)

รายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ใช้มาตรฐาน X.509 CRL Version 2 ซึ่งมีรายการดังต่อไปนี้

- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ของ TDID CA
- Issuer : ชื่อของผู้ให้บริการที่ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- Effective date : วันเวลาที่ออกรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- Next update : วันเวลาที่จะทำการปรับปรุงรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ครั้งถัดไป
- CRL Number : หมายเลขของรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
- Revocation List : รายการของใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน

7.2.2 **รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนและส่วนขยาย** (CRL and CRL entry extensions)

รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน จะถูกประกาศไว้ที่เว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยผู้ใช้บริการสามารถเข้ามา download เพื่อนำไปใช้งานได้

7.3 **รูปแบบของ** 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 ตามรูปแบบมาตราฐาน rfc2560 (https://www.ietf.org/rfc/rfc2560.txt)

-

7.3.2 **ส่วนขยายของ** OCSP (OCSP extensions)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะทำการ ยืนยันตัวตนของ OCSP ที่ส่งกลับ (OCSP Response) ด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ (OCSP Signer)

8 การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่าง ๆ และการประเมินความเสี่ยงอื่น ๆ (Compliance Audit and Other Assessment)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ภายใต้ชื่อของ TDID CA G2 ได้ยึดถือและปฏิบัติตาม มาตรฐาน ISO27001 (Information Security Management System : ISMS), สำหรับดำเนินการทางด้านประเมิณความเสี่ยง และ นโยบายด้านความมั่นคง โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายใน และ ผู้ตรวจสอบภายนอก มาตรฐาน WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) และ มาตรฐาน WebTrust for CA - SSL Baseline (WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security) ที่ถูกเผยแพร่ล่าสุดจาก http://www.cabforum.org สำหรับดำเนินการทางด้านจัดการและการออกใบรับรองอิเล็กทรอนิกส์ เพื่อให้มีความน่าเชื่อถือ โดยจัดให้มีการตรวจสอบ จากผู้ตรวจสอบที่ได้รับการยอมรับ

8.1 ความถี่หรือเหตุการณ์ของการประเมินผล (Frequency or Circumstances of Assessment)

ผู้ให้บริการออกใบรับรองออกใบรับรองอิเล็กทรอนิกส์ จะถูกประเมินตามเกณฑ์ข้อกำหนดของมาตรฐานต่างๆอย่างน้อยปีละ 1 ครั้ง ดังนี้

1. มาตราฐาน ISO27001
2. มาตราฐาน Webtrust for CA
3. มาตราฐาน Webtrust for CA - SSL Baseline

8.2 สถานะของผู้ประเมิน (Identity/Qualifications of Assessor)

ผู้ทำการประเมินมาตรฐาน ISO27001, WebTrust for CA และ Webtrust for CA - SSL Baseline เป็นผู้มีสิทธิ์ในการลงนามรับรองสำหรับมาตรฐานดังกล่าว

8.3 ความสัมพันธ์ของผู้ประเมินและผู้ถูกประเมิน (Assessor's Relationship to Assessed Entity)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อยู่ในฐานะผู้ว่าจ้าง และผู้รับการประเมิน

8.4 หัวข้อในการประเมิน (Topics Covered by Assessment)

หัวข้อการประเมินเป็นไปตามเกณฑ์ข้อกำหนดของมาตรฐาน ISO 27001, มาตรฐาน WebTrust for CA และ Webtrust for CA - SSL Baseline

8.5 การปฏิบัติเพื่อแก้ไขข้อบกพร่อง (Actions Taken as a Result of Deficiency)

หากพบข้อบกพร่องของระบบจากรายงานการประเมินจากผู้ตรวจสอบ ทางผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะดำเนินการแก้ไขข้อบกพร่องดังกล่าว ให้เสร็จภายใน 30 วัน หรือให้เสร็จภายในระยะเวลาที่ผู้ตรวจสอบกำหนด

8.6 **การรายงานผล** (Communication of Results)

