รายการอ้างอิง

1. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (ร่าง) รายงานการประชุมคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ครั้งที่ 3/2543 วันที่ 6 กรกฎาคม 2543. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ; 2543.
2. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. รายงานการประชุมคณะอนุกรรมการวางแผนพัฒนาเทคโนโลยีสารสนเทศ ครั้งที่ 1/2543. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ; 2543.
3. Charlie Kaufman, Radia Perlman and Mike Speciner. NETWORK SECURITY: PRIVATE Communication in a PUBLIC World. Englewood Cliffs, NewJersey 07632 : Prentice Hall PTR; 1995.
4. Shimshon Berkovits, Santosh Chokhani, Judith A. Furlong, Jisoo A. Geiter and Jonathan C. Guild. Public Key Infrastructure Study: Final Report. National Institute of Standards and Technology; 1994.
5. National Institute of Standards and Technology. ITL Bulletin – July 1997. National Institute of Standards and Technology; 1997.
6. William T. Polk and Nelson E. Hastings. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures. National Institute of Standards and Technology: [Online] Available from: http://csrc.nist.gov/pki/documents/B2B-article.pdf, [2000, Oct 10].
7. Tom Austin. PKI. Wiley Tech Brief Series. WILEY; 2001.
8. Russ Housley and Timpolk. Planning for PKI. Wiley Networking Council Series. WILEY; 2001.
9. Andrew Nash, William Duane, Celia Joseph and Derek Brink. PKI: Implementing and Managing E-Security. RSA PRESS; 2001
10. กองการเจ้าหน้าที่ สำนักปลัดกรุงเทพมหานคร. ข้อมูลสถิติจำนวนอัตรากำลังของกรุงเทพมหานคร. มกราคม 2544.
11. ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย. แผนแม่บทเทคโนโลยีสารสนเทศกรุงเทพมหานคร (พ.ศ.2544-2549). 2544.

12. S. Chookhani and W. Ford. RFC2527 – Internet X.509 Public Key Infrastructure Certificate Plicy and Certification Practices Framework. [Online] Available from http://www.ietf.org/rfc/rfc2527.txt, [2000, Oct 10].

ภาคผนวก

ภาคผนวก ก.

ตัวอย่างการประยุกต์ใช้คุณสมบัติของโครงสร้างพื้นฐานระบบกุญแจสาธารณะในโครงการของกรุงเทพมหานคร

แผนงาน/โครงการ	Authentication	Confidentiality	Integrity	Non-repudiation
แผนงานระบบสารสนเทศระดับกรุงเทพมหานคร				
1. โครงการ Object Master Directory	√	√	√	
2. โครงการระบบการจัดเก็บบันทึกถาวรอิเล็กทรอนิกส์	√	√	√	√
3. โครงการระบบรับแจ้งเหตุและติดตามงานด้านเทคโนโลยีสารสนเทศ	√	√	√	
4. โครงการจัดทำระบบคลังข้อมูล	√	√	√	
5. โครงการการกระจายและการขยายผลเทคโนโลยีสารสนเทศออกสู่ปริมณฑลกรุงเทพมหานคร	√	√	√	√
แผนงานโครงสร้างพื้นฐานด้านระบบเครือข่าย				
6. โครงการระบบเครือข่ายหลัก				
7. โครงการระบบ Campus Backbone				
8. โครงการกระจายจุดเข้าใช้เครือข่าย				
9. โครงการ Extranet Gateway	√	√	√	
10. โครงการระบบการประชุมทางไกล				
แผนงานโครงสร้างพื้นฐานด้านสารสนเทศภูมิศาสตร์				
11. โครงการเก็บข้อมูลภูมิศาสตร์พื้นฐาน	√	√	√	
12. โครงการระบบศูนย์ข้อมูลระยะที่ 3 และระยะที่ 4	√	√	√	
13. โครงการระบบข้อมูลชั้นดิน	√	√	√	
14. โครงการฐานข้อมูลกรรมสิทธิ์ด้านโครงสร้างพื้นฐานสาธารณะ	√	√	√	
แผนงานโครงสร้างพื้นฐานด้านข้อมูล				
15. โครงการสำรวจข้อมูลของสำนักต่าง ๆ ที่จะใช้ภายนอกสำนัก				
16. โครงการพจนานุกรมข้อมูล	√	√	√	

