

**Regional Seminar on Costs and Tariffs for Member Countries of the
Regional Group for Asia and Oceania (SG3RG-AO) (former TAS Group)**

Hanoi, Vietnam, March 4-6, 2009

Document 7

**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

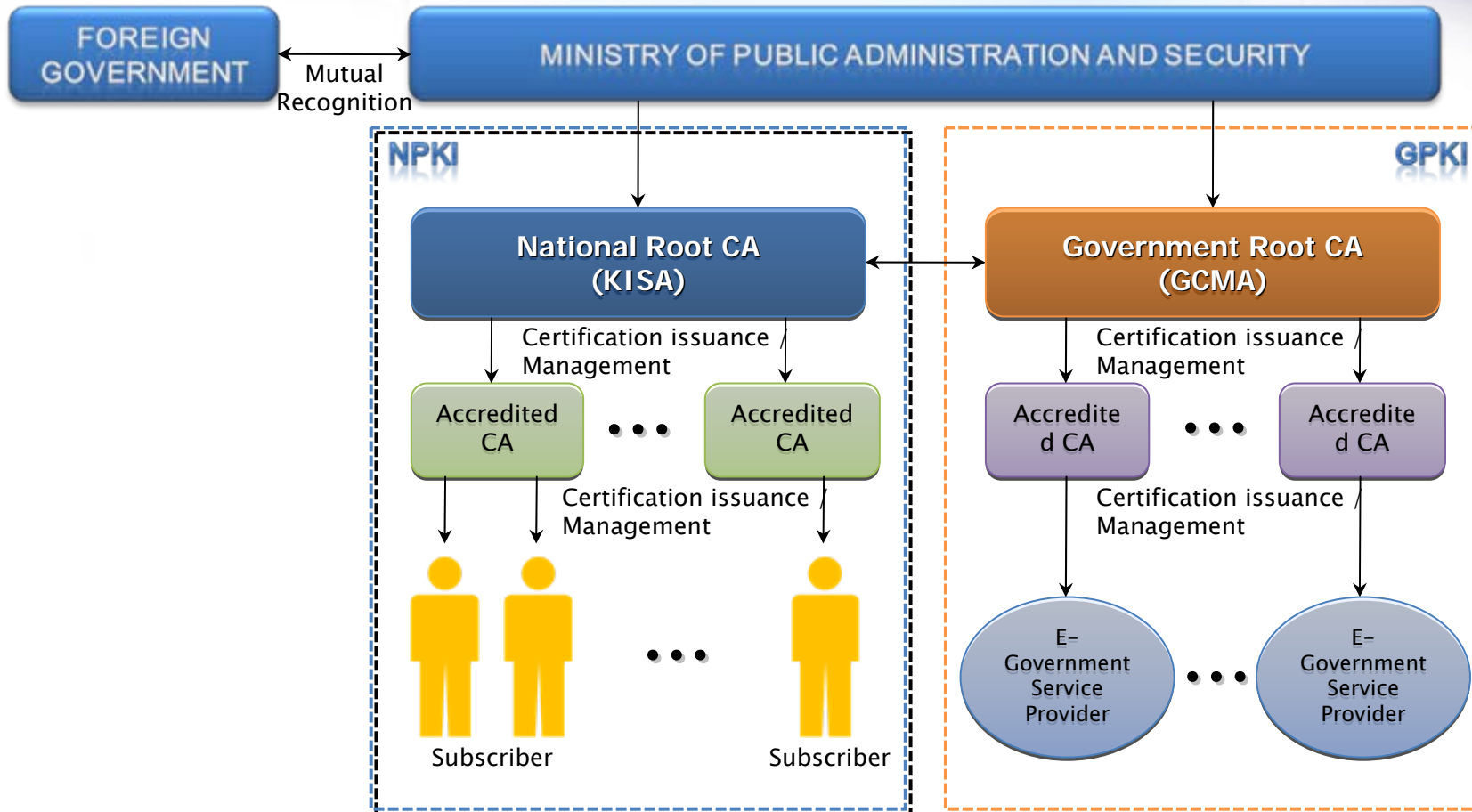
- ◆ Established in 1999 under the Electronic Signature Act
- ◆ Competent Authority : MOPAS
- ◆ Root CA : KISA (Korea Information Security Agency)
- ◆ Main Customer : Individual, Company