รายงานผลการประเมิน อยู่ในรูปแบบของ รายงานการตรวจสอบ (Compliance Report)

9 ข้อกำหนดอื่นๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

9.1 ค่าธรรมเนียม (Fees)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะจัดเก็บค่าธรรมเนียมจากกรณีดังต่อไปนี้

1. การออกใบรับรองอิเล็กทรอนิกส์
2. การออกใบรับรองอิเล็กทรอนิกส์ใหม่แทนใบรับรองอิเล็กทรอนิกส์เดิมที่หมดอายุ

โดยสามารถตรวจสอบค่าธรรมเนียมได้จากเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.1.1 ค่าธรรมเนียมในการออกใบรับรองอิเล็กทรอนิกส์หรือต่ออายุใบรับรองอิเล็กทรอนิกส์(Certificate issuance or renewal fees)

ค่าธรรมเนียมในการออกใบรับรองอิเล็กทรอนิกส์ หรือออกใบรับรองอิเล็กทรอนิกส์ใหม่แทนใบรับรองเดิมที่หมดอายุ จะแสดงไว้เป็นส่วนหนึ่งของใบคำขอใบรับรองอิเล็กทรอนิกส์ที่ได้จากระบบให้บริการใบรับรองอิเล็กทรอนิกส์

9.1.2 ค่าธรรมเนียมในการเรียกดูใบรับรอง (Certificate access fees)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ไม่มีการเรียกเก็บค่าธรรมเนียม ในกรณีที่ผู้ใช้บริการเรียกดูใบรับรองอิเล็กทรอนิกส์

9.1.3 ค่าธรรมเนียมในการเรียกดูข้อมูลสถานะของใบรับรองอิเล็กทรอนิกส์ (Revocation or status information access fees)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีการเรียกเก็บค่าธรรมเนียม ในกรณีที่ผู้ใช้บริการเรียกดูข้อมูลของCRL ซึ่งถูกเผยแพร่ไว้ที่เว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.1.4 ค่าใช้จ่ายอื่นๆ (Fees for other services)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่มีการเรียกเก็บค่าธรรมเนียม ในกรณีที่ผู้ใช้บริการ download เอกสาร แนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) ไปพิจารณา

9.1.5 นโยบายในการคืนเงิน (Refund policy)

ถ้าผู้ใช้บริการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ภายใน 15 วัน หลังจากที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปให้ผู้ใช้บริการแล้ว ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะไม่คิดค่าใบรับรองอิเล็กทรอนิกส์ดังกล่าว

9.2 ความรับผิดชอบทางด้านการเงิน(Financial Responsibility)

9.2.1 ประกันภัย (Insurance coverage)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มีประกันภัยเครื่องอุปกรณ์อิเล็กทรอนิกส์ ประกันภัยทรัพย์สินคุ้มครองภัยจากเหตุการณ์ความไม่สงบ และ ประกันภัยอัคคีภัยสำหรับสถานที่ติดตั้งระบบให้บริการใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.2.2 สินทรัพย์อื่น ๆ (Other assets)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เป็นนิติบุคคลจดทะเบียนตามกฎหมายไทย โดยสามารถตรวจสอบข้อมูลสินทรัพย์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ใน งบแสดงฐานะทางการเงิน เว็บไซต์ของกรมพัฒนาธุรกิจ กระทรวงพาณิชย์

9.2.3 การทำประกันที่ครอบคลุมในส่วนของผู้ใช้บริการ (Insurance or warranty coverage for end-entities)

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

9.3 การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้กำหนดขอบเขตการรักษาความลับของข้อมูลทางธุรกิจอันได้แก่ แผนทางธุรกิจ ข้อมูลการขาย ความลับทางการค้า และข้อมูลที่ได้จากบุคคลที่สาม ภายใต้ข้อตกลงในการให้บริการกับผู้ใช้บริการหรือในสัญญา หรือเอกสารการให้บริการฉบับต่าง ๆ

9.3.1 ขอบเขตของข้อมูลที่ไม่สามารถนำมาเผยแพร่ (Scope of confidential information)