แผนงาน/โครงการ	Authentication	Confidentiality	Integrity	Non-repudiation
17 โครงการ IDM (Integrated Data Model)	√	√	√	
18 โครงการ Componentization				
แผนงานโครงสร้างพื้นฐานด้าน Information Portal				
19. โครงการระบบสำนักงานอัตโนมัติ	√	√	√	√
20. โครงการ Citizen Information Service Portal	√	√	√	√
21. โครงการ Public Address Portal		√	√	√
22. โครงการ Electronic Commerce Portal	√	√	√	√
23. โครงการ BMA Intranet Portal	√	√	√	√
24. โครงการ BMA Extranet Portal	√	√	√	√
แผนงานโครงสร้างพื้นฐานด้านอุปกรณ์คอมพิวเตอร์				
25. โครงการจัดหาเครื่องไมโครคอมพิวเตอร์ให้กับกรุงเทพมหานคร				
26. โครงการปรับปรุงประสิทธิภาพเครื่องแม่ข่าย				
27. โครงการปรับปรุงสภาพแวดล้อมห้องอุปกรณ์คอมพิวเตอร์				
28. โครงการปรับปรุงกฎระเบียบในการจัดซื้อ จัดจ้าง บำรุงรักษาอุปกรณ์คอมพิวเตอร์				
แผนงานโครงสร้างพื้นฐานด้านระบบสนับสนุน				
29. โครงการระบบกุญแจสาธารณะ	√	√	√	√
30. โครงการสร้างวัฒนธรรมด้านความมั่นคง				
แผนงานพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ				
31. โครงการปรับปรุงกฎระเบียบการจ้างงาน และผลตอบแทนเพื่อส่งเสริมบุคลากรที่มีความรู้ทางเทคโนโลยีสารสนเทศ				
32. โครงการฝึกอบรมต่อเนื่อง				
33. โครงการปรับปรุงหลักสูตรการอบรมเทคโนโลยีสารสนเทศเฉพาะสิ่งที่จำเป็น				
34. โครงการสร้าง Job Profile	√	√	√	

แผนงาน/โครงการ	Authentication	Confidentiality	Integrity	Non-repudiation
แผนงานตามภารกิจหลักของแต่ละสำนัก				
35 โครงการศึกษาและออกแบบระบบสนับสนุนการตัดสินใจของผู้บริหารกรุงเทพมหานคร				
36 โครงการศึกษาและวางแผนแม่บทระบบสารสนเทศสำนักการแพทย์ กรุงเทพมหานคร				
37. โครงการศึกษาเพื่อกำหนดแนวทางการพัฒนาระบบสารสนเทศสาธารณสุข				
38. โครงการพัฒนาการบริหารเวชภัณฑ์ด้วยระบบเครือข่ายคอมพิวเตอร์	√	√	√	√
39. โครงการพัฒนาระบบข้อมูลยาด้ายระบบเครือข่ายคอมพิวเตอร์	√	√	√	√
40. โครงการระบบฐานข้อมูลแหล่งกำเนิดมลพิษจากสถานประกอบการที่เป็นอันตรายต่อสุขภาพ	√	√	√	√
41. โครงการจัดทำระบบเครือข่ายสำหรับโรงเรียนในสังกัดกรุงเทพมหานคร				
42. โครงการศึกษาเพื่อจัดทำแผนหลักและวางระบบสารสนเทศของสำนักการโยธา กรุงเทพมหานคร				
43. โครงการศึกษาและวางระบบสารสนเทศของสำนักการระบายน้ำ กรุงเทพมหานคร				
44. โครงการศึกษาเพื่อจัดทำแผนหลักและวางระบบสารสนเทศของสำนักรักษาความสะอาด กรุงเทพมหานคร				
45. โครงการติดตั้งและพัฒนาระบบสารสนเทศของสำนักสวัสดิการสังคม กรุงเทพมหานคร	√	√	√	√
46. โครงการระบบสารสนเทศของกองโรงงานช่างกล	√	√	√	√
47. โครงการวิเคราะห์และออกแบบระบบสารสนเทศของสำนักพัฒนาชุมชน กรุงเทพมหานคร				

