Thai Digital ID CA

แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์

(Certification Practice Statement)

version 1.0

ประวัติการปรับปรุงเอกสาร

Doc. Version	Status	Date of Issue	Issued By …	Comments
1.0	Official	08-09-11	TDID PCA	

หมายเหตุ :

TDID PCA = TDID Policy Creation Authority

(Copyright © 2011 Thai Digital ID Co., Ltd.)

สารบัญ

ประวัติการปรับปรุงเอกสาร 2
1 บทนำ (Introduction) 7
1.1 ข้อมูลเบื้องต้นทั่วไป (Overview) 7
1.2 ชื่อเอกสาร (Document Name and Identification) 7
1.3 บุคคลที่เกี่ยวข้อง (PKI Participants) 7
1.3.1 ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority): TDID CA 7
1.3.2 หน่วยงานรับลงทะเบียน (Registration Authority): TDID RA 7
1.3.3 ผู้ใช้บริการ (Subscriber) 7
1.3.4 คู่กรณีที่เกี่ยวข้อง (Relying Party) 7
1.3.5 บุคคลอื่น ๆ ที่เกี่ยวของ (Other Participants) 8
1.4 การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage) 8
1.5 การบริหารจัดการเกี่ยวกับแนวนโยบายและแนวปฏิบัติ (Policy Administration) 9
1.6 คำนิยามและคำย่อ (Definitions and Acronyms) 10
2 ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities) 13
2.1 การเผยแพร่ข้อมูลเกี่ยวกับการให้บริการและการออกใบรับรองอิเล็กทรอนิกส์ของ TDID CA 13
2.2 ความสม่ำเสมอในการเผยแพร่ข้อมูล (Frequency of Publication) 13
2.3 การควบคุมการเข้าถึง (Access Controls) 13
3 การระบุและยืนยันตัวบุคคล (Identification and Authentication) 14
3.1 การกำหนดรูปแบบของชื่อ (Naming) 14
3.2 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอใช้บริการครั้งแรก (Initial Identity Validation) 14
3.3 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอออกกุญแจใหม่ (Identification and Authentication for Re-key Requests) 14
3.4 การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรอง (Identification and Authentication for Revocation Requests) 14
4 ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operational Requirements) 15
4.1 การยื่นขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application) 15
4.2 การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing) 17
4.3 การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance) 17
4.4 การยอมรับใบรับรองอิเล็กทรอนิกส์ (Certificate Acceptance) 17
4.5 การใช้กุญแจคู่ และใบรับรองอิเล็กทรอนิกส์ (Pair and Certificate Usage) 18
4.6 การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal) 18
4.7 การรับรองกุญแจคู่ใหม่ (Certificate Re-key) 18
4.8 การปรับแต่งใบรับรองอิเล็กทรอนิกส์ (Certificate Modification) 18

(Copyright © 2011 Thai Digital ID Co., Ltd.)

4.9 การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension) 18
4.9.1 เหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Circumstances for Revocation)..... 19
4.9.2 ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Revocation) 19
4.9.3 ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Procedure for Revocation Request) 19
4.9.4 ระยะเวลาที่ใช้ในการเพิกถอน (Revocation Request Grace Period)..... 20
4.9.5 เหตุการณ์ที่ต้องระงับการใช้งานใบรับรองอิเล็กทรอนิกส์ (Circumstances for Suspension) 20
4.9.6 ผู้ที่สามารถขอระงับใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Suspension)..... 20
4.9.7 ขั้นตอนการระงับใบรับรองอิเล็กทรอนิกส์ (Procedure for Suspension Request)..... 21
4.9.8 ขอบเขตของระยะเวลาในการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์..... 21
4.9.9 ความถี่ในการประกาศรายการเพิกถอนใบรับรอง (CRL Issuance Frequency)..... 21
4.9.10 ข้อปฏิบัติสำหรับการตรวจสอบรายการเพิกถอนใบรับรอง (CRL Checking Requirements) 21
4.9.11 การตรวจสอบสถานะของใบรับรองและการเพิกถอนใบรับรองแบบออนไลน์ (On-line Revocation/Status Checking Availability)..... 21
4.10 บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)..... 21
4.11 การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription) 21
4.12 การเก็บรักษาและการกู้คืนกุญแจ(Key Escrow and Recovery) 22
5 การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)..... 23
5.1 การควบคุมความมั่นคงปลอดภัยทางกายภาพ (Physical Security Controls)..... 23
5.1.1 สถานที่ตั้งและการก่อสร้างสถานที่ (Site Location and Construction)..... 23
5.1.2 การเข้าถึงทางกายภาพ (Physical Access) 23
5.1.3 การควบคุมความมั่นคงปลอดภัยด้านกายภาพ (Physical Security Controls) 23
– ระบบไฟฟ้าและระบบปรับอากาศ (Power and Air Conditioning) 24
– การป้องกันภัยจากน้ำ (Water Exposures)..... 24
– การป้องกันอัคคีภัย (Fire Prevention and Protection)..... 24
– การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage)..... 24
5.2 การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls) 24
5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles) 24
5.2.2 จำนวนบุคคลที่ต้องการต่องาน (Number of Persons Required Per Task) 26
5.2.3 การระบุและพิสูจน์ความมีตัวตนแท้จริงของเจ้าหน้าที่ปฏิบัติงาน (Identification and Authentication for each Role)..... 26
5.2.4 การรั่วไหลของข้อมูลสำคัญและความต่อเนื่องของการให้บริการ (Compromise and Disaster Recovery)..... 26
5.2.5 การเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียน (CA or RA Termination) 26
6 การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)..... 27
6.1 การสร้างและติดตั้งคู่คีย์ (Key Pair Generation and Installation)..... 27

(Copyright © 2011 Thai Digital ID Co., Ltd.)

6.1.1 การสร้างกุญแจคู่ (Key Pair Generation) 27
6.1.2 การส่งมอบกุญแจส่วนตัว (Private Key Delivery to Entity)..... 27
6.1.3 การส่งมอบกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปยังผู้ใช้บริการ (CA Public Key Delivery to Users)..... 27
6.1.4 ขนาดของกุญแจ (Key Sizes)..... 27
6.1.5 การสร้างตัวแปรกุญแจสาธารณะ (Public Key Parameters Generation) 27
6.1.6 การตรวจสอบคุณภาพของตัวแปร (Parameter Quality Checking) 27
6.1.7 การสร้างกุญแจคู่จากอุปกรณ์หรือซอฟต์แวร์ (Hardware/Software Key Generation) 28
6.1.8 จุดประสงค์ของการใช้กุญแจ (Key Usage Purposes)..... 28
6.2 การปกป้องกุญแจส่วนตัว (Private Key Protection) และการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls) 28
6.2.1 มาตรฐานของโมดูลที่ใช้ในการเข้ารหัสลับ (Standards for Cryptographic Module) 28
6.2.2 การควบคุมกุญแจส่วนตัวของผู้ให้บริการ (Private Key (n out of m) Multi-Person Control) .. 28
6.2.3 การฝากกุญแจส่วนตัว (Private Key Escrow) 28
6.2.4 การสำรองกุญแจส่วนตัว (Private Key Backup) 28
6.2.5 การบันทึกถาวรกุญแจส่วนตัว (Private Key Archival)..... 28
6.2.6 กุญแจส่วนตัวภายในโมดูลการเข้ารหัส (Private Key Entry into Cryptographic Module)..... 28
6.2.7 วิธีการนำกุญแจส่วนตัวมาใช้งาน (Method of Activating Private Key) 29
6.2.8 วิธีเลิกการใช้งานกุญแจส่วนตัว (Method of Deactivating Private Key)..... 29
6.2.9 การจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls) 29
6.2.10 การทำลายกุญแจส่วนตัว……28
6.3 รายละเอียดอื่นเกี่ยวกับการจัดการและบริหารกุญแจคู่ (Other Aspects of Key Pair Management) .. 29
6.3.1 การเก็บรักษากุญแจสาธารณะ (Public Key Archival)..... 29
6.3.2 ระยะเวลาใช้งานของกุญแจส่วนตัวและกุญแจสาธารณะ (Usage Periods for the Public and Private Keys) 29
6.4 ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data) 30
6.4.1 การสร้างข้อมูลและการนำข้อมูลไปใช้ในการติดตั้งใบรับรอง (Activation Data Generation and Installation) 30
6.4.2 การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรอง (Activation Data Protection) 30
6.5 การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)..... 30
6.5.1 ข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ที่มีลักษณะเฉพาะ (Specific Computer Security Technical Requirements)..... 30
6.5.2 การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating)..... 30
6.6 การควบคุมวงจรทางเทคนิคของระบบให้บริการ (Life Cycle Security Controls) 30
6.6.1 การควบคุมในการพัฒนาระบบ (System Development Controls)..... 30
6.6.2 การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัย (Security Management Controls).... 31

(Copyright © 2011 Thai Digital ID Co., Ltd.)

