National ITMX CA

Certificate Practice Statement

Version 1.0

Information in this document is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from Thai Digital ID Company Limited.

Written and published in Bangkok Thailand by Thai Digital ID Company Limited.

Copyright ©2007 Thai Digital ID Company Limited,
ACN 3030196149.

All Rights Reserved.

สารบัญ

1 บทนำ (Introduction) 8
1.1 ข้อมูลเบื้องต้นทั่วไป (Overview) 8
1.2 ชื่อเอกสาร (Document Name and Identification) 8
1.3 บุคคลที่เกี่ยวข้อง (PKI Participants) 9
1.3.1 ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority): National ITMX CA (NITMX CA) 9
1.3.2 หน่วยงานรับลงทะเบียน (Registration Authority): ITMX RA 9
1.3.3 ผู้ใช้บริการ (Subscriber) 9
1.3.4 คู่กรณีที่เกี่ยวข้อง (Relying Party) 9
1.3.5 บุคคลอื่น ๆ ที่เกี่ยวข้อง (Other Participants) 9
1.4 การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage) 9
1.5 การบริหารจัดการเกี่ยวกับแนวนโยบายและแนวปฏิบัติ (Policy Administration) 10
1.6 คำนิยามและคำย่อ (Definitions and Acronyms) 11
2 การเผยแพร่ข้อมูลและความรับผิดชอบในการเก็บรักษาข้อมูล (Publication and Repository Responsibilities) 14
2.1 การเผยแพร่ข้อมูลเกี่ยวกับการให้บริการและการออกใบรับรองอิเล็กทรอนิกส์ของ NITMX CA 14
2.2 ความสม่ำเสมอในการเผยแพร่ข้อมูล (Frequency of Publication) 14
2.3 การควบคุมการเข้าถึง (Access Controls) 14
2.4 แหล่งเก็บข้อมูล (Repositories) 14
3 การระบุและยืนยันตัวบุคคล (Identification and Authentication) 15
3.1 การกำหนดรูปแบบของชื่อ (Naming) 15
3.2 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอใช้บริการครั้งแรก (Initial Identity Validation) 15
3.3 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอออกกุญแจใหม่ (Identification and Authentication for Re-key Requests) 15
3.4 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรอง (Identification and Authentication for Revocation Requests) 15
4 ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operational Requirements) 16
4.1 การยื่นขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application) 16
4.2 การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing) 16
4.3 การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance) 16
4.4 การใช้กุญแจคู่ และใบรับรองอิเล็กทรอนิกส์ (Pair and Certificate Usage) 16
4.5 การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal) 16
4.6 การรับรองกุญแจคู่ใหม่ (Certificate Re-key) 17
4.7 การปรับแต่งใบรับรองอิเล็กทรอนิกส์ (Certificate Modification) 17

(Copyright © 2007 Thai Digital ID Company Limited)

4.8 การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension) 17
4.8.1 ในเหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์ 17
4.8.2 ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Revocation) 17
4.8.3 ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Procedure for Revocation Request) 18
4.8.4 ระยะเวลาที่ใช้ในการเพิกถอน (Revocation Request Grace Period)..... 18
4.8.5 เหตุการณ์ที่ต้องระงับการใช้งานใบรับรองอิเล็กทรอนิกส์ (Circumstances for Suspension) 18
4.8.6 ผู้ที่สามารถขอระงับใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Suspension)..... 19
4.8.7 ขั้นตอนการระงับใบรับรองอิเล็กทรอนิกส์ (Procedure for Suspension Request)..... 19
4.8.8 ขอบเขตของระยะเวลาในการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์..... 19
4.8.9 ความถี่ในการประกาศรายการเพิกถอนใบรับรอง (CRL Issuance Frequency)..... 19
4.8.10 ข้อปฏิบัติสำหรับการตรวจสอบรายการเพิกถอนใบรับรอง (CRL Checking Requirements) 19
4.8.11 การตรวจสอบสถานะของใบรับรองและการเพิกถอนใบรับรองแบบออนไลน์ (On-line Revocation/Status Checking Availability)..... 19
4.8.12 ขอบเขตของการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์ 20
4.9 บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)..... 20
4.10 การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription) 20
5 การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)..... 21
5.1 การควบคุมความมั่นคงปลอดภัยทางกายภาพ (Physical Security Controls)..... 21
5.1.1 สถานที่ตั้งและการก่อสร้างสถานที่ (Site Location and Construction)..... 21
5.1.2 การเข้าถึงทางกายภาพ (Physical Access)..... 21
5.1.3 ระบบไฟฟ้าและระบบปรับอากาศ (Power and Air Conditioning)..... 21
5.1.4 การป้องกันภัยจากน้ำ (Water Exposures)..... 21
5.1.5 การป้องกันอัคคีภัย (Fire Prevention and Protection)..... 21
5.1.6 การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage)..... 22
5.1.7 การกำจัดสิ่งที่ไม่ใช้ (Waste Disposal) 22
5.1.8 สถานที่ให้บริการสำรอง (Secondary Site Backup)..... 22
5.2 การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls) 22
5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles) 22
5.2.2 จำนวนบุคคลที่ต้องการต่องาน (Number of Persons Required Per Task) 24
5.2.3 การระบุและพิสูจน์ความมีตัวตนแท้จริงของเจ้าหน้าที่ปฏิบัติงาน (Identification and Authentication for each Role)..... 24
5.3 การควบคุมบุคคล (Personnel Controls)..... 24
5.3.1 ประวัติ คุณสมบัติ ประสบการณ์และข้อกำหนดประวัติ (Background, qualifications, experience, and clearance requirements) 24
5.3.2 วิธีดำเนินการในการตรวจสอบประวัติ (Background Check Procedures) 24
5.3.3 การฝึกอบรมบุคลากร (Training Requirements)..... 24

(Copyright © 2007 Thai Digital ID Company Limited)

5.3.4 ความถี่ในการทบทวนการฝึกอบรม (Retraining Frequency and Requirements) 25
5.3.5 การลงโทษเกี่ยวกับการดำเนินการโดยไม่ได้รับอนุญาต (Sanctions for Unauthorized Actions) 25
5.3.6 เอกสารประกอบสำหรับบุคลากร (Documentation Supplied to Personnel)..... 25
5.4 กระบวนการตรวจสอบข้อมูลการลงบันทึกเหตุการณ์ (Audit Logging Procedures) 25
5.4.1 ชนิดของเหตุการณ์ (Types of Event Recorded) 25
5.4.2 ความถี่ในการประมวลผลข้อมูลการลงบันทึกเหตุการณ์ (Frequency of Processing Log)..... 26
5.4.3 ระยะเวลาที่จะเก็บข้อมูลการลงบันทึกเหตุการณ์ (Retention Period for Audit Log)..... 26
5.4.4 การป้องกันข้อมูลการลงบันทึกเหตุการณ์ (Protection of Audit Log)..... 26
5.4.5 ขั้นตอนการสำรองเก็บข้อมูลการลงบันทึกเหตุการณ์ (Audit Log Backup Procedure)..... 26
5.4.6 ระบบการเก็บข้อมูลการลงบันทึกเหตุการณ์ (Audit Collection System)..... 26
5.4.7 การแจ้งไปยังบุคคลที่เกี่ยวข้อง (Notification to Event-Causing Subject)..... 26
5.5 การเก็บรักษาข้อมูลบันทึก (Records Archival) 27
5.5.1 รูปแบบของข้อมูล (Types of Event Recorded) 27
5.5.2 ระยะเวลาที่เก็บรักษา (Retention Period for Archive)..... 27
5.5.3 การป้องกันข้อมูลที่สำรองไว้ (Protection of Archive)..... 27
5.5.4 นโยบายการสำรองข้อมูล (Archive Backup Procedures) 27
5.5.5 ระบบสำรองข้อมูล (Archive Collection System) 27
5.5.6 วิธีการปฏิบัติเพื่อตรวจสอบข้อมูลที่สำรองไว้ (Procedures to Obtain and Verify Archive Information) 28
5.6 การเปลี่ยนคู่คีย์ (Key Changeover)..... 28
5.7 ความผิดพลาดของระบบและการฟื้นฟูระบบ (Compromise and Disaster Recovery)..... 28
5.7.1 เครื่องคอมพิวเตอร์, ซอฟต์แวร์ และ/หรือ ข้อมูลเกิดความผิดพลาด(Computing Resources, Software, and/or Data Are Corrupted)..... 28
5.7.2 เมื่อ PKI Entity ถูกยกเลิก (Entity Public Key Is Revoked) 28
5.7.3 เมื่อ PKI Entity ถูกละเมิด (Entity Key Is Compromised)..... 28
5.7.4 ความปลอดภัยจากธรรมชาติหรือจากภัยพิบัติอื่นๆ (Secure Facility after a Natural or other type of Disaster)..... 29
5.8 การยกเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ หน่วยงานออกใบรับรองอิเล็กทรอนิกส์ (CA or RA Termination)..... 29
5.8.1 บทนำ..... 29
5.8.2 การยกเลิกการให้บริการธุรกิจ CA อย่างมีแบบแผน (CA Business Operations Programmed Termination) 29
5.8.3 การยกเลิกการให้บริการธุรกิจ CA อย่างไม่มีแบบแผน (CA Business Operations Non-programmed Termination)..... 30
5.8.4 การยกเลิกการให้บริการธุรกิจ RA อย่างมีแบบแผน (RA Business Operations Programmed Termination) 31

(Copyright © 2007 Thai Digital ID Company Limited)

5.8.5 การยกเลิกการให้บริการธุรกิจ RA อย่างไม่มีแบบแผน (RA Business Operations Non-programmed Termination) 31
5.8.6 วิธีการในการประเมิน (Evaluation Mechanism) 31
6 การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls) 32
6.1 การสร้างและติดตั้งคู่คีย์ (Key Pair Generation and Installation) 32
6.1.1 การสร้างกุญแจคู่ (Key Pair Generation) 32
6.1.2 การส่งมอบกุญแจส่วนตัว (Private Key Delivery to Entity) 32
6.1.3 การส่งมอบกุญแจสาธารณะไปยังผู้ให้การรับรองฯ (Public Key Delivery to Certificate Issuer) 32
6.1.4 การส่งมอบกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปยังผู้ใช้ (CA Public Key Delivery to Users) 32
6.1.5 ขนาดของกุญแจ (Key Sizes) 32
6.1.6 การสร้างตัวแปรกุญแจสาธารณะ (Public Key Parameters Generation) 33
6.1.7 การตรวจสอบคุณภาพของตัวแปร (Parameter Quality Checking) 33
6.1.8 การสร้างกุญแจคู่จากอุปกรณ์หรือซอฟต์แวร์ (Hardware/Software Key Generation) 33
6.1.9 จุดประสงค์ของการใช้กุญแจ (Key Usage Purposes) 33
6.2 การปกป้องกุญแจส่วนตัว (Private Key Protection) และการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls) 33
6.2.1 มาตรฐานของโมดูลที่ใช้ในการเข้ารหัสลับ (Standards for Cryptographic Module) 33
6.2.2 การควบคุมกุญแจส่วนตัวของผู้ให้บริการ (Private Key (n out of m) Multi-Person Control) 33
6.2.3 การฝากกุญแจส่วนตัว (Private Key Escrow) 33
6.2.4 การสำรองกุญแจส่วนตัว (Private Key Backup) 34
6.2.5 การเก็บรักษากุญแจส่วนตัวของผู้ให้บริการ (Private Key Archival) 34
6.2.6 กุญแจส่วนตัวภายในโมดูลการเข้ารหัส (Private Key Entry into Cryptographic Module) .. 34
6.2.7 วิธีการนำกุญแจส่วนตัวมาใช้งาน (Method of Activating Private Key) 34
6.2.8 วิธีเลิกการใช้งานกุญแจส่วนตัว (Method of Deactivating Private Key) 34
6.2.9 วิธีการทำลายกุญแจส่วนตัว (Method of Destroying Private Key) 34
6.2.10 การจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls) 34
6.3 รายละเอียดอื่นเกี่ยวกับการจัดการและบริหารกุญแจคู่ (Other Aspects of Key Pair Management) .. 35
6.3.1 การเก็บรักษากุญแจสาธารณะ (Public Key Archival) 35
6.3.2 ระยะเวลาใช้งานของกุญแจส่วนตัวและกุญแจสาธารณะ (Usage Periods for the Public and Private Keys) 35
6.4 ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data) 35
6.4.1 การสร้างข้อมูลและการนำข้อมูลไปใช้ในการติดตั้งใบรับรอง (Activation Data Generation and Installation) 35
6.4.2 การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรอง (Activation Data Protection) 35

