The Status of Korea PKI

Cryptography & Electronic Signature Team

KISA

2020. 6.

KISA Korea Internet & Security Agency

Agenda

1. Overview
2. PKI Business Models in Korea
3. Revised DIGITAL SIGNATURE ACT

1 Overview

NPKI & GPKI

National PKI

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

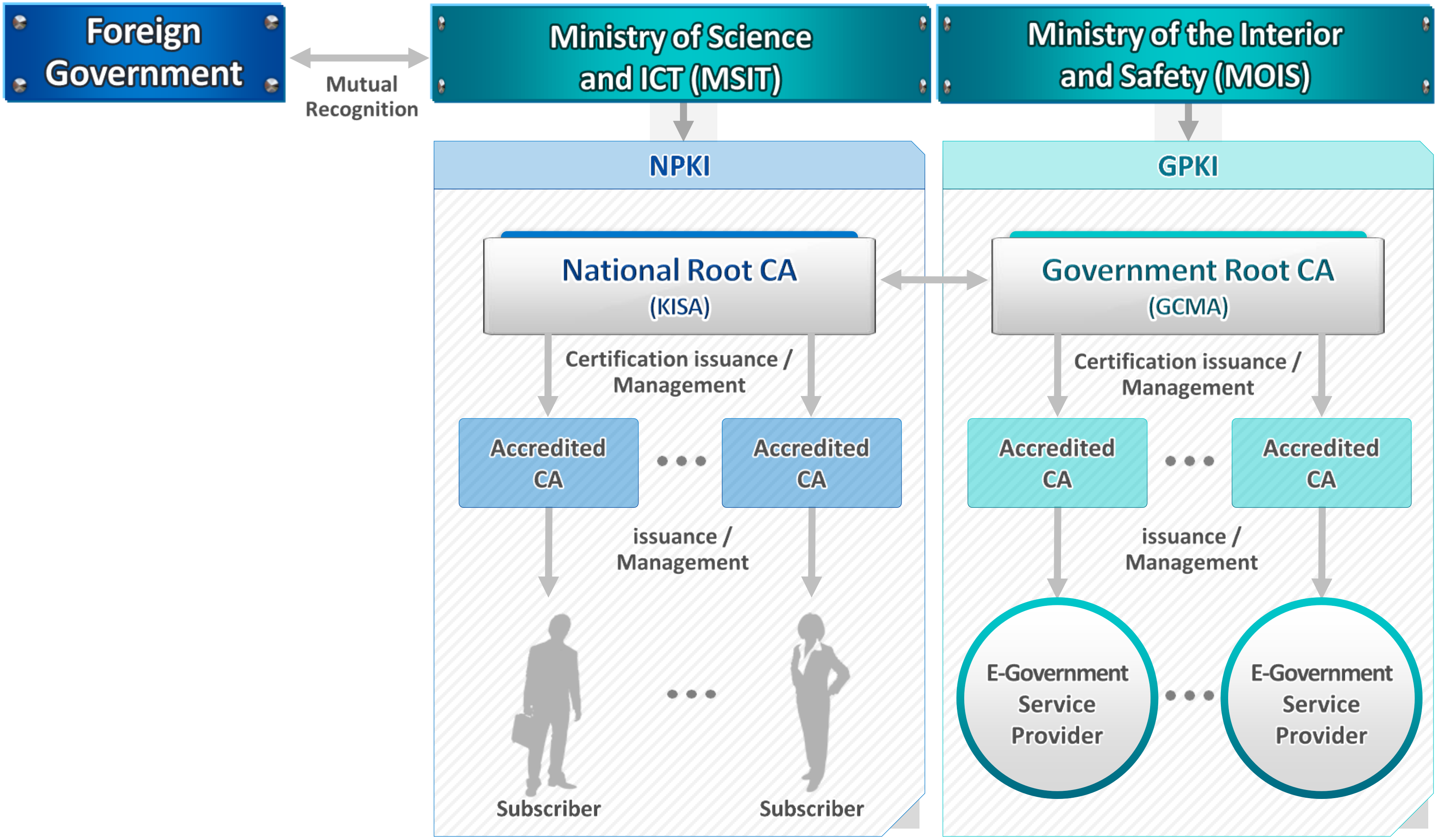
※ MSIT(Ministry of Science and ICT)