แผนงาน/โครงการ	Authentication	Confidentiality	Integrity	Non-repudiation
48. โครงการวิเคราะห์และออกแบบระบบสารสนเทศของสำนักการจราจรและขนส่ง กรุงเทพมหานคร				
49. โครงการจัดทำระบบคอมพิวเตอร์เครือข่ายของสำนักผังเมือง กรุงเทพมหานคร				
แผนงานตามภารกิจหลักในส่วนที่เป็นระบบเสริมสำหรับแต่ละสำนัก				
50. โครงการประชาสัมพันธ์และเผยแพร่โครงการที่ดำเนินการเสร็จแล้ว	√	√	√	√
51. โครงการศูนย์บริหารสถานการณ์ฉุกเฉินกรุงเทพมหานคร	√	√	√	√
52. โครงการระบบการจัดเก็บภาษี	√	√	√	√
53. โครงการระบบ High Level Project Management System เพื่อควบคุมและการจัดการ	√	√	√	√
54. โครงการระบบฐานข้อมูลผู้รับจ้าง	√	√	√	√
55. โครงการระบบสนับสนุนเทคโนโลยีสารสนเทศผู้บริหารระดับสูงเพื่อการบริหารและการตัดสินใจ	√	√	√	√
56. โครงการบรรจุแผนสาขาด้านเทคโนโลยีสารสนเทศ				
57. โครงการรายงานผลกระทบสิ่งแวดล้อม	√	√	√	√
58. โครงการระบบข้อมูลขนส่งมวลชน	√	√	√	√

ภาคผนวก ข.

ตัวอย่างโครงสร้างเนื้อหาของ Certificate Policy และ Certificate Practices Statement

1. INTRODUCTION
   - 1.1 Overview
   - 1.2 Identification
   - 1.3 Community and Applicability
     - 1.3.1 Certification authorities
     - 1.3.2 Registration authorities
     - 1.3.3 End entities
     - 1.3.4 Applicability
   - 1.4 Contact Details
     - 1.4.1 Specification administration organization
     - 1.4.2 Contact person
     - 1.4.3 Person determining CPS suitability for the policy
2. GENERAL PROVISIONS
   - 2.1 Obligations
     - 2.1.1 CA obligations
     - 2.1.2 RA obligations
     - 2.1.3 Subscriber obligations
     - 2.1 4 Relying party obligations
     - 2.1 5 Repository obligations
   - 2.2 Liability
     - 2.2.1 CA liability
     - 2.2.2 RA liability
   - 2.3 Financial responsibility
     - 2.3.1 Indemnification by relying parties
     - 2.3.2 Fiduciary relationships
     - 2.3.3 Administrative processes

2.4 Interpretation and Enforcement

2.4.1 Governing law

2.4.2 Severability, survival, merger, notice

2.4.3 Dispute resolution procedures

2.5 Fees

2.5.1 Certificate issuance or renewal fees

2.5.2 Certificate access fees

2.5.3 Revocation or status information access fees

2.5.4 Fees for other services such as policy information

2.5.5 Refund policy

2.6 Publication and Repository

2.6.1 Publication of CA information

2.6.2 Frequency of publication

2.6.3 Access controls

2.6.4 Repositories

2.7 Compliance audit

2.7.1 Frequency of entity compliance audit

2.7.2 Identity/qualifications of auditor

2.7.3 Auditor's relationship to audited party

2.7.4 Topics covered by audit

2.7.5 Actions taken as a result of deficiency

2.7.6 Communication of results

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

2.8.2 Types of information not considered confidential

2.8 3 Disclosure of certificate revocation/suspension information

2.8 4 Release to law enforcement officials

2.8.5 Release as part of civil discovery

2.8.6 Disclosure upon owner's request

2.8.7 Other information release circumstances

2.9 Intellectual Property Rights

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Rules for interpreting various name forms