(Copyright © 2007 Thai Digital ID Company Limited)

6.5 การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)..... 35
6.5.1 ข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ที่มีลักษณะเฉพาะ (Specific Computer Security Technical Requirements)..... 35
6.5.2 การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating). 36
6.6 การควบคุมวงจรทางเทคนิคของระบบให้บริการ (Life Cycle Security Controls)..... 36
6.6.1 การควบคุมในการพัฒนาระบบ (System Development Controls)..... 36
6.6.2 การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัย (Security Management Controls) 36
6.6.3 การแบ่งระดับความปลอดภัยของวงจรทางเทคนิคของระบบให้บริการ (Life Cycle Security Ratings) 36
6.7 การควบคุมความปลอดภัยทางเครือข่าย (Network Security Controls)..... 36
6.8 การประทับเวลา (Timestamping)..... 36
7 การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ และรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)..... 37
7.1 รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)..... 37
7.1.1 รูปแบบ (Profile)..... 37
7.1.2 ข้อมูลเพิ่มเติมของใบรับรอง (Certificate Extension)..... 37
7.1.3 รูปแบบของชื่อ (Name Forms)..... 37
7.2 รูปแบบรายการเพิกถอนใบรับรอง (CRL Profile)..... 38
7.2.1 รูปแบบ (Profile)..... 38
8 การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่าง ๆ และการประเมินความเสี่ยงอื่น ๆ (Compliance Audit and Other Assessment)..... 39
9 ข้อกำหนดอื่น ๆ และประเด็นกฎหมาย (Other Business and Legal Matters)..... 40
9.1 ค่าธรรมเนียม (Fees)..... 40
9.2 การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)..... 40
9.3 นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)..... 40
9.4 ทรัพย์สินทางปัญญา (Intellectual Property Rights)..... 40
9.5 คำรับรอง (Representations and Warranties)..... 40
9.6 การบอกเลิกคำรับรอง (Disclaimers of Warranties)..... 40
9.7 ข้อจำกัดความรับผิด (Limitations of Liability)..... 40
9.8 การเลิกสัญญา (Term and Termination)..... 41
9.9 การแก้ไขปรับปรุงแนวนโยบาย (Amendments)..... 41
9.10 แนวปฏิบัติการระงับข้อพิพาท (Dispute Resolution Procedures)..... 41

(Copyright © 2007 Thai Digital ID Company Limited)

1 บทนำ (Introduction)

1.1 *ข้อมูลเบื้องต้นทั่วไป (Overview)*

บริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด (National ITMX Co., Ltd. - ITMX) ได้มีการเปลี่ยนชื่อมาจาก บริษัท เอทีเอ็ม พูล จำกัด เมื่อวันที่ 8 กรกฎาคม 2548 เพื่อขยายขอบเขตการดำเนินธุรกิจ และการให้บริการอย่างกว้างขวางยิ่งขึ้น เพื่อรองรับความก้าวหน้า และการเปลี่ยนแปลงที่เกิดขึ้นอย่างรวดเร็วของธุรกรรม พาณิชย์อิเล็กทรอนิกส์ (e-Commerce) และการทำธุรกรรมทางการเงินผ่านสื่ออิเล็กทรอนิกส์ทั้งในและต่างประเทศ

ภายใต้แนวทางการดำเนินงาน และนโยบายจากธนาคารแห่งประเทศไทย ระบบไอทีเอ็มเอ๊กซ์ (ไอทีเอ็มเอ๊กซ์ หรือ ITMX มาจาก Interbank Transaction Management and Exchange) ได้จัดทำขึ้นเพื่อเป็นโครงสร้างพื้นฐานด้านระบบการชำระเงิน โดยมีหน้าที่ แลกเปลี่ยน จัดการ ประมวลผลรายการที่เกิดขึ้นระหว่างธนาคารสมาชิก และสถาบันการเงิน ซึ่งจะช่วยอำนวยความสะดวกต่อประชาชนในการทำธุรกรรมทางการเงินผ่านสื่ออิเล็กทรอนิกส์ด้วยระบบที่มีความปลอดภัย มีประสิทธิภาพ มีความสามารถในการปรับเปลี่ยน และตอบสนองอย่างรวดเร็ว รองรับการเปลี่ยนแปลงทางธุรกิจที่เกิดขึ้นตลอดเวลา และเพื่อเป็นการรองรับด้านการทำธุรกรรมอย่างปลอดภัยในการรับ-ส่งข้อมูล ระหว่าง บริษัท ฯ และ สมาชิก ITMX จึง ได้จัดตั้ง CA ภายใต้ชื่อ “NITMX CA” ขึ้นเมื่อปี 2550 โดยใช้บริการจัดตั้งและบริหารจัดการ CA (CA Hosting Service) ของบริษัทไทยดิจิทัลไอดี จำกัด

คำชี้แจงทางปฏิบัติ (Certification Practice Statement) ฉบับนี้ เป็นเอกสารที่อธิบายถึงแนวทางปฏิบัติในการประกอบการออกใบรับรองอิเล็กทรอนิกส์ของ NITMX CA เช่น วิธีการระบุและยืนยันตัวบุคคล การดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ รูปแบบใบรับรองอิเล็กทรอนิกส์ประเภทต่างๆที่ให้บริการ การควบคุมความมั่นคงปลอดภัย ฯลฯ ทั้งนี้เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบและเข้าใจ ตลอดจนใช้เป็นแนวทางในการประยุกต์ใช้งานใบรับรองฯต่อไป

1.2 *ชื่อเอกสาร (Document Name and Identification)*

เอกสารฉบับนี้เรียกว่า “คำชี้แจงทางปฏิบัติ (Certification Practice Statement)” หรือเรียกว่า “CPS” ของผู้ให้บริการ โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ เพื่อให้ทราบและเข้าใจถึงข้อความที่ระบุในเอกสารที่ใช้เป็นแนวทางในการดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ ในกรณีที่มีข้อความขัดแย้งกันระหว่าง CP กับ CPS และข้อความนั้นไม่ได้ถูกระบุเฉพาะเจาะจงสำหรับ CP ให้ถือข้อความใน CPS เป็นสำคัญ

(Copyright © 2007 Thai Digital ID Company Limited)

1.3 *บุคคลที่เกี่ยวข้อง (PKI Participants)*

1.3.1 ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority): National ITMX CA (NITMX CA)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หมายความว่า ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ซึ่ง สร้างและออกใบรับรองอิเล็กทรอนิกส์เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List หรือมีชื่อย่อว่า CRL) ตามความถี่ที่เหมาะสม

1.3.2 หน่วยงานรับลงทะเบียน (Registration Authority): ITMX RA

คือ ผู้ซึ่งทำหน้าที่รับลงทะเบียน เมื่อมีการยื่นคำขอใช้บริการ คำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ ของข้อมูลที่ผู้ใช้บริการให้ไว้ตามแบบคำขอที่ผู้ให้บริการกำหนดขึ้น

1.3.3 ผู้ใช้บริการ (Subscriber)

คือ องค์กร หรือ นิติบุคคล หรือ เอนทิตี้ใด ๆ ที่ได้รับใบรับรองอิเล็กทรอนิกส์ จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์(NITMX CA)

1.3.4 คู่กรณีที่เกี่ยวข้อง (Relying Party)

คือ บุคคล นิติบุคคล หรือ เอนทิตี้อื่นใดที่เชื่อถือลายมือชื่อดิจิทัล อันเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง หรือ เชื่อถือใบรับรองอิเล็กทรอนิกส์ ดังนั้น คู่กรณีที่เกี่ยวข้องอาจเป็นผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือ อาจไม่ใช่ผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ก็ได้ แต่เป็นผู้ซึ่งกระทำการหรืองดเว้นกระทำการใด ๆ เพราะเชื่อถือลายมือชื่อดิจิทัลหรือใบรับรองอิเล็กทรอนิกส์ โดยการใช้กุญแจสาธารณะที่อยู่ในใบรับรองนั้นในการตรวจสอบตัวตนที่แท้จริงของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัลและมีชื่อปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์

1.3.5 บุคคลอื่น ๆ ที่เกี่ยวข้อง (Other Participants)

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

1.4 *การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)*

(Copyright © 2007 Thai Digital ID Company Limited)

ใบรับรองที่ผู้ให้บริการออกให้แก่ผู้ใช้บริการนั้นได้มีการจำกัดการใช้งานไว้สำหรับองค์กรสมาชิก(เป็นใบรับรององค์กร-Corporate Certificate) โดยประกอบไปด้วยใบรับรองประเภทต่างๆ ดังนี้

1) 1) ใบรับรองอิเล็กทรอนิกส์สำหรับระบบ Single/Bulk Payment Service เป็นใบรับรองที่สนับสนุนการใช้ลายมือชื่อดิจิทัล (Digital Signature) และการเข้ารหัสลับข้อมูล (Data Encryption) เพื่อสร้างความปลอดภัยสำหรับข้อมูลรายการโอนเงินระหว่าง Sending Bank และ Receiving Bank โดยมี ITMX เป็นตัวกลางในการรับส่งข้อมูลการโอนเงิน คัดแยกและคำนวณดุลเพื่อหักบัญชีระหว่างธนาคารสมาชิก2) ใบรับรองอิเล็กทรอนิกส์สำหรับระบบ Web Portal Service (WPS) เป็นใบรับรองที่สนับสนุนการใช้รายมือชื่อดิจิทัล (Digital Signature) เพื่อการยืนยันการเรียกดูข้อมูลของธนาคารสมาชิก ผ่านระบบ WPS

1.5 *การบริหารจัดการเกี่ยวกับแนวนโยบายและแนวปฏิบัติ (Policy Administration)*

รายละเอียดที่อยู่ของหน่วยงาน NITMX CA ที่ทำหน้าที่ในการดูแลและปรับปรุงเอกสารแนวนโยบายและแนวปฏิบัตินี้

Name:	NITMX CA
ACN:	3011253465
Trading as:	NITMX CA
OID:	1.3.6.1.4.1.28098.2.1.1
Postal Address:	93/1 GPF Witthayu, 17th Fl., Tower A, Wireless Road, Lumpini, Patumwan, Bangkok 10330, Thailand
Phone:	+66-2-6506800
Fax:	+66-2-6506808
Domain Name:	www.itmx.co.th
Email Address:	support@thaidigitalid.com (ในฐานะที่บริษัทไทย ดิจิทัล ไอดี จำกัด เป็นผู้บริหารจัดการ CA ให้กับบริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด)
Contact:	Thai Digital ID Co.,Ltd. 4th floor, Kasikorn Bank Building, 142 Silom Road, Bangrak Bangkok 10500 Thailand Tel +66 (0)-2634-3230 (ในฐานะที่บริษัทไทย ดิจิทัล ไอดี จำกัด เป็นผู้บริหารจัดการ CA ให้กับบริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด)

(Copyright © 2007 Thai Digital ID Company Limited)

