PKI Development in Thailand

Chaichana Mitrpant
Electronic Transactions Development Agency (Public Organization), Thailand
Increase the Volume and the Value by creating and strengthening application back-ends.
2002

Electronic Transactions Act B.E. 2544 became effective
First CA was set up under Government IT Services (Ministry of S&T)

2005

Electronic Transactions Commission approved the Trust model for Thailand.
The National Root CA is to be run by MICT

2009

Creation of Thailand PKI Association (http://www.thailandpki.org)

2011

NRCA role transferred to ETDA

2013

- Root Key Generation Ceremony
- MOU with private subordinate CAs and overseas CA
Beginning of Thailand National Root CA

Electronic Transaction Commission (ETC) approved the establishment of the Root CA as trust anchor of Thailand on July 18, 2005.
NRCA Development in Thailand

NRCA Phase 1
- Held seminar about NRCA operation
- Study in PKI field about
  - Certificate/CRL Profile
  - Guideline from foreign CA

NRCA Phase 2
- Held the training about PKI for gov. agency that related e-Logistics
- Held seminar about PKI and e-Logistics

NRCA Phase 3
- Study and develop Trust Mark
- Held seminar about PKI
- Improvement of NRCA CP/CPS
- Technical testing with Foreign CA (HK)

NRCA Phase 4
- Issue cert. to subordinated CA (Private CA)
- Preparation for certified the WebTrust std. (2 in 3 principle)
- NRCA CP/CPS Improvement

2007-2008
- Provide infrastructure for NRCA
- Make CP/CPS in the 1st draft

2008-2009
- Operate and MA NRCA system
- Domestic Interoperability Testing
- International Interoperability Testing (TW)

2010-2011
- Study the guideline for accredited CA from foreign CA
- Study how to bring NRCA certificate into MS Trust List

2011-2012
- Operate and MA NRCA system

Transferred to ETDA
Key Activities

**Thailand NRCA System**
- Infrastructure setup
- System has been operated following Trust Services Principles and Criteria for Certification Authorities (WebTrust)
- Audit pre-assessment is in progress

**Subordinate CA**
- MOU signing with CAT, TOT, TDID
- Interoperability testing
- Approach to Customs to perform impact analysis on migrating digital certificates to Thailand NRCA

**Overseas CA**
- MOU signing with Hong Kong Post
- Interoperability testing
- Cooperation with National Root CA of ASEAN member countries is under discussion
Certification Authorities in Thailand

Private Sector CAs
- CAT Telecom Public Company Limited (CAT)
- TOT Public Company Limited (TOT)
- Thai Digital ID Company Limited (TDID)

Public Sector CAs
- Anti-Money Laundering Office (AMLO)
- Bank of Thailand (BOT)
- Securities and Exchange Commission (SEC)
- Ministry of Finance
- Revenue Department
- Department of Provincial Administration
In 2013, The domestic CA Interoperability Test project was setup under NRCA

- Participants: Thailand NRCA, Subordinate CAs (CAT, TOT, Thai Digital ID)
- Trust Model: Hierarchical (Root CA)
- Testing Application: S/MIME
Cross-border CA Interoperability Test

In 2013: Thailand and Hong Kong

- Participants: Thailand NRCA, Hong Kong Post
- Trust Model: Cross Recognition
- Testing Application: S/MIME
PKI and e-Authentication Applications

- Image Cheque Clearing and Archive System (ICAS), Bank of Thailand
- National Single Window projects
- e-Payment System (PCC)
- Interbank Transaction Management and Exchange (ITMX)
- Bangkok Mass Transit Project, Office of Transport and Traffic Policy and Planning, Ministry of Transportation
- Paperless Customs project, Department of Customs, Ministry of Finance
- E-Passport project, Department of Consular Affairs, Ministry of Foreign Affairs
- Certificate for government officers, Ministry of Information and Communication Technology
Image Cheque Clearing & Archive System (ICAS)

- Hash/Fingerprint: to verify integrity of image cheque
- Digital Signature: to verify cheque data and non-repudiation of sending bank

Data Preparation

Capture + Data entry

Capture

Data entry

Gateway (Sending Bank)

Sending Bank

Gateway (Paying Bank)

Paying Bank

ICS

Image Cheque Clearing & Archive System (ICAS)
Image Cheque Clearing & Archive System (ICAS)
Image Cheque Clearing & Archive System (ICAS)
Securities and Exchange Commission

Company employee

Create eDoc

Authorized employee

Digitally sign

Header

Signature

<?xml ......>
<title> ...... </title>
<perion> ...... </period>
<year>......</year>
<detail>
รายงานฐานะการเงินของบริษัท ก. ประจ าไตรมาสที่ 4 ปี 2547
……………………
……………………
</detail>