Government PKI

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

※ MOIS(Ministry of the Interior and Safety)

PKI Scheme


Foreign Government
Mutual Recognition
Ministry of Science and ICT (MSIT)
Ministry of the Interior and Safety (MOIS)
NPKI
GPKI
National Root CA
(KISA)
Government Root CA
(GCMA)
Certification issuance / Management
Certification issuance / Management
Accredited CA
Accredited CA
Accredited CA
Accredited CA
issuance / Management
issuance / Management
Subscriber
Subscriber
E-Government Service Provider
E-Government Service Provider

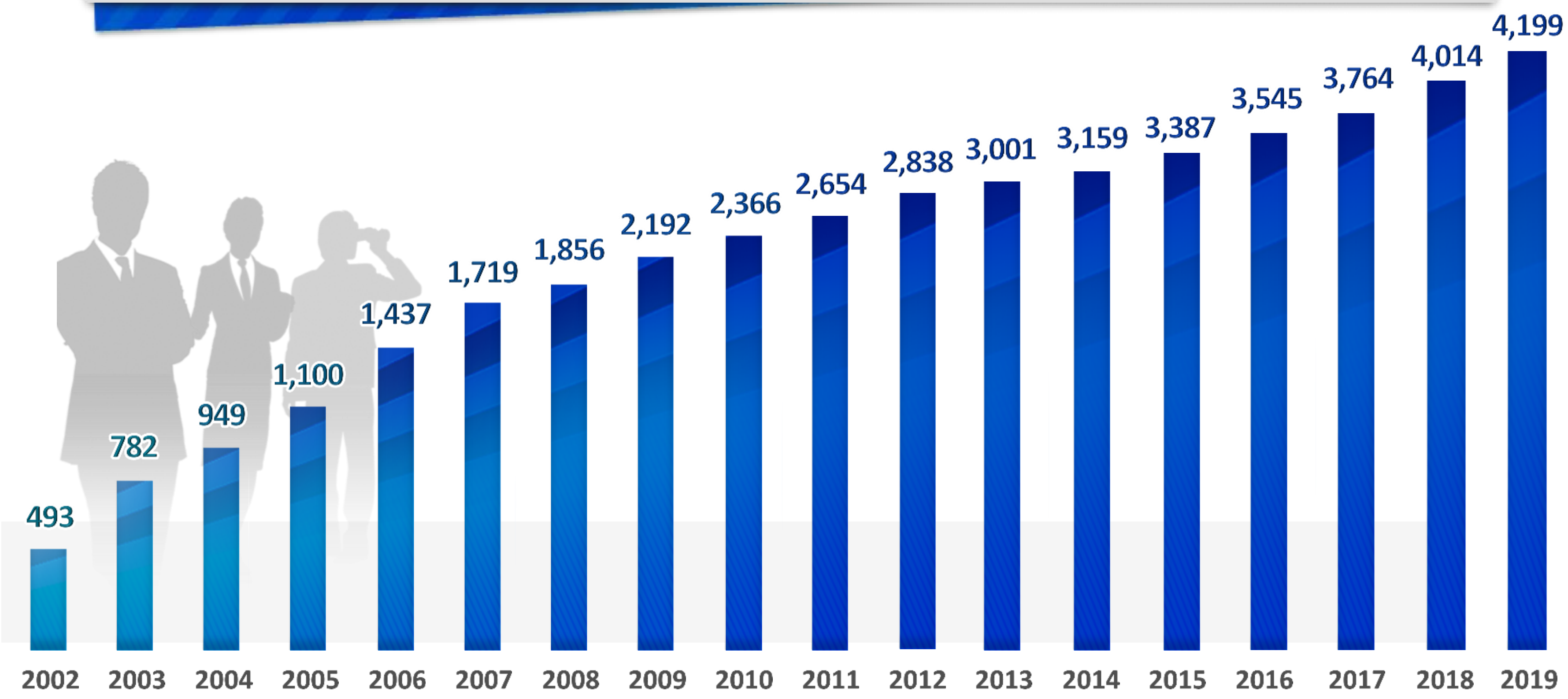
Accredited CA

5 CA are accredited by MSIT until now

Accredited CA	Accredited Date	Website