Government PKI

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

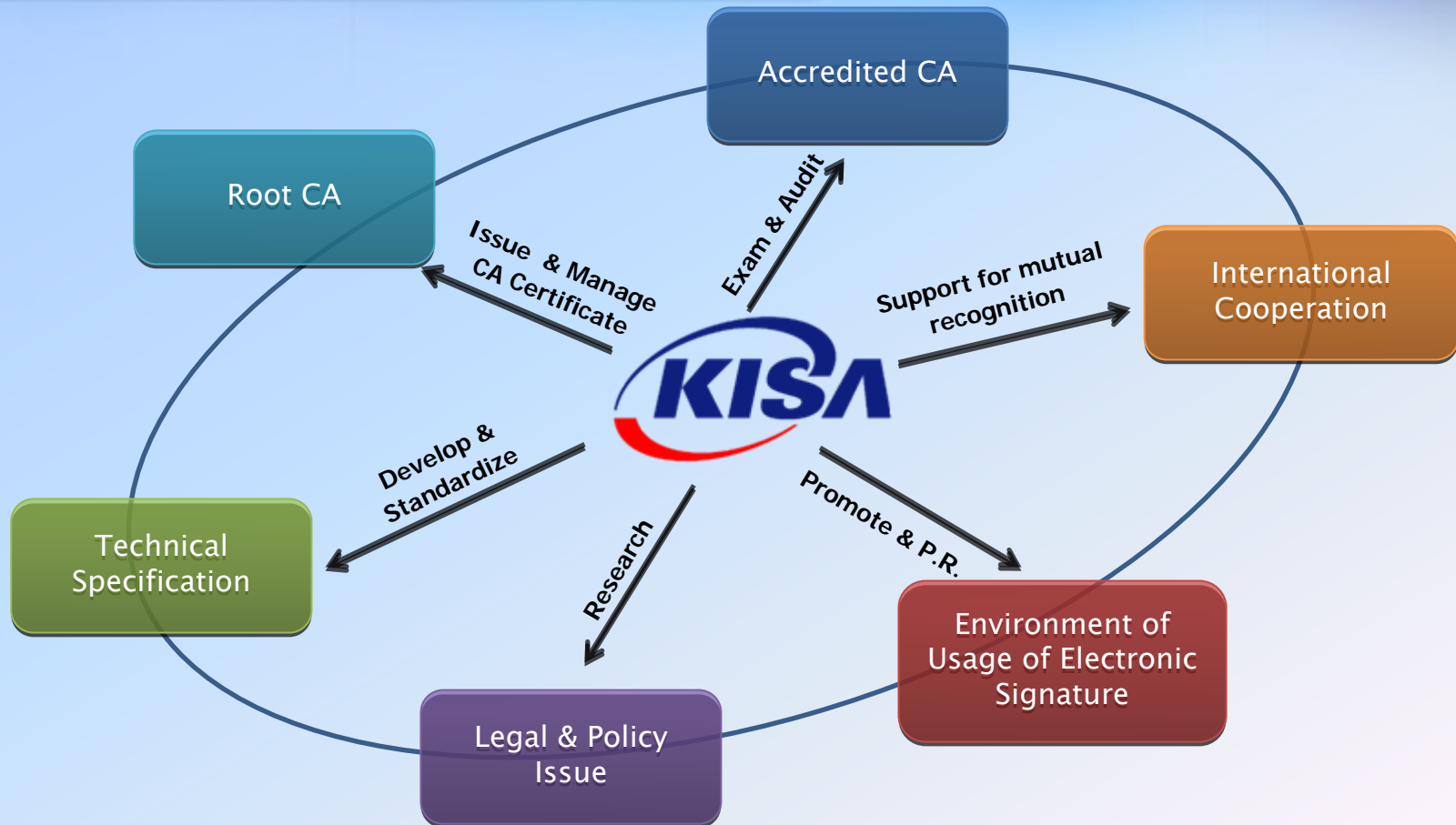
Overview

PKI Scheme



Overview

Role of the Root CA (KISA)

