2006

An Investigation of Digital Certificates For Government Officials: A Thailand Case

Waraporn Jirachiefpattana
National Institute of Development Administration

Ajin Jirachiefpattana
The e-Government Development and Promotion Bureau

An Investigation of Digital Certificates For Government Officials: A Thailand Case

Waraporn Jirachiefpattana
School of Applied Statistics, National Institute of Development Administration
Bangkok, Thailand,
E-Mail: waraporn@as.nida.ac.th

Ajin Jirachiefpattana
The e-Government Development and Promotion Bureau, Ministry of Information and Communication
Technology, Bangkok, Thailand,
E-Mail: ajin@mict.go.th

ABSTRACT

Digital certificates are the building blocks of Public Key Infrastructure (PKI) that create and manage electronic credentials, allowing the use of digital signatures and their underlying keys and certificates across the Internet. This infrastructure is very important for e-service, e-commerce and even e-government in Thailand. Thailand's Ministry of Information and Communication Technology (MICT) issued digital certificates for Thai government officials as a part of the national ICT master plan (IT 2010). Therefore, the aim of this paper is to examine how this project was initiated, planned, carried out, terminated and evaluated, and how appropriate risk strategies were formulated.

Keywords:Project planning and management, Digital certificates, e-Government, Public Key Infrastructure (PKI).

INTRODUCTION

In Thailand, Public Key Infrastructure (PKI) technologies (Adams and Lloyd, 1999; Ford and Baum, 2001) have been introduced in the private sector, especially in financial businesses, more than five years ago. These technologies have been used to create and manage electronic credentials to allow the use of digital signatures and certificates across the Internet. However, such technologies are still new and complicated for Thai people and Thai government officials. Presently, only few people understand and use these PKI technologies. Compared to the business sector, a number of Thai government officials who understand and use PKI are less.

In December 2001, the Electronic Transactions Law and Electronic Signatures Law had been merged and enacted in Thailand, as well as the Electronic Transactions Act B.E. 2544 (2001). These two laws recognize the legal effect of data messages by treating them as the functional equivalent of written evidence as a means to promote reliable electronic transactions through the use of electronic signatures. However, many government officials do not fully understand these laws.

In order for Thailand to become an e-Society, the current Thai government has promoted and supported all government agencies to implement e-services through the Internet. To have secure communications when using e-services through the Internet, the government certainly has had to implement a strong security infrastructure using PKI technologies. Having a strong security infrastructure, Thai government needed to implement a digital certificate project, which is a main and important part of PKI. As a result, citizens would get secure e-services. Therefore, the aim of this paper is to examine how this project was initiated, planned, carried out, terminated and evaluated, and how appropriate risk strategies were formulated.

PROJECT MOTIVATION AND SCOPE

In February 1996, IT2000 was announced by the National IT Committee (NITC), which is a high-level policy body chaired by the Prime Minister and endorsed by the Cabinet. IT2000 put forward the vision for the country to

properly exploit IT to achieve economic prosperity and social equity. As a result, from IT2000, the NITC secretariat has teamed up with the policy innovation center to conduct a research and develop a ten-year National IT Policy for the period 2001-2010, or IT2010. To achieve the goals, IT 2010 identified five main flagships: e-Government, e-Education, e-Society, e-Commerce, and e-Industry. On September 2002, the ICT Master Plan from 2002-2006 had been approved by the Cabinet. This national master plan established a framework for e-Government under the 4R slogan: Red-tape reduction, Rapid response, Rural coverage, and Round the clock.

National IT Policy Framework

IT-2010

ICT Master Plan 2002-2006

Top priority

IT 2010 identified five main flagships: e-Government, e-Education, e-Society, e-Commerce, e-Industry

- **Establish framework for e-Government under the 4R slogan: Red-tape reduction, Rapid response, Rural coverage, and Round the clock.**