KICA Korea Information Certificate Authority Inc.	2000. 02. 10	http://www.signgate.com
SIGNKOREA Certification Authority	2000. 02. 10	http://www.signkorea.co.kr
yessign	2000. 04. 12	http://www.yessign.com
CROSSCERT	2001. 11. 24	http://www.crosscert.com
TRADE Sign	2002. 03. 11	http://www.tradesign.net

Accredited CA

- 5 Accredited CAs issued accredited certificate to subscriber around 41 million in total

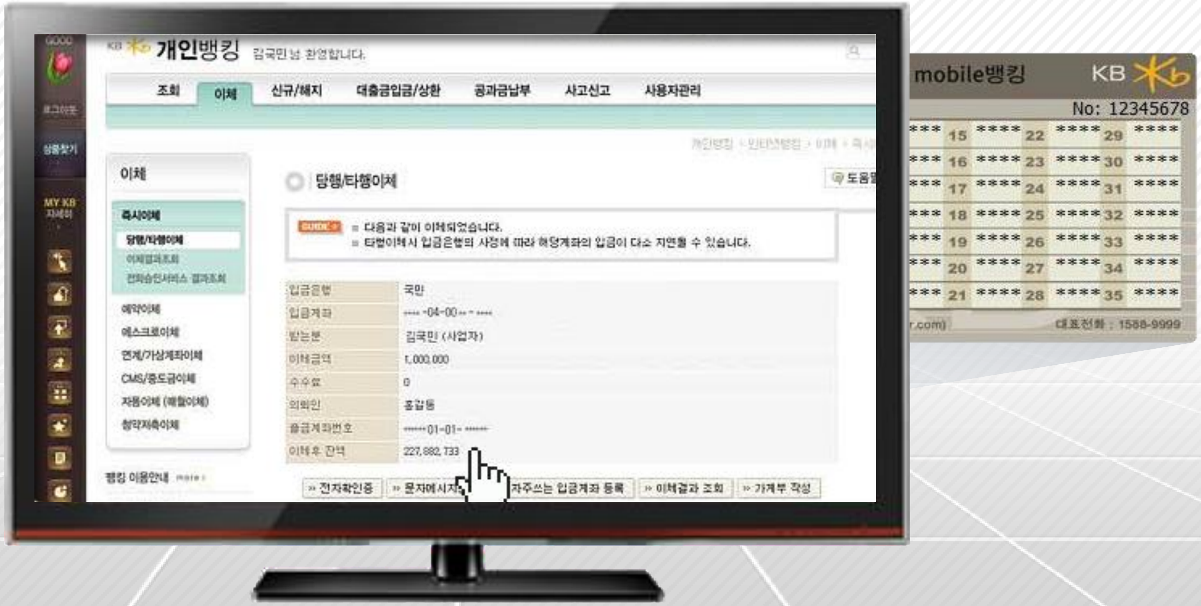


Accredited Certificate Subscriber (Unit : 10 thousand)

2 PKI Business Model in Korea

Online Banking

- All the Banks and Post Office provide internet banking service using accredited certificate



김국민님 환영합니다.

당행/타행이체

- 다음과 같이 이체되었습니다.
- 타행이체시 입금은행의 사정에 따라 해당계좌의 입금이 다소 지연될 수 있습니다.

