

A large, textured green moss ball is centered on a white background. The words "KeyToken" are written in a bold, yellow, sans-serif font across the middle of the moss ball.

KeyToken

INDEX

01 보안토큰이란

02 시장동향

03 제품소개

04 적용분야

05 회사소개

1

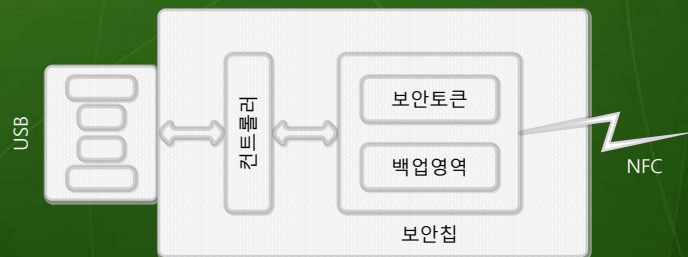
보안전oken이란?

- 물리적 보안 및 암호 연산 기능을 가진 칩을 내장하고 있어 해킹 등으로부터 공인인증서 유출을 방지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장매체입니다. - 한국인터넷진흥원(KISA) 홈페이지 중에서 -

2

보안전oken의 구조

- 스마트카드 IC는 CPU, RAM, ROM, 암호 연산 가속기 등이 내장된 One Chip Computer로, 각종 물리적 공격 및 부채널 공격을 방지하는 기술이 적용되어 현존하는 가장 안전한 보안칩입니다.



3

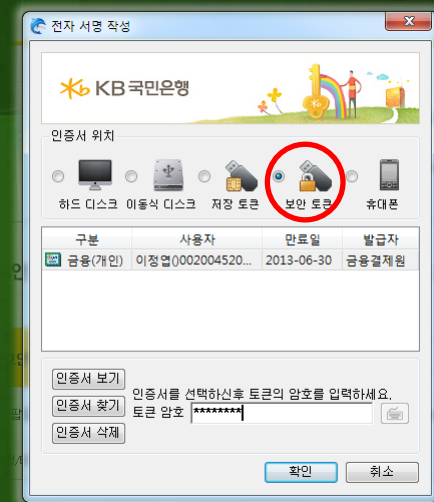
보안토큰의 필요성

- 공인인증서 유출로 인한 금융사고가 급증하고 있습니다.
 - "광고메일인 줄 알았는데..." 공인인증서 해킹해 예금 빼내 - YTN, 2012.02.23 -
 - "공인인증서 발급에 필요한 개인정보, PC·이메일 어디에도 보관하지 마세요" - 조선일보, 2011.09.15 -
 - 국감에서 해킹 시연..."공인인증서도 통째로 유출" - YTN, 2011.09.20 -
- 보안토큰은 공인인증서를 스마트카드 IC 내부에서만 사용하여 공인인증서의 유출을 원천적으로 방지합니다.

4

보안토큰의 사용

- 은행, 증권사, 보험사, 신용카드사 등 대부분의 금융기관과 전자민원24 등 공공기관 홈페이지에서 사용하실 수 있습니다.
- 공인인증서를 USB메모리에 넣어서 사용하는 방법과 유사하여, 사용하기 쉽습니다.



1

공인인증서 시장동향

- 시장의 동향

- 인터넷뱅킹 사고 급증

⇒ 사고 건수는 지난해 72건에서 올해는 7월말 기준 443건으로 이미 작년의 6배를 넘었다.
피해금액도 작년 6억 6,000만원에서 올해 7월말 32억 9,000만원으로 5배 이상 증가했다.

- 금융감독원 국정감사 자료, 2012/10 -

- 스마트폰 뱅킹의 급성장

⇒ 스마트폰 기반 모바일뱅킹서비스의 이용 건수와 금액(일평균 기준)은 1,182만건, 7,900억원으로
전분기대비 각각 13.0%, 14.7% 증가 - 한국은행, 2012년 2/4분기 국내 인터넷뱅킹서비스 이용
현황 -

- 각종 언론 보도 및 개인적 경험으로, 많은 사람들이 PC 해킹 · 스마트폰 해킹 · USB 메모리 분실 ·
스마트폰 분실 등 으로 공인인증서가 유출될 수 있다는 두려움을 가지고 있음

- 시장의 요구사항

- 공인인증서 저장매체와 관련된 개선사항으로는 '해킹 등 개인정보 외부유출 방지'(65.1%)가
가장 중요한 것으로 나타났으며, 앞으로 공인인증서 활용이 확대되기를 희망하는 서비스 분야는
'핸드폰, 스마트폰 기반 모바일 뱅킹'이 59.8%(1순위 응답기준)로 가장 높은 것으로 나타났다.