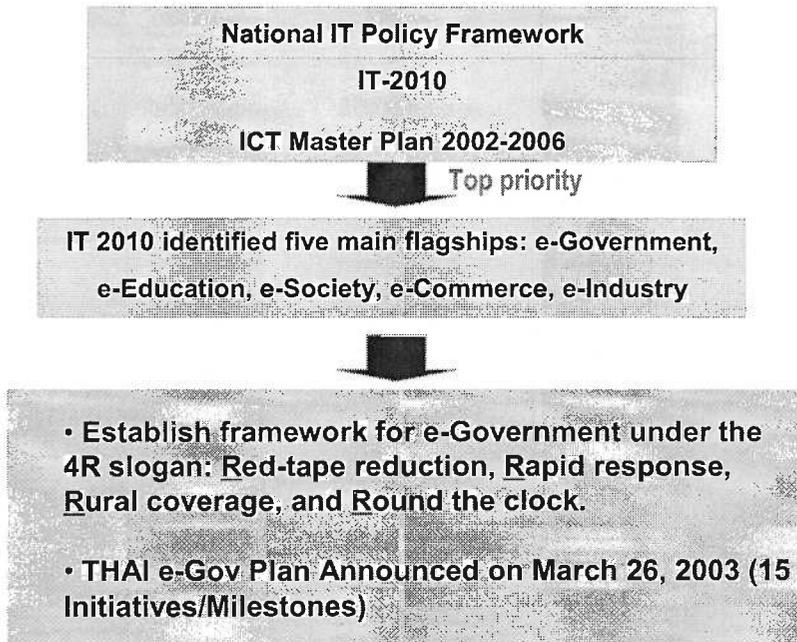- **THAI e-Gov Plan Announced on March 26, 2003 (15 Initiatives/Milestones)**

Figure 1: Project Motivation

On 26th March 2003, the Thailand e-Government plan was announced and approved by the Cabinet. It consisted of 15 initiatives/milestones, as follows:

    (1)   At least one web site in every government department;
    (2)   A web board in every government department;
    (3)   The e-Citizen service portal (www.ecitizen.go.th);
    (4)   E-mail accounts and addresses for all government employees;
    (5)   ICT one stop center;
    (6)   Government Data Exchange (GDX);
    (7)   Government Contact Center (GCC);
    (8)   Departmental Operation Center (DOC)/Ministerial Operation Center (MOC)/Prime Ministerial Operation Center (PMOC);
    (9)   Smart cards for Thai citizens;
    (10)   Digital certificates for Thai government officials;
    (11)   Cyber inspector team;
    (12)   Common government applications (back office) such as Government Financial Management Information System (GFMIS);
    (13)   e-Procurement system;
    (14)   Business Process Re-engineering (BPR) and re-organization;
    (15)   CIO cooperation team.

As shown in the above list, one of the 15 initiatives was the Digital Certificates for Thai Government Officials project. The aims of this project were to issue digital certificates to government officials using Public Key Infrastructure (PKI) technologies; and to promote government officials using digital certificates at least for signing

e-mails so that electronic communication will be secure. As shown in Figure 1, the project motivation is summarized.

PROJECT TEAM ORGANIZATION

After being assigned to implement this project as a part of the e-Government plan, the MICT permanent secretary first set up a steering committee and then two more committees later on. These committees were the Procurement Committee and the Examination and Acceptance Committee. The steering committee consisted of the permanent secretary as the chair of the committee, the deputy permanent secretary and four MICT senior government officials representing four departments under MICT (i.e. the Software Industry Promotion Agency (SIPA), the Post and Telegraph Department, the Meteorological Department, and National Statistical Office (NSO) as members of the committee), and the director of the ICT Industry Promotion Bureau, who was assigned to be a member and the secretary of the committee.
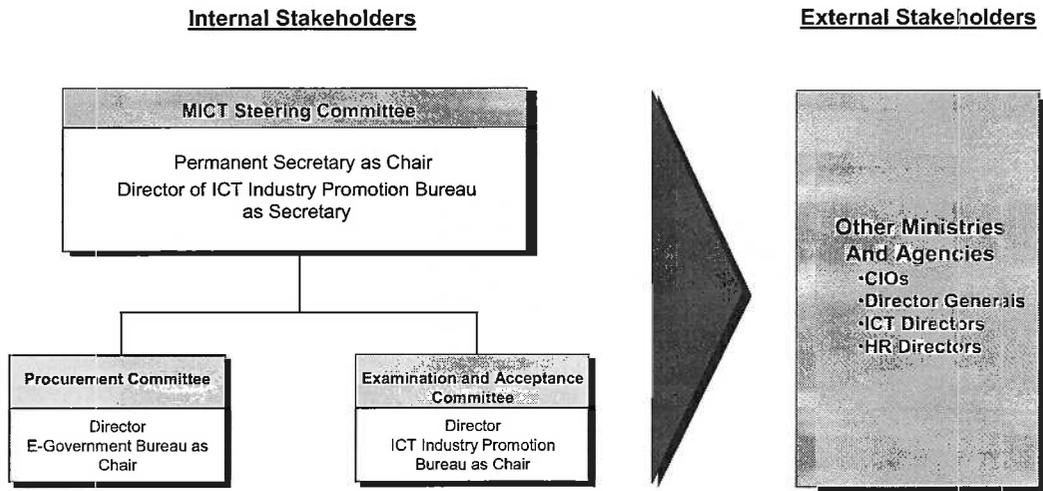