입금은행	국민
입금계좌	**** -04-00** - ****
받는분	김국민 (사업자)
이체금액	1,000,000
수수료	0
의뢰인	홍길동
출금계좌번호	******01-01- ******
이체후 잔액	227,882,733

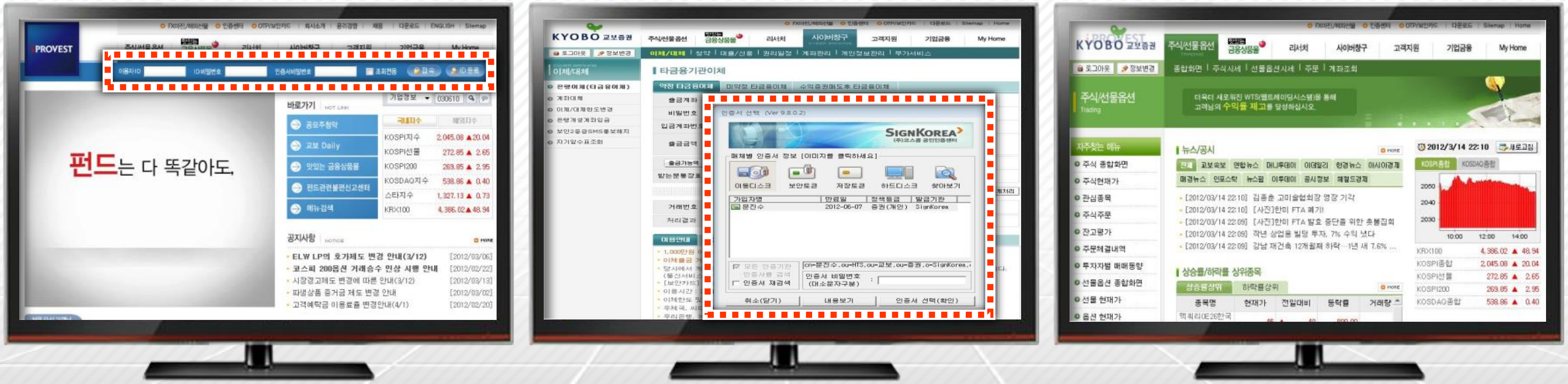
No: 12345678

***	15	****	22	****	29	****
***	16	****	23	****	30	****
***	17	****	24	****	31	****
***	18	****	25	****	32	****
***	19	****	26	****	33	****
***	20	****	27	****	34	****
***	21	****	28	****	35	****

r.com) 대표전화 : 1588-9999

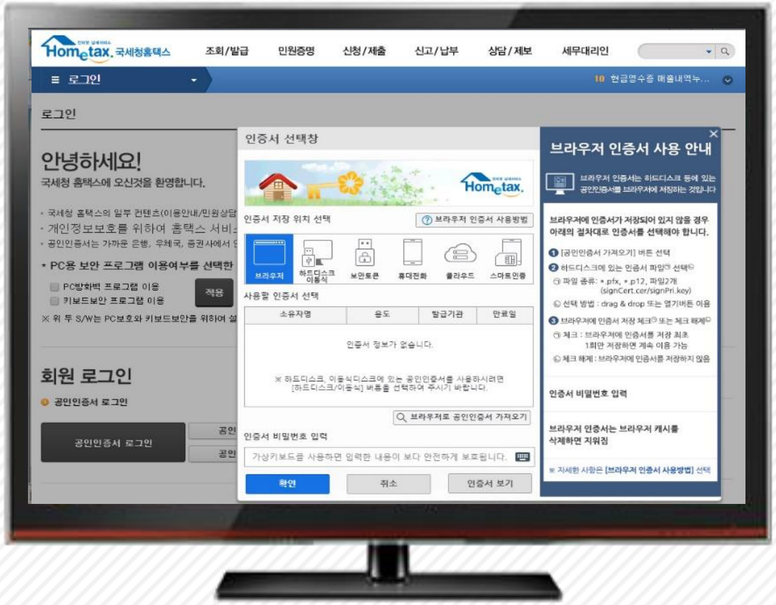
Online Stock trading

- Security corporations provide online stock service based on using the accredited certificate
- Online stock trading services recommend using accredited certificates for secure online transaction ('03. 3)



Public Service

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



국세청 홈택스에 오신것을 환영합니다.