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

คำศัพท์	**ความหมาย**
Thai Digital ID Root CA (TDID RCA)	บริษัทไทยดิจิทัล ไอดี จำกัด เป็นผู้ให้บริการรับรองการออกใบรับรองอิเล็กทรอนิกส์ของ ผู้ประกอบการ National ITMX Certification Authority: NITMX CA
ผู้ให้บริการออกใบรับรอง อิเล็กทรอนิกส์ / ผู้ให้บริการ (Certification Authority : NITMX CA)	NITMX CA Service เป็นบริการออกใบรับรองอิเล็กทรอนิกส์ ของ บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด โดยทำหน้าที่ให้บริการเกี่ยวกับการออกใบรับรอง อิเล็กทรอนิกส์ เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
หน่วยงานรับลงทะเบียน (Registration Authority : N ITMX RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ คำขอเพิกถอนใบรับรอง หรือต่ออายุใบรับรอง โดยทำการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ของข้อมูลที่ผู้ใช้บริการให้ไว้
ใบรับรอง / ใบรับรอง อิเล็กทรอนิกส์ (Digital Certificate)	เอกสารอิเล็กทรอนิกส์ที่เป็นองค์ประกอบส่วนหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะที่ผู้ให้บริการออกให้แก่ผู้ใช้บริการ ซึ่งอาจหมายถึงบุคคลธรรมดา นิติบุคคลเครื่องมือ หรือ อุปกรณ์ ซึ่งเอกสารอิเล็กทรอนิกส์ดังกล่าวสอดคล้องตามมาตรฐาน X.509 Version 3 Certificate โดยมีรายการอย่างน้อย ดังนี้ – เวอร์ชั่นของใบรับรอง – หมายเลขของใบรับรอง – วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลของผู้ถือใบรับรอง – ชื่อของผู้ให้บริการ – วัน เวลาที่เริ่มต้นและสิ้นสุดของการใช้ใบรับรอง – ชื่อของผู้ถือใบรับรอง – กุญแจสาธารณะของผู้ถือใบรับรองและวิธีการที่ใช้ในการสร้าง
ผู้ใช้บริการ (Subscriber)	นิติบุคคลได้แก่ – นิติบุคคลที่ยื่นคำขอใช้บริการใบรับรองต่อผู้ให้บริการ เมื่อมีการออกใบรับรองจะมีการระบุชื่อนิติบุคคลของผู้ใช้บริการไว้ในใบรับรอง (หมายเหตุ : การดำเนินการยื่นคำขอใช้บริการหรือคำ

(Copyright © 2007 Thai Digital ID Company Limited)

	ขอให้ดำเนินการใดของผู้ใช้บริการต่อผู้ให้บริการ ให้ดำเนินการโดยบุคคลที่มีอำนาจหรือได้รับมอบอำนาจเป็นตัวแทนของนิติบุคคล เพื่อกระทำการในฐานะนิติบุคคลนั้น)
กุญแจ (Key)	สัญลักษณ์หรือลำดับของสัญลักษณ์ หรือสัญญาณไฟฟ้าที่เกี่ยวเนื่องกับสัญลักษณ์ที่นำมาเข้ารหัสข้อมูลหรือถอดรหัสข้อมูล
กุญแจส่วนตัว (Private Key)	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการ ถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ และ กุญแจส่วนตัวนี้จะนำไปใช้สร้างลายมือชื่อดิจิทัล
กุญแจสาธารณะ (Public Key)	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษา ความลับของข้อมูลอิเล็กทรอนิกส์นั้น
กุญแจคู่ (Key Pair)	กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะ โดยที่สามารถใช้กุญแจสาธารณะตรวจสอบว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้
ลายมือชื่อดิจิทัล (Digital Signature)	ลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่งที่สร้างขึ้นโดยการนำข้อมูลอิเล็กทรอนิกส์มาแปลงเป็นตัวเลขและใช้กับระบบกุญแจคู่ โดยนำไปคำนวณร่วมกับกุญแจส่วนตัวของเจ้าของลายมือชื่อ โดยที่สามารถใช้กุญแจสาธารณะของเจ้าของลายมือชื่อมาตรวจสอบได้ว่าเป็นลายมือชื่อดิจิทัลที่ได้สร้างขึ้นโดยกุญแจส่วนตัวของเจ้าของลายมือชื่อดิจิทัลนั้นหรือไม่ และข้อมูลอิเล็กทรอนิกส์ที่ได้มีการลงลายมือชื่อดิจิทัลนั้นได้มีการแก้ไข

(Copyright © 2007 Thai Digital ID Company Limited)

	เปลี่ยนแปลงภายหลังการลงลายมือชื่อหรือไม่
การเพิกถอนใบรับรอง (Certificate Revocation)	การทำให้ใบรับรองไม่สามารถใช้ได้อีกต่อไปหลังจากการเพิกถอนใบรับรองซึ่งส่งผลให้กุญแจส่วนตัวของผู้ใช้บริการนั้นไม่สามารถใช้ในการสร้างลายมือชื่อดิจิทัลหรือถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ได้ ทั้งนี้ไม่มีผลกระทบกับใบรับรองหรือกุญแจสาธารณะ ซึ่งยังคงสามารถใช้ในการตรวจสอบลายมือชื่อดิจิทัลที่สร้างขึ้นก่อนการเพิกถอนใบรับรองได้
รายการเพิกถอนใบรับรอง (Certificate Revocation List : CRL)	รายการใบรับรองที่ถูกเพิกถอนการใช้งาน
คู่กรณีที่เกี่ยวข้อง (Relying Party)	ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองหรือลายมือชื่อดิจิทัล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองไปใช้ในการตรวจสอบตัวตนของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัล และมีชื่อปรากฏอยู่ในใบรับรอง
ไดเรกทอรี (Directory)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดการเพื่อให้สามารถสืบค้นข้อมูลได้อย่างรวดเร็วและเป็นตามมาตรฐานไดเรกทอรี (X.500 หรือ LDAP)
ฐานข้อมูล (Database)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดเก็บแบบที่เอื้อให้โปรแกรมคอมพิวเตอร์สามารถเข้าถึง จัดการและปรับเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว
คำชี้แจงทางปฏิบัติ (Certification Practice Statement : CPS)	คำชี้แจงของผู้ให้บริการที่ใช้ในการออกหรือเพิกถอนใบรับรอง ซึ่งแสดงรายละเอียดเกี่ยวกับนโยบายความปลอดภัยและกระบวนการหรือขั้นตอนใน การให้บริการ

(Copyright © 2007 Thai Digital ID Company Limited)

2 การเผยแพร่ข้อมูลและความรับผิดชอบในการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

2.1 *การเผยแพร่ข้อมูลเกี่ยวกับการให้บริการและการออกใบรับรองอิเล็กทรอนิกส์ของ* NITMX *CA*

นโยบายใบรับรองอิเล็กทรอนิกส์และคำชี้แจงทางปฏิบัตินี้ ได้รับการตีพิมพ์ทางอิเล็กทรอนิกส์ในรูปแบบของ PDF บนเว็บไซต์ของผู้ให้บริการหรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

www.itmx.co.th

2.2 *ความสม่ำเสมอในการเผยแพร่ข้อมูล (Frequency of Publication)*

ผู้ให้บริการจะปรับปรุงนโยบายใบรับรองอิเล็กทรอนิกส์ (CP) และคำชี้แจงทางปฏิบัติ (CPS) ให้ทันสมัยอยู่เสมอ โดยจะประกาศทางเว็บไซต์ของผู้ให้บริการ (http://www.itmx.co.th) หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้ เพื่อใช้สำหรับการอ้างอิงแก่ผู้ใช้บริการ และบุคคลทั่วไป

2.3 *การควบคุมการเข้าถึง (Access Controls)*

CP และ CPS สามารถดาวโหลดผ่านทางเว็บไซต์ www.itmx.co.th หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้ได้ ในขณะที่การเข้าถึงข้อมูลของใบรับรองอิเล็กทรอนิกส์ ผ่านทาง X.500 Directory สามารถทำได้โดยค้นหาข้อมูลจาก Attribute Certificate เช่น ชื่อ สกุล ของผู้ใช้ใบรับรอง ผ่านระบบการตรวจสอบสถานะใบรับรองบนเว็บไซต์ www.itmx.co.th หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

2.4 *แหล่งเก็บข้อมูล (Repositories)*

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ใช้ LDAP directory (X.500 Directory)ในการเก็บข้อมูลใบรับรองอิเล็กทรอนิกส์ของลูกค้าทั้งหมด โดยสามารถเข้าดูข้อมูลใบรับรองได้ที่เว็บไซต์ของผู้ให้บริการหรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

www.itmx.co.th

(Copyright © 2007 Thai Digital ID Company Limited)

3 การระบุและยืนยันตัวบุคคล (Identification and Authentication)

3.1 *การกำหนดรูปแบบของชื่อ (Naming)*

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

3.2 *การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอใช้บริการครั้งแรก (Initial Identity Validation)*

การระบุและยืนยันหรือพิสูจน์ตัวผู้ขอใช้บริการเพื่อออกใบรับรองนั้น เป็นหน้าที่ของหน่วยงานรับลงทะเบียน โดยผู้ขอใช้บริการต้องกรอกแบบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ เพื่อขอใช้ใบรับรองพร้อมทั้งแนบหลักฐานที่ใช้ในการสมัครขอใช้บริการ ให้แก่หน่วยงานรับลงทะเบียน NITMX RA โดยรายละเอียดอยู่ในหัวข้อ 4.1

3.3 *การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอออกกุญแจใหม่ (Identification and Authentication for Re-key Requests)*

ผู้ใช้บริการต้องกรอกแบบคำขอสมัครใช้ใบรับรองอิเล็กทรอนิกส์ใหม่ และส่งให้กับหน่วยงานรับลงทะเบียน (NITMX RA)

3.4 *การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรอง (Identification and Authentication for Revocation Requests)*

ผู้ใช้บริการที่ต้องการเพิกถอนใบรับรอง ต้องแจ้งต่อผู้ให้บริการโดยตรง เมื่อผู้ให้บริการได้รับแจ้งความต้องการเพิกถอนใบรับรองและตรวจสอบตามขั้นตอนแล้ว จะดำเนินการเพิกถอนใบรับรองตามที่แจ้งไว้และประกาศในรายการเพิกถอนใบรับรอง

(Copyright © 2007 Thai Digital ID Company Limited)

4 ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operational Requirements)

4.1 *การยื่นขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application)*

ผู้สมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ควรปฏิบัติตามขั้นตอนต่อไปนี้

- กรอกใบสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ โดยใส่ข้อมูลให้ครบถ้วน
- จัดเตรียมหลักฐานที่ใช้ในการประกอบการสมัครขอใช้ใบรับรองอิเล็กทรอนิกส์
- ส่งใบสมัคร พร้อมหลักฐานประกอบการสมัครมาที่หน่วยงานรับลงทะเบียน

4.2 *การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)*

หน่วยงานรับลงทะเบียนจะพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ โดยดูจากใบสมัครคำร้องขอใช้ใบรับรองอิเล็กทรอนิกส์ และหลักฐานต่างๆที่ใช้ประกอบการพิจารณาขอใช้ใบรับรองอิเล็กทรอนิกส์ ต้องถูกต้อง และครบถ้วนถึงจะดำเนินการออกใบรับรองอิเล็กทรอนิกส์ให้กับผู้สมัคร แต่ถ้าส่วนหนึ่งส่วนใดของใบสมัคร หรือหลักฐานประกอบการขอใบรับรองอิเล็กทรอนิกส์ไม่ครบถ้วน ก็จะส่งคืนผู้สมัคร พร้อมทั้งบอกถึงสาเหตุดังกล่าว

4.3 *การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)*

- ใบรับรองอิเล็กทรอนิกส์ที่ออกให้กับผู้ขอใช้บริการนั้น ต้องผ่านขั้นตอนของการตรวจสอบข้อมูลต่างๆ โดยขั้นตอนของการรับลงทะเบียนจะประกอบไปด้วย การยืนยันข้อมูลของผู้ขอใช้บริการ, พิสูจน์เอกสารการสมัคร และตรวจสอบความครบถ้วนสมบูรณ์ของการลงนามในเอกสารหลักฐานต่างๆทั้งหมด จากผู้ขอใช้บริการ
- ใบรับรองอิเล็กทรอนิกส์ที่ออกโดย NITMX CA มีอายุ 2 ปี โดยเริ่มนับตั้งแต่เวลาที่ออกใบรับรองอิเล็กทรอนิกส์นั้น

4.4 *การใช้กุญแจคู่ และใบรับรองอิเล็กทรอนิกส์ (Pair and Certificate Usage)*

- ใบรับรองอิเล็กทรอนิกส์สำหรับนิติบุคคล เป็นใบรับรองที่สนับสนุนการใช้ลายมือชื่อดิจิทัล (Digital Signature) และการเข้ารหัสลับข้อมูล (Data Encryption) เพื่อใช้ร่วมกับโปรแกรมประยุกต์ หรือ เว็บไซต์ ของบริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด ที่ต้องการการสนับสนุนทางด้านความปลอดภัย หรือ การยืนยันตัวบุคคล

