Introduction to PKI

November, 2006

Kang, Young-Chul
CEO of KICA,
BAWG Leader of Asia PKI Forum
(asia44@signgate.com)
List of Contents

1. PKI Overview
2. The Status of PKI in Korea and Applications
3. PKI based e-Procurement
4. Introduction to KICA
1. PKI Overview
On the Internet, Nobody knows you’re a dog

"On the Internet, nobody knows you’re a dog."
1.1 e-Commerce Market Size in Korea

- **Rapidly expanding area**
- **Reach to 27.5% of total trading volume in 2005**

**Source:** e-Commerce statistics (2005 Korea National Statistical Office)
1.2 Increase of Cyber Crime in Korea

![Bar chart showing the increase of cyber crime from 2001 to 2005.]

Source: Cyber Terror Response Center

- Cyber Crime Types
  - Hacking (Intrusion, Data Theft, Dos Attack), Virus, Fraud, Defamation

www.signgate.com copyright@1999-2006 KICA,Inc.
1.3 Issued problems of e-Commerce

Online characteristics

- Remote connection & no face to face contact
- Difficult to verify who does issue transactions
- Difficult to prove ‘transaction was happened’

- Risk of breach about transactions and personal profile
- Difficult to secure transmitted contents
- Easy to make forgery document / Difficult to prove electrical document is in original state
1.4 Possible Security Holes

- Breach of personal profile and credit card information at transaction
- Breach of personal profile in shared computer
- Cyber stealing
- Hacking on cyber securities & bank account / Stock price manipulation
- ID and password stealing

Need of Strong Security Protection with PKI technology
1.5 PKI Solution to Hacking attempts

**Problem**
- Difficult to verify identity
- Easy to make forgery or modification on contents
- Repudiate transactions
- Breach information

**Matched security method**
- Authentication of identity
- Guarantee Integrity
- Non-repudiation
- Confidentiality

**Protection Technology**
- Digital Signature Technology (User authentication)
- Digital Signature Technology (Message authentication)
- Digital Signature Technology (Message authentication)
- Encryption Technology (Message authentication)
1.6 PKI (Public Key Infrastructure)?

**Definition**
A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

**Elements of PKI**
- Certificate System: CA, RA, DS, OCSP, TSA
- Service Policy: CPS (Certification Practices Statement)
- PKI Application: e-tax, e-bank, e-trade
1.7 PKI System

Admin: Administrator Program
Clients: Client S/W
CA: Certificate Authority Server
RA: Registration Authority Server
DS: Directory Server
OCSP: Online Certificate Status Protocol Server
VA: Validation Authority Server
HSM: Hardware Security Module (Accelerator)
TS: Time Stamp Module
TSA: Time Stamp Authority Server
DVCS: Data Validation Certification Server
KRS: Key Roaming Server
Etc.: Other Service Server
※ All networks and servers are double connected (Fault Tolerant)
Definition

Digital signature is an unique digital data; it is applied to a document keeping the unique information of the signer with the digital signature creation key and make it possible to verify the entity authentication of document and whether there was modifications or not.

It is not an Electronic signature but a Digital signature.
## 1.9 Comparison

<table>
<thead>
<tr>
<th>Concept</th>
<th>Electronic Signature</th>
<th>Digital Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concept</strong></td>
<td>Electronic data as an identifier</td>
<td>Digital signature using asymmetric encryption / decryption method</td>
</tr>
<tr>
<td><strong>Problem</strong></td>
<td>Reusable</td>
<td>Impossible to reuse</td>
</tr>
<tr>
<td><strong>No forgery</strong></td>
<td>Can’t make a signed document without a private key</td>
<td></td>
</tr>
<tr>
<td><strong>No modification</strong></td>
<td>Can’t modify the signed document without the private key</td>
<td></td>
</tr>
<tr>
<td><strong>Entity Authentication</strong></td>
<td>The private key holder is the maker of the document</td>
<td></td>
</tr>
<tr>
<td><strong>No reuse</strong></td>
<td>Can’t substitute the digital signature of “A” document to “B”</td>
<td></td>
</tr>
<tr>
<td><strong>Non-repudiation</strong></td>
<td>Can’t repudiate signing of the private key holder</td>
<td></td>
</tr>
</tbody>
</table>