- 한국인터넷진흥원(KISA), 대국민 전자서명 이용실태조사, 2011/12 -

2

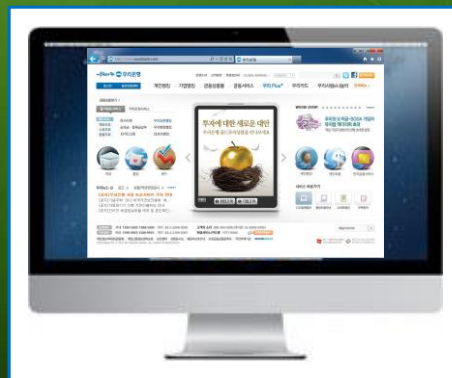
기존 보안토큰 업체들

- 보안토큰
 - 현재 한국인터넷진흥원(KISA) 인증을 받은 제품들은 다수 있지만, 홍보가 많이 되지 않아서 일반인들이 보안토큰에 대해서 잘 알고 있지 못합니다.
- USB메모리 겸용 보안토큰
 - 보안USB 제품 중에서 보안토큰과 USB메모리 겸용 제품이 있지만, 발열 문제로 일반인에게는 판매되지 않고 조달용으로만 판매되고 있습니다.
- 지문보안토큰
 - 조달청 입찰용 지문보안토큰이 판매되고 있으나, 특수용도이고 가격이 높습니다.
- 블루투스 보안토큰
 - 지문보안토큰 제품 중에서 스마트폰과 블루투스로 연결하여 사용할 수 있는 제품이 있지만, 특수용도이고 가격이 높으며 배터리를 사용함으로 충전 관리를 하여야 합니다.
- 스마트폰용 보안토큰
 - USIM 보안토큰 : 보안토큰 기능을 추가한 USIM 카드
 - 금융microSD : 보안토큰 기능 등을 추가한 microSD 메모리

1

NFC 보안토큰 : KeyToken (Keypair가 세계 최초로 개발)

- NFC 보안토큰은 PC와 스마트폰에서 모두 공인인증서를 안전하게 사용할 수 있습니다.
- ※ NFC 보안토큰과 금융앱의 연동은 현재 진행중입니다.
- ※ 스마트폰에서 현재의 방식보다 안전한 방식으로 공인인증서를 사용할 수 있는 방법도 제공되며, 이 방식은 바로 사용 가능합니다.



Computer

↔
USB



⚡
NFC



NFC SmartPhone

microSD 리더기

- PC용 microSD 리더기
- microSDHC 사용가능
- 최대 20MB/s 전송속도
- 최대 64GB 지원

NFC 보안토큰

- 공인인증서용 보안토큰
- PC와 스마트폰 겸용
- 배터리가 필요없음
- 쉬운 사용법

USB메모리

- PC용 USB메모리
- 최대 18MB/s 쓰기속도
- 최대 20MB/s 읽기속도
- 8G / 16G / 32G / 64G

기술 융합

다양한 제품군

 **KeyToken HSM**

 **KeyToken MSD**

 **KeyToken USB**

2

KeyToken HSM

- 공인인증서를 안전하게 사용할 수 있는 NFC 보안토큰입니다.
- 하나의 장치로 PC와 스마트폰에서 모두 안전하게 이용하실 수 있습니다.
- 스마트폰과는 완전히 근접시켜야 동작하므로 보안성이 뛰어납니다.
- 배터리를 사용하지 않습니다.



앞면



뒷면

3

KeyToken MSD

- KeyToken HSM의 모든 기능 + PC용 microSD 리더기
- 사용자가 원하는 용량과 성능의 microSD/SDHC를 이용하실 수 있습니다.
- microSD 리더기는 최대 20MB/s의 전송속도를 지원합니다.
- microSD 리더기는 최대 64GB의 microSD를 지원합니다.



앞면



뒷면

4

KeyToken USB

- KeyToken HSM의 모든 기능 + PC용 USB 메모리
- USB 메모리 8G의 경우 최대 18MB/s 쓰기, 20MB/s 읽기의 성능을 가집니다.
- USB 메모리는 8G/16G/32G/64G 크기가 제공됩니다.
- 타사 대비 저발열입니다.



앞면



뒷면

	스마트폰용 보안토큰	PC용 보안토큰	PC용 microSD 리더기	PC용 USB메모리	특이사항
보안토큰	X	O	X	X	
지문보안토큰	X	O	X	X	조달청 입찰용 가격이 높음
USB메모리 겸용 보안토큰	X	O	X	O	발열이 심함
USIM 보안토큰	O	X	X	X	보안문제 가능성 ¹⁾
금융microSD	O	X	X	X	보안문제 가능성 ¹⁾
블루투스 보안토큰	O	O	X	X	보안문제 가능성 ²⁾ 배터리 관리 필요 ³⁾
KeyToken HSM	O	O	X	X	
KeyToken MSD	O	O	O	X	
KeyToken USB	O	O	X	O	

¹⁾ 스마트폰과 항상 연결되어 있어(인증 매체 분리의 원칙에 위배), 공인인증서가 부정 사용될 가능성이 존재합니다.