4.5 *การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal)*

ทุกๆสิ้นเดือนเจ้าหน้าที่ของหน่วยงานรับลงทะเบียนจะทำการรวบรวมข้อมูลของใบรับรองอิเล็กทรอนิกส์ที่จะหมดอายุในอีก 2 เดือนข้างหน้า และจะทำการแจ้งผู้ใช้บริการล่วงหน้า 2 เดือน ถ้าใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการกำลังจะหมดอายุ โดยทางเจ้าหน้าที่ของหน่วยงานรับลงทะเบียนจะส่งแบบฟอร์มไปสอบถาม เพื่อยืนยันการต่ออายุการใช้งานใบรับรองอิเล็กทรอนิกส์

(Copyright © 2007 Thai Digital ID Company Limited)

4.6 *การรับรองกุญแจคู่ใหม่ (Certificate Re-key)*

การออกใบรับรองใหม่หลังจากใบรับรองเก่าหมดอายุ หรือถูกเพิกถอน ผู้สมัครต้องส่งใบสมัครขอใช้บริการใบรับรองใหม่ และหลักฐานประกอบมาที่หน่วยงานรับลงทะเบียน

4.7 *การปรับแต่งใบรับรองอิเล็กทรอนิกส์ (Certificate Modification)*

ในกรณีที่ผู้สมัครขอใช้ใบรับรองต้องการปรับเปลี่ยนแก้ไขข้อมูลของใบรับรองที่ได้ออกไปแล้วนั้น จะต้องยื่นเอกสารประกอบเพื่อขอยกเลิกใบรับรอง เดิม พร้อมทั้งเอกสารเพื่อขอสมัครใหม่

4.8 *การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension)*

สำหรับบริการการเพิกถอนและพักใช้ใบรับรองนั้น ผู้ให้บริการออกใบรับรอง จะดำเนินการเมื่อได้รับคำขอเพิกถอนหรือพักใช้ใบรับรองจากผู้ใช้บริการ หรือได้รับคำสั่งโดยชอบด้วยกฎหมายให้ดำเนินการดังกล่าว

4.8.1 ในเหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์

การเพิกถอนใบรับรองอิเล็กทรอนิกส์คือกระบวนการทางเทคนิคและนโยบาย ที่จะทำการยกเลิกใบรับรอง โดยผู้ให้บริการหรือผู้ขอใช้ใบรับรองจะสามารถขอเพิกถอนใบรับรองได้ในกรณีดังต่อไปนี้

- มีผู้อื่นล่วงรู้กุญแจส่วนตัวหรือมีผู้อื่นสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ขอใช้ใบรับรองไปใช้งาน
- มีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ขอใช้ใบรับรอง
- อุปกรณ์ที่ใช้ในการเก็บกุญแจส่วนตัวสูญหายหรือไม่สามารถใช้งานได้
- องค์กรผู้ขอใช้ใบรับรองได้เลิกกิจการ
- ผู้ใช้บริการ ต้องการเปลี่ยนแปลงข้อมูลที่อยู่ในใบรับรอง
- ผู้ใช้บริการไม่ปฏิบัติตามข้อกำหนดและเงื่อนไขในคำชี้แจงทางปฏิบัติของ NITMX CA หรือข้อตกลงการใช้บริการ
- มีคำสั่งของศาลหรือต้องดำเนินการตามกฎหมาย
- มีผู้อื่นที่ล่วงรู้กุญแจส่วนตัวของ NITMX CA
- NITMX CA ระงับหรือยกเลิกการให้บริการ
- กรณีอื่นๆ ที่ NITMX CA พิจารณาแล้วว่าจะมีผลกระทบต่อความมั่นคงปลอดภัยของการให้บริการออกใบรับรอง

4.8.2 ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Revocation)

- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียน

(Copyright © 2007 Thai Digital ID Company Limited)

- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์(องค์กรหรือนิติบุคคลเจ้าของใบรับรองอิเล็กทรอนิกส์)

4.8.3 ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Procedure for Revocation Request)

1. กรอกแบบคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ พร้อมทั้งลงลายมือชื่อกำกับ
2. ส่งแบบคำขอเพิกถอนใบรับรองและหลักฐานประกอบให้เจ้าหน้าที่หน่วยงานรับลงทะเบียน
3. เจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบแบบคำขอเพิกถอนใบรับรองและหลักฐาน
4. หลังจากเจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบแบบคำขอเพิกถอนใบรับรองและหลักฐานเรียบร้อย เจ้าหน้าที่หน่วยงานรับลงทะเบียนจึงจะทำการเพิกถอนใบรับรอง

ข้อสังเกต

การเพิกถอนใบรับรองอิเล็กทรอนิกส์ ไม่ได้เป็นการลบใบรับรองอิเล็กทรอนิกส์ออกไปจากฐานข้อมูล

4.8.4 ระยะเวลาที่ใช้ในการเพิกถอน (Revocation Request Grace Period)

หลังจากเจ้าหน้าที่หน่วยงานรับลงทะเบียนได้รับคำขอเพิกถอนใบรับรอง และได้ทำการตรวจสอบความถูกต้องแล้ว เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะทำการเพิกถอนใบรับรองภายใน 1 วันทำการ (นับต่อจากวันทำการที่ได้รับเอกสาร)

4.8.5 เหตุการณ์ที่ต้องระงับการใช้งานใบรับรองอิเล็กทรอนิกส์ (Circumstances for Suspension)

การระงับใบรับรองอิเล็กทรอนิกส์คือการทำให้ไม่สามารถนำใบรับรองมาใช้ได้ชั่วคราว โดยผู้ให้บริการหรือผู้ขอใช้ใบรับรองจะสามารถระงับใบรับรองได้ในกรณีดังต่อไปนี้

- คาดว่าอาจจะมีผู้อื่นล่วงรู้กุญแจส่วนตัว หรือคาดว่าอาจจะมีผู้อื่นสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ขอใช้ใบรับรองไปใช้งาน
- คาดว่าอาจจะมีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ขอใช้ใบรับรอง
- ผู้ใช้บริการไม่ปฏิบัติตามข้อกำหนดและเงื่อนไขในคำชี้แจงทางปฏิบัติของ NITMX CA หรือข้อตกลงการใช้บริการ
- มีคำสั่งของศาลหรือต้องดำเนินการตามกฎหมาย

(Copyright © 2007 Thai Digital ID Company Limited)

4.8.6 ผู้ที่สามารถขอระงับใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Suspension)

- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียน
- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์

4.8.7 ขั้นตอนการระงับใบรับรองอิเล็กทรอนิกส์ (Procedure for Suspension Request)

1. กรอกแบบคำขอระงับใบรับรองอิเล็กทรอนิกส์ พร้อมทั้งลงลายมือชื่อกำกับ
2. ส่งแบบคำขอระงับใบรับรองและหลักฐานประกอบให้เจ้าหน้าที่หน่วยงานรับลงทะเบียน
3. เจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบแบบคำขอระงับใบรับรองและหลักฐาน
4. หลังจากเจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบแบบคำขอระงับใบรับรองและหลักฐานเรียบร้อย เจ้าหน้าที่หน่วยงานรับลงทะเบียนจึงจะทำการระงับใบรับรอง

4.8.8 ขอบเขตของระยะเวลาในการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์

ใบรับรองอิเล็กทรอนิกส์ที่ถูกระงับการใช้งานสามารถนำกลับมาใช้งานต่อได้ ก็ต่อเมื่อหน่วยงานรับลงทะเบียนได้รับเอกสารคำร้องขอให้ยกเลิกการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการเท่านั้น

4.8.9 ความถี่ในการประกาศรายการเพิกถอนใบรับรอง (CRL Issuance Frequency)

NITMX CA จะทำการประกาศรายการเพิกถอนใบรับรองทุกๆ 20 นาที

4.8.10 ข้อปฏิบัติสำหรับการตรวจสอบรายการเพิกถอนใบรับรอง (CRL Checking Requirements)

คู่กรณีที่เกี่ยวข้องที่ต้องการใช้งานใบรับรองอิเล็กทรอนิกส์ที่ออกโดย NITMX CA จะต้องทำการตรวจสอบรายการเพิกถอนใบรับรองก่อนที่จะมีการใช้งานที่เกี่ยวกับใบรับรองนั้น

4.8.11 การตรวจสอบสถานะของใบรับรองและการเพิกถอนใบรับรองแบบออนไลน์ (On-line Revocation/Status Checking Availability)

การตรวจสอบสถานะของใบรับรองและการเพิกถอนใบรับรองนั้นสามารถดำเนินการแบบออนไลน์ได้ผ่านทางเว็บไซต์ของ NITMX CA ที่ www.itmx.co.th หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

(Copyright © 2007 Thai Digital ID Company Limited)

4.8.12 ขอบเขตของการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์

ใบรับรองอิเล็กทรอนิกส์ที่ถูกระงับการใช้งานสามารถนำกลับมาใช้งานต่อไปได้ ก็ต่อเมื่อหน่วยงานรับลงทะเบียนได้รับเอกสารคำร้องขอให้ยกเลิกการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการ

4.9 *บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)*

ผู้ใช้บริการสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้ทางเว็บไซต์ www.itmx.co.th ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

4.10 *การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription)*

ผู้ใช้บริการสามารถเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ได้ โดยส่งแบบฟอร์มการขอยกเลิกการใช้บริการใบรับรองอิเล็กทรอนิกส์ พร้อมเอกสารหลักฐานที่กำหนด มาที่หน่วยงานรับลงทะเบียน โดยรายละเอียดของเอกสารที่กำหนด สามารถดูได้ที่ www.itmx.co.th หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

(Copyright © 2007 Thai Digital ID Company Limited)

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

5.1 *การควบคุมความมั่นคงปลอดภัยทางกายภาพ (Physical Security Controls)*

5.1.1 สถานที่ตั้งและการก่อสร้างสถานที่ (Site Location and Construction)

สถานที่ตั้งของหน่วยงานออกใบรับรองของผู้ให้บริการตั้งอยู่ที่ เลขที่ 142 ชั้น 4 อาคารธนาคารกสิกรไทย ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพฯ 10500 ซึ่งมีการปฏิบัติงานในสิ่งแวดล้อมที่มีความปลอดภัยตามมาตรฐาน ISO27001

5.1.2 การเข้าถึงทางกายภาพ (Physical Access)

การเข้าถึงพื้นที่ของระบบบริการออกใบรับรอง จะอนุญาตให้สามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่มีสิทธิ์ หรือ ผู้มาเยือนภายใต้การดูแลจากเจ้าหน้าที่ที่มีสิทธ์เท่านั้น และในการที่จะเข้าถึงพื้นที่ของระบบได้นั้นเจ้าหน้าที่จำเป็นต้องใช้รหัสผ่าน บัตรประจำตัวพนักงาน (RFID) และต้องผ่านการสแกนม่านตา (Iris Scan) โดยกำหนดเจ้าหน้าที่ที่มีสิทธิ์ให้มีจำนวนน้อยที่สุด พร้อมทั้งจะมีการเก็บข้อมูลบันทึกการเข้าออกในพื้นที่บริการทั้งหมดด้วย

5.1.3 ระบบไฟฟ้าและระบบปรับอากาศ (Power and Air Conditioning)

ระบบบริการทั้งหมดจะใช้ระบบไฟฟ้าจากแหล่งจ่ายไฟฟ้าแบบมาตรฐาน พร้อมทั้งยังมีเครื่องกำเนิดไฟฟ้าแบบส่วนตัวและเครื่องกำเนิดไฟฟ้าแบบต่อเนื่อง(UPS) เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง

ในระบบบริการจะมีระบบปรับอากาศเพื่อควบคุมอุณหภูมิและความชื้น 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

(Copyright © 2007 Thai Digital ID Company Limited)

5.1.6 การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage)

สื่อที่ใช้สำรองข้อมูลทุกประเภทจะถูกเก็บรักษาไว้ในห้องที่มีความปลอดภัย ในหลายๆ สถานที่

5.1.7 การกำจัดสิ่งที่ไม่ใช้ (Waste Disposal)

