Korea National PKI status and Directions for Market Promotion

2009. 3

JinSoo Lim,
IT Infrastructure Protection Division
Korea Certification Authority Central
Email: jslim@kisa.or.kr

Korea Certification Authority Central
Contents

Overview
PKI Policy
Certificate Promotion
PKI Business Models
PKI Cost Policy
Future Work
Overview
Overview

National PKI
- Established in 1999 under the Electronic Signature Act
- Competent Authority: MOPAS
- Root CA: KISA (Korea Information Security Agency)
- Main Customer: Individual, Company

Government PKI
- Established in 2001 under the E-Government Act
- Competent Authority: MOPAS
- Root CA: GCMA (Government Certification Management Authority)
- Main Customer: Public Servants

※ MOPAS (Ministry of Public Administration and Security)
Overview

Electronic Signature Act

- Ensure the security and reliability of electronic documents and to promote their use
- Promoting nationwide informationalization and improving convenience in people's living standard

Electronic Signature Act, Decree and Ordinance

- CA accreditation
- Accredited CA’s Operation
- Accredited CA’s Protection measure
- Accredited CA’s CPS

Regulation on Accredited CA’s Facility and Equipment
Guideline for Certification Practice
Regulation on Accredited CA’s protective measures
Accredited CPS Framework

Technical Specification
Overview

Accredited CA

- 5 CA are accredited by MOPAS until now

<table>
<thead>
<tr>
<th>Accredited CA</th>
<th>Accredited Date</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG</td>
<td>2000. 02. 10</td>
<td><a href="http://www.signgate.com">http://www.signgate.com</a></td>
</tr>
<tr>
<td>SignKorea Certification Authority</td>
<td>2000. 02. 10</td>
<td><a href="http://www.signkorea.co.kr">http://www.signkorea.co.kr</a></td>
</tr>
<tr>
<td>yessign</td>
<td>2000. 04. 12</td>
<td><a href="http://www.yessign.com">http://www.yessign.com</a></td>
</tr>
<tr>
<td>CrossCert</td>
<td>2001. 11. 24</td>
<td><a href="http://www.crosscert.com">http://www.crosscert.com</a></td>
</tr>
<tr>
<td>TRADESIGN.net Digital Certificate</td>
<td>2002. 03. 11</td>
<td><a href="http://www.tradesign.net">http://www.tradesign.net</a></td>
</tr>
</tbody>
</table>
Overview

Accredited CA

- 5 Accredited CAs issued accredited certificate to subscriber around 18 million in total

Accredited Certificate Subscriber (Unit: Million)
PKI Policy
PKI Policy

Accreditation Requirement

- Financial Capability
  - Capital: More than 8 million US dollars
- Personnel Capability
  - Personnel: More than 12 persons for CA operation
- Facilities and Equipments
  - Subscriber Registration, Key Management, Certificate Management, Subscriber’s S/W and Security Operation Procedure

CA Accreditation Renewal

- Accreditation is valid for 2 years
- Apply for MOPAS no later than 30 days before its expiration
PKI Policy

Accreditation Procedure

Applicant

Request CA Accreditation

Grant Accreditation

MOPAS
- Document Receipt
- Document Review
- Actual Examination
- Evaluation & Decision

Report the result

KISA
- Actual examination

Actual Examination Delegation
KISA audit the Accredited CA operation every year
- Confirm whether the CA managed their operation securely
- KISA provides self-assessment guideline to accredited CA

Accredited CAs

Apply for Audit

Auditing

Audit Criteria
- Guideline on Electronic Signature Certification Practices
- Guideline on Accredited CA’s protective measures

KISA

Submit Audit results

MOPAS
PKI Policy

PKI Interoperability

- Interoperability pilot project between Korea, Japan, Singapore and Taiwan ('01 ~ '03)
- Developing the certificate profile applicable in e-trade ('02.4)
- Developing the interoperable API among the e-trade S/W ('03.9)
- Domestic interoperability of a certificate ('02.4 ~ '03.9)
- Interoperability between National PKI and Government PKI ('02.4)
  - NPKI certificate can be used to e-Government services
- Interoperability among the accredited CA ('03.9)
PKI Business Model
19 Banks and Post Office provide internet banking service based on accredited certificate

Internet banking users must use the accredited certificate for secure online transaction (’02. 9)
Credit card should be used with accredited certificate to enhance the security of electronic payment process.

Regarding the transaction of over 300,000 won in Internet shopping, purchasers are required to use accredited certificate ('05. 11)
Security corporations provide online stock service based on the accredited certificate.

