บทที่ 4

นโยบายและการบริหารจัดการ

นโยบายด้านความมั่นคงปลอดภัยถือเป็นสิ่งที่มีความสำคัญมากสำหรับหน่วยงานใหญ่ ๆ อย่างกรุงเทพมหานคร ทั้งนี้เพื่อให้ง่ายต่อการบริหารจัดการด้านความมั่นคงปลอดภัยและเป็นการวางรากฐานขององค์กรให้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของระบบงานสารสนเทศและข้อมูล ระบบรักษาความมั่นคงปลอดภัยที่ดีมิได้เกิดจากการใช้เทคโนโลยีที่ดีแต่เพียงอย่างเดียว ต้องประกอบด้วยกระบวนการหรือขั้นตอนการปฏิบัติที่ชัดเจน สำหรับเป็นบรรทัดฐานในการปฏิบัติของบุคลากรในระดับต่าง ๆ ของกรุงเทพมหานคร

โครงสร้างพื้นฐานระบบกุญแจสาธารณะเป็นเทคโนโลยีด้านความมั่นคงปลอดภัยที่เอื้อประโยชน์ต่อการสื่อสารในโลกของอิเล็กทรอนิกส์ให้มีความปลอดภัยและน่าเชื่อถือ อย่างไรก็ดีการนำโครงสร้างพื้นฐานระบบกุญแจสาธารณะมาประยุกต์ใช้งานยังมีรายละเอียดในแง่ของการนำมาใช้งานอีกมาก จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการกำหนดนโยบายและการบริหารจัดการที่เป็นรูปธรรมเพื่อกำหนดรายละเอียดเหล่านั้น ผู้วิจัยได้นำเสนอประเด็นหลัก ๆ ดังนี้

4.1. แนวทางนโยบายด้านโครงสร้างพื้นฐานระบบกุญแจสาธารณะ

4.1.1. การจัดตั้งตำแหน่งผู้บริหารระดับสูงฝ่ายความมั่นคงด้านสารสนเทศ (CSO – Chief Security Officer)

ความมั่นคงปลอดภัยของข้อมูลและสารสนเทศขององค์กรเป็นเรื่องที่มีความสำคัญอย่างยิ่งและครอบคลุมงานในทุกส่วน ผู้บริหารระดับสูงต้องให้ความสำคัญและสนับสนุนอย่างต่อเนื่อง เนื่องจากระบบความมั่นคงปลอดภัยมิใช่เรื่องของเทคโนโลยีแต่เพียงอย่างเดียว จำเป็นต้องมีนโยบายอย่างชัดเจน รวมถึงการสร้างวัฒนธรรมขององค์กรให้เห็นความสำคัญของระบบรักษาความมั่นคงปลอดภัย เพื่อให้ระบบรักษาความมั่นคงปลอดภัยเป็นไปอย่างมีประสิทธิภาพและสัมฤทธิ์ผล

ตำแหน่งผู้บริหารระดับสูงฝ่ายความมั่นคงด้านสารสนเทศ มีหน้าที่ในด้านการบริหารงานด้านความมั่นคงปลอดภัยขององค์กร ครอบคลุมงานทุกส่วนทั้งความมั่นคงปลอดภัยด้านกายภาพ ความมั่นคงปลอดภัยในระบบงานสารสนเทศและข้อมูล ความมั่นคงปลอดภัยด้านระบบเครือข่าย รวมถึงการกู้ระบบจากสถานการณ์วิกฤติและการจัดการในสถานการณ์ที่ถูกจู่โจม

กรุงเทพมหานครอาจพิจารณาให้เป็นหน้าที่ของรองผู้ว่าราชการกรุงเทพมหานครฝ่ายบริหาร โดยมีรองปลัดกรุงเทพมหานครทำหน้าที่ในส่วนการดำเนินการในระดับปฏิบัติการ