ข้อมูลที่เป็นความลับ ซึ่งไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ มีดังนี้

- ข้อมูลรายการที่ออกใบรับรองอิเล็กทรอนิกส์
- กุญแจส่วนตัวของผู้ใช้บริการ
- Audit record
- Audit report
- แผนความต่อเนื่องทางธุรกิจ

9.3.2 **ข้อมูลที่สามารถนำมาเผยแพร่ได้** (Information not within the scope of confidential information)

ใบรับรองอิเล็กทรอนิกส์ ใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ เป็นข้อมูลที่ไม่เป็นความลับ สามารถนำมาเปิดเผยได้ ส่วนข้อมูลอื่น ที่ยังไม่สามารถตีความได้ว่าเป็นความลับ หรือไม่ จะถูกพิจารณาให้เป็นไปตามกฎหมายที่เหมาะสม

9.3.3 **ความรับผิดชอบในการปกป้องข้อมูลที่เป็นความลับ** (Responsibility to protect confidential information)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะไม่เปิดเผยข้อมูลซึ่งเป็นความลับของผู้ใช้บริการ กับหน่วยงานที่ไม่เกี่ยวข้องโดยเด็ดขาด

9.4 นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)

การดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จะต้องได้รับความยินยอมจากผู้ใช้บริการ ก่อนจะมีการเปิดเผยข้อมูลส่วนบุคคล ยกเว้นกรณีที่จำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคล ในกรณีที่ต้องดำเนินการตามกฎหมายฉบับต่างๆ หรือเมื่อมีคำสั่งศาล

9.4.1 **แผนการรักษาความเป็นส่วนตัว**(Privacy plan)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์กำหนดแผนการรักษาความเป็นส่วนตัว โดยการจัดเก็บและรักษาข้อมูลของผู้ใช้บริการ เป็นความลับ

9.4.2 **ข้อมูลส่วนบุคคล**(Information treated as private)

ข้อมูลที่เกี่ยวข้องกับการสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ซึ่งประกอบไปด้วยเอกสาร หลักฐานประกอบต่างๆ รวมถึงข้อมูลที่กรอกบนแบบฟอร์ม ในการดำเนินการเกี่ยวกับการขอใบรับรองอิเล็กทรอนิกส์ การพักใช้ใบรับรองอิเล็กทรอนิกส์ และ การเพิกถอนใบรับรองอิเล็กทรอนิกส์ ถือเป็นข้อมูลส่วนบุคคลทั้งสิ้น

9.4.3 **ข้อมูลที่ไม่ถือว่าเป็นข้อมูลส่วนบุคคล**(Information not deemed private)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการ ยินยอมและรับทราบว่า ข้อมูลที่อยู่ในใบรับรองอิเล็กทรอนิกส์ เป็นข้อมูลที่ไม่เป็นความลับ

9.4.4 **ความรับผิดชอบในการป้องกันข้อมูลส่วนบุคคล**(Responsibility to protect private information)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มีหน้าที่รักษาความลับข้อมูลส่วนบุคคลอย่างเคร่งครัด

9.4.5 **การแจ้งให้ทราบและได้รับการยินยอมในการใช้ข้อมูลส่วนบุคคล** (Notice and consent to use private information)

กรณีมีเหตุอันควรที่จำเป็นต้องเปิดเผยข้อมูลส่วนตัวของผู้ใช้บริการ ทางผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะต้องได้รับความยินยอมจากผู้ใช้บริการ เป็นลายลักษณ์อักษรเสียก่อน

9.4.6 **การเปิดเผยข้อมูลตามกระบวนการยุติธรรม** (Disclosure pursuant to judicial or administrative process)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ขอสงวนสิทธิ์ในการเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ ในกรณีที่ศาลร้องขอ เพื่อใช้ในกระบวนการยุติธรรม ภายใต้กฎหมายไทย

9.4.7 **กรณีในการเปิดเผยข้อมูลต่างๆ** (Other information disclosure circumstances)