6.6.3 การแบ่งระดับความปลอดภัยของวงจรทางเทคนิคของระบบให้บริการ (Life Cycle Security Ratings) 31
6.7 การควบคุมความปลอดภัยทางเครือข่าย (Network Security Controls) 31
6.8 ข้อกำหนดสำหรับการประทับเวลาในการบันทึกต่าง ๆ (Time-Stamping) 30
7 การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ และรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles) 32
7.1 รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile) 32
7.1.1 รูปแบบ (Profile) 32
7.1.2 ข้อมูลเพิ่มเติมของใบรับรอง (Certificate Extension) 32
7.1.3 รูปแบบของชื่อ (Name Forms) 32
7.2 รูปแบบรายการเพิกถอนใบรับรอง (CRL Profile) 33
7.2.1 รูปแบบ (Profile) 33
8 การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่าง ๆ และการประเมินความเสี่ยงอื่น ๆ (Compliance Audit and Other Assessment) 34
9 ข้อกำหนดอื่น ๆ และประเด็นกฎหมาย (Other Business and Legal Matters) 35
9.1 ค่าธรรมเนียม (Fees) 35
9.2 การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information) 35
9.3 นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information) 35
9.4 ทรัพย์สินทางปัญญา (Intellectual Property Rights) 35
9.5 คำรับรอง (Representations and Warranties) 35
9.6 การบอกเลิกคำรับรอง (Disclaimers of Warranties) 35
9.7 การเลิกสัญญา (Term and Termination) 35
9.8 ข้อจำกัดความรับผิด (Limitations of Liability) 36
9.9 ค่าสินไหมทดแทน (Indemnities) 36

(Copyright © 2011 Thai Digital ID Co., Ltd.)

1 บทนำ (Introduction)

1.1 *ข้อมูลเบื้องต้นทั่วไป (Overview)*

เอกสารฉบับนี้เรียกว่า "แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certification Practice Statement)" ซึ่งจะเรียกว่า "CPS"(ซีพีเอส) โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ Thai Digital ID Certification Authority (TDID CA)

1.2 *ชื่อเอกสาร (Document Name and Identification)*

เอกสารฉบับนี้เรียกว่า "แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ (Certification Practice Statement)" หรือเรียกว่า "CPS" ของผู้ให้บริการ โดยมีวัตถุประสงค์ในการชี้แจงแก่บุคคลทุกฝ่ายที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ เพื่อให้ทราบและเข้าใจถึงข้อความที่ระบุในเอกสารที่ใช้เป็นแนวทางในการดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ ในกรณีที่มีข้อความขัดแย้งกันระหว่าง CP กับ CPS และข้อความนั้นไม่ได้ถูกระบุเฉพาะเจาะจงสำหรับ CP ให้ถือข้อความใน CPS เป็นสำคัญ

1.3 *บุคคลที่เกี่ยวข้อง (PKI Participants)*

1.3.1 ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority): TDID CA

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

1.3.2 หน่วยงานรับลงทะเบียน (Registration Authority): TDID RA

คือ ผู้ซึ่งทำหน้าที่รับลงทะเบียน เมื่อมีการยื่นคำ ขอใช้บริการ คำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ ของข้อมูลที่ผู้ใช้บริการให้ไว้ตามแบบคำขอที่ผู้ให้บริการกำหนดขึ้น

1.3.3 ผู้ใช้บริการ (Subscriber)

คือ บุคคล นิติบุคคล หรือ เอนทิตี้ใด ๆ ที่ได้รับใบรับรองอิเล็กทรอนิกส์ จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (TDID CA)

1.3.4 คู่กรณีที่เกี่ยวข้อง (Relying Party)

คือ บุคคล นิติบุคคล หรือ เอนทิตี้อื่นใดที่เชื่อถือลายมือชื่อดิจิทัล อันเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง หรือ เชื่อถือใบรับรองอิเล็กทรอนิกส์ ดังนั้น คู่กรณีที่เกี่ยวข้องอาจเป็น

(Copyright © 2011 Thai Digital ID Co., Ltd.)

ผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือ อาจไม่ใช่ผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ก็ได้ แต่เป็นผู้ซึ่งกระทำการหรืองดเว้นกระทำการใด ๆ เพราะเชื่อถือลายมือชื่อดิจิทัลหรือใบรับรองอิเล็กทรอนิกส์ โดยการใช้กุญแจสาธารณะที่อยู่ในใบรับรองอิเล็กทรอนิกส์นั้นในการตรวจสอบตัวตนที่แท้จริงของผู้ขอใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัลและมีชื่อปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์

1.3.5 บุคคลอื่น ๆ ที่เกี่ยวของ (Other Participants)

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

1.4 *การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)*

ชนิดของใบรับรองอิเล็กทรอนิกส์ที่ออกโดย TDID CA ประกอบด้วย ใบรับรองอิเล็กทรอนิกส์ 3 ชนิด คือ

1. **Personal Certificate** คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้บุคคลหรือ ประชาชนทั่วไป เพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองประเภทนี้มีอายุการใช้งานทั้งแบบ 2 ปี และ 3 ปี
2. **Enterprise Certificate** คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกให้กับนิติบุคคล ซึ่งอาจเป็นหน่วยงาน หรือ องค์กร ภาครัฐ และเอกชน ที่มีความต้องการใช้งานใบรับรองฯเพื่อรักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ โดยใบรับรองประเภทนี้มีอายุการใช้งานทั้งแบบ 2 ปี และ 3 ปี
3. **Web Server Certificate (SSL Certificate)** คือ ใบรับรองอิเล็กทรอนิกส์ที่ออกสำหรับใช้ยืนยันตัวตนของ Web Server โดยใบรับรองประเภทนี้มีอายุการใช้งานทั้งแบบ 1 ปี และ 2 ปี

(Copyright © 2011 Thai Digital ID Co., Ltd.)

1.5 *การบริหารจัดการเกี่ยวกับแนวนโยบายและแนวปฏิบัติ (Policy Administration)*

รายละเอียดที่อยู่ของหน่วยงาน TDID CA ที่ทำหน้าที่ในการดูแลและปรับปรุงเอกสารแนวนโยบายและแนวปฏิบัตินี้

Name:	Thai Digital ID CA
ACN:	3030196149
Trading as:	TDID CA
OID:	1.3.6.1.4.1.28113.2.2.1
Postal Address:	4th Floor, Room 2, Kasikorn Bank Building, 142 Silom Road, Bangrak, Bangkok, Thailand 10500
Phone:	+66-2237-6363
Fax:	+66-2237-6364
Domain Name:	www.thaidigitalid.com
Email Address:	support@thaidigitalid.com
Contact:	Thai Digital ID Co., Ltd. 4th Floor, Room 2, Kasikorn Bank Building, 142 Silom Road, Bangrak, Bangkok, Thailand 10500 Tel +66-2237-6363

(Copyright © 2011 Thai Digital ID Co., Ltd.)

1.6 *คำนิยามและคำย่อ (Definitions and Acronyms)*

คำศัพท์	**ความหมาย**
ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ / ผู้ให้บริการ (Certification Authority : TDID CA)	บริษัท ไทยดิจิทัล ไอดี จำกัด ภายใต้ TDID CA Service ทำหน้าที่ให้บริการเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ รวมทั้งเผยแพร่สถานะของใบรับรองอิเล็กทรอนิกส์ที่มีการเพิกถอนในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
หน่วยงานรับลงทะเบียน (Registration Authority : TDID RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ คำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยทำการตรวจสอบและยืนยันความถูกต้องสมบูรณ์ของข้อมูลที่ผู้ใช้บริการให้ไว้
ใบรับรอง / ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)	เอกสารอิเล็กทรอนิกส์ที่เป็นองค์ประกอบส่วนหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะของผู้ใช้บริการ ซึ่งอาจหมายถึงบุคคลธรรมดา นิติบุคคลเครื่องมือ หรือ อุปกรณ์ ซึ่งเอกสารอิเล็กทรอนิกส์ดังกล่าวสอดคล้องตามมาตรฐาน X.509 Version 3 Certificate โดยมีรายการอย่างน้อย ดังนี้ – เวอร์ชั่นของใบรับรอง – หมายเลขของใบรับรอง – วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลของผู้ถือใบรับรอง – ชื่อของผู้ให้บริการ – วัน เวลาที่เริ่มต้นและสิ้นสุดของการใช้ใบรับรอง – ชื่อของผู้ถือใบรับรอง – กุญแจสาธารณะของผู้ถือใบรับรองและวิธีการที่ใช้ในการสร้าง
ผู้ใช้บริการ (Subscriber)	บุคคลหรือนิติบุคคลที่ยื่นคำขอใช้บริการใบรับรองแก่ผู้ให้บริการ เมื่อมีการออกใบรับรองจะมีการระบุชื่อนิติบุคคลของผู้ใช้บริการไว้ในใบรับรอง
กุญแจ (Key)	สัญลักษณ์หรือลำดับของสัญลักษณ์ หรือสัญญาณไฟฟ้าที่เกี่ยวเนื่องกับสัญลักษณ์ที่นำมาเข้ารหัสข้อมูลหรือถอดรหัสข้อมูล
กุญแจส่วนตัว (Private Key)	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ และกุญแจส่วนตัวนี้จะนำไปใช้สร้าง ลายมือชื่อดิจิทัล

(Copyright © 2011 Thai Digital ID Co., Ltd.)