4.1.2. การจัดตั้งคณะกรรมการกำหนดนโยบายด้านความมั่นคงปลอดภัย

คณะกรรมการกำหนดนโยบายด้านความมั่นคงปลอดภัย มีหน้าที่ในการกำหนดนโยบายด้านความมั่นคงปลอดภัย (Security Policy) ของกรุงเทพมหานคร ซึ่งเป็นระเบียบปฏิบัติในด้านความมั่นคงปลอดภัยในระบบงานสารสนเทศและข้อมูล ทั้งนี้ในด้านขั้นตอนหรือกระบวนการที่เกี่ยวข้องกับโครงสร้างพื้นฐานระบบกุญแจสาธารณะควรอ้างอิงไปยังนโยบายด้านใบรับรองกุญแจสาธารณะ

4.1.3. การจัดตั้งคณะกรรมการกำหนดนโยบายด้านใบรับรองกุญแจสาธารณะ

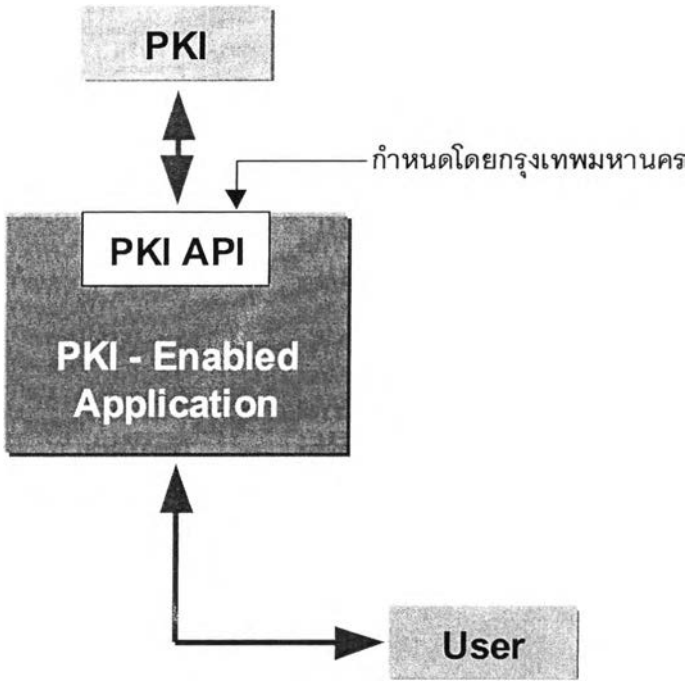
คณะกรรมการกำหนดนโยบายด้านใบรับรองกุญแจสาธารณะ มีหน้าที่ในการกำหนดนโยบายด้านใบรับรองกุญแจสาธารณะ (Certificate Policy) ของกรุงเทพมหานคร นโยบายด้านใบรับรองกุญแจสาธารณะเป็นนโยบายด้านความมั่นคงปลอดภัยที่เกี่ยวข้องโดยตรงกับการนำโครงสร้างพื้นฐานระบบกุญแจสาธารณะมาประยุกต์ใช้งาน

นโยบายด้านใบรับรองกุญแจสาธารณะมีความเกี่ยวข้องกับแง่มุมทั้งด้านเทคนิค ด้านกฎหมาย และการดำเนินงานขององค์กร คณะกรรมการหรือผู้ที่มีส่วนในการกำหนดนโยบายควรมาจากกลุ่มบุคคลหลักได้แก่ หน่วยงานด้านระบบความมั่นคงปลอดภัย หน่วยงานด้านกฎหมาย หน่วยงานที่เป็นเจ้าของระบบงานสารสนเทศที่มีความสำคัญต่อการสนับสนุนงานหลักขององค์กร และหน่วยงานสนับสนุนด้านเทคนิค