Report submission

Acknowledgement

Validation results
National Single Window

1. Electronic Documents Exchange Hub
2. Regulation Mechanisms including costing and service level agreements
3. ICT Systems of Gov Agencies
4. ICT Infrastructure and Enabling Laws
5. Software Vendors and Value-Added Services
6. Traders and Logistics Providers

6 Key Components for Thailand SW e-Logistics Development

- Data Submission for e-Customs Declaration, e-Manifest, e-Permit, e-License, e-Certificates, etc.
- e-Payment (MICT/Banks)
- Back-end IT & Messaging Connectivity (MICT:PGA)
- Process Simplification - NESDB/PGA
- Data Harmonization - MICT & Customs
- Digital Signature/Certificate Authority (MICT:CAT:TOT)

* ebMS = e-Business Messaging Services
* DEP = One-Stop Exporter Service Dept. of Export Promotion

Port Authority Thailand
Air Port
Dept of Disease Control
Dept of Fisheries
Customs Dept
Dept Foreign Trade Government Agencies (29)
ASEAN Single Window Or other countries
Thailand PKI Association Opening and the seminar

“Key to Information Security of Thailand : Public Key Infrastructure”

5-6 August, 2009 at Stock Exchange of Thailand

Guest Speakers (Taiwan): ITRI, Taiwan CA Inc., CHT, Taiwan Stock Exchange
Background

- Many CAs in various countries in ASEAN have already started and developed their national PKI structure operations.

- **Problem:** A Lack of CA-CA interoperability among countries.

- **Solution:** The establishment of cross border working initiatives to develop a mutually agreement of inter-working PKI framework.

- There is a need to ensure that parties in different PKI domains can interoperate.
CA-CA Interoperability Project in ASEAN (Phase 1)

- **Objective:** To develop an appropriate CA-CA Interoperability framework for across PKI domains in ASEAN member states.

- **Scope:** Between 2 countries, focusing on technical issues.

Thailand invited Singapore to participate in this project because of its readiness and potential to take cooperative part in the project.

- **Appropriate Trust Model:** Certificate Trust List (CTL)

  - 2 models for testing:
    - ASEAN Trust Authority/ Local Trust Authority
  - Application used for the test:
    - S/MIME and Secure Sockets Layer (SSL)
  - Test Results:
    - 2 countries can be interoperable using Certificate Trust List (CTL) Model.
    - Test results were within expectations.
CA-CA Interoperability Project in ASEAN (Phase 2)

Phase 2 (2010)

- Workshop on CA-CA Interoperability among ASEAN member states

Objectives

- To organize workshop conference on CA-CA Interoperability Framework in ASEAN as well as discussion forum for sharing ideas among participants
- To explore PKI technology enhancement in ASEAN member states
- To promote the CA establishment in ASEAN member states

Venue

- August 5-6, 2010 at Siam City Hotel, Bangkok, Thailand
CA-CA Interoperability Project in ASEAN
(Phase 2)

Participants (Total 30)

- Invited speakers: economies that have success cases about different PKI trust models: Japan, EU, PAA, Singapore and Taiwan
- ASEAN Delegates

Considerations from the meeting

Issue#1: Legal recognition of foreign e-Signature

The meeting concluded that it was individual member state that could make the decision with the recognition of foreign electronic signature.

Issue#2: Recognition Criteria

The meeting recommended to set up a task force to create electronic signature recognition criteria as EU's and PAA's electronic signature documentation.

Issue#3: Interoperability Model

The meeting agreed that the Trust List model should be used in ASEAN and needed to consider the advantages vs. disadvantages of related standards such as the Certificate Trust List (CTL) of Microsoft, the Trusted List from EU, and etc.
CA-CA Interoperability Project in ASEAN  
(Phase 3)

Phase 3 (2012)

- Intra-ASEAN Secure Transaction Framework Project

Expected Outcomes

- Creating a technical framework that suits the ASEAN community's environment and how two-factor authentication could be utilized
- Updating legal status of electronic signature between ASEAN community

Methodology: Research

- A local research team with expert consultants will identify key issues related to the creation of the framework for Intra-ASEAN secure transaction based on the analysis of the following ground works:
  - Study of background information including standards, guideline, best practices, existing surveys,
  - Survey ASEAN member states' current status on the infrastructure supporting secure transactions.
PKI Survey in ASEAN

Objectives:
- To evaluate the PKI status of each country in ASEAN
- To encourage PKI cooperation within the ASEAN member states

Method: PKI Questionnaire
- Consist of 8 parts:
  - Personal Information
  - CA situation
  - PKI-enabled applications
  - Collaboration
  - Legal issues
  - PKI promotion
  - Obstacles of PKI implementation
  - PKI road map

The summary of questionnaire is based on information from 14 CAs in ASEAN, which provided by 7 out of 10 ASEAN member states.