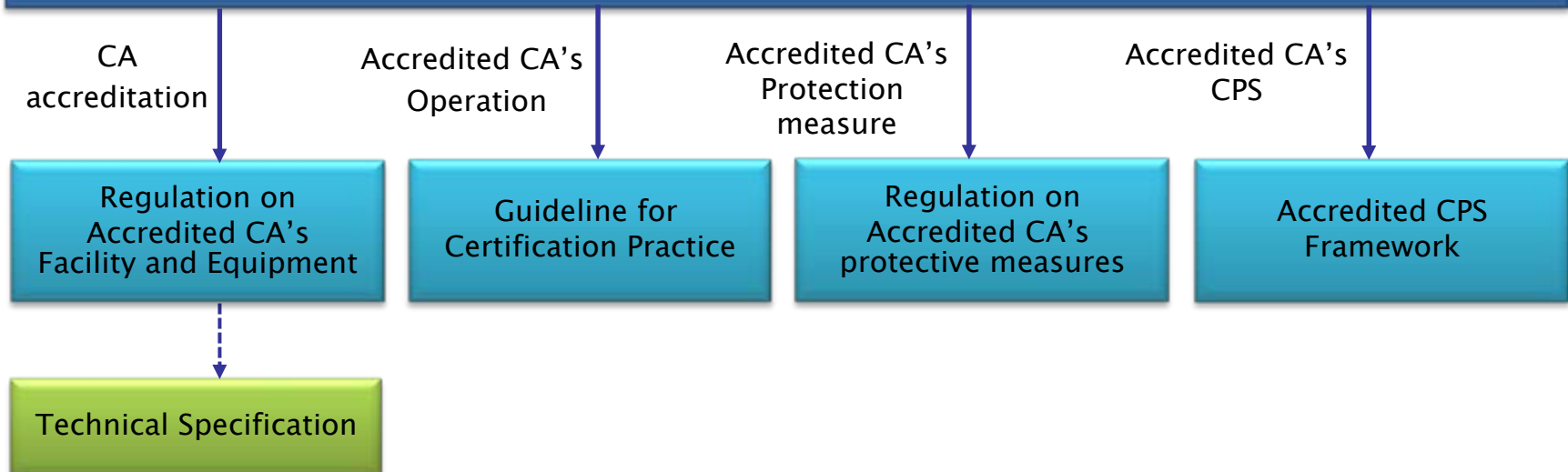


Overview

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



Overview

Accredited CA

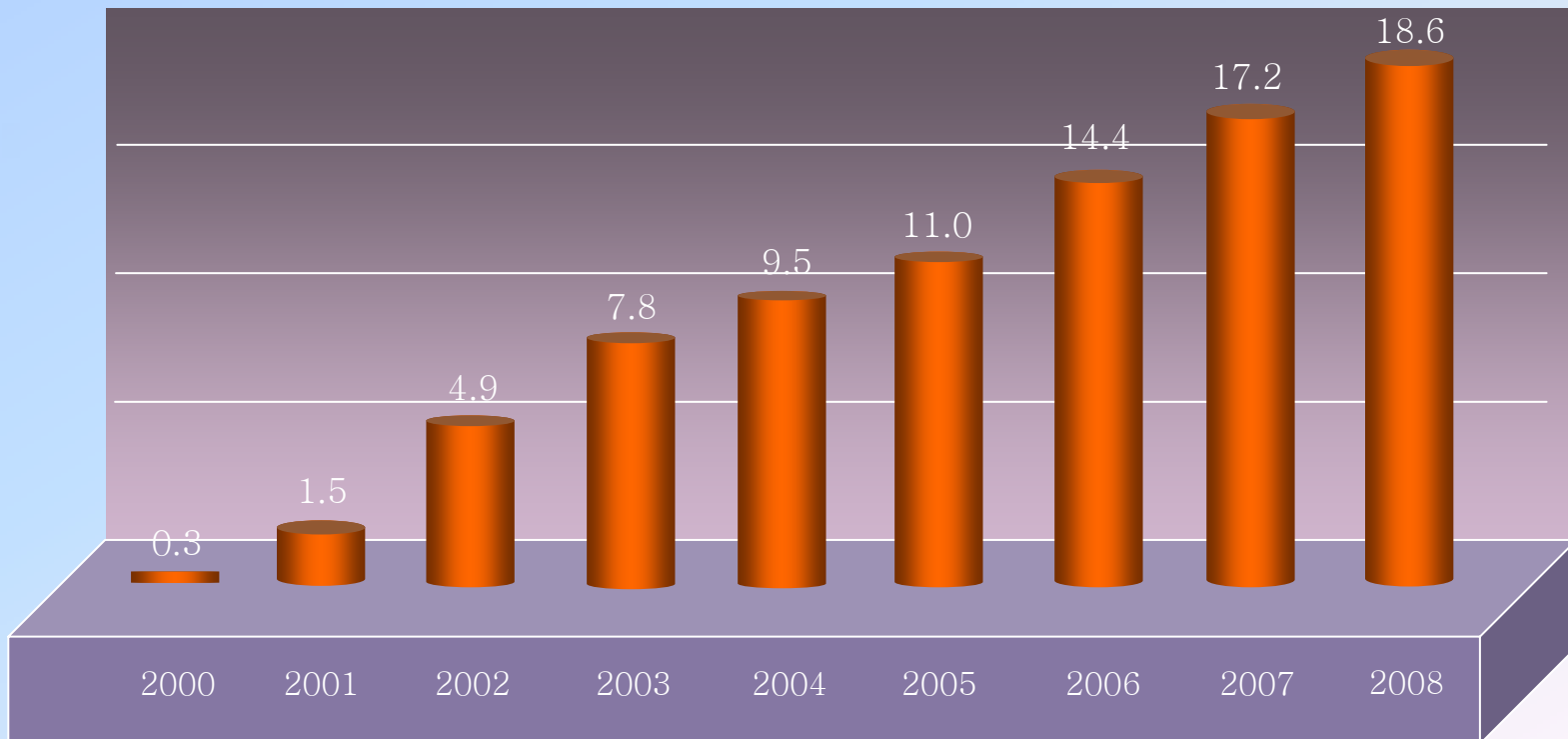
- ◆ 5 CA are accredited by MOPAS until now

Accredited CA	Accredited Date	Website
 SG	2000. 02. 10	http://www.signgate.com
 SIGNKOREA Certification Authority	2000. 02. 10	http://www.signkorea.co.kr
 yes sign	2000. 04. 12	http://www.yessign.com
 CROSSCERT	2001. 11. 24	http://www.crosscert.com
 TRADESIGNnet Digital Certificate	2002. 03. 11	http://www.tradesign.net

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

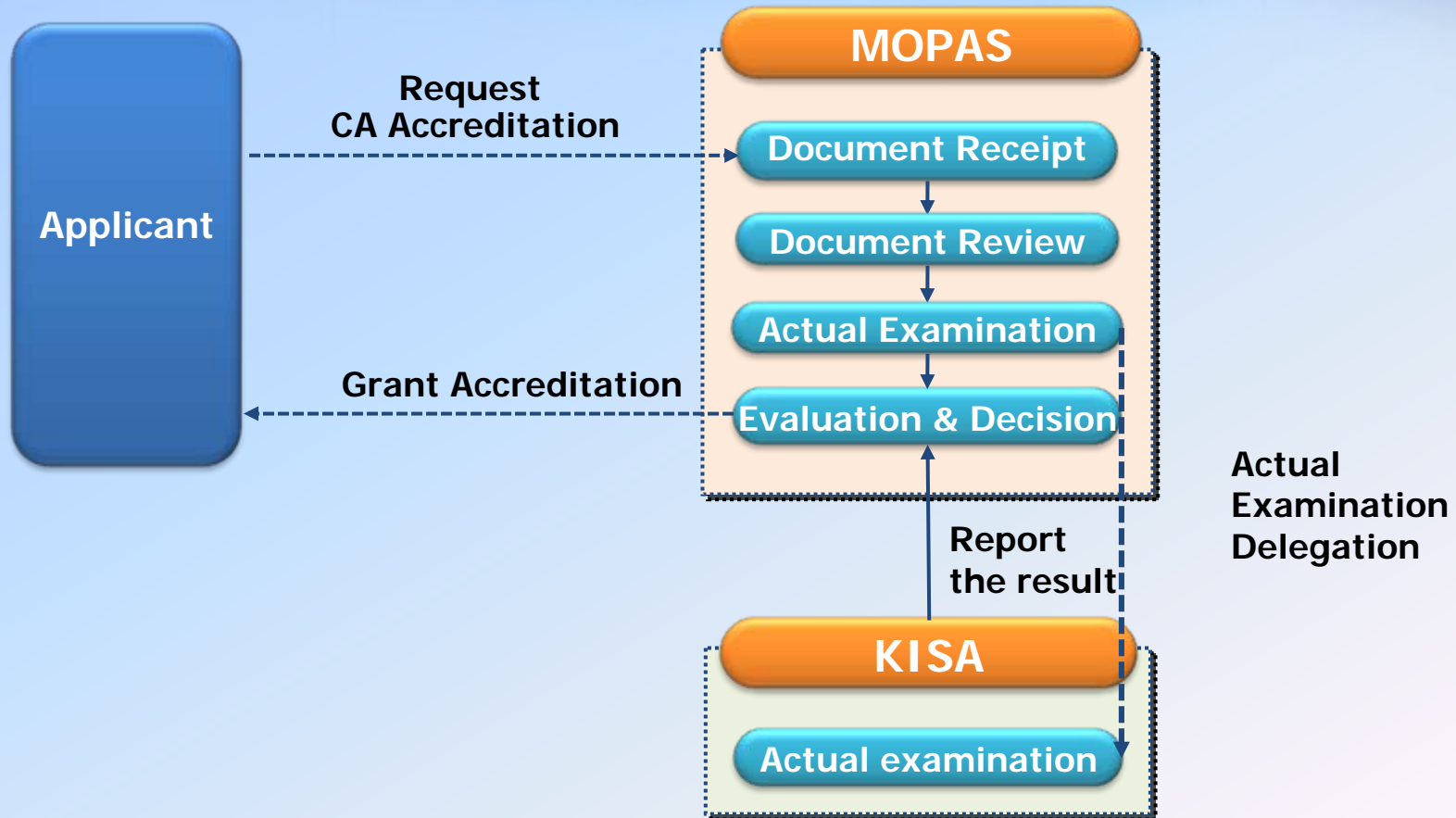
- ◆ Financial Capability
 - ◆ Capital : More than 8 million US dollars
- ◆ Personnel Capability
 - ◆ Personnel : More than 12 persons for CA operation
- ◆ Facilities and Equipments
 - ◆ Subscriber Registration, Key Management, Certificate Management, Subscriber's S/W and Security Operation Procedure