4.2. แนวทางการบริหารจัดการ

4.2.1. การกำกับการพัฒนาระบบงานสารสนเทศ

ระบบงานสารสนเทศใด ๆ ที่กรุงเทพมหานครได้กำหนดให้เป็น PKI-Enabled Application กรุงเทพมหานครต้องกำกับการพัฒนาระบบงานสารสนเทศให้เป็นไปตามมาตรฐานหรือนโยบายด้านความมั่นคงปลอดภัยที่ได้วางไว้ ทั้งนี้เพื่อให้ง่ายต่อการบริหารจัดการด้านความมั่นคงปลอดภัย โดยมีหน่วยงานด้านเทคโนโลยีสารสนเทศของกรุงเทพมหานครทำหน้าที่ในการจัดเตรียมข้อกำหนด PKI API (Public Key Infrastructure Application Programming Interface) ที่กรุงเทพมหานครใช้ รวมถึงการให้ความรู้ และกำกับการจัดสร้างระบบงานสารสนเทศให้เป็นไปตามนโยบายและข้อกำหนดของกรุงเทพมหานครที่ได้วางไว้ ทั้งนี้ความสัมพันธ์ขององค์ประกอบที่เกี่ยวข้องในระบบสารสนเทศที่เป็น PKI-Enabled Application แสดงดังรูปที่ 4.1



รูปที่ 4.1 องค์ประกอบของระบบสารสนเทศที่เป็น PKI-Enabled Application

ระบบงานสารสนเทศใด ๆ ที่จะพัฒนาเป็น PKI-Enabled Application จะต้องใช้ API ซึ่งรองรับระบบโครงสร้างพื้นฐานระบบกุญแจสาธารณะ ปัจจุบัน API มาตรฐานดังกล่าวถูกออกแบบให้ระบบสารสนเทศที่เรียกใช้งานเป็นอิสระจากผลิตภัณฑ์ของผู้ผลิตแต่ละยี่ห้อ[9] กล่าวคือสามารถใช้ API เดียวกันนี้ในการเข้าใช้โครงสร้างพื้นฐานระบบกุญแจสาธารณะจากผู้ผลิตต่างกัน ตัวอย่าง API มาตรฐานหลัก ๆ ได้แก่

1) Microsoft CryptoAPI จากบริษัทไมโครซอฟท์
2) Common Data Security Architecture จาก Open Group
3) Generic Security Service API จาก Internet Engineering Task Force's Common Authentication Technology Working Group

4.2.2. การจัดการระบบโครงสร้างพื้นฐานระบบกุญแจสาธารณะให้ครบวงจร

การประยุกต์ใช้งานระบบโครงสร้างพื้นฐานระบบกุญแจสาธารณะ เกี่ยวข้องกับกระบวนการตั้งแต่การออกใบรับรอง การใช้งานใบรับรอง การเพิกถอนหรือยกเลิกใบรับรอง การสร้างความรู้ความเข้าใจแก่ผู้ใช้งาน การประชาสัมพันธ์ ตลอดจนการวางแผนการแก้ไขปัญหาพื้นฐาน และการกู้ระบบจากสถานการณ์วิกฤติต่าง ๆ

ทั้งนี้การวางแผนการบริหารจัดการระบบโครงสร้างพื้นฐานระบบกุญแจสาธารณะต้องคำนึงถึงกระบวนการในทุกส่วน เพื่อให้การดำเนินงานของทั้งระบบเป็นไปอย่างครบวงจร และเป็นการป้องกันและจัดการปัญหาที่เกิดขึ้นอย่างเป็นระบบ

4.2.3. การบริหารให้เกิดความเชื่อมั่นใน CA

ความเชื่อมั่นของผู้ใช้งานและผู้เกี่ยวข้องทั้งภายในและภายนอกองค์กรเป็นสิ่งจำเป็นอย่างยิ่งสำหรับการสร้างระบบรักษาความมั่นคงปลอดภัย เพราะเมื่อปราศจากความเชื่อมั่นแล้ว ระบบรักษาความมั่นคงปลอดภัยจะไม่สามารถสร้างประโยชน์ให้แก่องค์กรได้อย่างเต็มที่