7 member states consist of Malaysia, Myanmar, the Philippines, Singapore, Cambodia, Vietnam and Thailand.
PKI Survey in ASEAN

Types of Certificate in ASEAN

- Most CAs in ASEAN provide personal certificates, enterprise certificates and SSL certificates.

Key Utilization

- Single key (1-key pair) is mostly used in ASEAN.
- Dual key is only used with personal certificate and enterprise certificate.
PKI Survey in ASEAN

PKI-enabled Applications

- E-mail security and e-Passport applications are most widely used in ASEAN.
Obstacles of PKI Promotion

- The immature of PKI market and lack of PKI knowledge are the most important obstacles in ASEAN.

- Admissibility of e-Document in court
- Legal enforceability of e-Document
- e-Signature
- CA
- To Support e-Transactions
- e-Payment eServices
- Information Security
- The Royal Decree regulating Electronic Payment Services Business B.E. 2551 (2008) (the “ePayment Royal Decree”)

Functional Equivalent Approach
Technology Neutrality
Party Autonomy

To Support Cross Border e-Transactions
Draft of Electronic Transactions No. 3 Act B.E. ....

United Nations Convention on the Use of Electronic Communications in International Contracts

UNCITRAL Model Law on Electronic Commerce and Guide to Enactment 2001
UNCITRAL Model Law on Electronic Signatures and Guide to Enactment 2001
Law regarding PKI

Electronic Transactions Act B.E. 2544

- Laws Relating to e-Transactions
- Establishment of Electronic Transaction Commission (ETC)
Law regarding PKI

Electronic Transactions Act B.E. 2544

- Objective: To promote the reliability of the electronic transaction to enable them to have the same legal effect as that given to transactions made by traditional means.
- Status: effective in April 2002

Royal Decrees

- (Draft) CA Service Provider Regulation
- To certify the reliability of CA service providers
Sections Related to CA

Chapter 2: Electronic Signatures

• **Section 28:** CA shall
  — follow its CP and CPS
  — make sure information in certificates is accurate and complete
  — Provide means for relying party to validate information associated with a certificate
  — Utilize trustworthy systems, procedures and human resources in performing its services.

• **Section 29:** Trustworthy factors: financial and human resources, quality of hardware and software, procedures related to its services, availability of information on the signatories, regularity and extent of audit by an independent body, relevant certification (i.e., ISO 27001, WebTrust)

• **Section 31:** A certificate issued in a foreign country shall have the same legal effect as a certificate issued in the country if the level of reliability used in issuing such certificate is not lower than as prescribed in this Act.
Sections Related to CA

Chapter 3: Service Business Relating to Electronic Transactions

• **Section 32.** Service business relating to electronic transaction shall be subject to prior notification, registration or license. -> to be prescribed in a Royal Decree.

• **Section 33.** Notification, registration, licensing processes are to be specified in a Royal Decree.

• **Section 34.** CA compliance with the rules specified in licensing terms.
National Root CA: NRCA

Missions

2013
- System Setup
- Sub-CA Issuance
- Compliance with Intl. Standards

2014
- Link with Foreign CAs in ASEAN
- PKI Application Promotion & Training

2015
- Extend link to other regions

Moving forward to
- Increasing trustworthiness of CA (Register in Webtrust)
- PKI-application for e-Gov: e-Health, e-Court
- Laws to be enacted: CA regulation, Privacy law
Member Countries shall develop and implement their National Single Windows in a timely manner for the establishment of the ASEAN Single Window.

Number of Transactions via Thai National Single Window

June 2014

Date

Number of Messages + Digital Signature

From www.thainsw.net
Dream to See This Scenario Come True (AEC 2015)

ASEAN Single Window (ASW) Model
Prototype Flowchart Of Information Processing

- Customs
- OGAs
- Banking and Insurance Agency
- Transport Community
- Trading Community
- National Single Window
- International Link
- Secure Connectivity
- Customs Declaration/Duty
- Permit Approval
- Payment
- Manifest/ Vessel/Flight/ Handling Info
- Commercial Documents


9 National Single Windows
**Current Situation**

- Total Times to The import & Export Procedure: 8 days
- Current Semi-automatic approval for Checking Products
- Capital of the Procedure:
  - Import: 750 dollar
  - Export: 585 dollar
- Thai ranking: TOP 20

**Issues to be solved**

- Information Transfer Technology for B2G/G2B/B2B
- Improvement of law on NSW

**ETDA Proposes**

- Technology Standard & Security Standard
- Digital Signature

- ETDA is responsible for NRCA LAW
- To amend ETA
- To Draft New Regulations supporting NSW