CA Accreditation Renewal

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

PKI Policy

Accreditation Procedure



PKI Policy

Regular Audit of Accredited CA

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



- Guideline on Electronic Signature Certification Practices
- Guideline on Accredited CA's protective measures

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 a e-Government services
- ◆ Interoperability among the accredited CA ('03.9)



PKI Business Model

PKI Business Models

Internet Banking

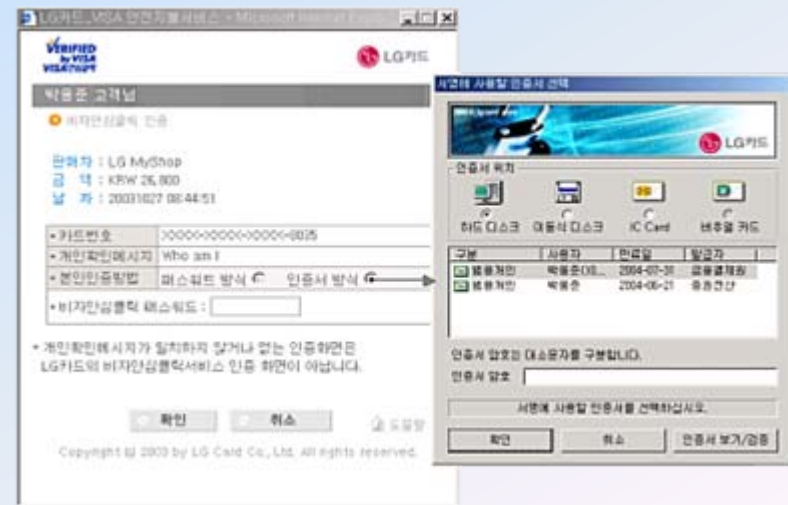
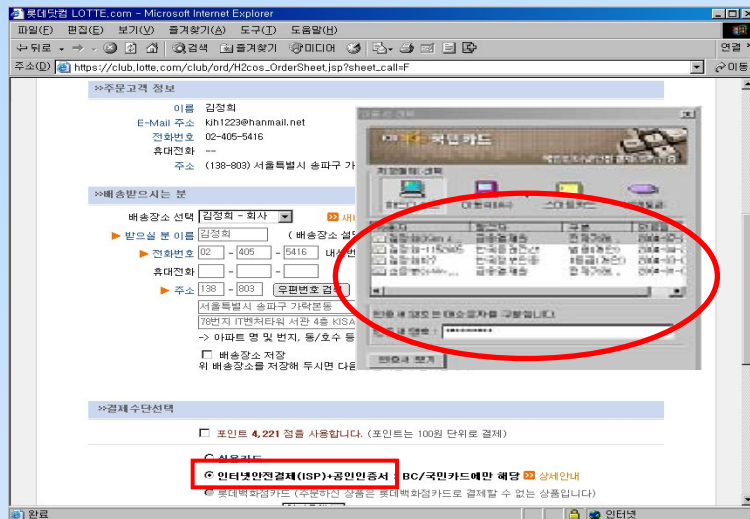
- ◆ 19 Banks and Post Office provide internet banking service based on accredited certificate
- ◆ Internet banking users must use the accredited certificate for secure online transaction ('02. 9)