²⁾ 블루투스는 연결 거리가 최대 10m여서, 공인인증서가 부정 사용될 가능성이 존재합니다.

³⁾ 스마트폰과 보안토큰을 연동시키기 위해서는 배터리가 항상 충전되어 있어야 합니다.

1

주요 예상 수요처

■ 은행

- 현재 스마트폰에서 금융거래를 하고 있는 사람들 중에서 공인인증서가 들어 있는 스마트폰의 분실을 걱정하는 사람들이 의외로 많으며, 이 때문에 모바일 금융거래를 사용하지 않는 사람들도 많습니다. KeyToken은 이러한 문제를 해결함으로써 모바일 금융거래를 더욱 활성화시킬 것입니다.

■ 증권사

- 은행과 마찬가지로 KeyToken은 스마트폰의 공인인증서 유출 문제를 해결함으로써 MTS를 활성화하여 증권사의 수익을 증가시킬 것입니다.

■ 신용카드사

- KeyToken의 보안칩은 신용카드, 교통카드, 전자통장 등의 기능을 추가할 수 있어서 PC와 스마트폰에서 안전한 결제 수단으로 사용될 수 있습니다.

■ 게임사

- 게임 사용자 인증 및 게임 소프트웨어 배포를 위한 기존 제품은 PC 전용이며, 발열 문제도 있습니다. KeyToken은 스마트폰에서도 게임 사용자 인증을 할 수 있으며 발열도 적습니다.

■ 소프트웨어 및 하드웨어 개발사

- KeyToken은 소프트웨어 복사 방지 장치로 사용할 수 있으며, 보안 장비의 Key 관리용 토큰으로도 응용할 수 있습니다.

보안 제품

- Key 관리
- S/W 복사방지
- 보안USB
- PC보안

공공기관

- 행정안전부
- 스마트폰 전자정부
- 국방부
- 전자 증명서 보안

금융기관

- 은행 금융거래
- 증권사 주식거래
- 신용카드사 결제
- 보험사 고객센터

교육 및 게임

- 사용자 인증
- 콘텐츠 배포
- 전자결제
- 부가서비스

일반 기업

- 전자 신분증
- 사원 출입통제
- 인트라넷 로그인
- 전자문서 보안



회사명	주식회사 키페어	대표자	이 정 업
설립일	2011년 9월	연락처	Tel. 031-757-7463 Fax. 031-757-7464
주 소	경기도 성남시 수정구 복정동 가천대학교 (구,경원대학교) 새롬관 B103 (www.keypair.co.kr)		

❖ 대표자 약력

- 공학박사 : 고려대학교 정보보호대학원
- 스마트카드 전문가 : Native COS, Java Applet
- 보안 소프트웨어 개발 : Software Crypto Library
- 보안 하드웨어 개발 : Crypto Co-processor Design
- 보안토큰 개발 : 세계 최초 NFC 보안토큰
- 벤처투자 및 영업활동 : 미래에셋벤처투자 및 ING생명

Software Crypto Library

- ❖ RSA, DSA, AES, 3DES, KCDSA, ARIA, SEED
 - 순수 자체 기술로 개발 (라이선스 문제 해결)
 - 고속 암호연산 (인라인 어셈블리로 최적화)
 - 국정원 암호모듈검증 계획
- ❖ PKCS#11
 - 한국인터넷진흥원(KISA) 인증 획득

Smartcard Technology

- ❖ Native COS
 - 삼성 Calm16, ARM SC100 코어 기반의 Chip Operating System
 - ISO7816 T=0 & T=1, ISO14443 Type B 통신 프로토콜 구현
 - 암호 가속기를 직접 제어하여 고속 암호연산 구현
 - K-Cash, T-money 규격
- ❖ Javacard Applet
 - PKCS#11 HSM Applet 구현

Hardware Security Module

- ❖ 보안토큰
 - 세계최초 NFC 보안토큰 (스마트폰과 PC에서 사용 가능)
 - USB 메모리 겸용 보안토큰
 - 한국인터넷진흥원(KISA) 인증 획득
- ❖ 암호 가속기 보드
 - 순수 자체 기술로 암호칩 설계
 - DB 암호화 가속기, SSL 가속기
 - 국정원 암호모듈검증 계획

Passion for Smart Card