- Encryption/Decryption Type: RSA, DSS (Digital Signature Standard), ESIGN, Schnorr, KCDSA
## 1.10 Feature of electronic document

<table>
<thead>
<tr>
<th>ITEM</th>
<th>Paper document</th>
<th>Electronic document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>Paper</td>
<td>Digital media</td>
</tr>
<tr>
<td>Delivery</td>
<td>Mail, hand over</td>
<td>Network transmission</td>
</tr>
<tr>
<td>Safety of contents</td>
<td>Difficult to make forgery document or to modify</td>
<td>Easy to make forgery document or modification</td>
</tr>
<tr>
<td></td>
<td>Identification possible from physical characteristics of paper</td>
<td>Impossible to acknowledge forgery</td>
</tr>
<tr>
<td>Entity Authentication</td>
<td>Handwriting signature, Seal</td>
<td>Digital Signature</td>
</tr>
</tbody>
</table>
1.11 Functions of Digital Signature

Confidentiality

Integrity

Encryption

Hacker (Tapping)

Source Authentication

Entity Authentication

Non-Repudiation

※ Pictures are taken from the CryptMail User’s Guide, Copyright (C) 1994 Utimaco Belgium, with the kind permission of Kurt Schoenmaekers, Managing Director.
2. The Status of PKI in Korea and Applications
# 2.1 Related Digital Signature Law

<table>
<thead>
<tr>
<th>Name of Act</th>
<th>The ministry and office concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Signature Act</td>
<td>Ministry of Information and Communication (MIC)</td>
</tr>
<tr>
<td>Information and Communications Work Business Act</td>
<td>Ministry of Information and Communication (MIC)</td>
</tr>
<tr>
<td>Electronic Government Act</td>
<td>Ministry of Government Administration and Home Affairs (MOGAHA)</td>
</tr>
<tr>
<td>Framework Act on Electronic Transaction</td>
<td>Ministry of Commerce, Industry and Energy (MOCIE)</td>
</tr>
<tr>
<td>Consumer Protection in Electronic Commerce, etc. Act</td>
<td>Fair Trade Commission (FTC)</td>
</tr>
</tbody>
</table>

[Personal Information Protection Act] Enactment Propulsion
2.2 Electronic Signature Act (1/4)

Purpose of Enactment

Digital Message

- Promote usage of Digital documents
- Guarantee safety & trust

- Grant legal validity on certified digital signature
- Enhance comport level of nation people & boost national infrastructure construction
2.2 Electronic Signature Act (2/4)

Main Focus

Article 3 (Effect, etc., of Digital Signature)

(1) Signature, signature and seal, or name and seal, it shall be deemed that such requirements are satisfied
(2) Signer of the electronic message concerned and that there has been no alteration in contents of such message

Authentication, Confidentiality, Non-repudiation, Integrity

Grant legal validity on certified digital signature
2.2 Electronic Signature Act (3/4)

Main Focus

Article 4 (Designation of Accredited Certification Authority)

(1) Designation as a accredited certification authority an entity that is deemed to be capable of performing authorized certification work in a secure and reliable manner

Secure Technology, Physical environment, Financial capability

Guarantee safety & trust
2.2 Electronic Signature Act (4/4)

Main Focus

Article 26(A Liability of reparation)

- Reparation for Injury
- Imputation a reason to party
- Burden of proof to licensed CA

Duty of Insurance

Protection of subscriber & User
2.3 Root CA Architecture in Korea

Digital Signature Authentication Management System

- MIC (Policy Agency)
  - Law. System arrangement
  - Plan national authentication
  - Licensed CA management