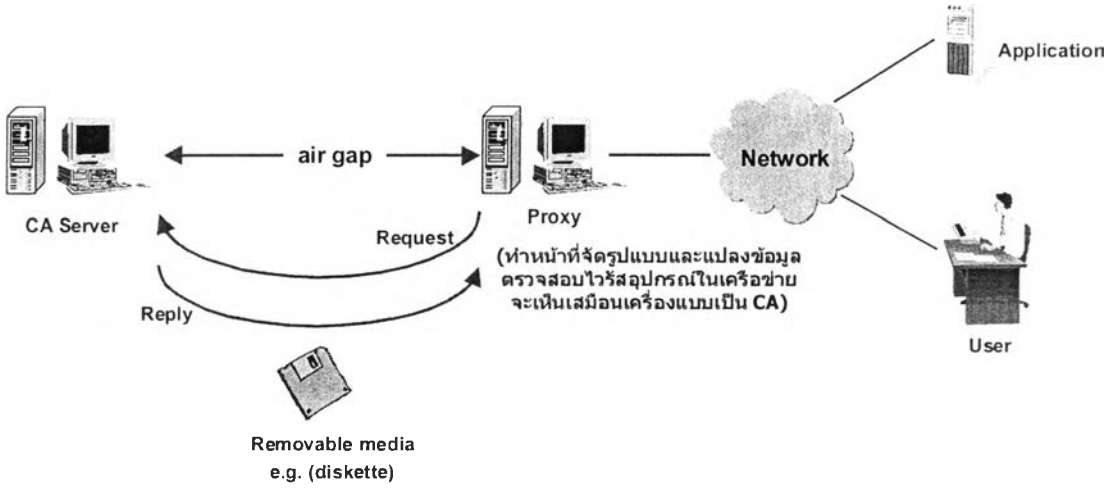
การบริหารจัดการให้เกิดความเชื่อมั่นในโครงสร้างพื้นฐานระบบกุญแจสาธารณะของกรุงเทพมหานคร จึงเป็นสิ่งที่มีความสำคัญยิ่ง ในการนี้กรุงเทพมหานครควรพิจารณาการนำเทคโนโลยีมาปรับใช้อย่างเหมาะสมเพื่อให้เกิดความเชื่อมั่น ตัวอย่างเช่น

1) Air Gap เป็นการแยกเครื่องคอมพิวเตอร์เช่น CA Server ออกจากระบบเครือข่าย และใช้ Removable Media เช่น Diskette เป็นอุปกรณ์ในการโอนถ่ายข้อมูลเข้าสู่ระบบเครือข่ายดังแสดงในรูปที่ 4.2

2) Off-site Backup and Recovery เป็นกระบวนการสำรองและกู้คืนข้อมูล และนำสื่อบันทึกข้อมูลจัดเก็บในที่ปลอดภัยและต่างสถานที่กับระบบที่สำรองข้อมูลไว้ เช่น ตู้นิรภัยของธนาคาร เป็นต้น

3) Full-time Security Officer เป็นการจัดให้มีเจ้าหน้าที่ที่ทำหน้าที่ด้านการดูแลรักษาความมั่นคงปลอดภัยระบบโดยเฉพาะ

4) Internal and External Auditor เป็นการจัดให้มีผู้ตรวจสอบทั้งภายในและภายนอก เพื่อทำหน้าที่ตรวจสอบและประเมินนโยบาย การบริหารจัดการและผลการปฏิบัติตามนโยบายขององค์กรอย่างสม่ำเสมอ



รูปที่ 4.2 เทคโนโลยี Air Gap

4.3. ตัวอย่างการประยุกต์ใช้คุณสมบัติของโครงสร้างพื้นฐานระบบกุญแจสาธารณะในโครงการของกรุงเทพมหานคร

ระบบรักษาความมั่นคงปลอดภัยโดยทั่วไป จะสามารถให้บริการขั้นพื้นฐานดังนี้

1) การระบุตัวบุคคล (Authentication) – ความสามารถในการระบุได้ว่าบุคคลที่ติดต่อสื่อสาร เป็นบุคคลตามที่กล่าวอ้างจริง

2) การรักษาความลับ (Confidentiality) – ความสามารถในการรักษาความลับมิให้ผู้อื่นที่ไม่มีสิทธิ์อำนาจสามารถรับทราบข้อมูลที่จัดเก็บหรือสื่อสารได้