Figure 2: Project Team Organization

LIST OF MINISTRIES AND AGENCIES	
▸ Ministry of Information and Communication Technology	▸ Ministry of Labor
▸ Secretariat of the Prime Minister	▸ Ministry of Natural Resources and Environment
▸ Ministry of Agriculture and Cooperatives	▸ Ministry of Public Health
▸ Ministry of Commerce	▸ Ministry of Science and Technology
▸ Ministry of Culture	▸ Ministry of Social Development and Human Security
▸ Ministry of Defense	▸ Ministry of Tourism and Sports
▸ Ministry of Education	▸ Ministry of Transport
▸ Ministry of Energy	▸ Bureau of the Budget
▸ Ministry of Finance	▸ Office of the National Economic and Social Development Board (NESDB)
▸ Ministry of Foreign Affairs	▸ Office of the Civil Service Commission (OCSC)
▸ Ministry of Industry	▸ Office of the Prime Minister
▸ Ministry of Interior	▸ Office of the Public Sector Development Commission (OPDC)
▸ Ministry of Justice	▸ Comptroller General's Department

Table 1: Ministries and Agencies involved
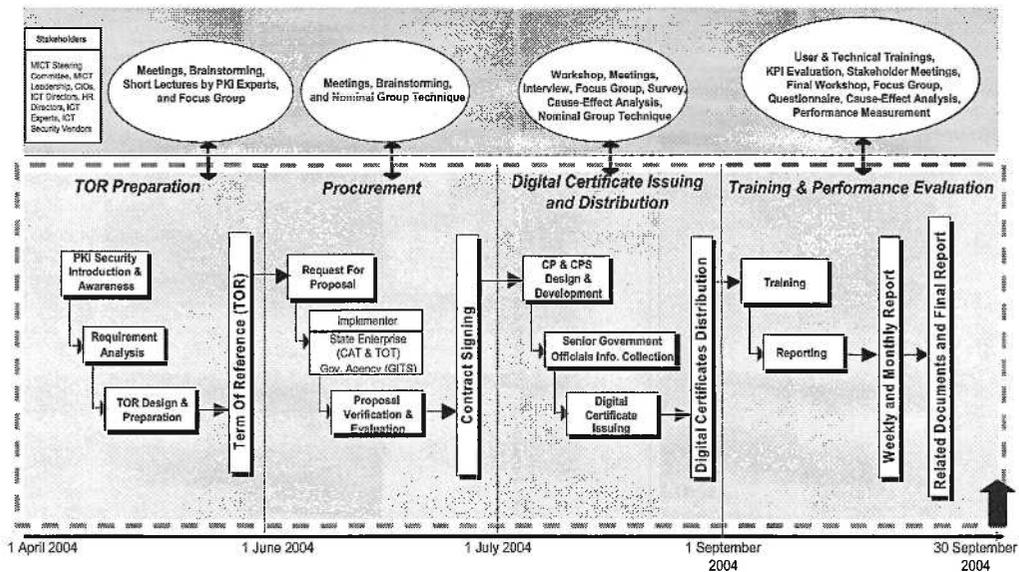
ure 3: Key Phases and Activities