กรณีมีเหตุอันควรที่จำเป็นต้องเปิดเผยข้อมูลส่วนตัวของผู้ใช้บริการนอกเหนือจากข้อ 9.4.6 ผู้ให้บริการ จะต้องได้รับความยินยอมจากผู้ใช้บริการนั้น เป็นลายลักษณ์อักษรเสียก่อน

9.5 ทรัพย์สินทางปัญญา (Intellectual Property Rights)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นเจ้าของสิทธิ์ในทรัพย์สินทางปัญญาแต่เพียงผู้เดียวในเอกสารนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) ฉบับนี้ และสงวนสิทธิ์ใดๆ ที่มีอยู่หรือเกิดจากเอกสารฉบับนี้

9.6 คำรับรอง (Representations and Warranties)

9.6.1 **คำรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์** (CA representations and warranties)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รับรองว่า

- การอนุมัติการออกใบรับรองอิเล็กทรอนิกส์ตามคำร้องขอ จะดำเนินการภายใต้การควบคุมดูแลอย่างเข้มงวดจากผู้ให้บริการ เพื่อป้องกันมิให้เกิดข้อผิดพลาด
- ใบรับรองที่ออกจากระบบให้บริการใบรับรองอิเล็กทรอนิกส์ สอดคล้องตามมาตรฐานของแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/ Certification Practice Statement) ฉบับนี้
- การให้บริการตรวจสอบสถานะใบรับรองอิเล็กทรอนิกส์ ผ่าน LDAP Repository เป็นไปตามข้อกำหนดของแนวนโยบาย/แนวปฏิบัติใบรับรอง

อิเล็กทรอนิกส์(Certificate Policy/ Certification Practice Statement) ฉบับนี้

9.6.2 **คำรับรองของหน่วยงานรับลงทะเบียน(RA representations and warranties)**

หน่วยงานรับลงทะเบียน รับรองว่า

- ข้อมูลในใบคำขอใบรับรองอิเล็กทรอนิกส์ พร้อมเอกสารประกอบที่เกี่ยวข้อง จะถูกตรวจสอบโดยละเอียดรอบคอบ และไม่มีการบิดเบือนข้อมูลใดๆ นอกเหนือจากข้อมูลที่ปรากฏในใบคำขอใบรับรองอิเล็กทรอนิกส์
- ข้อมูลในใบคำขอใบรับรองอิเล็กทรอนิกส์ จะถูกส่งไปยังผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ภายใต้การควบคุมดูแลอย่างเข้มงวดจากหน่วยงานรับลงทะเบียน เพื่อป้องกันมิให้เกิดข้อผิดพลาด
- ใบรับรองอิเล็กทรอนิกส์ที่ออกจากระบบให้บริการใบรับรองอิเล็กทรอนิกส์สอดคล้องตามมาตรฐานของแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์(Certificate Policy/ Certification Practice Statement) ฉบับนี้

9.6.3 **คำรับรองของผู้ใช้บริการ** (Subscriber representations and warranties)

ผู้ใช้บริการ รับรองว่า

- ใบรับรองอิเล็กทรอนิกส์ ที่ผู้ใช้บริการได้รับจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ถือเป็นใบรับรองอิเล็กทรอนิกส์ที่จะนำมาใช้งาน ตามประเภทและขอบเขตการใช้งานของใบรับรองอิเล็กทรอนิกส์ตามที่ผู้ใช้บริการสมัครขอใช้บริการและเป็นไปตามแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certificate Policy/Certification Practice Statement) ฉบับนี้
- จะจัดเก็บกุญแจส่วนตัวไว้อย่างปลอดภัย และรักษาไว้ไม่ให้ถูกใช้โดยผู้อื่น
- ข้อมูลในใบคำขอใบรับรองอิเล็กทรอนิกส์ และเอกสารประกอบอื่นๆ มีความถูกต้องแท้จริงทุกประการ
- ข้อมูลในใบรับรองอิเล็กทรอนิกส์ อันเป็นส่วนหนึ่งที่มาจากข้อมูลในใบสมัครขอใบรับรองอิเล็กทรอนิกส์ เป็นข้อมูลที่ถูกต้องแท้จริงทุกประการ
- ผู้ใช้บริการ เป็นบุคคล หน่วยงาน หรือองค์กร ที่ไม่ได้ประกอบธุรกิจให้บริการออกใบรับรองอิเล็กทรอนิกส์ (CA Provider)