กุญแจสาธารณะ (Public Key)	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น
กุญแจคู่ (Key Pair)	กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะ โดยที่สามารถใช้กุญแจสาธารณะตรวจสอบว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้
ลายมือชื่อดิจิทัล (Digital Signature)	ลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่งที่สร้างขึ้นโดยการนำข้อมูลอิเล็กทรอนิกส์มาแปลงเป็นตัวเลขและใช้กับระบบกุญแจคู่ โดยนำไปคำนวณร่วมกับกุญแจส่วนตัวของเจ้าของลายมือชื่อ โดยที่สามารถใช้กุญแจสาธารณะของเจ้าของลายมือชื่อมาตรวจสอบได้ว่าเป็นลายมือชื่อดิจิทัลที่ได้สร้างขึ้นโดยกุญแจส่วนตัวของเจ้าของลายมือชื่อดิจิทัลนั้นหรือไม่ และข้อมูลอิเล็กทรอนิกส์ที่ได้มีการลงลายมือชื่อดิจิทัลนั้นได้มีการแก้ไขเปลี่ยนแปลงภายหลังการลงลายมือชื่อหรือไม่
การเพิกถอนใบรับรอง (Certificate Revocation)	การทำให้ใบรับรองไม่สามารถใช้ได้อีกต่อไปหลังจากการเพิกถอนใบรับรองซึ่งส่งผลให้กุญแจส่วนตัวของผู้ใช้บริการนั้นไม่สามารถใช้ในการสร้างลายมือชื่อดิจิทัลหรือถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ได้ ทั้งนี้ไม่มีผลกระทบกับใบรับรองหรือกุญแจสาธารณะ ซึ่งยังคงสามารถใช้ในการตรวจสอบลายมือชื่อดิจิทัลที่สร้างขึ้นก่อนการเพิกถอนใบรับรองได้
รายการเพิกถอนใบรับรอง (Certificate Revocation List : CRL)	รายการใบรับรองที่ถูกเพิกถอนการใช้งาน
คู่กรณีที่เกี่ยวข้อง (Relying Party)	ผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองหรือลายมือชื่อดิจิทัล โดยการนำกุญแจสาธารณะที่อยู่ในใบรับรองไปใช้ในการตรวจสอบตัวตนของผู้ใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัล และมีชื่อปรากฏอยู่ในใบรับรอง

(Copyright © 2011 Thai Digital ID Co., Ltd.)

ไดเรกทอรี (Directory)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดการ เพื่อให้สามารถสืบค้นข้อมูลได้อย่างรวดเร็วและเป็นตามมาตรฐานไดเรกทอรี (X.500 หรือ LDAP)
ฐานข้อมูล (Database)	ที่เก็บรวบรวมข้อมูล โดยข้อมูลที่เก็บนั้นได้มีการจัดเก็บแบบที่เอื้อให้โปรแกรมคอมพิวเตอร์สามารถเข้าถึง จัดการและปรับเปลี่ยนข้อมูลได้ง่ายและรวดเร็ว

(Copyright © 2011 Thai Digital ID Co., Ltd.)

2 ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

2.1 *การเผยแพร่ข้อมูลเกี่ยวกับการให้บริการและการออกใบรับรองอิเล็กทรอนิกส์ของ TDID CA*

แนวปฏิบัติใบรับรองอิเล็กทรอนิกส์นี้ได้รับการตีพิมพ์ทางอิเล็กทรอนิกส์ในรูปแบบของ PDF บนเว็บไซต์ของผู้ให้บริการ

www.thaidigitalid.com

2.2 *ความสม่ำเสมอในการเผยแพร่ข้อมูล (Frequency of Publication)*

ผู้ให้บริการจะปรับปรุงนโยบายใบรับรองอิเล็กทรอนิกส์ (CP) และคำชี้แจงทางปฏิบัติ (CPS) ให้ทันสมัยอยู่เสมอ โดยจะประกาศทางเว็บไซต์ของผู้ให้บริการ (http://www.thaidigitalid.com) เพื่อใช้สำหรับการอ้างอิงแก่ผู้ใช้บริการ และบุคคลทั่วไป

2.3 *การควบคุมการเข้าถึง (Access Controls)*

CP และ CPS สามารถดาวน์โหลดผ่านทางเว็บไซต์ www.thaidigitalid.com ได้

(Copyright © 2011 Thai Digital ID Co., Ltd.)

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)*

การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเพื่อออกใบรับรองนั้น เป็นหน้าที่ของหน่วยงานรับลงทะเบียนโดยผู้ใช้บริการต้องกรอกแบบคำขอใช้บริการใบรับรองอิเล็กทรอนิกส์ เพื่อขอใช้ใบรับรองพร้อมทั้งแนบหลักฐานที่ใช้ในการสมัครขอใช้บริการ ให้แก่หน่วยงานรับลงทะเบียน TDID RA โดยรายละเอียดอยู่ในหัวข้อ 4.1

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

ผู้ใช้บริการต้องกรอกแบบคำขอสมัครใช้ใบรับรองอิเล็กทรอนิกส์ใหม่ และส่งหลักฐานให้กับหน่วยงานรับลงทะเบียน TDID RA โดยรายละเอียดอยู่ในหัวข้อ 4.1 และ 4.3

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

ผู้ใช้บริการที่ต้องการเพิกถอนใบรับรอง ต้องแจ้งต่อผู้ให้บริการโดยตรง เมื่อผู้ให้บริการได้รับแจ้งความต้องการเพิกถอนใบรับรองและตรวจสอบตามขั้นตอนแล้ว จะดำเนินการเพิกถอนใบรับรองตามที่แจ้งไว้และประกาศในรายการเพิกถอนใบรับรอง โดยรายละเอียดอยู่ในหัวข้อ 4.9

(Copyright © 2011 Thai Digital ID Co., Ltd.)

4 ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operational Requirements)

4.1 *การยื่นขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application)*

ผู้สมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ควรปฏิบัติตามขั้นตอนต่อไปนี้

1. บุคคลที่สมัครขอใบรับรองอิเล็กทรอนิกส์สามารถเป็นได้ทั้งบุคคลที่ขอใบรับรองอิเล็กทรอนิกส์ในนามบุคคล และบุคคลที่ได้รับมอบหมายจากองค์กรให้ดำเนินการสมัครขอใบรับรองอิเล็กทรอนิกส์ในนามองค์กร เพื่อใช้รักษาความมั่นคงปลอดภัยให้กับธุรกรรมอิเล็กทรอนิกส์ประเภทต่าง ๆ ที่กำหนดไว้ในหัวข้อ 1.4
2. กระบวนการยื่นคำขอใบรับรองอิเล็กทรอนิกส์

ผู้สมัครขอใช้ใบรับรองอิเล็กทรอนิกส์ควรปฏิบัติตามขั้นตอนต่อไปนี้

กรณีการขอใบรับรองประเภท Personal Certificate

1) กรอกใบสมัครขอใช้ใบรับรอง โดยใส่ข้อมูลให้ครบถ้วน
2) จัดเตรียมหลักฐานที่ใช้ในการประกอบการสมัครขอใช้ใบรับรองดังนี้
   - ระเบียบและเงื่อนไขในการใช้ใบรับรอง
   - **สำเนาบัตรประชาชนของผู้ขอใช้บริการ** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง(Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
   - **สำเนาทะเบียนบ้านของผู้ขอใช้บริการ** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาใบอนุญาตทำงาน (Work Permit) แสดงสถานที่พำนักในประเทศไทย พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
3) ส่งใบสมัคร พร้อมหลักฐานประกอบการสมัคร มาที่หน่วยงานรับลงทะเบียน

กรณีการขอใบรับรองประเภท Enterprise Certificate

1) กรอกใบสมัครขอใช้ใบรับรอง โดยใส่ข้อมูลให้ครบถ้วน
2) จัดเตรียมหลักฐานที่ใช้ในการประกอบการสมัครขอใช้ใบรับรองดังนี้
   - ระเบียบและเงื่อนไขในการใช้ใบรับรอง
   - **สำเนาหนังสือรับรองการเป็นนิติบุคล** ที่มีอายุไม่เกิน 90 วัน(3 เดือน) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยกรรมการ ผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท(ถ้ามี)
   - **สำเนาทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.20)** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยกรรมการผู้มีอำนาจ
   - **สำเนาบัตรประชาชนของกรรมการผู้มีอำนาจ** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

(Copyright © 2011 Thai Digital ID Co., Ltd.)