Figure 4: Project Gantt Chart
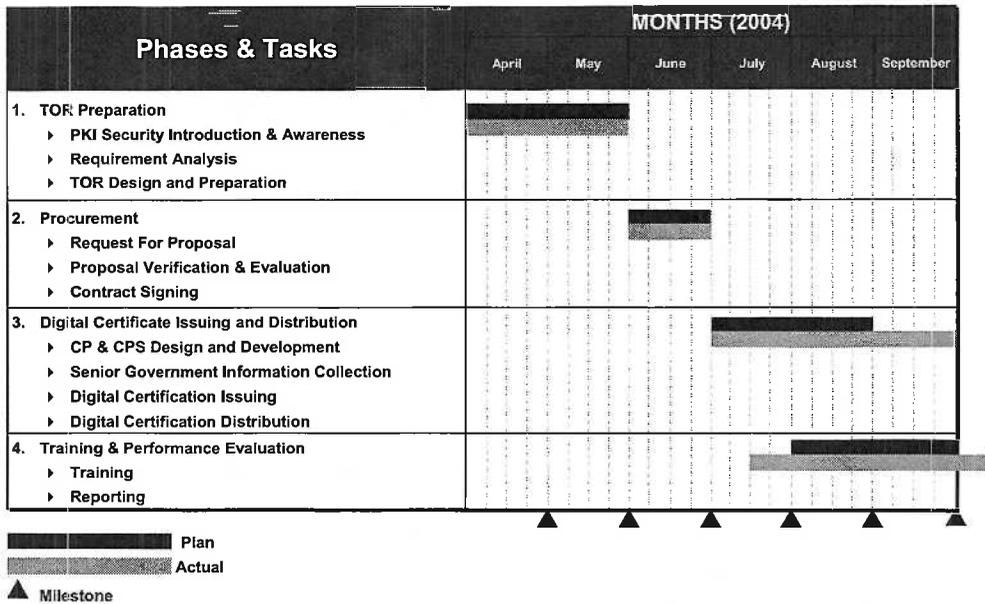
	Risk	Mitigation Strategy
Organizational and Change Management	▸ Lack of centralized leadership role to oversee the project and to coordinate cross-organizational efforts ▸ No comprehensive communications plan in place	▸ Strong leadership of the MICT Steering Committee to drive project ▸ Comprehensive communications developed and disseminated
Project Resources / Financial	▸ Lack of sufficient initial investment resources to realize project objectives ▸ Lack of sufficient ongoing budgetary support for Operations and Maintenance	▸ Accurate project cost estimates are developed and disseminated to ensure sufficient initial and on-going budgetary resources are obtained ▸ Budget allocated to address the action plans laid out in the strategy
Technical / Technology	▸ Insufficient technical infrastructure to support the project's objectives ▸ Complex technological and cross-organizational integration issues	▸ Technical Infrastructure upgrade costs are included in the e-Government project cost estimates ▸ The e-Government project established to develop government-wide standards
Business / Operational	▸ Lack of staff and users with the appropriate knowledge, skills and abilities ▸ Time limitation	▸ Training, workshops and instruction manuals are provided to key staff and users ▸ Good project management
Data / Information	▸ Electronic government information is not complete and not well defined, and cross-organizational information sharing standards are not defined	▸ Government-wide data standards are developed for inter-operability
Strategic	▸ Strategy has not been clearly defined and communicated	▸ Communications Plan developed to inform and educate all stakeholders on the progress / challenges of the implementation strategy

Figure 5: Risk Management

Durin the kick-off meeting of this project, a brief description for the need for this project and who should be members and the focal point of the steering committee was discussed. Then a decision concerning who would be project team members and the focal point was made. Additionally, the steering committee set up a communication plan with external stakeholders such as CIOs, director generals, ICT directors and HR directors from other ministries or other agencies. Figure 2 presents both internal and external stakeholders related to this project. The list of ministries and agencies involved in the project is presented in Table 1.

The major roles of MICT steering committee are to determine overall strategy direction, to allocate resources, to review progress on a weekly basis, to communicate strategic objectives and goals to all stakeholders, to approve re-calibration/reprioritization of change management initiatives as necessary, to review and intervene on issues which would impact the implementation schedule or cost, and to oversee coordination and integration with other ministries/agencies.