PKI Business Models

Internet Shopping : Credit Card

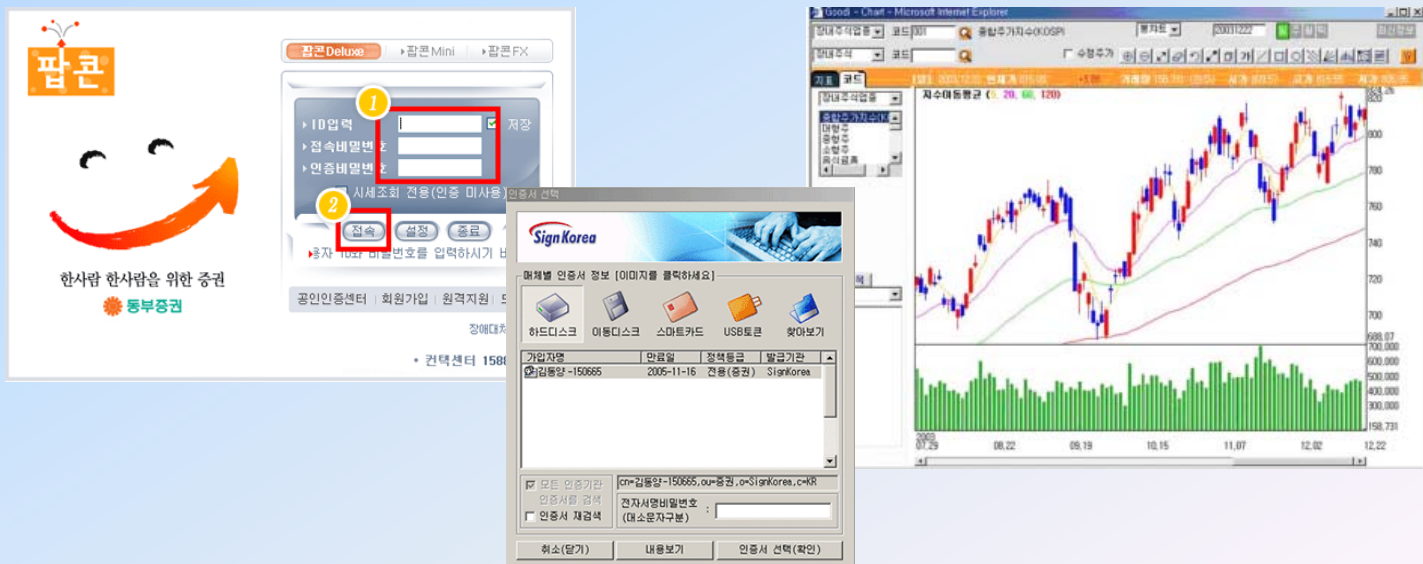
- ◆ Credit card should be used with accredited certificate to enhance the security of electronic payment process
- ◆ Regarding the transaction of over 300,000 won in Internet shopping, purchasers are required to use accredited certificate ('05. 11)



PKI Business Models

Online Stock

- ◆ 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)



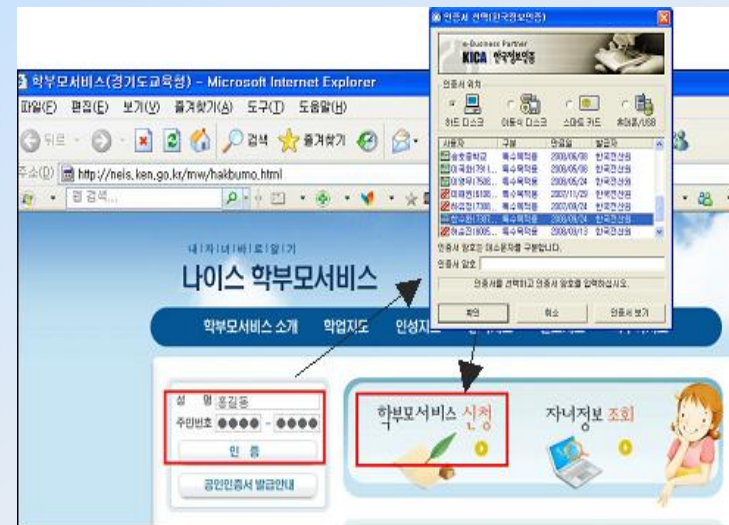
PKI Business Models

Public Service

- ◆ 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)

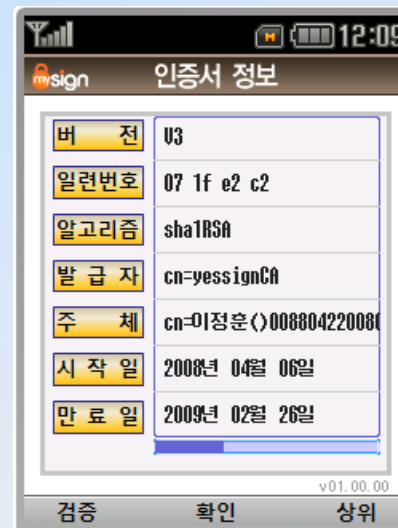


NEIS(National Education Information System)

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

Certificate Promotion

Electronic Signature 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



PKI-KR 2007



Workshop for PKI Technique in 2008

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



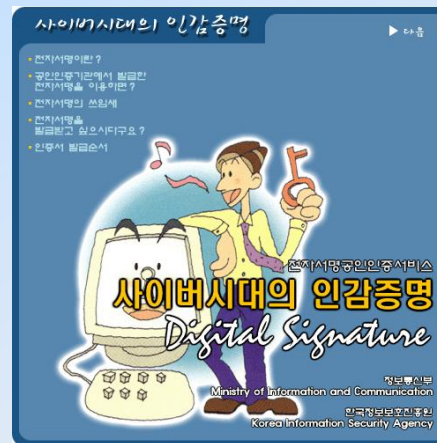
Certificate Promotion

Public Relations

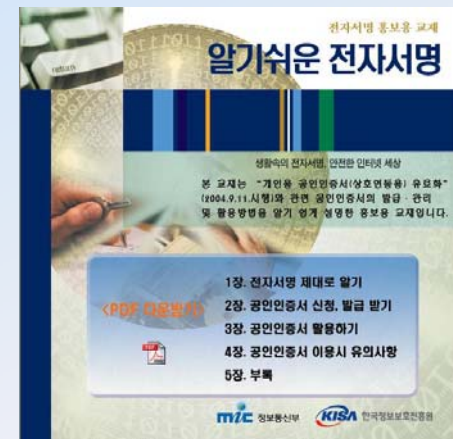
- ◆ Release leaflets, posters and stickers for electronic signature use to Banks, Public Offices, etc
- ◆ Published teaching materials for using accredited certificate and release them to major information education facilities