- KISA (Root CA)
  - National Authentication system operation
  - Field test for licensed CA designation
  - Issue certificate for licensed CA

- Accredited CA
  - Authentication management
  - Provide CA service
  - Certificate issuance
  - Certificate termination / renewal

Government

Root CA

Digital Signature Authentication Management Center

Licensed CA

Korea Information Security Agency

1st 2nd 3rd 4th 5th 6th

KICA KOSCOM KFTC NIA CROSSCERT KTNET

MIC (Policy Agency)

KISA (Root CA)

Accredited CA
### 2.4 Types of Accredited Certificate

<table>
<thead>
<tr>
<th>Types</th>
<th>Entity</th>
<th>Certificate Usage Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Individual</td>
<td>All electronic transactions</td>
</tr>
<tr>
<td></td>
<td>Corporation</td>
<td>All electronic transactions</td>
</tr>
<tr>
<td>Specific</td>
<td>-</td>
<td>G2C, Bank, Insurance</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>G2C, Stock, Insurance</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>G4C, Credit Card</td>
</tr>
</tbody>
</table>
2.5 Number of Accredited Certificate

(Scale: number)

Number of annual issuance of certificates (As of April 30, 2006; published by MIC)
2.6 Applied Areas of PKI in Korea

- Internet Banking
- Online Stock Trading
- E-Government system
- E-Contract
- E-Tax Receipt system
- etc Purpose
2.6.1 PKI BM in e-Government

Petition Service
(Identify oneself online by certificates)

Personal Management inside Government
- All employees inside Government

Digital Signature & Seal
- Distribute certificates
- Develop and enhance system adopting certificates

E-Supply (G2B)
(Online bidding with certificate)

Enhance computerization
- Sharing national resource information

4 Major Insurances data exchange
(Labor, Medical care, Pension, Industrial disaster)
Internet access with certificate

Regional Administration
- Service for counties
- Access with certificates

Taxation
- National Tax Agency
- Access with certificates

National Financing Information System
- Based on Internet banking, etc

Electric document system
- Interoperable with other systems

Education Administration System
- 16 Educational department
- Teachers can assess with cert.

www.signgate.com copyright@1999-2006 KICA, Inc.
2.6.2 Internet Banking

- Request account information
- Currency transfer
- Payment, etc.
(Should submit digital signature: Mandatory)

Clients

PKI Client S/W

Internet

Bank

Certificate Validation

PKI Server S/W

Banking Server

Accredited CA
(CA & OCSP Server)

Issue Certificate

security card

PKI Client S/W

Keyboard Security S/W
2.6.3 Home Tax Service

Accredited CA

Issue Certificate

Certificate validity authentication, Verify the data integrity

Internet

Taxpayer

PKI Client S/W

► Query tax information
► Declare tax
► Pay tax, etc.

National Tax Service

Home Tax Server

PKI Server S/W
2.6.4 Education Service

- Query education information
- Input records
- Issue petition, etc.

PKI Server S/W

PKI Client S/W

Accredited CA

Certificate validation

National Education Information System

Internet

Teachers

Students

Parents

Issue Certificate
3. PKI based e-Procurement
3.1 Need of e-Procurement system

Need PKI System

- Complex & Time Consuming
- Handy Work process making Mistakes (Negative)
- Difficult & Inefficiency
- Tons of documents
3.2 Structure of E-Procurement system

- E-Procurement Security Using PKI system

Certificate Authority

- Issue Certificate

User

Digital signature creation and transmission
(Encrypt document + Digital signature + Certificate)

E-Procurement system

- Timestamp Service
- Certification Service
3.3 Benefit of E-Procurement system

- **Effectiveness of PKI**

- **Evaluation of online document integrity**
- **Bidding applicant Company identity authentication**
- **Keeping dead line By time Stamping**
- **Bidding Non-repudiation**

**KONEPS**

KICA e-Bidding Server
With security add-on for Web Application Server
4. Introduction to KICA
4.1 KICA Establishment

Stage 1 ▶
Enforcement of laws and institutions
- Enacted “Electronic Signature Act.”
- Established “Korea Information Certificate Authority Inc.”