9.6.4 **คำรับรองของผู้เกี่ยวข้อง(Relying party representations and warranties)**

ในกรณีคำรับรองของผู้เกี่ยวข้อง ให้เป็นไปตามสัญญาหรือเงื่อนไขที่ผูกพันระหว่างผู้เกี่ยวข้องและคู่กรณี

9.6.5 **คำรับรองของผู้เข้าร่วมอื่น ๆ** (Representations and warranties of other participants)

ไม่มีการกำหนดคำรับรองสำหรับผู้เกี่ยวข้องอื่นๆ

9.7 ข้อจำกัดของการรับประกัน (Disclaimers of Warranties)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะไม่รับประกันใดๆ ไม่ว่าโดยชัดแจ้งหรือโดยปริยาย นอกเหนือจากที่ระบุไว้ในแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์(Certificate Policy/Certification Practice Statement) นี้ รวมถึงไม่รับประกันผลสัมฤทธิ์ในเชิงพาณิชย์ หรือในวัตถุประสงค์ใดโดยเฉพาะ

9.8 ข้อจำกัดความรับผิด (Limitations of Liability)

ความรับผิดชอบใดๆ ที่เกี่ยวกับใบรับรองซึ่งออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะจำกัดไว้ไม่เกิน 30 เท่าของราคาใบรับรองฯต่อกรณี ที่เกิดความเสียหาย

ทั้งนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะไม่รับผิดชอบในความเสียหายใดๆ อันเนื่องมาจาก หรือเกี่ยวข้องกับการใช้ใบรับรองอิเล็กทรอนิกส์ที่ผิดกฎหมาย หรือ นอกวัตถุประสงค์ที่ระบุไว้ในแนวนโยบาย/แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์(Certificate Policy/Certification Practice Statement) ฉบับนี้ หรือการละเมิดระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งไม่รับผิดในความเสียหายที่เป็นผลโดยอ้อม ความเสียหายที่เป็นผลสืบเนื่อง หรือความเสียหายอันเกิดจากพฤติการณ์พิเศษ หรือความสูญเสียรายได้ หรือผลกำไรในทางธุรกิจ

ข้อจำกัดความรับผิดตามวรรคแรกจะไม่ใช้บังคับ หากมีการกำหนดข้อจำกัดความรับผิด ของการใช้ใบรับรองอิเล็กทรอนิกส์ แต่ละประเภทไว้แล้ว ภายใต้เงื่อนไขหรือสัญญาอื่นที่เกี่ยวข้อง

9.9 ค่าสินไหมทดแทน (Indemnities)

ค่าสินไหมทดแทนให้เป็นไปตามข้อตกลงระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการ ทั้งนี้ ในกรณีที่คู่กรณีที่เกี่ยวข้องไม่ตรวจสอบสถานะการการเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ หากมีความเสียหายเกิดขึ้นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขอสงวนสิทธิ์ไม่รับผิดชอบชดใช้ค่าสินไหมทดแทนในความเสียหายดังกล่าว

9.10 เงื่อนไขและการยกเลิก (Term and Termination)

9.10.1 เงื่อนไข (Term)

เงื่อนไขใดๆ ที่เกี่ยวข้องกับการใช้ใบรับรองอิเล็กทรอนิกส์ ให้เป็นไปตามเงื่อนไขที่ระบุในเอกสารระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอ่นิกส์ ซึ่งเป็นเอกสารประกอบใบคำขอใบรับรองอิเล็กทรอนิกส์

9.10.2 การยกเลิก (Termination)

การขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ ต้องกระทำการโดยผู้ใช้บริการหรือผู้มีอำนาจกระทำการแทน

9.10.3 **ผลของการยกเลิกใช้บริการ**(Effect of termination and survival)