เอกสารหรือสื่อแม่เหล็กในแบบต่างๆ ที่ใช้เก็บข้อมูลที่เป็นความลับจะถูกทำลายโดย

1. กรณีที่เป็นสื่อแม่เหล็ก
   - การทำลายทิ้ง (Destruct)
   - การเขียนข้อมูลทับ (Overwrite)
2. กรณีที่เป็นเอกสาร
   - การทำลายทิ้งโดยเครื่องทำลายเอกสาร

5.1.8 สถานที่ให้บริการสำรอง (Secondary Site Backup)

สถานที่สำรองใช้ในการเก็บข้อมูลสำรอง และ สำรองสถานที่ปฏิบัติงาน โดยบุคคลที่ได้รับอนุญาตเท่านั้นจึงจะสามารถเข้าถึงสถานที่สำรองนี้ได้

5.2 *การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls)*

5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles)

จากการที่มีการใช้ระบบควบคุมการเข้าถึงและการบริหารจัดการกุญแจ ทำให้บุคคลเพียงคนเดียวไม่สามารถเข้าถึงระบบได้ทั้งหมด จึงต้องทำการแบ่งบทบาทหน้าที่เพื่อให้เป็นไปตามนโยบายความปลอดภัย ซึ่งเพื่อให้บรรลุวัตถุประสงค์ทำให้อย่างน้อยจะต้องมีบทบาทดังต่อไปนี้

5.2.1.1 บทบาทของผู้ให้บริการ (Trusted Roles for Certification Authority) แบ่งออกได้ ดังนี้

- ผู้จัดการฝ่าย CA Operation มีหน้าที่ดังนี้
  1. บริหารจัดการกุญแจส่วนตัวของผู้ให้บริการออกใบรับรอง
  2. กำหนดและดูแลนโยบายด้านความมั่นคงที่เกี่ยวข้องกับบริการใบรับรอง
  3. ตรวจสอบการทำงานของเจ้าหน้าที่ System Support และ System Administrator
- เจ้าหน้าที่ System Support มีหน้าที่ดังนี้
  1. กำหนดค่าตัวแปรสำคัญต่างๆ ให้กับระบบที่เกี่ยวข้องกับระบบให้บริการใบรับรอง
  2. บริหารและจัดการอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับระบบให้บริการใบรับรอง
  3. กำหนดค่าตัวแปรสำคัญต่างๆ ให้กับอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับระบบให้บริการใบรับรอง

(Copyright © 2007 Thai Digital ID Company Limited)

- เจ้าหน้าที่ System Administrator มีหน้าที่ดังนี้
    1. ปรับปรุงประสิทธิภาพการทำงาน (Performance Tuning) และปรับปรุงระบบรักษาความมั่นคง (Security Hardening) ให้กับเครื่องคอมพิวเตอร์
    2. บริหารจัดการกุญแจส่วนตัวของผู้ให้บริการออกใบรับรอง
    3. กำหนดและดูแลนโยบายด้านความมั่นคงที่เกี่ยวข้องกับบริการใบรับรอง
    4. ตรวจสอบการทำงานของเจ้าหน้าที่ System Support และ CA Operator
- เจ้าหน้าที่ CA Operator มีหน้าที่ดังนี้
    1. บริหารและจัดการเครื่องคอมพิวเตอร์สำหรับระบบให้บริการใบรับรอง
    2. ดูแลระบบปฏิบัติการ (Operating System) ของเครื่องคอมพิวเตอร์
    3. บริหารและจัดการระบบจัดเก็บข้อมูลของระบบให้บริการใบรับรอง

5.2.1.2 บทบาทของเจ้าหน้าที่รับลงทะเบียน (Trusted Roles for Registration Authority) แบ่งออกได้ ดังนี้

- เจ้าหน้าที่ RA Operator มีหน้าที่ดังนี้
    1. รับคำขอใช้บริการ
    2. พิสูจน์ความแท้จริงและตัวตนของผู้ใช้บริการ ก่อนขออนุมัติต่อ RA Administrator เพื่อดำเนินการขั้นตอนต่อไป
    3. ออกใบรับรองให้กับผู้ใช้บริการ หลังจากที่ได้รับการอนุมัติจาก RA Administrator
    4. รับคำขอเพิกถอนใบรับรอง
    5. พิสูจน์ความแท้จริงและตัวตนของผู้ใช้บริการ ก่อนขออนุมัติต่อ RA Administrator เพื่อดำเนินการขั้นตอนต่อไป
    6. เพิกถอนใบรับรองตามคำร้องขอของผู้ใช้บริการ หลังจากที่ได้รับการอนุมัติจาก RA Administrator
    7. ออกรายการเพิกถอนใบรับรอง

- เจ้าหน้าที่ RA Administrator มีหน้าที่ดังนี้
    1. พิจารณาอนุมัติการออกหรือเพิกถอนใบรับรองที่ RA Operator ส่งมาให้พิจารณา
    2. ตรวจสอบการทำงานของ RA Operator

(Copyright © 2007 Thai Digital ID Company Limited)

5.2.2 จำนวนบุคคลที่ต้องการต่องาน (Number of Persons Required Per Task)

การแบ่งบทบาทหน้าที่จะถูกแบ่งออกตามที่ได้กล่าวไว้แล้วข้างต้น ซึ่งจะทำให้มีความสมดุลในการปฏิบัติงาน พร้อมกับมีความปลอดภัยสูงสุด และสามารถตรวจสอบ โดยหลักการสำคัญสำหรับการแบ่งแยกหน้าที่ คือ

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

5.2.3 การระบุและพิสูจน์ความมีตัวตนแท้จริงของเจ้าหน้าที่ปฏิบัติงาน (Identification and Authentication for each Role)

บุคลากรที่จะมาปฏิบัติงานจะต้องผ่านการคัดเลือกตามกระบวนการอย่างเป็นทางการเพื่อแสดงถึง “การเป็นบุคคลที่ไว้วางใจได้”

5.3 *การควบคุมบุคคล (Personnel Controls)*

5.3.1 ประวัติ คุณสมบัติ ประสบการณ์และข้อกำหนดประวัติ (Background, qualifications, experience, and clearance requirements)

การคัดเลือกบุคคลที่จะเข้ามาปฏิบัติงานสำหรับระบบการให้บริการออกใบรับรองจะต้องผ่านการตรวจสอบประวัติ คุณสมบัติ ประสบการณ์ และข้อกำหนดประวัติ แล้วจึงนำข้อมูลดังกล่าวมาเปรียบเทียบกับผู้สมัครท่านอื่นๆด้วย เพื่อให้ได้บุคคลที่ดีที่สุด

5.3.2 วิธีดำเนินการในการตรวจสอบประวัติ (Background Check Procedures)

ทุกบุคคลจะต้องผ่านการตรวจสอบประวัติ พร้อมทั้งผ่านการคัดกรองทางด้านความปลอดภัย การทดลองงาน เพื่อให้ได้บุคคลที่จะมาทำหน้าที่ที่ต้องการความไว้วางใจได้

5.3.3 การฝึกอบรมบุคลากร (Training Requirements)

พนักงานทุกคนจะต้องผ่านการฝึกอบรมดังต่อไปนี้

- ความรู้เกี่ยวกับเทคโนโลยี Public Key Infrastructure (PKI)
- มาตรฐานด้านความมั่นคงของเทคโนโลยีสารสนเทศ
- การใช้งานระบบบริการใบรับรอง
  - วิธีการในการสำรองข้อมูล
  - วิธีการในการตรวจสอบระบบ

(Copyright © 2007 Thai Digital ID Company Limited)

- ความรู้พื้นฐานทางด้าน IT และวิธีการในการรักษาความมั่นคงและปลอดภัยของระบบคอมพิวเตอร์
- แนวโน้มทางด้านเทคโนโลยีด้านความปลอดภัย
- วิธีการใช้งานโปรแกรมประยุกต์ต่างๆ ที่จำเป็นต่อระบบ
- วิธีการใช้งานเครื่องมือและอุปกรณ์ต่างๆ ที่จำเป็นต่อระบบ
- ระบบ ISO 27001
- ความหมายและประสิทธิภาพของนโยบายใบรับรองและคำชี้แจงทางปฏิบัติ (CP และ CPS)

5.3.4 ความถี่ในการทบทวนการฝึกอบรม (Retraining Frequency and Requirements)

พนักงานทุกคนจะต้องได้รับการทบทวนการฝึกอบรมอย่างน้อยปีละ 1 ครั้ง หรือ มีการฝึกอบรมเพิ่มเติมในกรณีที่มีการอัพเกรดเวอร์ชั่นของซอฟต์แวร์

5.3.5 การลงโทษเกี่ยวกับการดำเนินการโดยไม่ได้รับอนุญาต (Sanctions for Unauthorized Actions)

ในกรณีที่พนักงานได้ดำเนินการโดยไม่ได้รับอนุญาตจาก CA Operation Manager พนักงานผู้นั้นจะได้รับการลงโทษตามระเบียบของบริษัทฯ

5.3.6 เอกสารประกอบสำหรับบุคลากร (Documentation Supplied to Personnel)

บุคลากรสามารถเรียกดูข้อมูลดังต่อไปนี้ได้

1. เอกสารประกอบสำหรับอุปกรณ์และซอฟต์แวร์
2. เอกสารของนโยบายต่างๆ รวมทั้งเอกสาร CP
3. คู่มือการใช้งานแอปพลิเคชั่นต่างๆ
4. วิธีการปฏิบัติงานต่างๆ รวมทั้งเอกสาร CPS

5.4 *กระบวนการตรวจสอบข้อมูลการลงบันทึกเหตุการณ์ (Audit Logging Procedures)*

เจ้าหน้าที่ผู้ดูแล NITMX CA ที่ได้รับมอบหมาย จะทำการตรวจสอบความมั่นคงปลอดภัยของระบบเป็นประจำ เพื่อช่วยในการควบคุมและแก้ไขความเสียหายที่อาจเกิดขึ้น โดยจะตรวจสอบจากข้อมูลบันทึกเหตุการณ์ต่างๆ (Log Event) และทำการบันทึกข้อมูลที่จำเป็นเพิ่มเติมเพื่อเป็นรายงานในการอ้างอิงต่อไป

5.4.1 ชนิดของเหตุการณ์ (Types of Event Recorded)

เหตุการณ์ที่ถูกบันทึกเพื่อใช้ในการตรวจสอบระบบ มีดังนี้

1. การเข้าใช้งานเครื่องให้บริการสำหรับปฏิบัติงานในรูปแบบต่างๆ
2. การจัดการเกี่ยวกับกุญแจและใบรับรอง
3. การเพิกถอนใบรับรองและการออกรายการเพิกถอนใบรับรอง

(Copyright © 2007 Thai Digital ID Company Limited)

4. การจัดการกับฐานข้อมูลของ NITMX CA
5. การปรับปรุงและเปลี่ยนแปลงฮาร์ดแวร์และซอฟต์แวร์
6. การบำรุงรักษาระบบคอมพิวเตอร์และสถานที่ติดตั้งระบบ

5.4.2 ความถี่ในการประมวลผลข้อมูลการลงบันทึกเหตุการณ์ (Frequency of Processing Log)

เจ้าหน้าที่ดูแลระบบจะเข้ามาตรวจสอบข้อมูลการลงบันทึกเหตุการณ์อย่างสม่ำเสมอ

5.4.3 ระยะเวลาที่จะเก็บข้อมูลการลงบันทึกเหตุการณ์ (Retention Period for Audit Log)

ข้อมูลการลงบันทึกเหตุการณ์ต่าง ๆ จะถูกเก็บไว้เป็นเวลาอย่างน้อย 10 ปี

5.4.4 การป้องกันข้อมูลการลงบันทึกเหตุการณ์ (Protection of Audit Log)

ระบบ NITMX CA จะทำการจัดเก็บข้อมูลการลงบันทึกเหตุการณ์ต่างๆ ไว้ในเครื่องเซิร์ฟเวอร์สำหรับบันทึกเหตุการณ์ต่างๆ ที่เกิดขึ้น ซึ่งจะมีแต่เจ้าหน้าที่ผู้ดูแล NITMX CA ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงและอ่านข้อมูลได้

5.4.5 ขั้นตอนการสำรองเก็บข้อมูลการลงบันทึกเหตุการณ์ (Audit Log Backup Procedure)

ข้อมูลการลงบันทึกเหตุการณ์ต่างๆ จะได้รับการบันทึกลงเทปในลักษณะแบบสมบูรณ์ (Full backup) ทุกวัน และยังมีการกระจายเทปไปเก็บตามสถานที่ต่างๆ เพื่อความปลอดภัยมากยิ่งขึ้นอีกด้วย