PROJECT PLAN AND SCHEDULE

Figure 3 shows four key phases and activities involved in each phase of this project. The first phase is TOR preparation which consists of three activities: PKI security introduction and awareness, requirement analysis, and TOR design and preparation. TOR is the output of this phase. The first activity "PKI security introduction and awareness" is very important since this project is concerned with digital certificates based on PKI which is one of the highly advanced technologies. As a result of this, the secretary of the steering committee invited PKI experts and PKI vendors to give short lectures about PKI to all members of the committee. In addition, the committee secretary organized site visits for the committee members to investigate certificate service providers in Thailand such as TOT, CAT Telecom and GITS (Government Information Technology Services), so that they could learn how they operate PKI/CA business. After that, the steering committee members shared opinions and knowledge, and had several discussions in many aspects. Finally, they knew what direction the project should go, and they chose to proceed in the outsourcing direction (Marchewka, 2006; Schwalbe, 2006). According to the project plan, this phase should start on 1st April 2004, and took for two months.

The second phase is procurement. Since there are a few companies in Thailand which provide PKI/CA services, after having the TOR, almost all members of the steering committee agreed that this project should use a special procurement procedure (i.e. not normal bidding). Consequently, the chair of the procurement committee sent three invitation letters attached with the TOR to two state enterprises: TOT and CAT Telecom, and one government agency, GITS, to request for proposal. After receiving the proposals submitted from CAT Telecom, TOT, and GITS, all members in the procurement committee verified and evaluated the proposals. The committee found that all three proposals complied with the TOR and the budget. As a consequence, three contacts were signed. The Nominal Group Technique (NGT) (Delbecq and Van de Van, 1971) was used in this phase. According to the project plan, this phase should start on 1st June 2004, and took for one month.

In the third phase, digital certificate issuing and distribution, three certificate service providers (TOT, CAT Telecom, and GITS) designed and developed Certificate Policy (CP) and Certificate Practice Statement (CPS), and then submitted them to the examination and acceptance committee to get approval. After getting approval, three certificate service providers proceed to design and distribute forms to all senior government officials (above the C7 level) for collecting personal information: first/given name, surname, position, organization, and email address. Such information would be parts of digital certificates. After obtaining such personal information, the Certificate Authority (CA) system of each of three certificate service providers (TOT, CAT Telecom, and GITS) would issue and securely deliver digital certificates to senior government officials. According to the project plan, this phase should start on 1st July 2004, and took for two months.

The last phase is training and performance evaluation. According to the project plan, this phase should start on 1st September 2004, and took for one month. In fact, during the third phase, the training activity already proceeded. There were both technical and user training courses. In Phase 3 and 4, three certificate service providers (TOT, CAT Telecom, and GITS) had to submit weekly reports to both the steering committee and the examination and acceptance committee, so that the committee members could monitor and manage the project. However, in the last phase, Phase 4, three certificate service providers submitted all related documents and official final reports; consequently the committee members could be able to evaluate the project performance.

PROJECT MONITORING

At the beginning of the implementation stage, the steering committee faced a problem that needed to be resolved. The problem was that the steering committee had to make a decision on who should be the authorized persons to verify and certify the personal information of senior government officials before CA (Certificate Authority) issued digital certificates for them. Every committee member was involved in this decision making process. There were three different opinions raised in the meeting, as follows:

(1) The human resource (HR) manager of each government department should be the person who verified the information of senior government officials working in the same department as the HR manager was. After verification, the information would be certified by the permanent secretary of the ministry, under which the department was.

(2) The HR manager had the same role as the first opinion, but after verification the information would be certified by the director of the department, in which senior government officials were working.

    (3) The HR manager of each government department would be the person who both verified and certified the information of senior government officials working in the same department as the HR manager was.

The panel was open for everyone to discuss in the possible ways to reach the final outcomes. In conclusion, the chairman made a final decision that the HR manager of each government department was the right person who had formally the full authorization to verify and certify the human resource information. Consequently, the secretary of the committee added this decision into the meeting minutes.

Figure 4 presents the project plan as a Gantt chart (Marchewka, 2006; Schwalbe, 2006). The dark blue bars represent the planned schedule, whereas the pink bars represent the actual progress. As shown in the Gantt chart, the actual progress of Phase 3 and 4 do not conform to the planned schedule. In Phase 3, there were problems in collecting English first name and English surname of some senior government officials, in collecting personal information of some senior government officials whose offices are located in rural areas, and in securely distributing digital certificates. In the last phase, Phase 4, the steering committee had found that training should start as early as they could in Phase 3. Therefore, the actual training moved to launch in Phase 3. Additionally, the receipt documents arrived the committee quite late. Consequently, the acceptance process took longer than the committee members foresaw.