3) การรักษาความถูกต้อง (Integrity) - ความสามารถในการรักษาหรือยืนยันความถูกต้องของข้อมูลมิให้มีการแก้ไขโดยไม่ทราบว่าข้อมูลถูกแก้ไขโดยไม่ปรากฏร่องรอย

4) การควบคุมความรับผิดชอบ (Non-repudiation) – ความสามารถในการป้องกันการปฏิเสธความรับผิดชอบ จากผู้เกี่ยวข้องว่ามิได้ส่งหรือรับข้อมูลดังกล่าว

โดยพื้นฐานของเทคโนโลยีการเข้ารหัสแบบกุญแจสาธารณะมีความสามารถในการให้บริการด้านรักษาความมั่นคงปลอดภัยทั้ง 4 ข้อ ทั้งนี้ขึ้นกับการนำไปประยุกต์ใช้งาน จากแผนงาน/โครงการตามแผนแม่บทเทคโนโลยีสารสนเทศกรุงเทพมหานคร (พ.ศ.2544-2549)[11] สามารถนำคุณสมบัติทั้ง 4 ด้านของโครงสร้างพื้นฐานระบบกุญแจสาธารณะมาประยุกต์ใช้ในงานด้านต่าง ๆ ดังแสดงตัวอย่างโครงการที่ประยุกต์ใช้งานในตารางที่ 4.1 ซึ่งรายละเอียดของโครงการทั้งหมดแสดงในภาคผนวก ก.

ตารางที่ 4.1 ตัวอย่างการประยุกต์ใช้คุณสมบัติของโครงสร้างพื้นฐานระบบกุญแจสาธารณะในโครงการของกรุงเทพมหานคร

แผนงาน/โครงการ	Authentication	Confidentiality	Integrity	Non-repudiation
แผนงานระบบสารสนเทศระดับกรุงเทพมหานคร				
1. โครงการระบบการจัดเก็บบันทึกถาวรอิเล็กทรอนิกส์	√	√	√	√
2. โครงการระบบรับแจ้งเหตุและติดตามงานด้านเทคโนโลยีสารสนเทศ	√	√		
แผนงานโครงสร้างพื้นฐานด้าน Information Portal				
3. โครงการระบบสำนักงานอัตโนมัติ	√	√	√	√
4. โครงการ Citizen Information Service Portal	√	√	√	√
5. โครงการ Electronic Commerce Portal	√	√	√	√
:::::::				

ดังจะเห็นได้จากตัวอย่างการประยุกต์ใช้คุณสมบัติของโครงสร้างพื้นฐานระบบกุญแจสาธารณะในโครงการของกรุงเทพมหานครในภาคผนวก ก. โครงการและระบบงานสารสนเทศต่าง ๆ ของกรุงเทพมหานครสามารถใช้งานระบบโครงสร้างพื้นฐานระบบกุญแจสาธารณะได้มาก โดยสามารถสรุปแบ่งตามประเภทของบริการขั้นพื้นฐานของระบบรักษาความมั่นคงปลอดภัยได้ดังตารางที่ 4.2 จากจำนวนโครงการทั้งสิ้น 58 โครงการ

ตารางที่ 4.2 จำนวนโครงการ แบ่งตามประเภทของบริการขั้นพื้นฐาน

ประเภทของบริการขั้นพื้นฐาน	จำนวนโครงการ	%
การระบุตัวบุคคล (Authentication)	32	55.2
การรักษาความลับ (Confidentiality)	33	56.9
การรักษาความถูกต้อง (Integrity)	33	56.9
การควบคุมความรับผิดชอบ (Non-repudiation)	22	37.9

ทั้งนี้เพื่อให้เห็นภาพชัดเจนถึงการนำโครงสร้างพื้นฐานระบบกุญแจสาธารณะไปประยุกต์ใช้งาน ผู้วิจัยขอยกตัวอย่างการประยุกต์ใช้งานในระบบงานสารสนเทศดังตารางที่ 4.3