- 국세청 홈택스의 일부 컨텐츠(이용안내/민원상담
- 개인정보보호를 위하여 홈택스 서비스
- 공인인증서는 가까운 은행, 우체국, 증권사에서

* PC용 보안 프로그램 이용여부를 선택한

□ PC방화벽 프로그램 이용
□ 키보드보안 프로그램 이용

※ 위 두 S/W는 PC보호와 키보드보안을 위하여 설

인증서 저장 위치 선택

사용할 인증서 선택

소유자명	용도	발급기관	만료일
인증서 정보가 없습니다.			

※ 하드디스크, 이동식디스크에 있는 공인인증서를 사용하시려면 [하드디스크/이동식] 버튼을 선택하여 주시기 바랍니다.

인증서 비밀번호 입력

가상키보드를 사용하면 입력한 내용이 보다 안전하게 보호됩니다.

브라우저 인증서 사용 안내

브라우저 인증서는 하드디스크 등에 있는 공인인증서를 브라우저에 저장하는 것입니다

브라우저에 인증서가 저장되어 있지 않을 경우 아래의 절차대로 인증서를 선택해야 합니다.

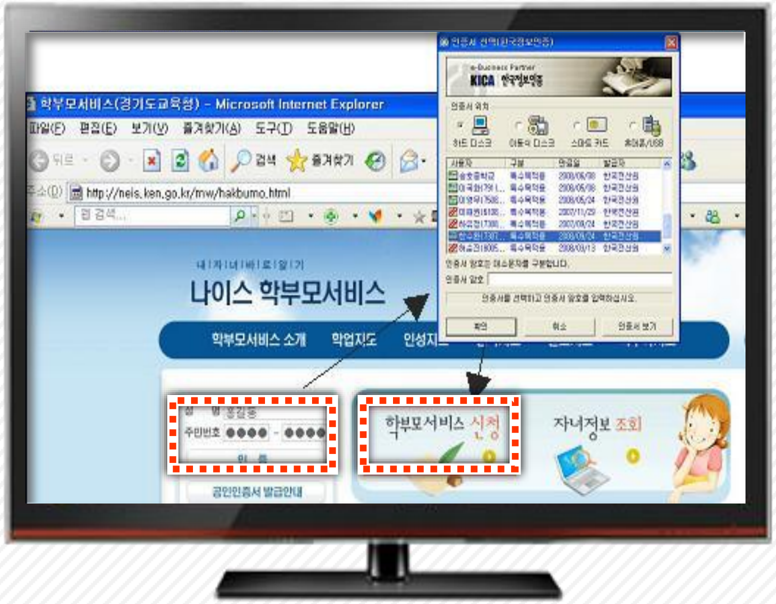
1. [공인인증서 가져오기] 버튼 선택
2. 하드디스크에 있는 인증서 파일㉠ 선택㉡
   - ㉠ 파일 종류: *.pfx, *.p12, 파일2개 (signCert.cer/signPri.key)
   - ㉡ 선택 방법 : drag & drop 또는 열기버튼 이용
3. 브라우저에 인증서 저장 체크㉠ 또는 체크 해제㉡
   - ㉠ 체크 : 브라우저에 인증서를 저장 최초 1회만 저장하면 계속 이용 가능
   - ㉡ 체크 해제 : 브라우저에 인증서를 저장하지 않음

