Internet Security Corp.

차세대 IC카드 **SECUREKEY™**을 이용한 인증 및 보안 사례

Case Study of Authentication and Data Security Using **SECUREKEY™**, the Next Generation IC Card

추성호, 장승규, 유일선, 제갈명, 강재홍
㈜인터넷시큐리티 기술연구소

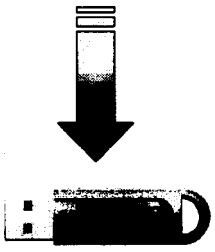
INTERNET SECURITY

한국전자거래학회 2000 종합학술대회

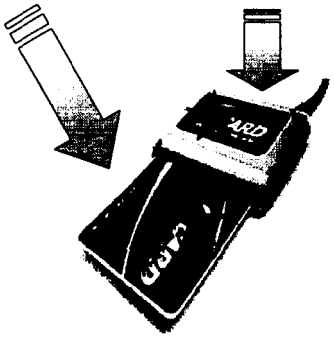
Internet Security Corp.

What's the **SECUREKEY™** ?

- **SECUREKEY™** = IC Card (SmartCard) + IC Card Reader



차세대 형태 (21C)

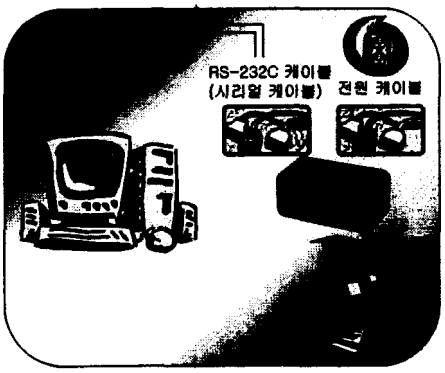


기존 형태 (20C)

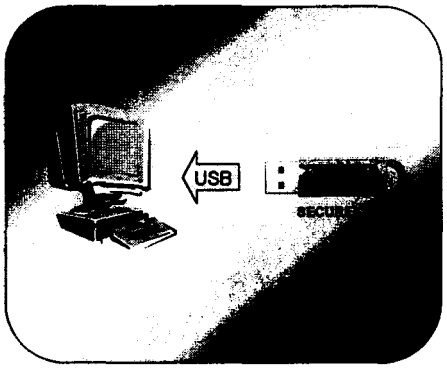
2 / 25

Internet Security Corp.

기존 시스템 구성



-기존 IC카드 시스템 -
복잡한 시스템 구성 (보안 취약성 증가)



- **SECUREKEY™** 시스템 -
단순한 시스템 구성

3 / 25

Internet Security Corp.

SECUREKEY™

◆ 개요

- PC표준 USB포트에 바로 연결하여 사용
- 열쇠 크기의 휴대용 개인 정보보호 장치
  - ◆휴대용 전자서명기
- 별도의 리더기가 필요 없음
- Strong Authentication (Two-Factor 인증)

USB
재부팅 없이 'Plug and Play'를 지원하고, 최대 127개의 장치를 연결할 수 있는 PC 표준 포트

4 / 25

Internet Security Corp.