ตารางที่ 4.3 ตัวอย่างระบบงานและรายละเอียดการประยุกต์ใช้งาน

ระบบงาน	การประยุกต์ใช้งาน
Citizen Information Service Portal	ระบบสารสนเทศนี้เป็นระบบที่ให้บริการแก่ประชาชนในการรับรู้ข่าวสารทั้งของส่วนบุคคล และข้อมูลทั่วไป สำหรับข้อมูลส่วนบุคคล ระบบจำเป็นต้องพิสูจน์ตัวบุคคลว่าเป็นผู้ใด เพื่อนำเสนอเฉพาะข้อมูลของบุคคลนั้น และเนื่องจากเป็นข้อมูลส่วนบุคคลการสื่อสารระหว่างผู้ใช้งานและระบบงานผ่านระบบเครือข่ายสาธารณะอย่างระบบเครือข่ายอินเตอร์เน็ตจำเป็นต้องผ่านการเข้ารหัสเพื่อรักษาความลับของข้อมูลซึ่งอาจทำผ่าน SSL ซึ่งเป็นวิธีการมาตรฐาน ในด้านการทำนิติกรรม ได้แก่ การแจ้ง และการขอใบอนุญาตต่าง ๆ เป็นต้น การนำลายมือชื่อดิจิตอลมาใช้จะทำให้สามารถตรวจสอบความถูกต้องของข้อมูลว่ามิได้ถูกแก้ไข และยืนยันได้ว่าเป็นของบุคคลดังกล่าวจริง กรณีที่จำเป็นต้องใช้เป็นหลักฐานในชั้นศาล ก็สามารถนำข้อมูลดังกล่าวที่ผ่านการลงลายมือชื่อดิจิตอลกลับมาพิสูจน์ได้
ระบบการจัดเก็บภาษี	ระบบสารสนเทศนี้เป็นระบบที่มุ่งเน้นให้เกิดการบริการที่ดีแก่ประชาชน ซึ่งสามารถตรวจสอบที่ตั้ง ข้อกำหนดด้านภาษีและประวัติต่าง ๆ ของสิ่งก่อสร้างของตน รวมถึงการชำระภาษีได้จากบ้านผ่านระบบเครือข่ายอินเตอร์เน็ต เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลจึงจำเป็นต้องผ่านการพิสูจน์ตัวบุคคลที่ใช้งาน และผ่านการเข้ารหัสเพื่อรักษาความลับของข้อมูลที่สื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ต และการที่จะสามารถชำระภาษีได้จากที่บ้าน การนำลายมือชื่อดิจิตอลมาใช้เพื่อสามารถตรวจสอบความถูกต้องของข้อมูลว่ามิได้ถูกแก้ไข และสามารถนำกลับมายืนยันในภายหลังในชั้นศาลกรณีที่เกิดปัญหาขึ้น ทั้งนี้ระบบสารสนเทศนี้ถ้าจัดทำในแบบครบวงจรจำเป็นต้องเชื่อมโยงระบบกับระบบของธนาคารเพื่อสามารถดำเนินการโอนเงินผ่านทางระบบอิเล็กทรอนิกส์ได้ ซึ่งข้อมูลที่ผ่านการลงลายมือชื่อดิจิตอลนี้เองที่จะเป็นข้อมูลที่ใช้ในการยืนยันการดำเนินงานในขั้นตอนต่าง ๆ ของผู้ใช้งาน

4.4. ตัวอย่างโครงสร้างเนื้อหา Certificate Policy และ Certificate Practices Statement

การกำหนดนโยบายด้านโครงสร้างพื้นฐานระบบกุญแจสาธารณะให้ครอบคลุมในรายละเอียดเป็นสิ่งที่ยาก จึงมีการกำหนดกรอบเนื้อหาของนโยบายขึ้นมาโดยหน่วยงาน Internet Engineering Task Force (IETF) เป็นเอกสารชื่อ RFC2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework[12] เพื่อให้หน่วยงานต่าง ๆ สามารถนำไปเป็นแนวทางในการจัดทำนโยบายด้านโครงสร้างพื้นฐานระบบกุญแจสาธารณะให้ครอบคลุมรายละเอียดในประเด็นต่าง ๆ อย่างครบถ้วน โดยมีโครงสร้างเนื้อหานโยบายดังแสดงในภาคผนวก ข.