인증서 비밀번호 입력

브라우저 인증서는 브라우저 캐시를 삭제하면 지워짐

※ 자세한 사항은 [브라우저 인증서 사용방법] 선택

HomeTax (National Tax Service)



NEIS (National Education Information System)

Smart Phone Banking

Smart Phone Banking service with certificate ('10~)

- Transferring a certificate from PC to smart phone
- Generating electronic signature in smart phone

HANA N Bank

IBK Corporate Banking

SHIN HAN Smartphone Banking

Mirae Asset M-Stock

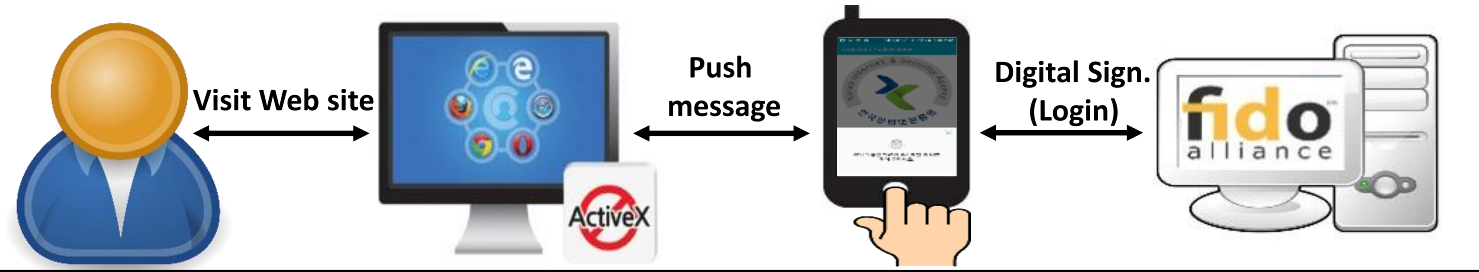
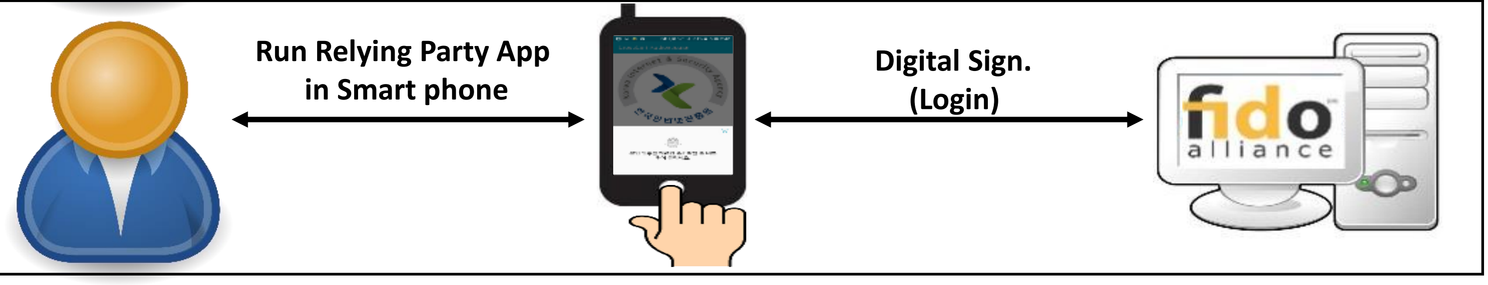
미래에셋증권 037620 66,200 ▾800 -1.19%

시가 66,500
고가 66,500
저가 66,000
전일종가 66,200
상한가 77,000
하한가 57,000
거래대금(백만) 1,730
거래량 26,119