5.4.6 ระบบการเก็บข้อมูลการลงบันทึกเหตุการณ์ (Audit Collection System)

การเก็บข้อมูลการลงบันทึกเหตุการณ์ต่าง ๆ จะปฏิบัติการโดยเจ้าหน้าที่ผู้ดูแล NITMX CA ที่ได้รับอนุญาตเท่านั้น

5.4.7 การแจ้งไปยังบุคคลที่เกี่ยวข้อง (Notification to Event-Causing Subject)

เจ้าหน้าที่ดูแลระบบ NITMX CA จะคอยตรวจสอบบันทึกเหตุการณ์ทุกวันเพื่อให้ทราบถึงเหตุการณ์ที่ไม่ปกติเกี่ยวกับความมั่นคงปลอดภัยของระบบ ทำให้สามารถรองรับและแก้ไขสถานการณ์ได้ทันท่วงที ทั้งนี้ หากเหตุการณ์ที่ไม่ปกติเกิดจากภายนอกระบบ จะมีการแจ้งไปยังบุคคลที่เกี่ยวข้องด้วย

(Copyright © 2007 Thai Digital ID Company Limited)

5.5 *การเก็บรักษาข้อมูลบันทึก (Records Archival)*

NITMX CA ในฐานะผู้ให้บริการบริหารจัดการระบบการออกใบรับรองอิเล็กทรอนิกส์ จะทำหน้าที่ในการเก็บรักษาข้อมูลที่เกี่ยวข้อง ดังที่จะอธิบายดังต่อไปนี้

5.5.1 รูปแบบของข้อมูล (Types of Event Recorded)

1. ข้อมูลคำร้องขอใบรับรอง
2. ใบรับรองและรายชื่อผู้ถูกเพิกถอนใบรับรอง
3. ข้อมูลที่ถูกสำรองไว้
4. ข้อมูลที่เกี่ยวข้องทั่วไป

5.5.2 ระยะเวลาที่เก็บรักษา (Retention Period for Archive)

5.5.2.1 การเก็บรักษากุญแจ (Secure maintenance of Keys)

การเก็บรักษากุญแจส่วนตัวของ CA จะถูกเก็บรักษาใน Hardware Security Module ที่ได้มาตรฐาน FIPS 140-2 Level 3

5.5.2.2 การเก็บรักษาใบรับรอง (Secure maintenance of Certificate)

ใบรับรองของ CA และ RA จะถูกเก็บรักษาไว้อย่างน้อย 10 ปี นับตั้งแต่การออกใบรับรองฯ ดังกล่าว

5.5.2.3 ระยะการเก็บรักษาข้อมูลที่สำรองไว้ (Term of archive maintenance)

ข้อมูลที่ใช้ในการตรวจสอบจะถูกเก็บรักษาไว้อย่างน้อย 10 ปี

5.5.3 การป้องกันข้อมูลที่สำรองไว้ (Protection of Archive)

ข้อมูลที่สำรองไว้จะเก็บไว้ในพื้นที่ที่มีความปลอดภัย โดยสามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น หรือ เป็นการผสมผสานการป้องกันระหว่างพื้นที่ที่มีความปลอดภัยพร้อมกับการเข้ารหัสข้อมูล พร้อมกันนี้ข้อมูลยังถูกป้องกันภัยจากสิ่งแวดล้อมที่เกิดจากอุณหภูมิ ความชื้น และ สนามแม่เหล็กอีกด้วย

5.5.4 นโยบายการสำรองข้อมูล (Archive Backup Procedures)

นโยบายในการสำรองข้อมูลได้ถูกสร้างขึ้นเพื่อตรวจสอบและให้แน่ใจว่าสามารถกู้ข้อมูลได้อย่างสมบูรณ์

5.5.5 ระบบสำรองข้อมูล (Archive Collection System)

การสำรองข้อมูลจะถูกจัดการด้วยระบบภายในโดยพนักงานที่มีหน้าที่รับผิดชอบเท่านั้น

(Copyright © 2007 Thai Digital ID Company Limited)

5.5.6 วิธีการปฏิบัติเพื่อตรวจสอบข้อมูลที่สำรองไว้ (Procedures to Obtain and Verify Archive Information)

จะมีการตรวจสอบความครบถ้วนถูกต้องของข้อมูลที่สำรองไว้ก็ต่อเมื่อ

1. เมื่อถึงรอบในการตรวจสอบความปลอดภัย
2. เมื่อมีความจำเป็นต้องตรวจสอบความปลอดภัย
3. เมื่อต้องการเตรียมการสำหรับการสำรองข้อมูล

5.6 *การเปลี่ยนคู่คีย์ (Key Changeover)*

ระยะเวลาของใบรับรองของผู้ให้บริการ NITMX CA คือ 10 ปี และเมื่อใบรับรองมีอายุเข้าสู่ปีที่ 6 ก็จะมีการสร้างคู่คีย์ของผู้ให้บริการใหม่ ตามมาตรฐาน X.509 ซึ่งใบรับรองนี้จะถูกรับรองโดย Thai Digital ID Root CA ภายใต้ข้อกำหนดดังนี้

1. ข้อกำหนดใน CP
2. ตามมาตรฐาน X.509
3. ตามมาตรฐานข้อมูลใบรับรอง

5.7 *ความผิดพลาดของระบบและการฟื้นฟูระบบ (Compromise and Disaster Recovery)*

5.7.1 เครื่องคอมพิวเตอร์, ซอฟต์แวร์ และ/หรือ ข้อมูลเกิดความผิดพลาด (Computing Resources, Software, and/or Data Are Corrupted)

ในกรณีที่เกิดความผิดพลาดหรือเสียหายเกิดขึ้นกับ เครื่องคอมพิวเตอร์, ซอฟต์แวร์ และ/หรือ ข้อมูล เจ้าหน้าที่ CA Operator จะดำเนินการวิเคราะห์แจะแก้ไขปัญหาตามขั้นตอนที่ระบุไว้ในแผนการตอบสนองเหตุการณ์ฉุกเฉินและฟื้นฟูระบบ

5.7.2 เมื่อ PKI Entity ถูกยกเลิก (Entity Public Key Is Revoked)

ได้มีการจัดสร้างแผน Contingency and Disaster Recovery Plan สำหรับจัดการกับปัญหาในกรณีที่ Thai Digital ID Root CA, NITMX CA และ RA ที่เกี่ยวข้อง ได้ถูกยกเลิก

5.7.3 เมื่อ PKI Entity ถูกละเมิด (Entity Key Is Compromised)

NITMX CA และ RA ภายใต้ CA ได้จัดสร้างแผนสำหรับในกรณีที่กุญแจส่วนตัวถูกละเมิด

(Copyright © 2007 Thai Digital ID Company Limited)

5.7.4 ความปลอดภัยจากธรรมชาติหรือจากภัยพิบัติอื่นๆ (Secure Facility after a Natural or other type of Disaster)

ในกรณีที่เกิดภัยพิบัติซึ่งส่งผลให้ระบบการปฏิบัติงาน CA เกิดความเสียหายไม่สามารถให้บริการได้ในพื้นที่หลัก ฝ่ายปฏิบัติการสำหรับ NITMX CA จะนำข้อมูลที่มีการสำรองและข้อมูลที่เก็บอยู่ที่ offsite เพื่อ restore รวมทั้งฟื้นฟูระบบตามแผนการฟื้นฟูระบบของบริษัทฯ ที่ศูนย์ปฏิบัติการสำรอง

5.8 *การยกเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ หน่วยงานออกใบรับรองอิเล็กทรอนิกส์ (CA or RA Termination)*

5.8.1 บทนำ

เนื้อหาในส่วนนี้จะอธิบายเกี่ยวกับการยกเลิกกิจการของส่วนใดส่วนหนึ่งของ TDID RCA ซึ่งรวมทั้ง NITMX CA ด้วยเช่นกัน โดยในส่วนนี้จะทำให้ลูกค้ามั่นใจได้ว่าลูกค้าจะไม่ถูกเอาเปรียบจากผู้ให้บริการได้ โดยจะมี 2 กรณีที่ NITMX CA จะเป็นผู้รับผิดชอบได้แก่

1. NITMX CA ตัดสินใจที่จะยกเลิกการให้บริการ
2. NITMX CA ถูกสภาวะแวดล้อมจากภายนอกให้ต้องยกเลิกการให้บริการ

5.8.2 การยกเลิกการให้บริการธุรกิจ CA อย่างมีแบบแผน (CA Business Operations Programmed Termination)

ถ้า TDID RCA ได้รับการแจ้งขอยกเลิกการให้บริการจาก CA ที่ถูกรับรองภายใต้ TDID RCA แล้ว

1. TDID RCA จะช่วยโอนใบรับรองของลูกค้าไปยังผู้ให้บริการ CA รายอื่น
2. ผู้ให้บริการ CA ที่ถูกรับรองภายใต้ TDID RCA จะต้องปฏิบัติดังนี้
   - ให้ TDID RCA เขียนประกาศแจ้งล่วงหน้า 6 เดือนเกี่ยวกับการยกเลิกการให้บริการ
   - ร่วมมือกับ TDID RCA ในการเลือก CA ที่เหมาะสมมาดำเนินการต่อไป
   - โอนกุญแจส่วนตัวของระบบ CA ที่จะยกเลิกการให้บริการไปยัง CA ที่จะมาแทนที่ โดยอาจจะต้องได้รับการยินยอมจาก TDID RCA ด้วย
   - โอนใบรับรองของลูกค้าไปยัง CA ที่จะมาแทนที่ โดยอาจจะต้องได้รับการยินยอมจาก TDID RCA ด้วย
   - ภายหลังจากที่ได้มีการโอนกุญแจส่วนตัวของผู้ให้บริการ CA เดิมไปยัง ผู้ให้บริการ CA รายใหม่ที่จะมาแทนที่แล้ว ผู้ให้บริการCA เดิมจะต้องทำลายกุญแจสาธารณะที่ทำการสำรองไว้ทั้งหมดในทันที
   - ต้องใช้เวลาอย่างเหมาะสมในการโอน เพื่อไม่ให้เกิดผลกระทบต่อการออกใบรับรองอิเล็กทรอนิกส์ใบใหม่ให้แก่ผู้ใช้

(Copyright © 2007 Thai Digital ID Company Limited)

3. นอกจากนี้ถ้าผู้ให้บริการ CA เดิมไม่สามารถตกลงกับผู้ให้บริการ CA รายใหม่ได้เกี่ยวกับการโอนกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ได้ ภายใน 90 วัน ก็จะต้องทำตามวิธีดังต่อไปนี้
   - องค์กรที่ให้บริการระบบ CA ที่จะมาแทนที่จะต้องแจ้ง TDID RCA และผู้ให้บริการ CA เดิม ถึงกำหนดการที่แน่นอนใหม่ในการโอนกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์
   - องค์กรที่ให้บริการระบบ CA ที่จะมาแทนที่จะต้องสามารถทดแทนผู้ให้บริการ CA เดิมได้ หลังจากมีการโอนกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ของผู้ใช้ โดยเงื่อนไขให้เป็นไปตามสัญญาที่เกี่ยวข้อง

5.8.3 การยกเลิกการให้บริการธุรกิจ CA อย่างไม่มีแบบแผน (CA Business Operations Non-programmed Termination)

ถ้าผู้ให้บริการ CA เดิมภายใต้การรับรองของ Thai Digital ID Root CA มีความจำเป็นต้องยกเลิกการให้บริการ ตัวแทนของผู้ให้บริการจะต้องแจ้งให้ TDID RCA ในทันที ซึ่งในกรณีนี้