PROJECT EVALUATION

In the first phase of the project, the steering committee defined the objectives, expected output and expected outcome which appear in TOR, and were used for performance evaluation. The project objectives were
- To issue digital certificates to senior government officials, and
- To promote senior government officials signing electronically e-mails so that electronic communication would be in a secure and trusted manner.

The project outputs were:
- Number of digital certificates issued to senior government officials by 30th September 2004,
- Number of senior government officials to be trained by 30th September 2004,
- Number of senior government officials electronically signing e-mails by 30th September 2004.

And the expected project outcome were:
- Building secure infrastructure for government network,
- Building PKI knowledge, skills and abilities for government officials, and
- Securing electronic information exchange among government officials.

Performance measures (financial, operating) were used to assess the impact of the strategic objectives on the overall performance over a period of time. Scorecards were used to measure ongoing performance against strategic plan commitments, as a tool to assess current results, to track progress towards future milestones and performance targets, and to start corrective actions where necessary (Kaplan and Norton, 1992; Kaplan and Norton, 1993). The committee had a regularly updated scorecard that is visible to the entire project. Throughout this project the committee had regular performance reviews that led to rewards and consequences when commitments were exceeded or not met.

During the performance evaluation process, the committee received a number of feedbacks which could be summarized as follows:
- No regulations supporting the use of electronic official documents and governmental e-services,
- Almost all government officials afraid of using digital certificates and digital signing because of lacking PKI understanding,
- Extending in future this project to cover more government officials, not only senior ones, due to the limited budget.

Since this project had a serious time limitation, the committee needed to have a good performance measurement, monitoring and management, and good management reporting.

RISK MANAGEMENT

In this project, risks could occur by internal and external factors. Consequently a risk analysis approach had been used to find the risk factors and cope with them (Boehm, 1991; Marchewka, 2006; Schwalbe, 2006).

The risks envisioned in this project could be categorized into six groups:
- Organizational and change management risks,
- Project resources/financial risks,
- Technical/Technology risks,
- Business/operational risks,
- Data/information risks,
- Strategic risks.

As a result of this, several steering committee meetings were conducted and finalized mitigation strategies for each group of risks. Figure 5 summarizes the risks related to this project, and how to mitigate these risks.

CONCLUSIONS

At the beginning of this project, the project team and almost all stakeholders involved in this project did not thoroughly understand these PKI technologies, and did not realize how importance of PKI and security implementation is. Therefore, knowledge and experiences were shared among all committee members and invited experts through weekly reports and meetings. In the meetings, topics of discussions included problems, performance, recommendations, and progress of work plan. Through this means, the knowledge and experiences of all committee members would increase, and consequently new ideas and comments were given in the following discussions. Reports and documents based on the knowledge and experiences gained from this project were prepared. In addition, more than three workshops were held to educate CIOs and senior government staff from almost all ministries about these technologies, and to exchange problems and experiences among participants. Finally they had improved their attitudes of PKI technologies and competence in order to reach strategic goals. In conclusion, PKI and security implementation has been very beneficial to senior officials in the ministry, especially improving the performance and security of using electronic communication and the Internet, and also creating new working culture - good governance and citizen participation.

REFERENCES

Adams, C., and Lloyd, S. (1999). Understanding Public-Key Infrastructure : Concepts, Standards, and Deployment Considerations. Macmillan Technical Publishing.

Ford, W., and Baum, M.S. (2001). Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption. Prentice Hall.

Marchewka, J. (2006). Information Technology Project Management: Providing Measureable Organizational Value. John Wiley & Sons.

Schwalbe, K. (2006). Information Technology Project Management. Thomson.

Delbecq, A and Van de Van, A. H. (1971) A Group Process Model for Identification and Program Planning. Journal of Applied Behavioral Sciences 7:466-492.

Kaplan, R. and Norton, D. (1992). The Balanced Scorecard: Measures that Drive Performance. Harvard Business Review (January-February): 71-79.

Kaplan, R. and Norton, D. (1993). Putting the Balanced Scorecard to Work. Harvard Business Review (September-October): 134-147.

Boehm, B. (1991). Software Risk Management: Principles and Practices. IEEE Software; 1, 32-41, January.