Leaflets for using certificate securely



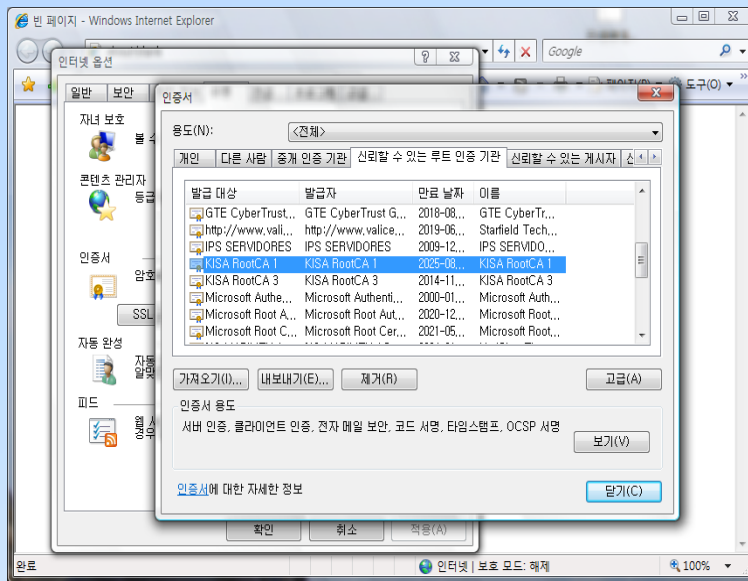
Teaching Materials for electronic signature



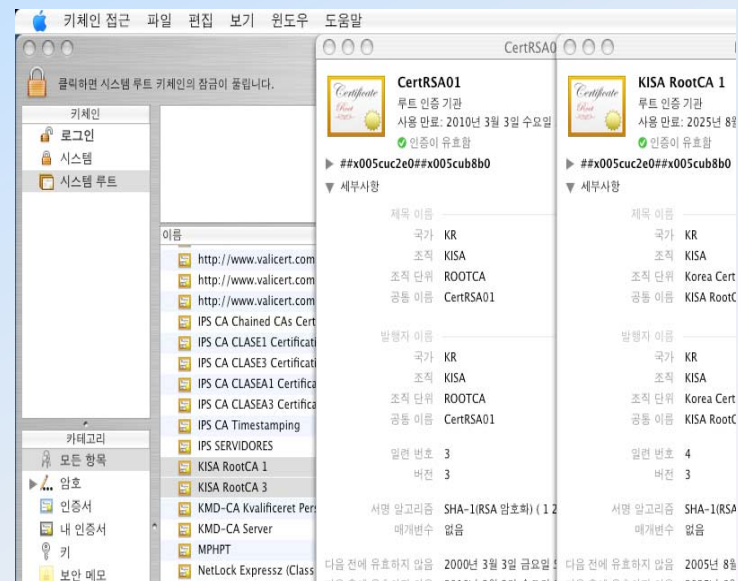
Certificate Promotion

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~)