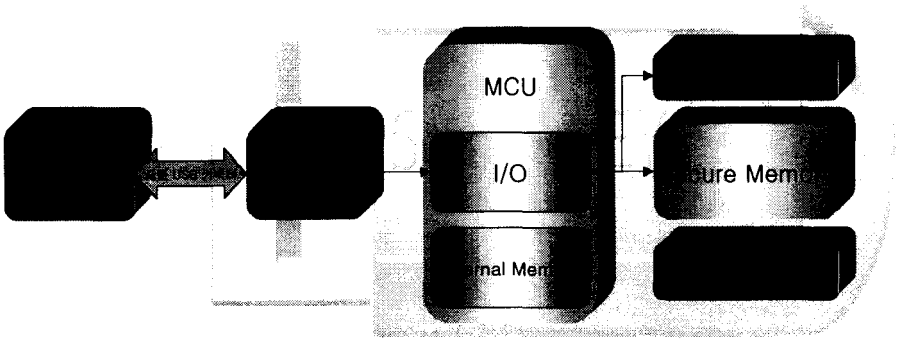
특 징

- 보안성
  - 내부 보안 메모리에 저장 : 안전한 비밀 정보 보관
- 강력한 인증
  - PIN (Personal Identity Number)과 비밀정보 동시 사용 : Two-Factor 인증
  - PKI 기반의 사용자 인증
- 휴대성
  - 열쇠 형태의 소형, 경량화된 제품
- 경제성
  - 별도의 리더기가 필요 없음
- 기술성
  - 순수 국내 기술과 부품 사용으로 다양한 응용 분야에 적용 가능
  - 세계 4번째, 국내 최초
  - 국외 표준 및 국내 표준, 국가 보안 정책 및 법규 준수

5 / 25

Internet Security Corp.

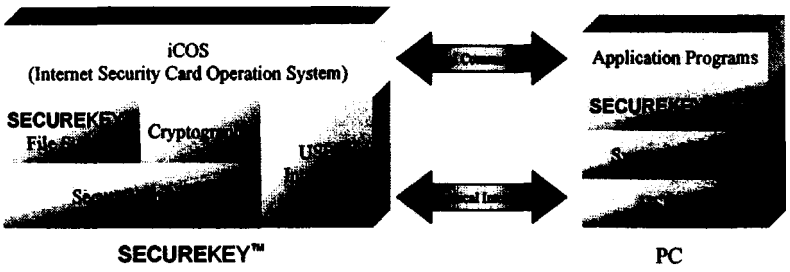
하드웨어 구성



6 / 25

Internet Security Corp.

하드웨어 구조

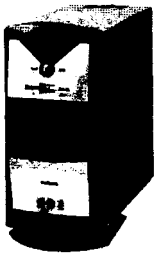


- IC카드 표준 (ISO 7816-4) 명령어 기반
- 암호화 / OTP (One-Time Password)
  - Session Key 사용 기능
- Flexible한 File System

7 / 25

Internet Security Corp.

사 양



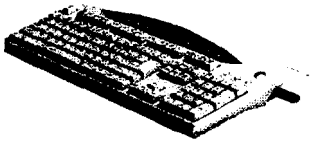
- 하드웨어
  - Microprocessor (RISC)
  - Secure Memory (2 Kbytes 이상)
- 소프트웨어
  - PKCS #11
  - X.509v2 Cert.
  - Microsoft WDM 기술 Device Driver (Windows 9x, NT, 2000)
  - Microsoft Cryptography APIs 지원 (CSP)
- 보안 알고리즘
  - DES, TripleDES, SEED (국산) 등
  - RSA, DSA, KCDSA (국산) 등
  - MD5, HAS-160 (국산) 등

8 / 25

Internet Security Corp.

기 능

◆ 전자상거래 응용
- 전자 지갑 (Digital Wallet)
- 전자 화폐 (Electric Payment, Electric Coin)
- 신용 카드 (Mondex, SET)
- 전자 서명



◆ 접근 제어 (Access Control)
- PIN 보안
  - ◆Failure Counting and Locking
- File System
  - ◆사용자 별, 읽기쓰기실행 권한 지정

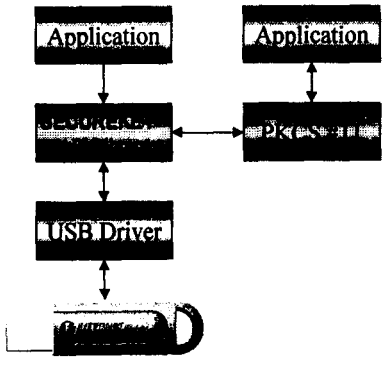
9 / 25

Internet Security Corp.