3.1.4 Uniqueness of names

3.1.5 Name claim dispute resolution procedure

3.1.6 Recognition, authentication and role of trademarks

3.1.7 Method to prove possession of private key

3.1.8 Authentication of organization identity

3.1.9 Authentication of individual identity

3.2 Routine Rekey

3.3 Rekey after Revocation

3.4 Revocation Request

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.2 Certificate Issuance

4.3 Certificate Acceptance

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

4.4.2 Who can request revocation

4.4.3 Procedure for revocation request

4.4.4 Revocation request grace period

4.4.5 Circumstances for suspension

4.4.6 Who can request suspension

4.4 7 Procedure for suspension request

4.4 8 Limits on suspension period

4.4.9 CRL issuance frequency (if applicable)

4.4.10 CRL checking requirements

4.4.11 On-line revocation/status checking availability

4.4.12 On-line revocation checking requirements

4.4.13 Other forms of revocation advertisements available

4.4.14 Checking requirements for other forms of revocation advertisements

4.4.15 Special requirements re key compromise

4.5 Security Audit Procedures

4.5.1 Types of event recorded

4.5.2 Frequency of processing log

4.5.3 Retention period for audit log

4.5.4 Protection of audit log

4.5.5 Audit log backup procedures

4.5.6 Audit collection system (internal vs external)

4.5.7 Notification to event-causing subject

4.5.8 Vulnerability assessments

4.6 Records Archival

4.6.1 Types of event recorded

4.6.2 Retention period for archive

4.6.3 Protection of archive

4.6.4 Archive backup procedures

4.6.5 Requirements for time-stamping of records

4.6.6 Archive collection system (internal or external)

4.6.7 Procedures to obtain and verify archive information

4.7 Key changeover

4.8 Compromise and Disaster Recovery

4.8 1 Computing resources, software, and/or data are corrupted

4.8 2 Entity public key is revoked

4.8.3 Entity key is compromised

4.8.4 Secure facility after a natural or other type of disaster

4.9 CA Termination

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

5.1.2 Physical access

5.1.3 Power and air conditioning

5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural Controls

5.2.1 Trusted roles

5.2.2 Number of persons required per task

5.2.3 Identification and authentication for each role

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

5.3.2 Background check procedures

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3 7 Contracting personnel requirements

5.3 8 Documentation supplied to personnel

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1 1 Key pair generation

6.1.2 Private key delivery to entity

6.1.3 Public key delivery to certificate issuer

6.1.4 CA public key delivery to users

6.1.5 Key sizes

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

7.1.2 Certificate extensions

7.1.3 Algorithm object identifiers

7.1.4 Name forms

7.1.5 Name constraints

7.1.6 Certificate policy Object Identifier

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical certificate policy extension

7.2 CRL Profile

7.2.1 Version number(s)

7.2.2 CRL and CRL entry extensions

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

8.2 Publication and notification policies

8.3 CPS approval procedures

ภาคผนวก ค.

ตัวอย่างผลิตภัณฑ์ด้านโครงสร้างพื้นฐานระบบกุญแจสาธารณะ

ผลิตภัณฑ์	รายละเอียด
1. Certificate Services	
บริษัทผู้ผลิต	Microsoft Corporation. (http://www.microsoft.com)
บริษัทตัวแทนในประเทศไทย	Microsoft (Thailand) Ltd. (http://www.microsoft.com/thailand)
ค่าซอฟต์แวร์	ฟรี (ทำงานเฉพาะบนระบบปฏิบัติการในตระกูล Microsoft Windows 2000 Server)
ข้อมูล ณ. วันที่	31 มกราคม 2546
2. Certificate Server	
บริษัทผู้ผลิต	Novell, Inc. (http://www.novell.com)
บริษัทตัวแทนในประเทศไทย	Novell Software (Thailand) Ltd. http://www.novell.com/offices/asiapac/thailand
ค่าซอฟต์แวร์	ฟรี (ทำงานเฉพาะบนระบบปฏิบัติการ Novell NetWare)
ข้อมูล ณ. วันที่	31 มกราคม 2546
3. Entrust Authority	
บริษัทผู้ผลิต	Entrust, Inc. (http://www.entrust.com)
บริษัทตัวแทนในประเทศไทย	บริษัท เอเซิร์ทส์ จำกัด (http://www.acerts.net)
ค่าซอฟต์แวร์	ต้องเสียค่าซอฟต์แวร์ลิขสิทธิ์
ข้อมูล ณ. วันที่	31 มกราคม 2546

ผลิตภัณฑ์	รายละเอียด
4. Certificate Management System	
บริษัทผู้ผลิต	America Online, Inc. (http://enterprise.netscape.com)
บริษัทตัวแทนในประเทศไทย	N/A
ค่าซอฟต์แวร์	N/A
ข้อมูล ณ. วันที่	31 มกราคม 2546
5. Onsite Key Manager	
บริษัทผู้ผลิต	Verisign, Inc. (http://www.verisign.com)
บริษัทตัวแทนในประเทศไทย	N/A
ค่าซอฟต์แวร์	N/A
ข้อมูล ณ. วันที่	31 มกราคม 2546
6. RSA Keon Certificate Authority	
บริษัทผู้ผลิต	RSA Security, Inc. (http://www.rsasecurity.com)
บริษัทตัวแทนในประเทศไทย	- NetOne Network Solution Co., Ltd. (http://www.net1.co.th) - MFEC Co., Ltd. (http://www.mfec.co.th)
ค่าซอฟต์แวร์	ต้องเสียค่าซอฟต์แวร์ลิขสิทธิ์
ข้อมูล ณ. วันที่	31 มกราคม 2546

ประวัติผู้เขียนวิทยานิพนธ์

นายสมคิด ลัฐิถาวณิชย์ สำเร็จการศึกษาระดับปริญญาบัณฑิต จากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปี พ.ศ.2538 เข้ารับการศึกษาระดับปริญญามหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปี พ.ศ.2542 ปัจจุบันทำงานที่บริษัท ซิม ซิสเต็ม (ประเทศไทย) จำกัด