**Goals**

- To reduce time frame for import & Export Procedure to be no more than 7 days
- Change to Fully-automatic approval

**Current Situation**

- 8 days
- 750 dollar
- 585 dollar
- TOP 20

**Goals**

- 7 days
- 750 dollar
- 585 dollar
- TOP 10

**Issues to be solved**

- Check product: 5%
- Reduce import & export procedure costs: 10%

**Goals**

- 5%
- 10%
- TOP
- 10
Core Principles of draft Royal Decree on rules and procedures for conducting electronic transactions for import, export, transit, and logistics through the National Single Window System B.E. ....

- Rules on information Security and data exchange standards through NSW
- Rules to supervise service providers (Gateway) in NSW

- Importance and High Volume of Data Interchange
- Due to the business’s role in confidence and reliability construction of data interchange
Thai business rules and the usage of message items must be complied with Regional guideline, CGI and ISO 20022.

NPMS is flexible for banks’ customisation which defined in Bank Guidelines. e.g. Tax Information and Remittance information.

Bank ID = CBID or BIC
Customer ID = Bank or Tax ID or BEI

Bank ID = BIC
Customer ID = BEI

BEI = Business Entity Identifier
BIC = Bank Identifier Code
CBID = Central Bank Code
TXID = Tax ID

ISO 20022 standard and business model (Message Definition Report: MDR)

Common Global Implementation guideline (CGI Template)

Regional guideline: ASEAN

National guidelines (NPMS)

NPMS Drafting committee

Financial Institutions

Derived From

Consistent With

Working Committee on Payment and Settlement System (WCPSS)

CGI Forum
Messaging Standard for enable STP

NPMS’s future messages

- FI-to-FI
  - Payment Clearing and Settlement
  - pac.008 / pac.002
- Low Value Transfer
- SMART
- High Value Transfer
- BAHTNET

4 customer-to-FI Payment messages defined by ISO 200222: NPMS

* C = customer
  FI = Financial Institution
Organizations adopting NPMS in Thailand

Commercial Banks
1. Bangkok Bank PCL
2. Kasikornbank PCL
3. Krung Thai Bank PCL
4. Siam Commercial Bank PCL
5. Citibank, N.A. (Bangkok Branch)
6. Standard Chartered Bank (Thai) PCL
7. CIMB Thai Bank PCL
8. Bank of Ayudhya PCL
9. Thai Military Bank PCL
10. Sumitomo Mitsui Banking Corporation (Bangkok Branch)
11. The Hongkong and Shanghai Banking Corporation Limited
12. Deutsche Bank AG (Bangkok Branch)
13. Mizuho Corporate Bank Limited (Bangkok Branch)

Government Agencies
14. The Customs Department
15. Office of the Rubber Replanting Aid Fund

Corporates
16. Bangkok Smartcard System Company Limited
17. SCG Chemicals Company Limited

Organizations planning to adopt NPMS
18. – 19. Two of customer of Bangkok banks
20. Bank of Tokyo Mitsubishi UFJ (Bangkok branch)
21. Kiatnakin Bank PCL
22. Government Housing Bank
23. Government Savings Bank

In Total 23 Organisations
Email: chaichana@etda.or.th
http://www.etda.or.th
Standard & policy drivers

Payment System Committee

Sub-committee on e-Transaction Standard

Electronic Transaction Commission

Policy & Plan

ETDA Executive Board of Director

NPMS Drafting Committee

NPMS Drafting Committee

BOT+ ETDA + Related stakeholders

Guidance & Standard

NPMS users

ETDA Executive Board of Director

NPMS Drafting Committee

BOT+ ETDA + Related stakeholders

Guidance & Standard

Business requirements

Thailand Payment Market Practice Group

Banks, Corporates, Payment service providers and Standard experts

Public Authorities

Guidance & Standard

ETDA Executive Board of Director

NPMS users

Providers e.g. NITMX / BAHTNET

41
Thailand Payments Market Practice Group (TH-PMPG)

- Specialist
- Banks
- Non-banks
- Corporates
- OGA

**TH-PMPG**

**Benefit**

- Discuss and solve market practice issues and possible impacts
- Review and testing the use of standards
- Propose and recommend implementation guideline
- Promote the use of standards and guideline among the members
- New business services
- Monetary support & compensation
- NPMS Award program and accreditation

**TH-PMPG**

**Benefit**

- Discuss and solve market practice issues and possible impacts
- Review and testing the use of standards
- Propose and recommend implementation guideline
- Promote the use of standards and guideline among the members
- New business services
- Monetary support & compensation
- NPMS Award program and accreditation