소프트웨어 구성

◆ USB Driver
- Microsoft WDM Device Driver

◆ **SECUREKEY™** APIs
- Object Oriented 기반의 Component Library
- Static, Shared/Dynamic APIs
- Multi-Application 지원



10 / 25

Internet Security Corp.

SECUREKEY™ API Library

- Device
  - Open / Close
  - Status
- PIN
  - Verify (Master PIN, User PIN)
  - Modify
- Cryptography
  - Session Key
  - Encrypt
  - Decrypt
- One Time Password
  - Challenge
  - Response
- File System
  - Create
  - Delete
  - Directory
  - Open / Close
  - Read / Write
- Etc.
  - Serial Number
  - LED Blink

11 / 25

Internet Security Corp.

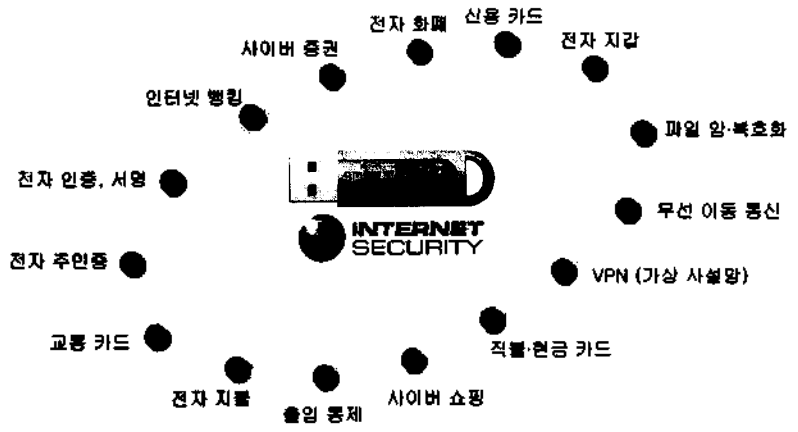
사용 절차

- 생산 – ㈜인터넷시큐리티
  - Low Level Format
  - 기본정보 (Serial Number, 초기 PIN) 입력
- 발급 – 관리자
  - 해당 Application에 맞게 Format
  - 필요한 Data 입력
  - User PIN, Issuer PIN 입력
  - 발급 프로그램 이용
- 사용 – 사용자
  - 만들어진 file에 자신의 정보를 저장
    - ID, password, 인증서, 기타 비밀정보
  - 응용 프로그램 이용
- 폐기 – 관리자
  - 사용 불능 상태로 설정

12 / 25

Internet Security Corp.

적용 분야



13 / 25

Internet Security Corp.

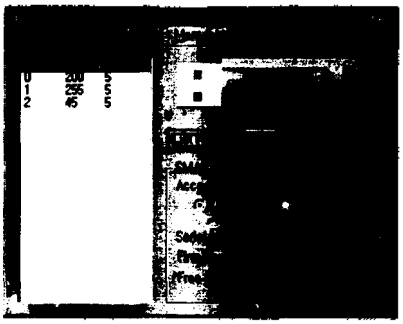
기술적 응용 분야

- 인터넷 뱅킹, 사이버 증권 (OTP, SSL)
- 전자상거래 (지갑, 화폐, 소액, 지불, 신용 카드)
- PKI 기반 시스템 (인증서, 전자 서명)
- PC 보안 (파일 암호화, 부팅 제어)
- Web Access Control (Microsoft NTLM, SSL)
- 전자 메일 보안 (SMIME, PGP)
- 원격 접속 제어 (RAS, Radius, TACACS+)
- Single Sign On (Microsoft NT/2000 logon, NTLM, Active Directory, Novell Netware)
- 네트웍 장비 및 전산 시스템 관리자
- 소프트웨어 불법 복제 및 사용 방지
- Virtual Private Network (S/W VPN, H/W 관리)
- 출입 통제

14 / 25

Internet Security Corp.