Stage 2 ▶
Approved by MIC as the first accredited CA
- Major Shareholders: MIC, Samsung SDS, LG, KT, SK Telecom, DAOU Tech, etc.
- Provide accredited CA services to various applications

February 10, 2000 Designated Accredited CA

Total USD 22M of Capital

Majority Shareholders: 84.15%
Stock Ownership Association: 6.54%
Minority Shareholders: 9.31%
## 4.2 Brief History

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
</table>
| 2006 | 04 Conducted PKI feasibility studies consulting (Philippines, Egypt, Vietnam)  
|      | 01 Developed linux based banking system and applied to ePost banking service |
| 2005 | 04 Launched OnePASS (Instead of NID Number) Service  
|      | 01 The NiS recognized our PKI solution as satisfactory conditions |
| 2004 | 12 Awarded the first prize by the Minister of Information and Communication  
|      | 10 Company granted ISMS (Information Security Management System) certification |
| 2003 | 12 Awarded a special prize in the second Information Security Award  
|      | 07 Passed the quality test of Wireless PKI CA system for SKT |
| 2002 | 12 Participated Hong Kong ITU Telecom ASIA 2002 as an exhibitor  
|      | 11 Provided e-Petition service to major 4 national insurers  
|      | 04 Provided licensed certificate to ‘Home tax service’ of National Tax Service  
|      | 03 Provided the 1st wireless PKI Certificate Authority service in the world |
| 2001 | 12 Certificate Authority service for the Internet banking of the Korea Post  
|      | 10 MOU with Digicert In Malaysia about interoperability, MOU with ID Safe in Singapore about interoperability  
|      | 08 Assigned as a Venture Company, Mr.Kang Young Chul appointed as the second CEO  
|      | 05 Signed Cooperation Agreement with Hong Kong Post for Global Interoperability  
|      | 01 Signed Wireless Certificate Partnership Agreements with KTF and KTm.com |
| 2000 | 11 Provided CA Service to Public Procurement Service for Electronic Bidding System  
|      | 10 World’s the first provision of Certification Authority Service to ASEM (Asia-Europe Meeting)  
|      | 06 Provided Certification Authority Service to Public Agency for Electronic Tax Payment System  
|      | 02 Approved by MIC as the first Accredited Certification Authority |
| 1999 | 07 Completed Construction of ‘signGATE’ Certification Center at Korea Information Certificate Authority Inc.  

www.signgate.com copyright@1999-2006 KICA,Inc.
4.3 Business Scope

PKI Technologies

Services
- Issuing Certificates (wired/wireless)
- Time Stamping
- Device Authentication
- i-PIN Service
- Domain hosting, …etc.

Solutions
- SignGATE CA System
- SignGATE TrustTax
- SignGATE Contract
- Crypto Toolkit (C, Java, XML)
- SignGATE EWS, …etc.

Global Business
- Cooperation MOU (China, Taiwan, HongKong, etc.)
- PKI Consulting
- Asia PKI Forum
# 4.5 Major Customers