Korea Internet & Security Agency

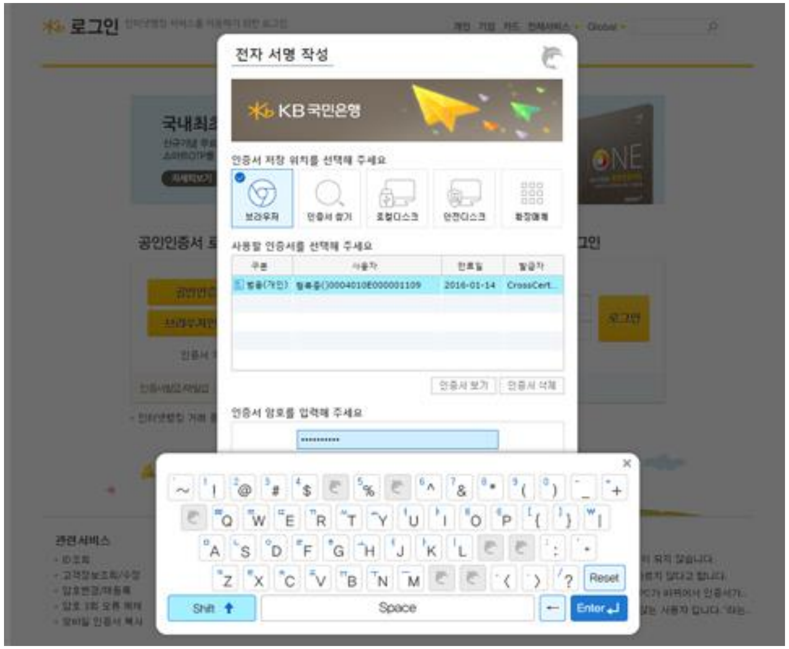
FIDO + PKI services

- FIDO authenticator(Fingerprint, Iris, etc) replaces the entering password of NPKI private key
- Store NPKI private key in Trust Zone embedded in the Smart phone
- No ActiveX in PC, Sensitive information is encrypted in Smart phone TEE

	Process
PC	 Visit Web site ActiveX Push message Digital Sign. (Login) fido alliance
Smart Phone	 Run Relying Party App in Smart phone Digital Sign. (Login) fido alliance

HTML5 Web Standard PKI Technology

- Store PKI private key in Web browser that supports HTML5
- HTML5 based PKI technology without downloading and installing any plugins



전자 서명 작성

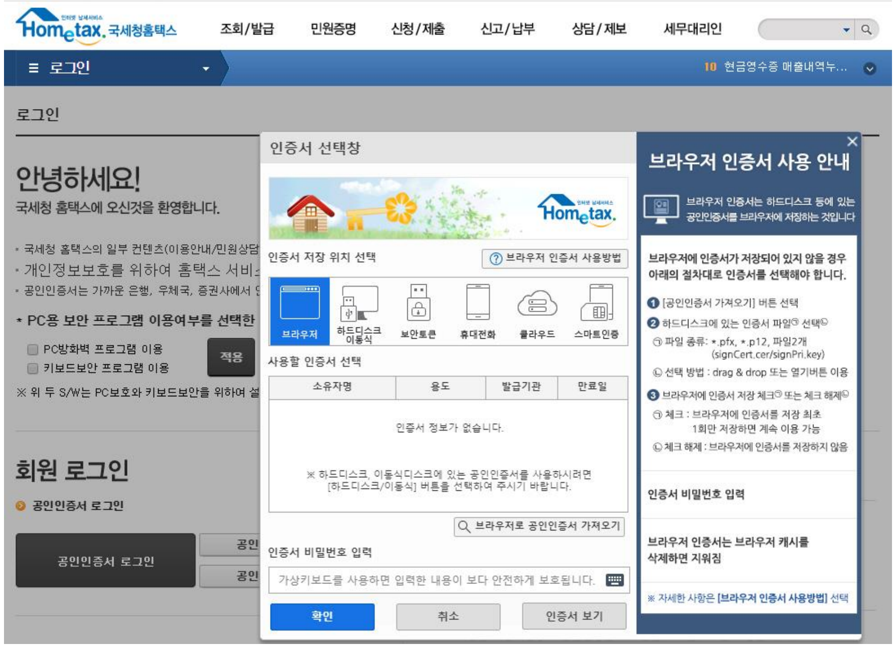
인증서 저장 위치를 선택해 주세요

사용할 인증서를 선택해 주세요

구분	사용자	만료일	발급자
법률(개인)	[illegible]()0004010E000001109	2016-01-14	CrossCert…

인증서 암호를 입력해 주세요

Kookmin Bank (Online Banking)



로그인

안녕하세요!