Online stock users must use the accredited certificate for secure online transaction ('03. 3)
PKI Business Models

- Housing subscription deposit system, Education, Medical information, e-bidding ('06)
- Housing subscription, the year-end tax adjustment, NEIS, National health Insurance, etc.

YesOne (The year-end tax adjustment web site)
NEIS (National Education Information System)
PKI Business Models

Mobile Banking

- Mobile banking service with certificate ('07~)
- Transferring a certificate from PC to mobile phone
- Generating electronic signature in mobile phone

Certificate Management S/W in Mobile Phone
Certificate Promotion
Electronic signature promotion with Seminars and Meetings

- Hold a PKI Seminar (PKI-KR) to share successful cases of electronic signature and technical issues in PKI
- Hold meetings with small size companies to introduce successful cases and electronic signature use
Certificate Promotion

Asia PKI Consortium

- Introduce the status of Asia country’s information security system, technique and policy
- Changing the name of APKI Forum with APKI Consortium (’07. 11)
- The field of activity is enlarged from PKI to information security

[Image of a meeting]
Certificate Promotion

- Release leaflets, posters and stickers for electronic signature use to Banks, Public Offices, etc.
- Published teaching materials for using accredited certificate and release them to major information education facilities.
Certificate Promotion

Enlarging the Certificate Use

Inclusion KISA Root CA Certificate in Web Browsers (~'08)
- Internet Explorer ('06.02), Safari ['07.03], Opera ('08.05), FireFox ('06~)
Certificate Promotion

Enlarging the Certificate Use

- Web server, Digital Contents ('06 ~ '07)
- SSL Server Certificate, Code Signing Certificate, Secure e-mail Certificate, etc

SSL Server Certificate
PKI Cost Policy
PKI Cost Policy

PKI Market Status

1.85 million certificates were issued until end of 2008

77% of Korean economical active population (2.4 million) is using certificates

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of certificates subscribers</th>
<th>Size of PKI Market</th>
</tr>
</thead>
<tbody>
<tr>
<td>'04</td>
<td>950</td>
<td>238</td>
</tr>
<tr>
<td>'05</td>
<td>1100</td>
<td>243</td>
</tr>
<tr>
<td>'06</td>
<td>1438</td>
<td>324</td>
</tr>
<tr>
<td>'07</td>
<td>1716</td>
<td>398</td>
</tr>
<tr>
<td>'08</td>
<td>1850</td>
<td></td>
</tr>
</tbody>
</table>
PKI Cost Policy

- Internet banking subscriber became 52.6 million at 2008
- 12.8 million certificates were issued for Internet banking at 2008
- 3.3 million Money transactions and 22.8 billion USD was transferred through Internet banking by using certificates at 2008
Most of certificates usages are Internet banking, credit card, online stocks and etc.
PKI Policy

Cost Policy

♦ Charging for Certificate ('04.9)
  ♦ Ensure finances to invest in new technology services and to improve profit structures for CA
    - Individual: 4,400 KRW (≒ 4.4 USD)
    - Corporation: 110,000 KRW (≒ 110 USD)

♦ Enforce a obligation to insurance joining of CA ('06. 7)
  ♦ Reinforce the certificate user protection against the e-transaction accidents
PKI Cost Policy

Issue of Cost Policy

- The actual benefits of certificates goes to service providers
  - But, it is the certificate users who are paying for the services

- Changing the cost policy is being issued
  - Proposal of changing the cost policy of certificates are also be issued
  - By charging validation service to service providers, such as Internet banking, insurance, on-line stocks and etc., instead of user certificates
Future Work
Future Work

Establishing a reliable u-Authentication System

- Extending the authentication means to Biometric, OTP with PKI certificate
- Extending the authentication object to devices
Future Work

- HSM Token as a secure storage ('06~)
  - Developing the technical specifications for HSM Token with certificate ('06~'07.8)
  - Carrying out the evaluation for the interoperability of HSM Token ('07.9~)
- USIM as a secure mobile storage ('08~)
  * HSM : Hardware Security Module
  * USIM : Universal Subscriber Identification Module
Future Work

The Prospects of Korea PKI Market

- Maintain PKI market growth by strengthening certificate safety, expanding the certificate usage and etc.

- Prepare the foundation of maintaining market growth by examining conversion of cost policy and etc.

- Developing new PKI business model
  - Issuing device certificates for manufacturers by constructing u-Authentication system for Ubiquitous society
Thank You

JinSoo Lim,
IT Infrastructure Protection Division
Korea Certification Authority Central
Email: jslim@kisa.or.kr