การเพิกถอนใบรับรองอิเล็กทรอนิกส์ ถือเป็นการสิ้นสุดความผูกพันระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ ผู้ใช้บริการทันที

การยกเลิกสัญญานี้ไม่ว่าด้วยเหตุประการใดก็ตาม จะไม่ถือเป็นการลบล้างหรือทำให้เสื่อมเสียซึ่งสิทธิและ/หรือ หน้าที่ และ/หรือ ความรับผิดใดๆที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และ ผู้ใช้บริการมีอยู่ต่อกันอันเนื่องมาจากการใดๆ อันได้กระทำไปตามเงื่อนไขและข้อตกลงตามเอกสารฉบับนี้ก่อนที่จะมีการเพิกถอนใบรับรองอิเล็กทรอนิกส์

9.11 การบอกกล่าวเป็นรายบุคคลและการสื่อสารกับผู้เข้าร่วม (Individual notices and communications with participants)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เปิดช่องทางในการให้ผู้ใช้บริการติดต่อผ่านทางโทรศัพท์ อีเมล์ ตามที่ระบุไว้ในเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.12 การแก้ไข เพิ่มเติมข้อตกลง (Amendments)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขอสงวนสิทธิ์ในการแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงใดๆ ในการให้บริการตามเอกสารฉบับนี้ได้

9.12.1 **ขั้นตอนในการการแก้ไข เพิ่มเติมหรือ เปลี่ยนแปลงข้อตกลง** (Procedure for amendment)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต้องการแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงในการให้บริการตามเอกสารฉบับนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะต้องแจ้งให้ผู้ใช้บริการหรือ หน่วยงานรับลงทะเบียนทราบล่วงหน้าไม่น้อยกว่า 90 วัน ก่อนจะประกาศบังคับใช้ โดยแจ้งเป็นหนังสือ หรือ อีเมล์ หรือ บนเว็บไซต์ www.thaidigitalid.com ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

9.12.2 **ระบบแจ้งเตือนในแต่ละช่วง** (Notification mechanism and period)

หากหน่วยงานรับลงทะเบียนหรือผู้ใช้บริการเห็นว่า การแก้ไข เพิ่มเติม ยกเลิก หรือเปลี่ยนแปลงข้อตกลงดังกล่าวเป็นการลดสิทธิ หรือประโยชน์อันพึงได้รับโดยชอบด้วยกฎหมายของตน หน่วยงานรับลงทะเบียน หรือ ผู้ใช้บริการมีสิทธิยกเลิกการใช้บริการตามเอกสารนี้ได้ โดยแจ้งให้ผู้ให้บริการทราบล่วงหน้าไม่น้อยกว่า 30 วันก่อนวันให้มีผลสิ้นสุดการใช้บริการ ทั้งนี้เว้นแต่เป็นการแก้ไข เพิ่มเติม ยกเลิก หรือ เปลี่ยนแปลง ตามที่กฎหมายกำหนด

9.12.3 **กรณีที่ OID จะถูกเปลี่ยน** (Circumstances under which OID must be changed)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไม่ระบุเหตุการณ์หรือกรณีที่จะมีการเปลี่ยน OID

9.13 บทบัญญัติการระงับข้อพิพาท (Dispute Resolution Procedures)

ในกรณีที่มีข้อพิพาทเกี่ยวกับการให้บริการออกใบรับรองอิเล็กทรอนิกส์ คู่สัญญาทุกฝ่ายจะใช้วิธีการเจรจาต่อรองเพื่อยุติข้อพิพาทที่เกิดขึ้นก่อน หากไม่สามารถยุติข้อพิพาทโดยวิธีการเจรจาต่อรองได้ภายใน(60) วัน นับแต่วันที่ข้อพิพาทเกิดขึ้น ให้คู่สัญญาระงับข้อพิพาทดังกล่าวโดยกระบวนการพิจารณาของอนุญาตตุลาการในกรุงเทพฯ ประเทศไทย ตามกฎระเบียบอนุญาโตตุลาการของสถาบันอนุญาโตตุลาการแห่งประเทศไทย ตามพระราชบัญญัติอนุญาโตตุลาการ พ.ศ. 2545 โดยคู่สัญญากำหนดให้มีอนุญาโตตุลาการจำนวน 3 ท่าน และให้การเลือกอนุญาโตตุลาการเป็นไปตาม ข้อบังคับสำนักงานศาลยุติธรรมว่าด้วยอนุญาโตตุลาการสถาบันอนุญาโตตุลาการ