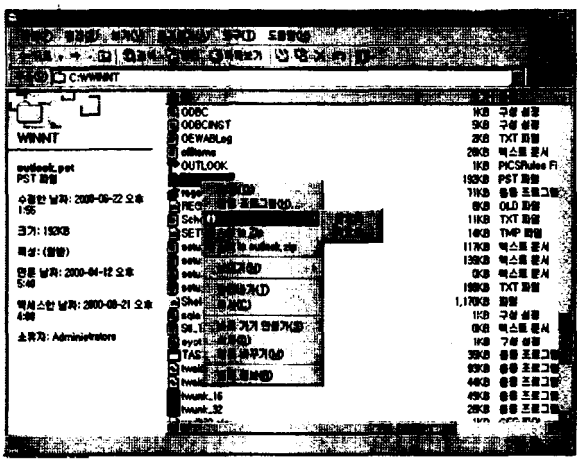
발급 프로그램



15 / 25

Internet Security Corp.

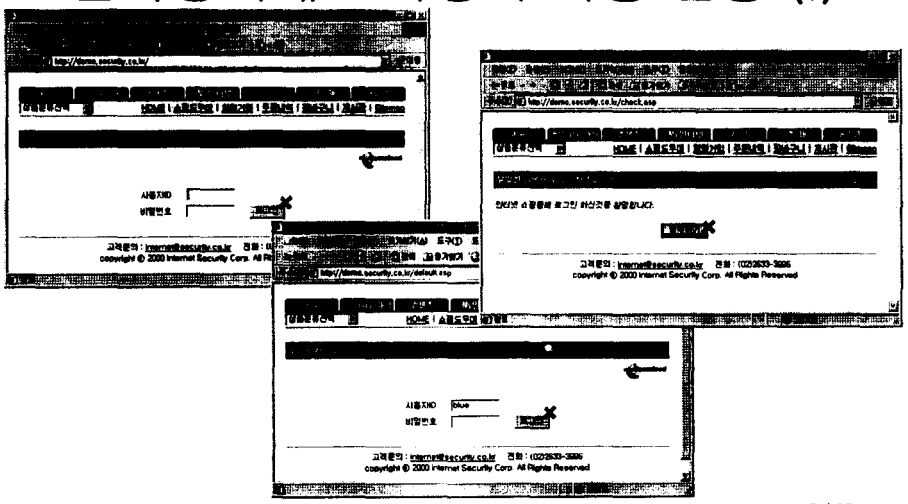
PC보안 - 파일 암/복호화



16 / 25

Internet Security Corp.

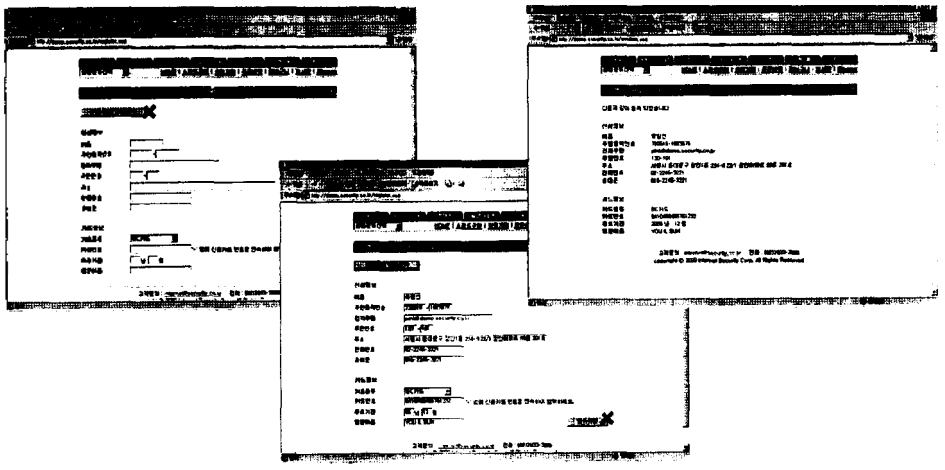
전자상거래 – 사용자 자동 인증 (I)



17 / 25

Internet Security Corp.