KISA Root CA Cert. in IE7

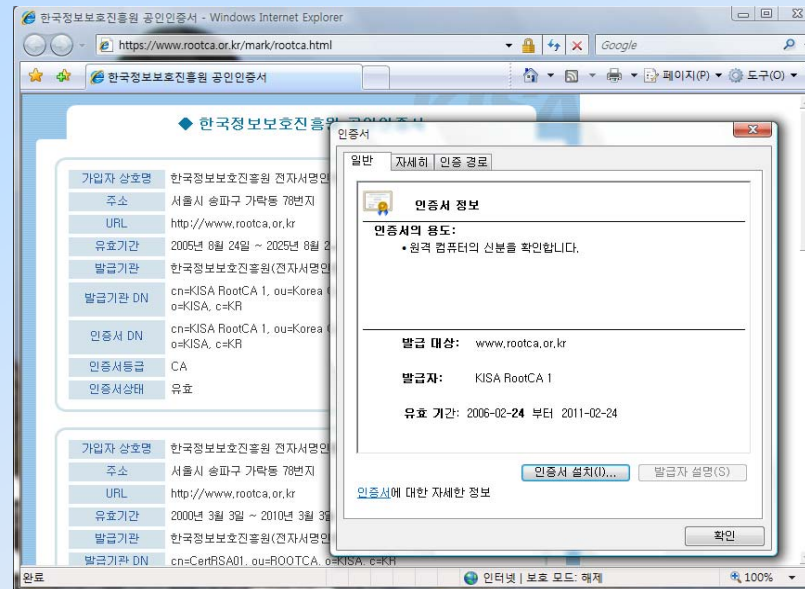


KISA Root CA Cert. in Mac OS X

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

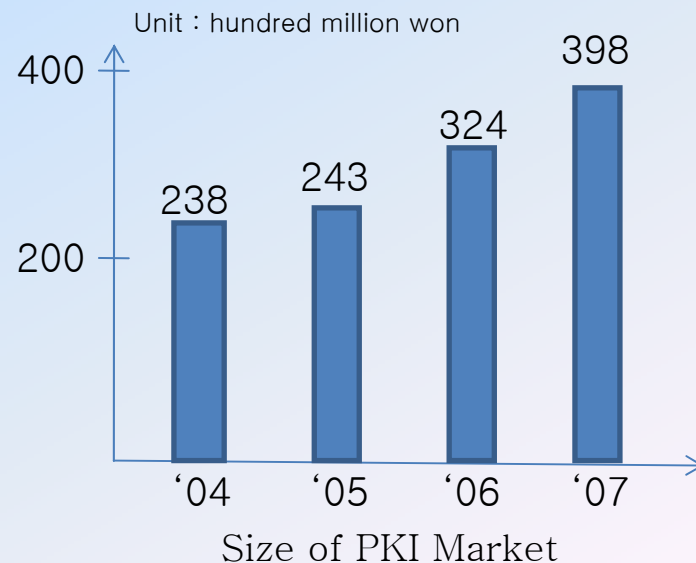
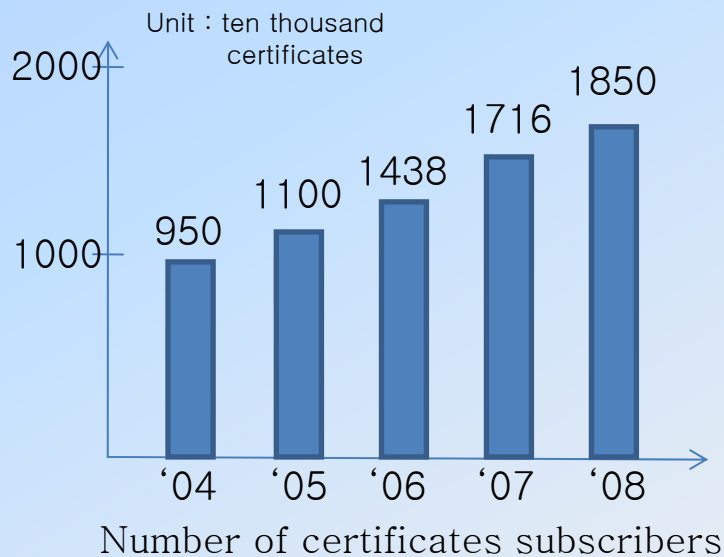


PKI Cost Policy

PKI Cost Policy

PKI Market Status1

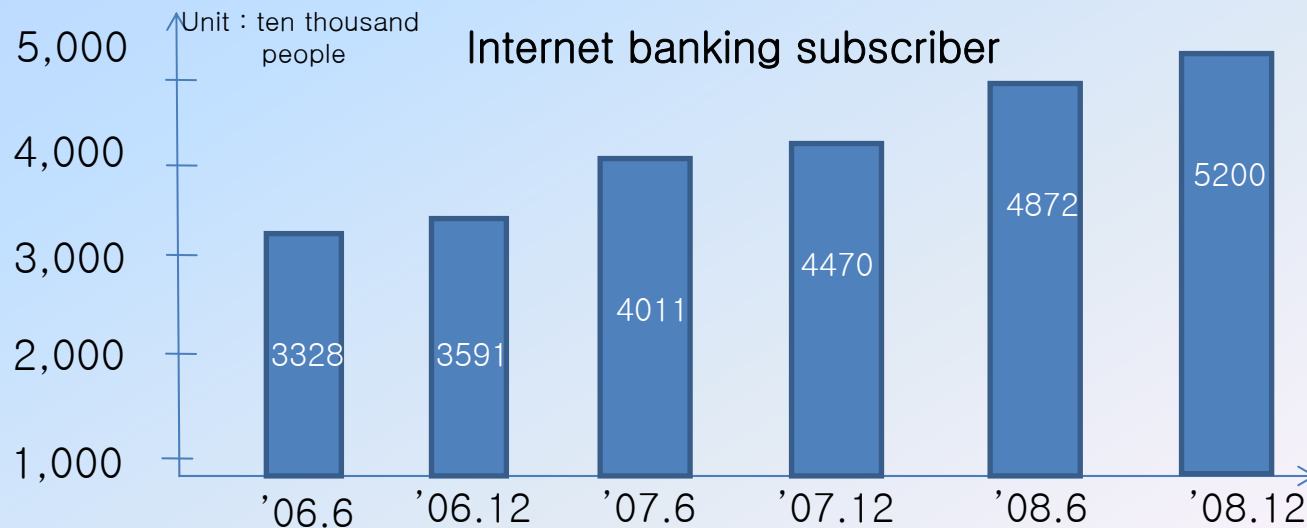
- ◆ 1.85million certificates were issued until end of 2008
- ◆ 77% of Korean economical active population (2.4million) is using certificates