การพิจารณาชี้ขาดข้อพิพาทโดยอนุญาโตตุลาการตามวรรคหนึ่ง ให้ถือตามข้อบังคับของสถาบันอนุญาโตตุลาการ สำนักระงับข้อพิพาท สำนักงานศาลยุติธรรม และตามกฎหมายที่ใช้บังคับอยู่ในขณะที่ชี้ขาดข้อพิพาท โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการ ตกลงที่จะเป็นผู้รับผิดชอบในค่าใช้จ่ายที่เกิดขึ้นจากการพิจารณาชี้ขาดข้อพิพาทซึ่งหมายความรวมทั้งค่าใช้จ่ายสำหรับอนุญาโตตุลาการของแต่ละฝ่ายและค่าใช้จ่ายของอนุญาโตตุลาการซึ่งเป็นบุคคลที่สาม ฝ่ายละครึ่งหนึ่ง

9.14 กฎหมายที่ใช้บังคับ (Governing Law)

ข้อตกลงใดๆ ที่กำหนดไว้ในเอกสารฉบับนี้ให้ตีความและบังคับใช้ตามกฎหมายไทย

9.15 การปฏิบัติตามกฎหมายที่ใช้บังคับ (Compliance with Applicable Law)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตกลงจะปฏิบัติตามกฎหมายไทยที่เกี่ยวข้องการให้บริการออกใบรับรองอิเล็กทรอนิกส์ ตามเอกสารฉบับนี้

9.16 บทบัญญัติเบ็ดเตล็ด (Miscellaneous provisions)

9.16.1 **ความตกลงเบ็ดเสร็จ** (Entire agreement)

เอกสารฉบับนี้รวมถึงใบคำขอใบรับรองอิเล็กทรอนิกส์และ ระเบียบและเงื่อนไขในการใช้ใบรับรองอิเล็กทรอนิกส์ ให้ถือเป็นข้อมูลสำคัญที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ชี้แจงและกำหนดเงื่อนไขในการบริหารจัดการใบรับรองอิเล็กทรอนิกส์ ต่อผู้ใช้บริการ และให้ถือว่าเป็นข้อตกลงระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และผู้ใช้บริการในการดำเนินการและปฏิบัติตามเอกสารดังกล่าว

9.16.2 **การโอนสิทธิ** (Assignment)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตกลงที่จะไม่โอนสิทธิ หน้าที่ตามเอกสารฉบับนี้ไม่ว่าแต่บางส่วนหรือทั้งหมดให้แก่บุคคลที่สาม เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจากผู้ใช้บริการก่อน

การให้ความยินยอมดังกล่าวตามวรรคหนึ่งไม่เป็นเหตุให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หลุดพ้นจากหน้าที่และความรับผิดใดๆ ตามสัญญานี้ และ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ยังคงต้องร่วมรับผิดในบรรดาความเสียหายใดๆ อันเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้รับโอนสิทธิ

9.16.3 **กรณีส่วนหนึ่งส่วนใดของข้อตกลงเป็นโมฆะ** (Severability)

ในกรณีที่ข้อความส่วนใดส่วนหนึ่งของเอกสารนี้เป็นโมฆะ ไม่สมบูรณ์ หรือ ไม่มีผลใช้บังคับตามกฎหมาย ให้ข้อความที่เป็นโมฆะไม่สมบูรณ์ หรือ ไม่มีผลใช้บังคับตามกฎหมายนั้นไม่มีผลกระทบกับข้อความอื่นๆ ในเอกสารฉบับนี้ที่สมบูรณ์และบังคับได้ตามกฎหมาย