กรณีกรรมการผู้มีอำนาจมอบอำนาจให้ผู้อื่นดำเนินการแทน ให้เพิ่ม

- **หนังสือมอบอำนาจ** ปิดอากรแสตมป์ 30 บาท
- **สำเนาบัตรประชาชนของผู้รับมอบอำนาจ**พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

3) ส่งใบสมัคร พร้อมหลักฐานประกอบการสมัคร มาที่หน่วยงานรับลงทะเบียน

กรณีการขอใบรับรองประเภท SSL Certificate ในนามบุคคล

1) กรอกใบสมัครขอใช้ใบรับรอง โดยใส่ข้อมูลให้ครบถ้วน
2) จัดเตรียมหลักฐานที่ใช้ในการประกอบการสมัครขอใช้ใบรับรองดังนี้
   - ระเบียบและเงื่อนไขในการใช้ใบรับรอง
   - **สำเนาบัตรประชาชนของผู้ขอใช้บริการ** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง(Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
   - **สำเนาทะเบียนบ้านของผู้ขอใช้บริการ** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาใบอนุญาตทำงาน(Work Permit)แสดงสถานที่พำนักในประเทศไทย พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
   - **สำเนาหนังสือรับรองการจดทะเบียน** Domain Name พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยผู้ขอใช้บริการ
3) จัดเตรียม CSR file ตามมาตรฐานที่ผู้ให้บริการกำหนด
4) ส่งใบสมัคร หลักฐานประกอบการสมัคร พร้อม CSR file มาที่หน่วยงานรับลงทะเบียน

กรณีการขอใบรับรองประเภท SSL Certificate ในนามนิติบุคคล

1) กรอกใบสมัครขอใช้ใบรับรอง โดยใส่ข้อมูลให้ครบถ้วน
2) จัดเตรียมหลักฐานที่ใช้ในการประกอบการสมัครขอใช้ใบรับรองดังนี้
   - ระเบียบและเงื่อนไขในการใช้ใบรับรอง
   - **สำเนาหนังสือรับรองการเป็นนิติบุคล** ที่มีอายุไม่เกิน 90 วัน(3 เดือน) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยกรรมการ ผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท(ถ้ามี)
   - **สำเนาทะเบียนภาษีมูลค่าเพิ่ม** (ภ.พ.20) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยกรรมการผู้มีอำนาจ
   - **สำเนาหนังสือรับรองการจดทะเบียน** Domain Name พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง โดยกรรมการผู้มีอำนาจ
   - **สำเนาบัตรประชาชนของกรรมการผู้มีอำนาจ** พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง(Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

กรณีกรรมการผู้มีอำนาจมอบอำนาจให้ผู้อื่นดำเนินการแทน ให้เพิ่ม

(Copyright © 2011 Thai Digital ID Co., Ltd.)

- **หนังสือมอบอำนาจ** ปิดอากรแสตมป์ 30 บาท
- **สำเนาบัตรประชาชนของผู้รับมอบอำนาจ**พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

3) จัดเตรียม CSR file ตามมาตรฐานที่ผู้ให้บริการกำหนด
4) ส่งใบสมัคร หลักฐานประกอบการสมัคร พร้อม CSR file มาที่หน่วยงานรับลงทะเบียน

4.2 *การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)*

หน่วยงานรับลงทะเบียนจะพิจารณาคำขอใบรับรอง โดยดูจากใบสมัครคำร้องขอใช้ใบรับรอง และหลักฐานต่างๆที่ใช้ประกอบการพิจารณาขอใช้ใบรับรอง ต้องมีความครบถ้วนและถูกต้องตามความเป็นจริง จึงจะดำเนินการออกใบรับรองให้กับผู้สมัคร โดยหากส่วนหนึ่งส่วนใดหรือทั้งหมดของใบสมัคร และ/หรือหลักฐานประกอบการขอใบรับรองไม่ครบถ้วน ไม่ถูกต้อง ก็จะส่งเอกสารคืนให้แก่ผู้สมัคร พร้อมทั้งแจ้งถึงความไม่ถูกต้องดังกล่าว

สำหรับระยะเวลาที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และเจ้าหน้าที่หน่วยงานรับลงทะเบียน ใช้ในการพิจารณาความถูกต้องของการยื่นคำขอใบรับรองอิเล็กทรอนิกส์ ใช้เวลาอย่างน้อย 1 วันทำการ (จันทร์-ศุกร์)

4.3 *การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)*

ขั้นตอนในการออกใบรับรอง มีดังต่อไปนี้

1. เจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบเอกสารหลักฐาน และ CSR file(ถ้ามี) ที่ได้รับจากผู้สมัครขอใช้ใบรับรอง ต้องมีความถูกต้องตรงกัน หากพบว่าข้อมูลไม่ตรงกันให้แจ้งผู้สมัครขอใช้ใบรับรอง
2. เมื่อตรวจสอบพบข้อมูลถูกต้องแล้ว เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะทำการบันทึกข้อมูลตามใบคำขอจากผู้สมัครขอใช้ใบรับรอง และออกใบรับรอง
3. เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะทำการตรวจสอบความถูกต้องของข้อมูลและใบรับรอง
4. เจ้าหน้าที่หน่วยงานรับลงทะเบียนส่งใบรับรองอิเล็กทรอนิกส์ซึ่งถูกบรรจุอยู่ภายใน Smartcard หรือ USB Token ถึงผู้สมัครขอใช้ใบรับรองผ่านทางไปรษณีย์ สำหรับกรณีที่เป็นใบรับรองประเภท Personal/Enterprise Certificate ส่วนใบรับรองประเภท SSL Certificate จะส่งผ่านทางจดหมายอิเล็กทรอนิกส์ (e-Mail)

4.4 *การยอมรับใบรับรองอิเล็กทรอนิกส์ (Certificate Acceptance)*

1. ข้อปฏิบัติของผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ที่ถือเป็นการยอมรับใบรองอิเล็กทรอนิกส์ โดยที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ จะถือว่าผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ยอมรับใบรับรองอิเล็กทรอนิกส์ที่ออกให้แล้ว
   - หากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มิได้รับการแจ้งการใดๆ จากผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ภายในเวลา 3 วันทำการ นับจากที่ได้มีการส่งใบรับรองอิเล็กทรอนิกส์ไปให้ผู้ใช้บริการ

(Copyright © 2011 Thai Digital ID Co., Ltd.)

2. ใบรับรองอิเล็กทรอนิกส์ที่ได้ยอมรับโดยผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ จะถูกเผยแพร่ผ่านทาง X.500 Directory ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

4.5 *การใช้กุญแจคู่ และใบรับรองอิเล็กทรอนิกส์ (Key Pair and Certificate Usage)*

1. ใบรับรองที่ TDID CA ออกให้แก่ผู้ใช้บริการนั้นได้มีการจำกัดการใช้งานเพื่อสนับสนุนการใช้ลายมือชื่อดิจิทัล (Digital Signature) และการเข้ารหัสลับข้อมูล (Data Encryption) สำหรับโปรแกรมประยุกต์ต่างๆเท่านั้น และผู้ใช้บริการไม่สามารถใช้งานกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ได้หลังจากใบรับรองอิเล็กทรอนิกส์ดังกล่าวหมดอายุลงหรือถูกเพิกถอน
2. ความรับผิดชอบของคู่กรณีที่เกี่ยวข้องในการใช้กุญแจสาธารณะหรือใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ ให้เป็นไปตามเงื่อนไขการใช้ใบรับรองอิเล็กทรอนิกส์แต่ละประเภทที่กำหนดโดยบริษัท ไทยดิจิทัล ไอดี จำกัด อย่างไรก็ตาม คู่กรณีที่เกี่ยวข้องต้องใช้ใบรับรองอิเล็กทรอนิกส์ตามแนวนโยบายและแนวปฏิบัติ และ ต้องตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ตามที่กำหนดในแนวนโยบายและแนวปฏิบัติ

4.6 *การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal)*

ในปัจจุบัน TDID CA ไม่มีนโยบายสำหรับการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการ โดยไม่มีการเปลี่ยนแปลงกุญแจสาธารณะของผู้ใช้บริการ หรือข้อมูลอื่นใดที่ปรากฏในใบรับรองอิเล็กทรอนิกส์

4.7 *การรับรองกุญแจคู่ใหม่ (Certificate Re-key)*

การรับรองกุญแจคู่ใหม่จะมีกระบวนการเช่นเดียวกันกับข้อ 4.1, 4.2 และ 4.3 โดยทุกๆสิ้นเดือนเจ้าหน้าที่ของหน่วยงานรับลงทะเบียนจะทำการรวบรวมข้อมูลของใบรับรองอิเล็กทรอนิกส์ที่จะหมดอายุในอีก 2 เดือนข้างหน้า เพื่อแจ้งผู้ใช้บริการให้ทราบล่วงหน้า 2 เดือน ถึงใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการที่กำลังจะหมดอายุลง โดยทางเจ้าหน้าที่ของหน่วยงานรับลงทะเบียนจะกระทำโดยแจ้งผ่านจดหมายอิเล็กทรอนิกส์

4.8 *การปรับแต่งใบรับรองอิเล็กทรอนิกส์ (Certificate Modification)*

ในกรณีที่ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ต้องการปรับเปลี่ยนแก้ไขข้อมูลของใบรับรองอิเล็กทรอนิกส์ที่ได้ออกไปแล้วนั้น จะต้องยื่นเอกสารประกอบเพื่อขอยกเลิกใบรับรอง เดิม พร้อมทั้งเอกสารเพื่อขอสมัครใหม่เท่านั้น

4.9 *การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension)*

สำหรับบริการการเพิกถอนและพักใช้ใบรับรองนั้น TDID CA จะดำเนินการเมื่อได้รับคำขอเพิกถอนหรือพักใช้ใบรับรองจากผู้ใช้บริการ หรือได้รับคำสั่งโดยชอบด้วยกฎหมายให้ดำเนินการดังกล่าว

(Copyright © 2011 Thai Digital ID Co., Ltd.)