<table>
<thead>
<tr>
<th>Model</th>
<th>Customers</th>
<th>Model</th>
<th>Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-Procurement</td>
<td>MND (Ministry of National Defense), PPS (Public Procurement Service), KEPCO, SKT, KTF, ... etc. (over 20 companies)</td>
<td>EDI for medical service</td>
<td>KT, DACOM, S1</td>
</tr>
<tr>
<td>e-Marketplace</td>
<td>Samsung Heavy Industries, Hyundai Heavy Industries, ... etc.</td>
<td>e-Warranty Service</td>
<td>ECFC (Electronic Contractors’ Financial Cooperative), CG (Construction Guarantee)</td>
</tr>
<tr>
<td>Digital Contract</td>
<td>KDC (Korea Development Cooperation), Kolon Engineering &amp; Construction, ... etc.</td>
<td>Internet Banking</td>
<td>MIC e-POST, Standard Chartered First Bank, Korea Exchange Bank, Woori Bank</td>
</tr>
<tr>
<td>e-Tax Service</td>
<td>LG Electronics, Lotte Department Store, Lotte Magnet, Sinshege Department Store, E-mart, Hyundai Department Store, ... etc.</td>
<td>Internet Insurance</td>
<td>Almost all insurance companies</td>
</tr>
<tr>
<td>Internet Shopping</td>
<td>Hansal CSN, InterPark, Auction, ... etc.</td>
<td>Internet Lottery</td>
<td>KRA (Korea Racing Agency)</td>
</tr>
<tr>
<td>Online Civil Service</td>
<td>Beyond Networks (SI Company), Local Governmental Office (Seo-Cho, Song-Pa, Gang-Nam Gu...etc.)</td>
<td>e-Marketplace for medicine</td>
<td>KT Medilinks, En2B</td>
</tr>
<tr>
<td>Home-Tax Service</td>
<td>NTS (National Tax Service), Pusan province office</td>
<td>e-Prescription</td>
<td>Ilsan Hospital, KT Medilinks, ... etc.</td>
</tr>
<tr>
<td>Others</td>
<td>Korail, KRIHS (Korea Research Institute for Human Settlements)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

More 200 major companies are customers of KICA
4.4 Strengths of KICA

Service Know-how
- No failure in service for 6 years
- Operational regulations
- Full sets of service utilities

Best Solutions
- Verified solutions in the field
- Well-prepared additional solutions
- 100% comply with international Standards

Total Solutions
- Hardware
- Software (applications)
- PKI Systems
- Network/System security facilities, ...

Ready To Transfer
- Be able to transfer the knowledge of PKI systems
- Provide source code and relevant documents
4.6 Establishment of PKI (1/3)

To establish safe and reliable Information society

Establishment Law (Electronic Signature), PKI Standards
Building PKI Center
Developing PKI enabled Applications

Government

PKI Model

Root CA

Accredited CA

Accredited Certificate

Application Service organizations or companies

Accredited Electronic Signature

Clients

Law, Policy, Standards
Certification Service
E-procurement, Internet Banking, E-commerce, etc

www.signgate.com copyright@1999-2006 KICA,Inc.
4.6 Establishment of PKI (2/3)

- Implementation Steps of PKI

**Phase 1. Preparations**
- Designing of PKI scheme
- Launching of PKI TFT
- Finding ways to finance

**Phase 2. Law & Regulation Setup**
- Setup decree (D.S)
- PKI Standardization

**Phase 3. PKI Center Construction**
- PKI systems
- Facilities / Equipment
- Operation guideline

**Phase 4. Education & Promotion**
- Education & Training
- Development of Promotional policies

**Phase 5. PKI Application Development**
- Pilot project
- RA Constructions
- Planning of long-term National PKI services
4.6 Establishment of PKI (3/3)

- **Estimated Cost for PKI**
  - Budget: Approximately **USD 7 million**
  - Time Cost: About to 6 Months

- **Root CA Center**
  - PKI System for root CA
  - Basic Facilities and Equipment

- **PKI Center**
  - Accredited CA Systems
  - Facilities and Equipment

- **Branch RA Construction**
  - RA Software / Hardware
  - Other Equipment (Smartcard)

- **Consulting**
  - Law & Regulation Setup
  - Accreditation & Auditing Details
  - Promotion Strategy

- **Education & Training**
  - Training for Operators (including operational know-how)
  - Education for Developers
  - Education for Manager

- **Establishment of National PKI**

**Budget**: Approximately **USD 7 million**

**Time Cost**: About to 6 Months
Thank you!