9.16.4 **ค่าใช้จ่ายที่เกิดขึ้นจากการผิดข้อตกลง (ค่าทนายความและการสละสิทธิ)** (Enforcement (attorneys' fees and waiver of rights))

หากฝ่ายใดที่เป็นฝ่ายปฏิบัติผิดข้อตกลงจะต้องชดใช้ ค่าใช้จ่ายที่เกิดขึ้นรวมทั้ง ค่าทนายความ ที่เกิดขึ้นจากการไม่ปฏิบัติตามข้อตกลงตามเอกสารฉบับนี้และหรือที่เกี่ยวข้องกับเอกสารฉบับนี้ ให้แก่อีกฝ่ายหนึ่ง

การผ่อนผัน ผ่อนเวลา หรือการละเว้นการใช้สิทธิครั้งใดครั้งหนึ่ง ที่ฝ่ายใดฝ่ายหนึ่งมีตามเอกสารฉบับนี้ ให้ถือว่าเป็นการผ่อนผัน ผ่อนเวลาและละเว้นสิทธิเฉพาะคร้ังนั้น คราวนั้นเท่านั้น และมิให้ถือว่าเป็นการสละสิทธิ ที่มีตามเอกสารฉบับนี้

9.16.5 **เหตุสุดวิสัย**(Force Majeure)

แต่ละฝ่ายไม่ต้องรับผิดในความเสียหายอันเนื่องมาจากการไม่สามารถปฏิบัติตามข้อตกลง หรือความล่าช้าในการปฏิบัติตามข้อตกลงตามเอกสารฉบับนี้ได้เพราะเหตุสุดวิสัย

ในกรณีที่ฝ่ายใดฝ่ายหนึ่งไม่สามารถปฏิบัติตามข้อตกลงในเอกสารฉบับนี้ได้ อันเนื่องมาจากเหตุสุดวิสัย ให้ฝ่ายที่ประสบเหตุสุดวิสัยแจ้งให้อีกฝ่ายหนึ่งทราบในทันทีโดยวาจาหรือโดยลายลักษณ์อักษรโดยการแจ้งดังกล่าวต้องระบุถึงสภาพของเหตุการณ์ที่เกิดเหตุสุดวิสัย ผลกระทบที่เกิดจากเหตุสุดวิสัย การกระทำที่เป็นการบรรเทาและแก้ไขเหตุสุดวิสัยที่เกิดขึ้น และฝ่ายที่กล่าวถึงเหตุสุดวิสัยจะต้องประมาณการถึงความเป็นไปได้ที่เหตุสุดวิสัยจะสิ้นสุดลงด้วย

เหตุสุดวิสัย หมายความถึง เหตุการณ์ที่อยู่นอกเหนือการควบคุมของคู่กรณีและเหตุการณ์ดังกล่าวส่งผลทำให้การปฏิบัติหน้าที่ของฝ่ายนั้นไม่สามารถกระทำได้ หรือพ้นวิสัยที่จะปฏิบัติหน้าที่ตามข้อตกลงในเอกสารฉบับนี้ได้ เช่น ภัยพิบัติตามธรรมชาติ แผ่นดินไหว ไฟ

ไหม้ การระเบิด การนัดหยุดงาน การพิพาทแรงงาน ชุมนุมประท้วง อุบัติเหตุ โรคระบาด พายุ น้ำท่วม สงคราม การปฏิวัติ สังคมปั่นป่วน การขาดแคลนน้ำ ไฟฟ้า เชื้อเพลิง แรงงาน เป็นต้น

ในกรณีที่เหตุสุดวิสัยเกิดขึ้นนานเกินกว่า 30 วัน คู่กรณีทั้งสองฝ่ายอาจตกลงหารือร่วมกันเพื่อยกเลิกการใช้บริการ หรือ การให้บริการออกใบรับรองอิเล็กทรอนิกส์ตามสัญญานี้ได้

9.17 **บทบัญญัติอื่น**(Other provisions)

ไม่มี