4.9.1 เหตุการณ์ที่ต้องเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Circumstances for Revocation)

การเพิกถอนใบรับรองอิเล็กทรอนิกส์คือการที่ไม่มีใครสามารถนำใบรับรองมาใช้ได้อีกต่อไป โดยผู้ให้บริการหรือผู้ขอใช้ใบรับรองจะสามารถเพิกถอนใบรับรองได้ในกรณีดังต่อไปนี้

- มีผู้อื่นล่วงรู้กุญแจส่วนตัวหรือมีผู้อื่นสามารถเข้าถึงหรือนำกุญแจส่วนตัวของผู้ขอใช้ใบรับรองไปใช้งาน
- มีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้กุญแจส่วนตัวของผู้ขอใช้ใบรับรอง
- อุปกรณ์ที่ใช้ในการเก็บกุญแจส่วนตัวสูญหายหรือไม่สามารถใช้งานได้
- องค์กรผู้ขอใช้ใบรับรองได้เลิกกิจการ
- ผู้ใช้บริการต้องการเปลี่ยนแปลงข้อมูลที่อยู่ในใบรับรอง เชน ชื่อ-นามสกุล เป็นต้น
- ผู้ใช้บริการไม่ปฏิบัติตามข้อกำหนดและเงื่อนไขในคำชี้แจงทางปฏิบัติของ TDID CA หรือข้อตกลงการใช้บริการ
- มีคำสั่งของศาลหรือต้องดำเนินการตามกฎหมาย
- มีผู้อื่นที่ล่วงรู้กุญแจส่วนตัวของ TDID CA
- TDID CA ระงับหรือยกเลิกการให้บริการ
- กรณีอื่นๆ ที่ TDID CA พิจารณาแล้วว่าจะมีผลกระทบต่อความมั่นคงปลอดภัยของการให้บริการออกใบรับรอง

4.9.2 ผู้ที่สามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Revocation)

- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียน
- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์

4.9.3 ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Procedure for Revocation Request)

1. กรอกแบบคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ พร้อมทั้งลงลายมือชื่อกำกับ
2. ส่งแบบคำขอเพิกถอนใบรับรองและหลักฐานประกอบให้เจ้าหน้าที่หน่วยงานรับลงทะเบียนโดยหลักฐานมีดังต่อไปนี้ คือ
   - กรณีสมัครมาในนามบุคคล ให้ใช้สำเนาบัตรประชาชนของผู้ขอใช้บริการ พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง(Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง
   - กรณีสมัครมาในนามนิติบุคคล ให้ใช้สำเนาหนังสือรับรองการเป็นนิติบุคล ที่มีอายุไม่เกิน 90 วัน(3 เดือน) พร้อมลงลายมือชื่อรับรองสำเนา

(Copyright © 2011 Thai Digital ID Co., Ltd.)

ถูกต้อง โดยกรรมการ ผู้มีอำนาจตามหนังสือรับรอง พร้อมประทับตราบริษัท(ถ้ามี)

3. เจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบแบบคำขอเพิกถอนใบรับรองและหลักฐาน
4. หลังจากเจ้าหน้าที่หน่วยงานรับลงทะเบียนตรวจสอบแบบคำขอเพิกถอนใบรับรองและหลักฐานเรียบร้อย เจ้าหน้าที่หน่วยงานรับลงทะเบียนจึงจะทำการเพิกถอนใบรับรอง

ข้อสังเกตุ

การเพิกถอนใบรับรองอิเล็กทรอนิกส์ ไม่ได้เป็นการลบใบรับรองอิเล็กทรอนิกส์ออกไปจากฐานข้อมูล

4.9.4 ระยะเวลาที่ใช้ในการเพิกถอน (Revocation Request Grace Period)

หลังจากเจ้าหน้าที่หน่วยงานรับลงทะเบียนได้รับคำขอเพิกถอนใบรับรอง และได้ทำการตรวจสอบความถูกต้องแล้ว เจ้าหน้าที่หน่วยงานรับลงทะเบียนจะทำการเพิกถอนใบรับรองภายใน 1 วันทำการ

4.9.5 เหตุการณ์ที่ต้องระงับการใช้งานใบรับรองอิเล็กทรอนิกส์ (Circumstances for Suspension)

การระงับใบรับรองอิเล็กทรอนิกส์คือการทำให้ไม่สามารถนำใบรับรองมาใช้ได้ชั่วคราว โดยผู้ให้บริการหรือผู้ขอใช้ใบรับรองจะสามารถระงับใบรับรองได้ในกรณีดังต่อไปนี้

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

4.9.6 ผู้ที่สามารถขอระงับใบรับรองอิเล็กทรอนิกส์ได้ (Who Can Request Suspension)

- ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
- หน่วยงานรับลงทะเบียน
- ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์

(Copyright © 2011 Thai Digital ID Co., Ltd.)

4.9.7 ขั้นตอนการระงับใบรับรองอิเล็กทรอนิกส์ (Procedure for Suspension Request)

1. ผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์โทรศัพท์แจ้งระงับการใช้งานใบรับรองอิเล็กทรอนิกส์ชั่วคราว (Suspension) ต่อหน่วยงานรับลงทะเบียน
2. เจ้าหน้าที่หน่วยงานรับลงทะเบียนสอบถามข้อมูลส่วนตัวของผู้แจ้งเพื่อยืนยันตัวบุคคล
3. เจ้าหน้าที่หน่วยงานรับลงทะเบียนทำการระงับการใช้ใบรับรองอิเล็กทรอนิกส์เป็นการชั่วคราว

4.9.8 ขอบเขตของระยะเวลาในการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์

ใบรับรองอิเล็กทรอนิกส์ที่ถูกระงับการใช้งานสามารถนำกลับมาใช้งานต่อได้ ก็ต่อเมื่อหน่วยงานรับลงทะเบียนได้รับคำร้องขอให้ยกเลิกการระงับการใช้งานใบรับรองอิเล็กทรอนิกส์จากผู้ใช้บริการเป็นลายลักษณ์อักษรเท่านั้น

4.9.9 ความถี่ในการประกาศรายการเพิกถอนใบรับรอง (CRL Issuance Frequency)

TDID CA จะทำการประกาศรายการเพิกถอนใบรับรองทุกๆ 2 ชั่วโมง

4.9.10 ข้อปฏิบัติสำหรับการตรวจสอบรายการเพิกถอนใบรับรอง (CRL Checking Requirements)

คู่กรณีที่เกี่ยวข้อง จะต้องทำการตรวจสอบรายการเพิกถอนใบรับรองก่อนที่จะมีการใช้งานที่เกี่ยวกับใบรับรองนั้น

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

การตรวจสอบสถานะของใบรับรองและการเพิกถอนใบรับรองนั้นสามารถดำเนินการแบบออนไลน์ได้ผ่านทางเว็บไซต์ของ TDID CA

4.10 *บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)*

ผู้ใช้บริการ และ/หรือคู่กรณีที่เกี่ยวข้องสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้ทางเว็บไซต์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือสามารถโทรมาสอบถามได้ที่หน่วยงานรับลงทะเบียน

4.11 *การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription)*

ผู้ใช้บริการสามารถเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ได้ โดยดำเนินการตามข้อ 4.9.3 ขั้นตอนการเพิกถอนใบรับรองอิเล็กทรอนิกส์

(Copyright © 2011 Thai Digital ID Co., Ltd.)

4.12 *การเก็บรักษาและการกู้คืนกุญแจ(Key Escrow and Recovery)*

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ของบริษัท ไทยดิจิทัล ไอดี จำกัด ไม่มีนโยบายการเก็บรักษากุญแจส่วนตัวของผู้ใช้บริการ ดังนั้นผู้ใช้บริการมีหน้าที่ในการจัดเก็บรักษากุญแจส่วนตัว ให้มีความปลอดภัย และ กุญแจส่วนตัวที่ออกให้โดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์นั้น จะต้องนำมาใช้งานให้เหมาะสมกับประเภทของใบรับรองที่ออกให้เท่านั้น

(Copyright © 2011 Thai Digital ID Co., Ltd.)