국세청 홈택스에 오신것을 환영합니다.

- 국세청 홈택스의 일부 컨텐츠(이용안내/민원상담
- 개인정보보호를 위하여 홈택스 서비스
- 공인인증서는 가까운 은행, 우체국, 증권사에서 (

* PC용 보안 프로그램 이용여부를 선택한

□ PC방화벽 프로그램 이용
□ 키보드보안 프로그램 이용

※ 위 두 S/W는 PC보호와 키보드보안을 위하여 설

회원 로그인

공인인증서 로그인

인증서 선택창

인증서 저장 위치 선택

사용할 인증서 선택

소유자명	용도	발급기관	만료일

인증서 정보가 없습니다.

※ 하드디스크, 이동식디스크에 있는 공인인증서를 사용하시려면 [하드디스크/이동식] 버튼을 선택하여 주시기 바랍니다.

인증서 비밀번호 입력

가상키보드를 사용하면 입력한 내용이 보다 안전하게 보호됩니다.

브라우저 인증서 사용 안내

브라우저 인증서는 하드디스크 등에 있는 공인인증서를 브라우저에 저장하는 것입니다

브라우저에 인증서가 저장되어 있지 않을 경우 아래의 절차대로 인증서를 선택해야 합니다.

1. [공인인증서 가져오기] 버튼 선택
2. 하드디스크에 있는 인증서 파일㉠ 선택㉡
   - ㉠ 파일 종류: *.pfx, *.p12, 파일2개 (signCert.cer/signPri.key)
   - ㉡ 선택 방법 : drag & drop 또는 열기버튼 이용
3. 브라우저에 인증서 저장 체크㉠ 또는 체크 해제㉡
   - ㉠ 체크 : 브라우저에 인증서를 저장 최초 1회만 저장하면 계속 이용 가능
   - ㉡ 체크 해제 : 브라우저에 인증서를 저장하지 않음

인증서 비밀번호 입력

브라우저 인증서는 브라우저 캐시를 삭제하면 지워짐

※ 자세한 사항은 [브라우저 인증서 사용방법] 선택

HomeTax (National Tax Service)

3 Revised DIGITAL SIGNATURE ACT

History of New Act

- Government announced a policy that is going to abolish the NPKI certificate(‘18)
- MSIT and KISA made a new Digital signature law(’18)
- MSIT submitted the law to National Assembly(’18)
- National Assembly passed The new DIGITAL SIGNATURE Act(’20.5)
- The new DIGITAL SIGNATURE Act was promulgated(’20.6)
- The new DIGITAL SIGNATURE Act is enforced(’20.12.10)

Main Changes

- Purpose : To promote various Electronic signatures
- Main Contents 1 : To abolish the “Authorized certificate” issued Accredited CAs
- Main Contents 2 : To extend the types of Electronic signatures that have legal effect.
- Main Contents 3 : Implementation of the recognition policy for compliance with operating standards

Main Changes

- Compare to Present

	AS-IS	TO-BE
Legal effect	Only “Authorized certificate”	All Electronic Signatures
Policy direction	Government lead (Designation by government)	Private sector lead (Anyone can service)
Service provider evaluation	(Essential) Pre-evaluation of technology, finance, facilities, regulations, etc.	(Not Essential) Technology, facilities, regulations, etc.

- Previous “Authorized certificate” may be used until renewal.

Internet On, Security In!

Thank you

leeyes@kisa.or.kr

KISA Korea Internet & Security Agency

GCCD Global Cybersecurity Center for Development