PKI Cost Policy

PKI Market Status2

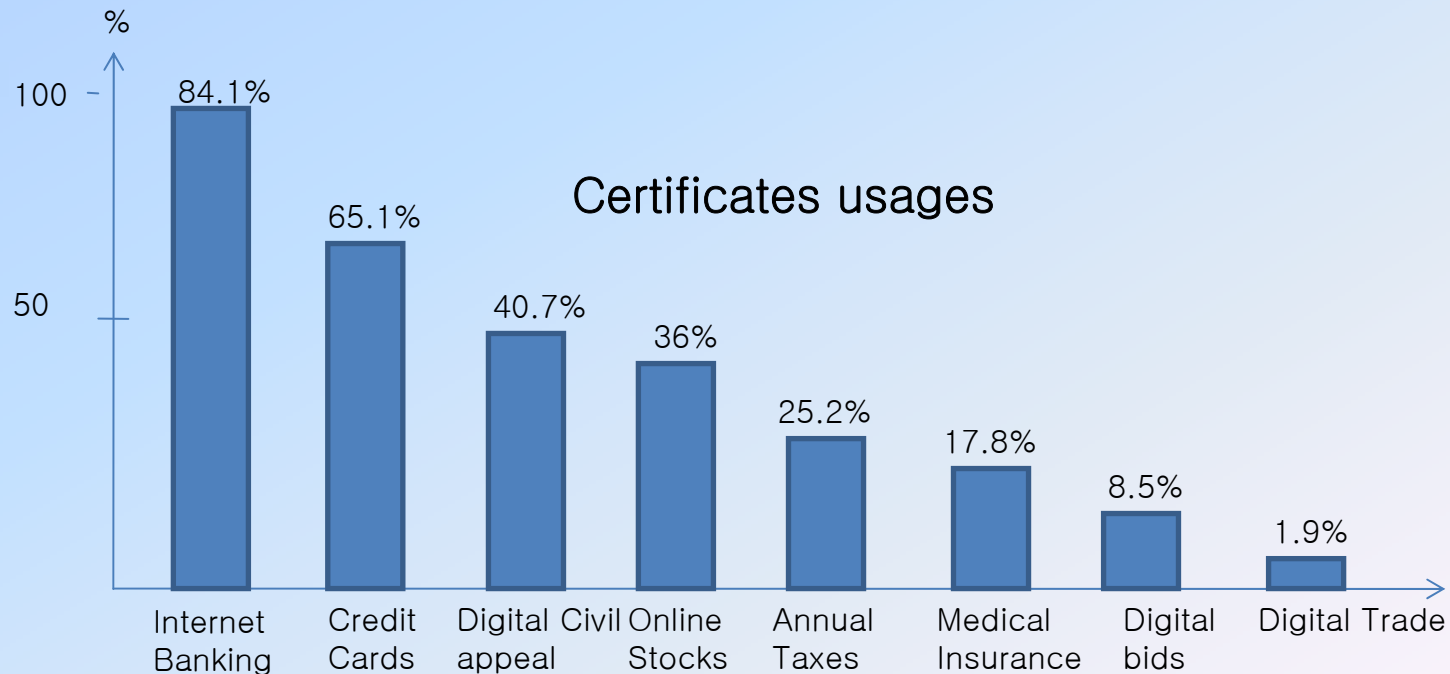
- ◆ Internet banking subscriber became 52.6million at 2008
- ◆ 12.8million certificates were issued for Internet banking at 2008
- ◆ 3.3 million Money transactions and 22.8billion USD was transferred through Internet banking by using certificates at 2008



PKI Cost Policy

Usage of Certificates

- ◆ 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 (\doteq 4.4 USD)
 - Corporation : 110,000 KRW (\doteq 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

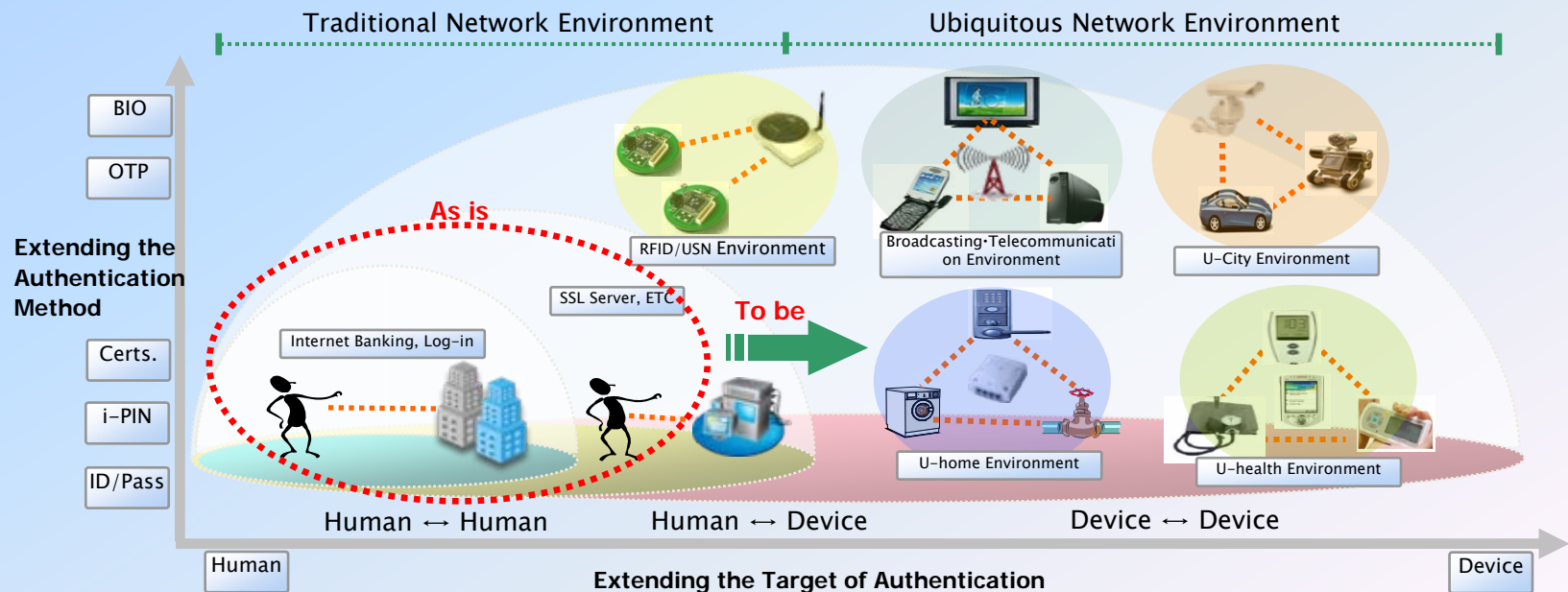


Future Work

Future Work

U-Authentication System

- ◆ Establishing a reliable u-Authentication System
 - ◆ Extending the authentication means to Biometric, OTP with PKI certificate
 - ◆ Extending the authentication object to devices



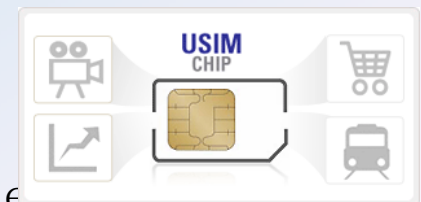
Future Work

Strengthen Security in PKI Service

- ◆ 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



HSM Token



USIM Chip

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



Korea Certification Authority Central