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 ห้อง 2 อาคารธนาคารกสิกรไทย ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพฯ 10500 ซึ่งมีการปฏิบัติงานในสิ่งแวดล้อมที่มีความปลอดภัยตามมาตรฐาน ISO27001 เพื่อประโยชน์ในการรักษาความปลอดภัยทางด้านกายภาพของระบบให้บริการออกใบรับรอง TDID CA จึงได้ติดตั้งอุปกรณ์รักษาความปลอดภัย ณ สถานที่ตั้งของระบบใหบริการ ดังนี้

1) โทรทัศน์วงจรปิด เพื่อประโยชน์ในการบันทึกภาพเหตุการณ์ภายในสถานที่ตั้ง

2) Door Hold Open Sounder ซึ่งจะส่งเสียงร้องเตือนเมื่อมีการเปิดประตูทิ้งค้างไว้เพื่อความปลอดภัยของสถานที่ตั้ง

4) ระบบ Smoke Detector เพื่อตรวจจับควันไฟ

5) อุปกรณดับเพลิงแบบ FM-200 ซึ่งมี (ก๊าซ) สารดับเพลิงที่ไม่ก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์

6) เสริมเหล็กทุกด้านของห้องที่ให้บริการระบบ TDID CA เพื่อป้องกันการทุบ, ขุด หรือเจาะผนัง, เพดาน, หรือพื้น

5.1.2 การเข้าถึงทางกายภาพ (Physical Access)

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

5.1.3 การควบคุมความมั่นคงปลอดภัยด้านกายภาพ (Physical Security Controls)

- สถานที่ตั้งของผู้ให้บริการมีการควบคุมการเข้าถึงและการจัดแบ่งพื้นที่ตามระดับความปลอดภัย และอนุญาตให้สามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่มีสิทธิ์ หรือ ผู้มาเยือนภายใต้การดูแลจากเจ้าหน้าที่ที่มีสิทธ์เท่านั้น

(Copyright © 2011 Thai Digital ID Co., Ltd.)

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

ระบบบริการทั้งหมดจะใช้ระบบไฟฟ้าจากแหล่งจ่ายไฟฟ้าแบบมาตรฐาน พร้อมทั้งยังมีเครื่องกำเนิดไฟฟ้าแบบส่วนตัวและเครื่องกำเนิดไฟฟ้าแบบต่อเนื่อง (UPS) เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง ในระบบบริการจะมีระบบปรับอากาศเพื่อควบคุมอุณหภูมิและความชื้นให้คงที่ โดยระบบปรับอากาศในส่วนนี้ จะเป็นอิสระจากระบบปรับอากาศของอาคารที่ตั้ง

– **การป้องกันภัยจากน้ำ (Water Exposures)**

ในส่วนพื้นที่ของการปฏิบัติงานได้มีการป้องกันภัยจากน้ำโดยจัดให้พื้นที่บริการอยู่สูงกว่าระดับน้ำและอาคารที่ตั้งไม่ใช่บริเวณที่เกิดน้ำท่วม และตัวอาคารยังได้ออกแบบให้อยู่สูงกว่าบริเวณโดยรอบอีก 6 นิ้ว

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

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

– **การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage)**

สื่อที่ใช้สำรองข้อมูลทุกประเภทจะถูกเก็บรักษาไว้ในห้องที่มีความปลอดภัย ในหลายๆ สถานที่

5.2 *การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls)*

5.2.1 บทบาทหน้าที่ที่ไว้วางใจ (Trusted Roles)

จากการที่มีการใช้ระบบควบคุมการเข้าถึงและการบริหารจัดการกุญแจ ทำให้บุคคลเพียงคนเดียวไม่สามารถเข้าถึงระบบได้ทั้งหมด จึงต้องแบ่งบทบาทหน้าที่เพื่อให้เป็นไปตามนโยบายความปลอดภัย โดยเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวทำให้อย่างน้อยจะต้องมีบทบาทดังต่อไปนี้

5.2.1.1 บทบาทของผู้ให้บริการ (Trusted Roles for Certification Authority) แบ่งออกได้ ดังนี้

- ผู้จัดการฝ่าย CA Operation มีหน้าที่ดังนี้
    - บริหารจัดการกุญแจส่วนตัวของผู้ให้บริการออกใบรับรอง
    - กำหนดและดูแลนโยบายดานความมั่นคงที่เกี่ยวของกับบริการใบรับรอง
    - ตรวจสอบการทำงานของเจ้าหน้าที่ System Support และ System Administrator
- เจ้าหน้าที่ System Support มีหน้าที่ดังนี้

(Copyright © 2011 Thai Digital ID Co., Ltd.)

- กำหนดค่าตัวแปรสำคัญต่างๆ ให้กับระบบที่เกี่ยวข้องกับระบบใหบริการใบรับรอง
- บริหารและจัดการอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับระบบให้บริการใบรับรอง
- กำหนดค่าตัวแปรสำคัญต่างๆ ให้กับอุปกรณ์เครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับระบบให้บริการใบรับรอง

- เจ้าหน้าที่ System Administrator มีหน้าที่ดังนี้
  - ปรับปรุงประสิทธิภาพการทำงาน (Performance Tuning) และปรับปรุงระบบรักษาความมั่นคง (Security Hardening) ให้กับเครื่องคอมพิวเตอร์
  - บริหารจัดการกุญแจส่วนตัวของผู้ให้บริการออกใบรับรอง
  - กำหนดและดูแลนโยบายดานความมั่นคงที่เกี่ยวของกับบริการใบรับรอง
  - ตรวจสอบการทำงานของเจ้าหน้าที่ System Support และ CA Operator
- เจ้าหน้าที่ CA Operator มีหน้าที่ดังนี้
  - บริหารและจัดการเครื่องคอมพิวเตอร์สำหรับระบบให้บริการใบรับรอง
  - ดูแลระบบปฏิบัติการ (Operating System) ของเครื่องคอมพิวเตอร์
  - บริหารและจัดการระบบจัดเก็บข้อมูลของระบบให้บริการใบรับรอง

5.2.1.2 บทบาทของเจ้าหน้าที่รับลงทะเบียน (Trusted Roles for Registration Authority) แบ่งออกได้ ดังนี้

- เจ้าหน้าที่ RA Operator มีหน้าที่ดังนี้
  - รับคำขอใช้บริการ
  - พิสูจน์ความแท้จริงและตัวตนของผู้ใช้บริการ
  - ออกใบรับรองให้กับผู้ใช้บริการ
  - รับคำขอเพิกถอนใบรับรอง
  - เพิกถอนใบรับรองตามคำร้องขอของผู้ใช้บริการ
  - ออกรายการเพิกถอนใบรับรอง

- เจ้าหน้าที่ RA Auditor มีหน้าที่ดังนี้
  - ตรวจสอบการทำงานของ RA Operator

(Copyright © 2011 Thai Digital ID Co., Ltd.)

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)

บุคคลากรที่จะมาปฏิบัติงานจะต้องผ่านการคัดเลือกตามกระบวนการอย่างเป็นทางการเพื่อแสดงถึง “การเป็นบุคคลที่ไว้วางใจได้”

5.2.4 การรั่วไหลของข้อมูลสำคัญและความต่อเนื่องของการให้บริการ (Compromise and Disaster Recovery)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีนโยบายในการจัดการกับการรั่วไหลของข้อมูลสำคัญและความต่อเนื่องของการให้บริการ โดยถ้ามีการรั่วไหลของข้อมูลสำคัญที่เกียวข้องกับกุญแจส่วนตัวของผู้ให้บริการหรือผู้ใช้บริการ จะมีการเพิกถอนใบรับรองอิเล็กทรอนิกส์ที่เกี่ยวข้องดังกล่าว

ในกรณีที่เกิดปัญหาหรือเหตุการณ์อันมีเหตุให้ระบบงานต้องหยุดชะงัก ผู้ให้บริการได้จัดทำแผนสำรอง (Business Continuity Plan) และแผนฉุกเฉิน (Disaster Recovery Plan) เพื่อจัดการกับเหตุการณ์ดังกล่าว

5.2.5 การเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียน (CA or RA Termination)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หรือเจ้าหน้าที่รับลงทะเบียนมีความจำเป็นต้องเลิกกิจการการให้บริการออกใบรับรองอิเล็กทรอนิกส์ ผู้ให้บริการจะทำการแจ้งให้ผู้ใช้บริการทราบล่วงหน้าอย่างน้อย 60 วัน โดยในกรณีนี้ บริษัทไทยดิจิทัล ไอดี จำกัด จะเป็นผู้หาวิธีการในการโอนย้ายระบบ หรือ จัดหาระบบใหม่แทน หรือ มีมาตรการอื่นที่เหมาะสมสำหรับการแก้ไขผลกระทบในการยกเลิกระบบการออกใบรับรองอิเล็กทรอนิกส์ แก่ผู้ใช้บริการ

(Copyright © 2011 Thai Digital ID Co., Ltd.)