1. TDID RCA จะช่วยโอนใบรับรองของลูกค้าไปยังผู้ให้บริการ CA รายอื่น
2. ผู้ให้บริการ CA ที่ถูกรับรองภายใต้ TDID RCA จะต้องปฏิบัติดังนี้
   - โอนกุญแจส่วนตัวของระบบ CA ที่จะยกเลิกการให้บริการไปยัง CA ที่จะมาแทนที่ โดยอาจจะต้องได้รับการยินยอมจาก TDID RCA ด้วย
   - โอนใบรับรองของลูกค้าไปยัง CA ที่จะมาแทนที่ โดยอาจจะต้องได้รับการยินยอมจาก TDID RCA ด้วย
   - ภายหลังจากที่ได้มีการโอนกุญแจส่วนตัวของผู้ให้บริการ CA เดิมไปยัง ผู้ให้บริการ CAรายใหม่ที่จะมาแทนที่แล้ว ผู้ให้บริการCA เดิมจะต้องทำลายกุญแจสาธารณะที่ทำการสำรองไว้ทั้งหมดในทันที
   - ต้องใช้เวลาอย่างเหมาะสมในการโอน เพื่อไม่ให้เกิดผลกระทบต่อการออกใบรับรองอิเล็กทรอนิกส์ใบใหม่ให้แก่ผู้ใช้
3. นอกจากนี้ถ้าผู้ให้บริการ CA เดิมไม่สามารถตกลงกับผู้ให้บริการ CA รายใหม่ได้เกี่ยวกับการโอนกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ได้ ภายใน 90 วัน ก็จะต้องทำตามวิธีดังต่อไปนี้
   - องค์กรที่ให้บริการระบบ CA ที่จะมาแทนที่จะต้องแจ้ง TDID RCA และผู้ให้บริการ CA เดิม ถึงกำหนดการที่แน่นอนใหม่ในการโอนกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์
   - องค์กรที่ให้บริการระบบ CA ที่จะมาแทนที่จะต้องสามารถทดแทนผู้ให้บริการ CA เดิมได้ หลังจากมีการโอนกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ของผู้ใช้ โดยเงื่อนไขให้เป็นไปตามสัญญาที่เกี่ยวข้อง

(Copyright © 2007 Thai Digital ID Company Limited)

5.8.4 การยกเลิกการให้บริการธุรกิจ RA อย่างมีแบบแผน (RA Business Operations Programmed Termination)

ถ้า TDID RCA หรือ NITMX CA ได้รับการแจ้งจาก RA ที่อยู่ภายใต้การรับรองของ NITMX CA ว่าจะยกเลิกการให้บริการธุรกิจ RA แล้ว

1. RA จะต้องแจ้งแก่ Thai Digital ID Root CA และ NITMX CA ล่วงหน้าอย่างน้อย 6 เดือน
2. TDID RCA ทำการโอนข้อมูลจาก RA เดิม ไปยัง RA ที่จะมาแทนที่

5.8.5 การยกเลิกการให้บริการธุรกิจ RA อย่างไม่มีแบบแผน (RA Business Operations Non-programmed Termination)

TDID RCA จะร่วมมือกับ NITMX CA เพื่อทำการโอนข้อมูลจาก RA เดิม ไปยัง RA ที่จะมาแทนที่ แต่ถ้าไม่มี RA ที่จะมาทดแทนได้ NITMX CA จะเป็นผู้ทำหน้าที่ RA ให้เอง

5.8.6 วิธีการในการประเมิน (Evaluation Mechanism)

5.8.6.1 การโอนข้อมูล NITMX CA (Transfer of NITMX CA Data)

NITMX CA ตกลงที่จะโอนกุญแจส่วนตัวและ ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ ให้กับCA ที่จะมาแทนที่ โดยขึ้นอยู่กับว่า NITMX CA ได้รับการชดเชยค่าใช้จ่ายที่เป็นธรรมหรือไม่ ถ้า NITMX CA ไม่สามารถตกลงกับ CA ที่จะมาแทนที่ได้ จะต้องให้ TDID RCA จัดหาผู้ประเมินที่มีความชำนาญเกี่ยวกับธุรกิจเทคโนโลยี โดยผู้ประเมินจะต้องไม่ถูกสนับสนุนโดย TDID RCA และ ไม่ได้ทำงานประจำที่ TDID RCA

(Copyright © 2007 Thai Digital ID Company Limited)

6 การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

6.1 *การสร้างและติดตั้งคู่คีย์ (Key Pair Generation and Installation)*

6.1.1 การสร้างกุญแจคู่ (Key Pair Generation)

กุญแจคู่ของ NITMX CA จะถูกสร้างและติดตั้งโดย NITMX CA ส่วน กุญแจคู่ของผู้ใช้บริการจะถูกสร้างโดย RA และรับรองโดย NITMX CA ที่ได้รับอนุญาตและถูกติดตั้งใน token ซึ่งเก็บรักษาโดยผู้ใช้บริการเอง (สำหรับใบรับรองอิเล็กทรอนิกส์ประเภทยืนยันตัวบุคคลและนิติบุคคล)

6.1.2 การส่งมอบกุญแจส่วนตัว (Private Key Delivery to Entity)

กุญแจส่วนตัวของผู้ใช้บริการจะถูกสร้างผ่านระบบ RA และรับรองโดย NITMX CA ซึ่งจัดเก็บอยู่ใน Token ซึ่งเป็นอุปกรณ์ที่มีความปลอดภัยสูง ไม่สามารถคัดลอก กุญแจส่วนตัวและข้อมูลอื่นใดออกไปได้ แล้วจึงส่งมอบ Token ให้ผู้ใช้บริการโดยตรง

6.1.3 การส่งมอบกุญแจสาธารณะไปยังผู้ให้การรับรองฯ (Public Key Delivery to Certificate Issuer)

การส่งมอบกุญแจสาธารณะของผู้ใช้บริการไปยังผู้ให้บริการเพื่อทำการรับรองให้เป็นไปโดยอัตโนมัติแบบปลอดภัย ภายใต้การทำงานของโปรแกรมประยุกต์ใช้งานของระบบ NITMX CA

6.1.4 การส่งมอบกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปยังผู้ใช้ (CA Public Key Delivery to Users)

กุญแจสาธารณะของ NITMX CA มีความจำเป็นต่อผู้ใช้บริการ โดยอาจจะกระจายไปพร้อมกับกุญแจของผู้ใช้บริการและใบรับรองอิเล็กทรอนิกส์ หรือ ดาวน์โหลดโดยผู้ใช้บริการจาก X.500 ไดเรคทอรี่ ของ NITMX CA

6.1.5 ขนาดของกุญแจ (Key Sizes)

ความยาวของกุญแจ NITMX CA จะถูกกำหนดในข้อมูลใบรับรองอิเล็กทรอนิกส์ โดยจะมีความยาว 2048 บิต ส่วนขนาดกุญแจของผู้ใช้ใบรับรอง มีขนาดอยู่ที่ 1024 บิต

(Copyright © 2007 Thai Digital ID Company Limited)

6.1.6 การสร้างตัวแปรกุญแจสาธารณะ (Public Key Parameters Generation)

ตัวแปรที่ใช้ในการสร้างกุญแจสาธารณะจะถูกสร้างโดย NITMX CA โดยยึดตามมาตรฐาน X.509 Version 3

6.1.7 การตรวจสอบคุณภาพของตัวแปร (Parameter Quality Checking)

คุณภาพของตัวแปรของกุญแจสาธารณะจะถูกตรวจสอบโดยอัตโนมัติจากโปรแกรมประยุกต์ใช้งานของระบบ NITMX CA

6.1.8 การสร้างกุญแจคู่จากอุปกรณ์หรือซอฟต์แวร์ (Hardware/Software Key Generation)

การสร้างกุญแจคู่ของ CA จะถูกจัดการโดยอุปกรณ์ที่เรียกว่า Hardware Security Module ซึ่งสอดคล้องมาตรฐานสากล FIPS 140-1 Level 3

6.1.9 จุดประสงค์ของการใช้กุญแจ (Key Usage Purposes)

จุดประสงค์ของการใช้กุญแจได้ถูกอธิบายไว้ในหัวข้อ 1.4 การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)

6.2 *การปกป้องกุญแจส่วนตัว (Private Key Protection) และการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls)*

6.2.1 มาตรฐานของโมดูลที่ใช้ในการเข้ารหัสลับ (Standards for Cryptographic Module)

โมดูลที่ใช้ในการเข้ารหัสของระบบ NITMX CA ได้มีการปฏิบัติตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-1 Level 3 ซึ่งเป็นมาตรฐานสากลในการสร้างและเก็บรักษากุญแจส่วนตัวของระบบ CA

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

กุญแจส่วนตัวของผู้ให้บริการได้มีการควบคุมการเข้าถึงแบบหลายบุคคล

6.2.3 การฝากกุญแจส่วนตัว (Private Key Escrow)

ไม่มีการรับฝากกุญแจส่วนตัว

(Copyright © 2007 Thai Digital ID Company Limited)

6.2.4 การสำรองกุญแจส่วนตัว (Private Key Backup)

มีการสำรองกุญแจส่วนตัวเฉพาะของ TDID RCA และ NITMX CA

6.2.5 การเก็บรักษากุญแจส่วนตัวของผู้ให้บริการ (Private Key Archival)

มีการจัดทำการสำรอง กุญแจส่วนตัวของผู้ให้บริการ โดยเก็บไว้ในอุปกรณ์ Hardware Security Module ซึ่งได้รับการรับรองตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-1 Level 3

6.2.6 กุญแจส่วนตัวภายในโมดูลการเข้ารหัส (Private Key Entry into Cryptographic Module)

กุญแจส่วนตัวของ NITMX CA ได้ถูกสร้างขึ้นภายในโมดูลนี้และมีรูปแบบของการเข้ารหัสและถอดรหัส ซึ่งได้รับการรับรองตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-1 Level 3 และจะนำมาถอดรหัสก็ต่อเมื่อมีการตรวจสอบสิทธิผ่านอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยสูงและมีการใส่รหัสผ่านที่ถูกต้องโดยเจ้าหน้าที่ดูแลระบบออกใบรับรอง NITMX CA เท่านั้น

6.2.7 วิธีการนำกุญแจส่วนตัวมาใช้งาน (Method of Activating Private Key)

กุญแจส่วนตัวของ NITMX CA จะถูกนำมาใช้งานได้เมื่อมีการตรวจสอบสิทธิผ่านอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยสูงและมีการใส่รหัสผ่านที่ถูกต้องโดยเจ้าหน้าที่ผู้ดูแลระบบออกใบรับรอง NITMX CA เท่านั้น

6.2.8 วิธีเลิกการใช้งานกุญแจส่วนตัว (Method of Deactivating Private Key)

กุญแจส่วนตัวของ NITMX CA จะถูกควบคุมโดย โมดูลฮาร์ดแวร์ที่มีการเข้ารหัส โดยการเลิกการใช้งาน จะกระทำโดยการใช้งานผ่าน ซอฟต์แวร์ แบบ log out และนำ token นั้นออกจากเครื่องอ่าน

6.2.9 วิธีการทำลายกุญแจส่วนตัว (Method of Destroying Private Key)

วิธีการทำลายกุญแจส่วนตัวจะทำโดยการฟอร์แมตข้อมูลใน token ผ่าน ซอฟต์แวร์

6.2.10 การจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls)

ผู้ให้บริการได้มีการจัดสร้างเอกสารการตรวจสอบความเสี่ยงเกี่ยวกับความปลอดภัย ซึ่งได้มีการระบุและจัดการกับความเสี่ยงที่ระดับสูงและสูงมาก เกี่ยวกับเรื่องการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับไว้แล้ว

(Copyright © 2007 Thai Digital ID Company Limited)

6.3 *รายละเอียดอื่นเกี่ยวกับการจัดการและบริหารกุญแจคู่ (Other Aspects of Key Pair Management)*

6.3.1 การเก็บรักษากุญแจสาธารณะ (Public Key Archival)

กุญแจสาธารณะจะถูกเก็บบันทึก ไว้ในใบรับรอง โดยใบรับรอง ได้ถูกจัดเก็บไว้ในฐานข้อมูลของ NITMX CA

6.3.2 ระยะเวลาใช้งานของกุญแจส่วนตัวและกุญแจสาธารณะ (Usage Periods for the Public and Private Keys)

ระยะเวลาใช้งานของกุญแจส่วนตัวและกุญแจสาธารณะ ของ TDID RCA คือ 20 ปี และระยะเวลาใช้งานของกุญแจส่วนตัวและกุญแจสาธารณะ ของ NITMX CA คือ 10 ปี

6.4 *ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data)*

6.4.1 การสร้างข้อมูลและการนำข้อมูลไปใช้ในการติดตั้งใบรับรอง (Activation Data Generation and Installation)

ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ ถูกสร้างอย่างปลอดภัย โดยโปรแกรมประยุกต์ใช้งานของระบบ NITMX CA

6.4.2 การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรอง (Activation Data Protection)

การป้องกันข้อมูลที่อยู่ในใบรับรอง สำหรับผู้ใช้บริการของระบบ NITMX CA จะถูกป้องกันด้วยรหัสลับเริ่มต้น โดยทุกครั้งที่มีการเข้าถึงใบรับรองผู้ใช้ต้องใส่รหัสลับให้ถูกต้องเสมอ

6.5 *การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)*

6.5.1 ข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ที่มีลักษณะเฉพาะ (Specific Computer Security Technical Requirements)

ผู้ให้บริการได้มีการจัดตั้งแผนความปลอดภัยของระบบ ที่ได้รวมข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์ไว้แล้ว

(Copyright © 2007 Thai Digital ID Company Limited)

6.5.2 การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating)

ผู้ให้บริการได้มีการจัดตั้งแผนความปลอดภัยของระบบ ที่ได้แบ่งระดับในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองอิเล็กทรอนิกส์ไว้แล้ว

6.6 *การควบคุมวงจรทางเทคนิคของระบบให้บริการ (Life Cycle Security Controls)*

6.6.1 การควบคุมในการพัฒนาระบบ (System Development Controls)

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

6.6.2 การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัย (Security Management Controls)

การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัยจะถูกควบคุมตามบทบาทหน้าที่ของเจ้าหน้าที่ผู้ดูแลระบบที่ได้กำหนดสิทธิ์ไว้แล้ว ตามหัวข้อ 5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles)

6.6.3 การแบ่งระดับความปลอดภัยของวงจรทางเทคนิคของระบบให้บริการ (Life Cycle Security Ratings)

ผู้ให้บริการได้มีการจัดสร้างเอกสารการตรวจสอบความเสี่ยงเกี่ยวกับความปลอดภัย ซึ่งได้มีการระบุและจัดการกับความเสี่ยงที่ระดับสูงและสูงมาก เกี่ยวกับความปลอดภัยของวงจรทางเทคนิคของระบบให้บริการ

6.7 *การควบคุมความปลอดภัยทางเครือข่าย (Network Security Controls)*

ระบบการควบคุมทางเครือข่ายสำหรับระบบ NITMX CA ได้ถูกออกแบบให้เป็นระบบเครือข่ายเฉพาะที่ใช้สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องเท่านั้น และมีการติดตั้งซอฟต์แวร์ ไฟล์วอล ในการป้องกันการบุกรุกจากการเข้าถึงภายนอก

6.8 *การประทับเวลา (Timestamping)*

ระบบการให้บริการออกใบรับรองมีการบันทึกเวลาของ ทุก ๆ รายการที่เกิดขึ้นในระบบ

(Copyright © 2007 Thai Digital ID Company Limited)

7 การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ และรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)

7.1 *รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)*

7.1.1 รูปแบบ (Profile)

ใบรับรองที่ออกโดย NITMX CA ใช้มาตรฐาน X.509 Version 3 Certificate ซึ่งมีรายการดังต่อไปนี้

- Version 3 : รุ่นที่ 3
- Serial Number : หมายเลขของใบรับรอง
- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลของ NITMX CA
- Issuer : ชื่อของผู้ให้บริการ
- Validity : วันเวลาที่เริ่มและสิ้นสุดการใช้ใบรับรอง
- Subject : ชื่อผู้ถือใบรับรอง
- Subject Public Key Information : กุญแจสาธารณะของผู้ใช้บริการและวิธีการที่ใช้ในการสร้าง

7.1.2 ข้อมูลเพิ่มเติมของใบรับรอง (Certificate Extension)

ข้อมูลเพิ่มเติมของใบรับรองที่ออกโดย NITMX CA ใช้มาตรฐาน X.509 v3 certificate extensions ซึ่งมีรายการอย่างน้อยดังต่อไปนี้

- Authority Key Identifier : ระบุถึงกุญแจสาธารณะของ NITMX CA
- Subject Key Identifier : ระบุถึงกุญแจสาธารณะในใบรับรอง
- Key Usage : วัตถุประสงค์ในการนำกุญแจไปใช้งาน
- Extended Key Usage : วัตถุประสงค์เพิ่มเติมในการนำกุญแจไปใช้งาน
- Basic Constraints : ระบุถึงประเภทของใบรับรองอิเล็กทรอนิกส์ว่าเป็นของผู้ใช้บริการหรือผู้ให้บริการออกใบรับรอง และจำนวนชั้นสูงสุดของห่วงโซ่ใบรับรอง (Certificate Chain) ที่ถูกทำการรับรองต่อกันเป็นทอดๆ
- Certificate Policies : ระบุถึงข้อมูลเพื่อใช้อ้างอิงไปยังนโยบายใบรับรอง โดยระบุในรูปของ Object Identifier (OID)

7.1.3 รูปแบบของชื่อ (Name Forms)

รูปแบบของชื่อในส่วนของ Certificate Issuer และ Certificate Subject ที่ระบุในใบรับรองที่ออกโดย NITMX CA คือ ชื่อเฉพาะตามมาตรฐาน X.500

(Copyright © 2007 Thai Digital ID Company Limited)

7.2 *รูปแบบรายการเพิกถอนใบรับรอง (CRL Profile)*

7.2.1 รูปแบบ (Profile)

รายการเพิกถอนใบรับรองที่ออกโดย NITMX CA ใช้มาตรฐาน X.509 CRL Version 2 ซึ่งมีรายการดังต่อไปนี้

- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลในรายการเพิกถอนใบรับรองของ NITMX CA
- Issuer : ชื่อของผู้ให้บริการที่ออกรายการเพิกถอนใบรับรอง
- Effective date : วันเวลาที่ออกรายการเพิกถอนใบรับรอง
- Next update : วันเวลาที่จะทำการปรับปรุงรายการเพิกถอนใบรับรองครั้งถัดไป
- Authority Key Identifier : ระบุถึงข้อมูลที่สัมพันธ์กับกุญแจสาธารณะของใบรับรองของผู้ให้บริการที่ใช้ในการสร้างรายการเพิกถอนใบรับรอง
- Revoked certificates : รายการของใบรับรองที่ถูกเพิกถอน

(Copyright © 2007 Thai Digital ID Company Limited)

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

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้ยึดมาตรฐาน ISO 27001 สำหรับดำเนินการทางด้านการประเมินความเสี่ยง และ นโยบายด้านความมั่นคง โดยจัดให้มีการตรวจสอบทั้งผู้ตรวจสอบภายใน และ ผู้ตรวจสอบภายนอก

(Copyright © 2007 Thai Digital ID Company Limited)

9 ข้อกำหนดอื่น ๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

9.1 *ค่าธรรมเนียม (Fees)*

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะจัดเก็บค่าธรรมเนียมจากกรณีดังต่อไปนี้

1. การออกใบรับรองอิเล็กทรอนิกส์
2. การต่ออายุใบรับรองอิเล็กทรอนิกส์

9.2 *การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)*

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้กำหนดขอบเขตการรักษาความลับของข้อมูลทางธุรกิจ อันได้แก่ แผนทางธุรกิจ ข้อมูลการขาย ความลับทางการค้า และข้อมูลที่ได้จากบุคคลที่สามภายใต้ข้อตกลงไม่เปิดเผยความลับ และความรับผิดของบุคคลที่เกี่ยวข้องซึ่งได้รับข้อมูลลับนั้น ที่ได้ระบุไว้ในระเบียบและเงื่อนไขการใช้ใบรับรอง

9.3 *นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)*

การดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จะต้องได้รับความยินยอมจากผู้ใช้บริการ ก่อนจะมีการเปิดเผยข้อมูลส่วนบุคคล ยกเว้นกรณีที่จำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลในกรณีที่ต้องดำเนินการตามกฎหมายฉบับต่าง หรือเมื่อมีคำสั่งศาล

9.4 *ทรัพย์สินทางปัญญา (Intellectual Property Rights)*

ผู้ให้บริการเป็นเจ้าของสิทธิในทรัพย์สินทางปัญญาแต่เพียงผู้เดียวในเอกสารนโยบายใบรับรองอิเล็กทรอนิกส์ฉบับนี้ และสงวนสิทธิ์ใดๆ ที่มีอยู่หรือเกิดจากเอกสารฉบับนี้

9.5 *คำรับรอง (Representations and Warranties)*

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รับรองว่า ข้อมูลหรือข้อเท็จจริงที่บันทึกไว้ในใบรับรองอิเล็กทรอนิกส์นั้นถูกต้อง ตามข้อตกลงในการให้บริการกับผู้ใช้บริการ

9.6 *การบอกเลิกคำรับรอง (Disclaimers of Warranties)*

การบอกเลิกคำรับรองได้กำหนดไว้ในสัญญาในการให้บริการฉบับต่าง ๆ

9.7 *ข้อจำกัดความรับผิด (Limitations of Liability)*

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้กำหนด มาตรการในการลดหรือจำกัดข้อจำกัดความรับผิดในเหตุการณ์ ซึ่งความรับผิดจะถูกจำกัดอยู่เฉพาะเหตุการณ์ หรือความผิดพลาดที่เกิดขึ้นจาก ระบบและหรือ บุคลากร ของผู้ให้บริการฯ อันก่อให้เกิดความเสียหายต่อผู้ใช้บริการ

(Copyright © 2007 Thai Digital ID Company Limited)

ทั้งนี้ขอบเขตความรับผิดของผู้ให้บริการจะรับผิดชอบเฉพาะการนำใบรับรองอิเล็กทรอนิกส์ไปใช้ตามวัตถุประสงค์ที่กำหนดไว้ในหัวข้อ 1.4 เท่านั้น

มาตรการในการดำเนินการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อลดความเสี่ยงของการเกิดเหตุการณ์ที่จะก่อให้เกิดความเสียหาย ได้แก่

1. จัดทำแผนฉุกเฉินและแผนการกู้ระบบ (Contingency & Disaster Recovery Plan) โดยมีการกำหนดเหตุการณ์ต่าง ๆ อย่างครอบคลุมและวิธีการในการแก้ไขและฟื้นฟูระบบ
2. มีการสำรองข้อมูล ระบบปฏิบัติการ ข้อมูลสำคัญทางด้านซอฟต์แวร์ ของระบบเป็นประจำทุกวัน
3. จัดเก็บข้อมูลสำรองไว้ในพื้นที่ปฏิบัติการ (local storage) และสถานที่สำรอง (offsite storage)
4. มีการทดสอบการใช้ข้อมูลสำรองอย่างสม่ำเสมอเพื่อให้แน่ใจว่าข้อมูลดังกล่าว สามารถนำมาใช้ได้ ในกรณีที่มีปัญหา
5. มีการทบทวนแผนฉุกเฉินและแผนการกู้ระบบ อย่างสม่ำเสมอ

9.8 *การเลิกสัญญา (Term and Termination)*

การเลิกสัญญาให้เป็นไปตามความประสงค์ของคู่สัญญาระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ ผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์

9.9 *การแก้ไขปรับปรุงแนวนโยบาย (Amendments)*

การแก้ไขปรับปรุงแนวนโยบายนี้ เป็นสิทธิ์และหน้าที่ของ บริษัท ศูนย์ประมวลผล จำกัด โดยเมื่อมีการปรับปรุงแนวนโยบาย จะทำการเผยแพร่ขึ้นสู่เว็บไซต์ของผู้ให้บริการออกใบรับรอง ที่ www.itmx.co.th หรือเว็บไซต์อื่นใดที่ผู้ให้บริการได้ระบุไว้

9.10 *แนวปฏิบัติการระงับข้อพิพาท (Dispute Resolution Procedures)*

ในกรณีที่มีข้อพิพาทเกิดขึ้นระหว่างคู่สัญญา ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะตรวจสอบความผิดพลาดและพิจารณารายละเอียดของสัญญาที่เกี่ยวข้องซึ่งมีการตกลงกันระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์ ซึ่งหากไม่สามารถตกลงกันได้ ให้นำข้อโต้แย้งสู่การพิจารณาของศาล เพื่อตัดสินต่อไป

(Copyright © 2007 Thai Digital ID Company Limited)