6 การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

6.1 *การสร้างและติดตั้งคู่กุญแจ (Key Pair Generation and Installation)*

6.1.1 การสร้างกุญแจคู่ (Key Pair Generation)

กุญแจคู่ของ TDID CA จะถูกสร้างและติดตั้งโดย TDID CA ส่วน กุญแจคู่ของผู้ใช้บริการจะถูกสร้างและถูกติดตั้งในสื่ออิเล็กทรอนิกส์ SmartCard, USB Token หรือ Hardware Security Module (HSM) ซึ่งเก็บรักษาโดยผู้ใช้บริการเอง

6.1.2 การส่งมอบกุญแจส่วนตัว (Private Key Delivery to Entity)

กุญแจส่วนตัวของผู้ใช้บริการจะถูกสร้างและจัดเก็บอยู่ใน สื่ออิเล็กทรอนิกส์ SmartCard, USB Token หรือ Hardware Security Module (HSM) ซึ่งเป็นอุปกรณ์ที่มีความปลอดภัยสูง ไม่สามารถคัดลอก กุญแจส่วนตัวและข้อมูลอื่นใดออกไปได้ โดยสื่ออิเล็กทรอนิกส์ดังกล่าว จะเก็บอยู่ที่ผู้ใช้บริการโดยตรง

6.1.3 การส่งมอบกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ไปยังผู้ใช้บริการ (CA Public Key Delivery to Users)

กุญแจสาธารณะของ TDID CA มีความจำเป็นต่อผู้ใช้บริการและผู้เกี่ยวข้อง โดยอาจจะกระจายไปพร้อมกับใบรับรองของผู้ใช้บริการ หรือ ดาวน์โหลดโดยผู้ใช้บริการจาก เวบไซต์ที่ TDID กำหนด

6.1.4 ขนาดของกุญแจ (Key Sizes)

ความยาวของกุญแจ TDID CA จะถูกกำหนดในข้อมูลใบรับรอง โดยจะมีขนาด 4096 บิต ส่วนขนาดกุญแจของผู้ใช้ใบรับรองอิเล็กทรอนิกส์ มีขนาดอยู่ที่ 1024 บิตขึ้นไป

6.1.5 การสร้างตัวแปรกุญแจสาธารณะ (Public Key Parameters Generation)

ตัวแปรที่ใช้ในการสร้างกุญแจสาธารณะจะถูกสร้างโดย TDID CA โดยยึดตามมาตรฐาน X.509 Version 3

6.1.6 การตรวจสอบคุณภาพของตัวแปร (Parameter Quality Checking)

คุณภาพของตัวแปรของกุญแจสาธารณะจะถูกตรวจสอบโดยอัตโนมัติจากโปรแกรมประยุกต์ใช้งานของระบบ TDID CA

(Copyright © 2011 Thai Digital ID Co., Ltd.)

6.1.7 การสร้างกุญแจคู่จากอุปกรณ์หรือซอฟต์แวร์ (Hardware/Software Key Generation)

การสร้างกุญแจคู่ของ CA จะถูกจัดการโดยอุปกรณ์ที่เรียกว่า Hardware Security Module ซึ่งสอดคล้องมาตรฐานสากล FIPS 140-2 Level 3 ส่วนการสร้างกุญแจคู่ของผู้สมัครจะใช้อุปกรณ์ Smartcard USB Token หรือ Hardware Security Module (HSM)ซึ่งสอดคล้องมาตรฐานสากล FIPS 140-2 Level 2 และ Level 3

6.1.8 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 TDID CA ได้มีการปฏิบัติตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 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

6.2.4 การสำรองกุญแจส่วนตัว (Private Key Backup)

มีการสำรองกุญแจส่วนตัวเฉพาะของ TDID CA

6.2.5 การบันทึกถาวรกุญแจส่วนตัว (Private Key Archival)

ไม่มีการบันทึกถาวรกุญแจส่วนตัว

6.2.6 กุญแจส่วนตัวภายในโมดูลการเข้ารหัส (Private Key Entry into Cryptographic Module)

กุญแจส่วนตัวของ TDID CA ได้ถูกสร้างขึ้นภายในโมดูลที่มีรูปแบบของการเข้ารหัสและถอดรหัส ซึ่งไดรับการรับรองตามมาตรฐาน Federal Information Processing

(Copyright © 2011 Thai Digital ID Co., Ltd.)

Standard (FIPS) 140-2 Level 3 และจะนำมาถอดรหัสก็ต่อเมื่อมีการตรวจสอบสิทธิผ่านอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยสูงและมีการใส่รหัสผ่านที่ถูกต้องโดยเจ้าหน้าที่ดูแลระบบออกใบรับรอง TDID CA เท่านั้น

6.2.7 วิธีการนำกุญแจส่วนตัวมาใช้งาน (Method of Activating Private Key)

กุญแจส่วนตัวของ TDID CA จะถูกนำมาใช้งานได้เมื่อมีการตรวจสอบสิทธิผ่านอุปกรณ์จัดเก็บข้อมูลที่เป็นฮาร์ดแวร์ที่มีมาตรฐานความปลอดภัยสูงและมีการใส่รหัสผ่านที่ถูกต้องโดยเจ้าหน้าที่ผู้ดูแลระบบออกใบรับรอง TDID CA เท่านั้น

6.2.8 วิธีเลิกการใช้งานกุญแจส่วนตัว (Method of Deactivating Private Key)

กุญแจส่วนตัวจะเลิกใช้งานได้ก็ต่อเมื่อมีการร้องขอจากผู้ใช้บริการหรือผู้เป็นเจ้าของกุญแจส่วนตัว โดยระบบ RA จะทำการยกเลิกการใช้งานกุญแจส่วนตัวนั้น

6.2.9 การจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Controls)

ผู้ให้บริการได้มีการจัดสร้างเอกสารการตรวจสอบความเสี่ยงเกี่ยวกับความปลอดภัย ซึ่งได้มีการระบุและจัดการกับความเสี่ยงที่ระดับสูงและสูงมาก เกี่ยวกับเรื่องการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับไว้แล้ว

6.2.10 การทำลายกุญแจส่วนตัว

ในกรณีที่ผู้ใช้บริการต้องการทำลายกุญแจส่วนตัว ให้ใช้โปรแกรมประยุกต์ในการเขียนค่าทับกุญแจส่วนตัว (overwriting the key)

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

6.3.1 การเก็บรักษากุญแจสาธารณะ (Public Key Archival)

กุญแจสาธารณะจะถูกเก็บบันทึก ไว้ในใบรับรอง โดยใบรับรอง ได้ถูกจัดเก็บไว้ในฐานข้อมูลของ TDID CA เป็นระยะเวลา 10 ปี

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

ระยะเวลาใช้งานของกุญแจส่วนตัวและกุญแจสาธารณะ ของ TDID CA คือ 10 ปี

(Copyright © 2011 Thai Digital ID Co., Ltd.)

6.4 *ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data)*

6.4.1 การสร้างข้อมูลและการนำข้อมูลไปใช้ในการติดตั้งใบรับรอง (Activation Data Generation and Installation)

ข้อมูลที่ใช้ในการสร้างและติดตั้งใบรับรองของผู้ใช้บริการ ถูกสร้างและจัดเก็บอย่างปลอดภัย ภายใต้มาตรฐาน FIPS 140 Level 2 หรือ Level 3

6.4.2 การป้องกันข้อมูลที่ใช้ในการติดตั้งใบรับรอง (Activation Data Protection)

การป้องกันข้อมูลที่ที่ใช้ในการติดตั้งใบรับรอง สำหรับผู้ใช้บริการของระบบ TDID CA จะเป็นไปตามกลไกการป้องกันด้วยอุปกรณ์ HSM ที่ได้ตามมาตรฐาน FIPS 140-2 Level 2 หรือ Level 3 เช่น อาจมีการใช้รหัสลับ หรือ อุปกรณ์ authentication อื่นใดเพื่อใช้ในการติดตั้งใบรับรอง

6.5 *การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)*

6.5.1 ข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ที่มีลักษณะเฉพาะ (Specific Computer Security Technical Requirements)

ผู้ให้บริการได้มีการจัดตั้งแผนความปลอดภัยของระบบ ที่ได้รวมข้อกำหนดทางเทคนิคในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองตามมาตรฐานความปลอดภัย ISO27001

6.5.2 การแบ่งระดับการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ (Computer Security Rating)

ผู้ให้บริการได้มีการจัดตั้งแผนความปลอดภัยของระบบ ที่ได้แบ่งระดับในการรักษาความมั่นคงและปลอดภัยของคอมพิวเตอร์ สำหรับการปฏิบัติงานให้บริการออกใบรับรองตามมาตรฐานความปลอดภัย ISO27001

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) และระบบได้ผ่านการรับรองมาตรฐาน Common Criteria EAL 4+

(Copyright © 2011 Thai Digital ID Co., Ltd.)

6.6.2 การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัย (Security Management Controls)

การควบคุมการจัดการในการรักษาความมั่นคงและปลอดภัยจะถูกควบคุมและบริหารภายใต้ระบบมาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ ISO 27001 ทั้งในส่วนของอุปกรณ์ (Tools) กระบวนการ (Procedure) และ บุคลากรซึ่งถูกควบคุมตามบทบาทหน้าที่ของเจ้าหน้าที่ผู้ดูแลระบบที่ได้กำหนดสิทธิ์ไว้แล้ว 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 TDID CA ได้ถูกออกแบบให้เป็นระบบเครือข่ายเฉพาะที่ใช้สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องเท่านั้น โดยมิได้มีการเชื่อมต่อกับระบบเครือข่ายภายนอก และมีการติดตั้งทั้งฮาร์ดแวร์และซอฟต์แวร์ ไฟล์วอล ในการป้องกันการบุกรุกจากการเข้าถึงภายนอก ระบบตรวจสอบผู้บุกรุก (Intrusion Detection System: IDS) และระบบป้องกันไวรัส (Anti-Virus)

6.8 *ข้อกำหนดสำหรับการประทับเวลาในการบันทึกต่าง ๆ (Time-Stamping)*

ข้อมูลของรายการที่เกี่ยวข้องกับการดำเนินการเกียวกับใบรับรอง อันได้แก่ การออกใบรับรอง การระงับใช้ใบรับรอง การเพิกถอนใบรับรอง จะถูกเก็บบันทึกและประทับเวลา ตามข้อกำหนดของซอฟต์แวร์ของระบบ CA

(Copyright © 2011 Thai Digital ID Co., Ltd.)

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

7.1 *รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)*

7.1.1 รูปแบบ (Profile)

ใบรับรองที่ออกโดย TDID CA ใชมาตรฐาน X.509 Version 3 Certificate ซึ่งมีรายการดังต่อไปนี้

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

7.1.2 ข้อมูลเพิ่มเติมของใบรับรอง (Certificate Extension)

ข้อมูลเพิ่มเติมของใบรับรองที่ออกโดย TDID CA ใช้มาตรฐาน X.509 V.3 certificate extensions ซึ่งมีรายการอย่างน้อยดังต่อไปนี้

- Authority Key Identifier : ระบุถึงกุญแจสาธารณะของ TDID CA
- Key Usage : วัตถุประสงค์ในการนำกุญแจไปใช้งาน
- Extended Key Usage : วัตถุประสงค์เพิ่มเติมในการนำกุญแจไปใช้งาน
- CRL Distribution Points : ระบุถึงที่อยู่ของรายการเพิกถอนใบรับรองฯ เพื่อใช้ตรวจสอบสถานะของใบรับรองฯ
- 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 TDID CA คือ ชื่อเฉพาะตามมาตรฐาน X.500

(Copyright © 2011 Thai Digital ID Co., Ltd.)

7.2 *รูปแบบรายการเพิกถอนใบรับรอง (CRL Profile)*

7.2.1 รูปแบบ **(Profile)**

รายการเพิกถอนใบรับรองที่ออกโดย TDID CA ใชมาตรฐาน X.509 CRL Version 2 ซึ่งมีรายการดังต่อไปนี้

- Signature Algorithm : วิธีการที่ใช้ในการสร้างลายมือชื่อดิจิทัลในรายการเพิกถอนใบรับรองของ TDID CA
- Issuer : ชื่อของผู้ให้บริการที่ออกรายการเพิกถอนใบรับรอง
- Effective date : วันเวลาที่ออกรายการเพิกถอนใบรับรอง
- Next update : วันเวลาที่จะทำการปรับปรุงรายการเพิกถอนใบรับรองครั้งถัดไป
- CRL Number : หมายเลขของรายการเพิกถอนใบรับรอง
- Revocation List : รายการของใบรับรองที่ถูกเพิกถอน

(Copyright © 2011 Thai Digital ID Co., Ltd.)

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

ผู้ให้บริการออกใบรับรอง ได้ยึดมาตรฐาน ISO 27001 สำหรับดำเนินการทางด้านการประเมินความเสี่ยง และ นโยบายด้านความมั่นคง โดยจัดให้มีการตรวจสอบทั้งผู้ตรวจสอบภายใน และ ผู้ตรวจสอบภายนอกจาก BVQI

(Copyright © 2011 Thai Digital ID Co., Ltd.)

9 ข้อกำหนดอื่น ๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

9.1 *ค่าธรรมเนียม (Fees)*

ผู้ให้บริการออกใบรับรอง จะจัดเก็บค่าธรรมเนียมจากกรณีดังต่อไปนี้

1. การออกใบรับรอง
2. การต่ออายุใบรับรอง

โดยสามารถตรวจสอบค่าธรรมเนียมได้จากเวบไซต์ www.thaidigitalid.com

9.2 *การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)*

ผู้ให้บริการออกใบรับรอง ได้กำหนดขอบเขตการรักษาความลับของข้อมูลทางธุรกิจ อันได้แก่ แผนทางธุรกิจ ข้อมูลการขาย ความลับทางการค้า และข้อมูลที่ได้จากบุคคลที่สามภายใต้ข้อตกลงในการให้บริการกับผู้ใช้บริการหรือในสัญญาหรือเอกสารการให้บริการฉบับต่าง ๆ

9.3 *นโยบายการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)*

การดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จะต้องได้รับความยินยอมจากผู้ใช้บริการ ก่อนจะมีการเปิดเผยข้อมูลส่วนบุคคล ยกเว้นกรณีที่จำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลในกรณีที่ต้องดำเนินการตามกฎหมายฉบับต่างๆ หรือเมื่อมีคำสั่งศาล

9.4 *ทรัพย์สินทางปัญญา (Intellectual Property Rights)*

ผู้ให้บริการเป็นเจ้าของสิทธิ์ในทรัพย์สินทางปัญญาแต่เพียงผู้เดียวในเอกสารนโยบายใบรับรองอิเล็กทรอนิกส์ฉบับนี้ และสงวนสิทธิ์ใดๆ ที่มีอยู่หรือเกิดจากเอกสารฉบับนี้

9.5 *คำรับรอง (Representations and Warranties)*

ผู้ให้บริการออกใบรับรอง รับรองว่า ข้อมูลหรือข้อเท็จจริงที่บันทึกไว้ในใบรับรองนั้นถูกต้อง ตามข้อตกลงในการให้บริการกับผู้ใช้บริการ

9.6 *การบอกเลิกคำรับรอง (Disclaimers of Warranties)*

การบอกเลิกคำรับรองให้เป็นไปตามข้อกำหนดในข้อตกลงในการให้บริการกับผู้ใช้บริการหรือในสัญญาหรือเอกสารการให้บริการฉบับต่าง ๆ

9.7 *การเลิกสัญญา (Term and Termination)*

การเลิกสัญญาให้เป็นไปตามความประสงค์ของคู่สัญญาระหว่างผู้ให้บริการออกใบรับรอง และ ผู้ใช้บริการใบรับรอง

(Copyright © 2011 Thai Digital ID Co., Ltd.)

9.8 *ข้อจำกัดความรับผิด* *(Limitations of Liability)*

กรณีที่ผู้ใช้บริการได้รับความเสียหาย อันเนื่องมาจากความผิดพลาดในการให้บริการออกใบรับรองอิเล็กทรอนิกส์ และ/หรือเกิดจากความจงใจหรือประมาทเลินเล่อ ของ ผู้ให้บริการ ผู้ให้บริการตกลงจะรับผิดชดใช้ความเสียหายให้แก่ผู้ใช้บริการในวงเงินไม่เกิน 30,000 บาท ทั้งนี้ การรับผิดชดใช้ความเสียหายดังกล่าวจะไม่รวมถึงความเสียหายที่ไม่อาจคาดการณ์ได้ ความเสียหายที่เป็นผลต่อเนื่อง หรือความสูญเสียทางธุรกิจ หรือความเสียหายในเชิงลงโทษ

ทั้งนี้ ข้อจำกัดความรับผิดดังกล่าวจะไม่นำมาใช้ หาก มีการกำหนดข้อจำกัดความรับผิด ของการใช้ใบรับรองฯ แต่ละประเภท ภายใต้เงื่อนไขหรือสัญญาที่ให้บริการที่เกี่ยวข้อง แล้ว

9.9 *ค่าสินไหมทดแทน* *(Indemnities)*

ค่าสินไหมทดแทนให้เป็นไปตามข้อตกลงระหว่างผู้ให้บริการออกใบรับรองและผู้ใช้บริการ ทั้งนี้ ในกรณีที่คู่กรณีที่เกี่ยวข้องไม่ตรวจสอบสถานะการเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ หากมีความเสียหายเกิดขึ้นคู่กรณีที่เกี่ยวข้องนั้นต้องรับผิดชดใช้ค่าสินไหมทดแทนในความเสียหายดังกล่าว

(Copyright © 2011 Thai Digital ID Co., Ltd.)