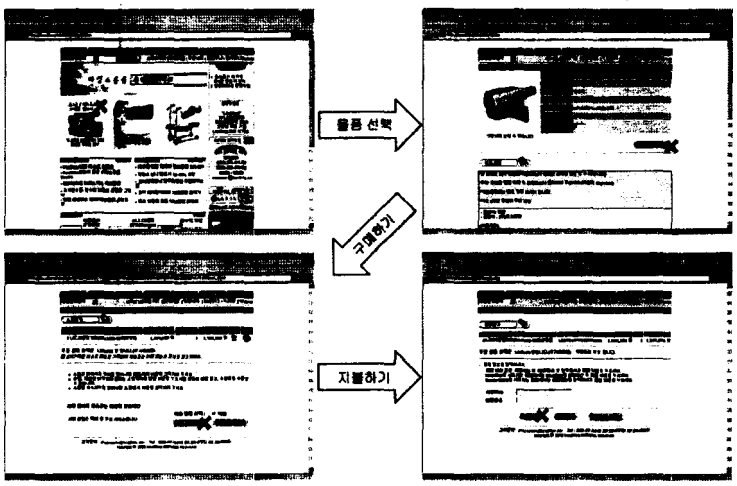
전자상거래 – 사용자 등록 (II)



18 / 25

Internet Security Corp.

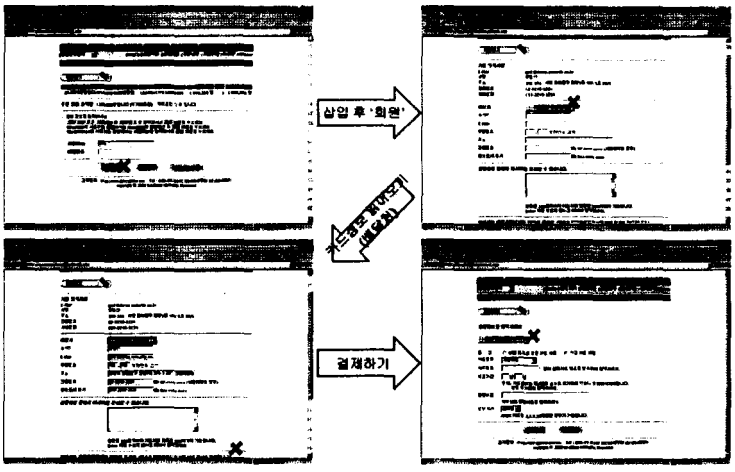
전자상거래 – 웹쇼핑 (I)



19 / 25

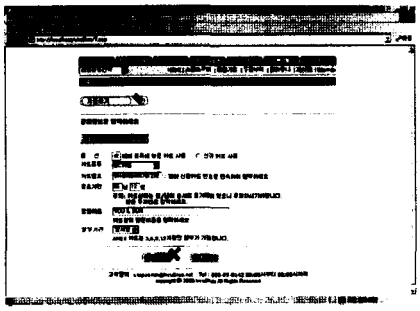
Internet Security Corp.

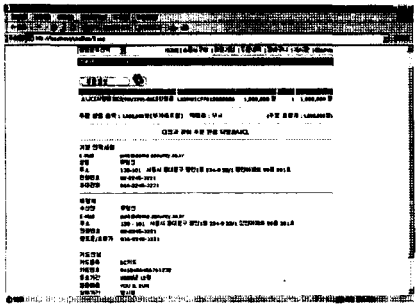
전자상거래 – 웹쇼핑 (II)



20 / 25

전자상거래 – 웹쇼핑 (III)





개발 방향

- 다양한 응용 프로그램과 연동
  - Software Development Kit 제공
  - 전자 메일 클라이언트, 웹 브라우저 Embedding
- 표준 인터페이스 수용
  - PKCS #11, Microsoft Crypto API (MS CryptAPI), Java Cryptography Environment (JCE)
- 다양한 OS 지원
  - Linux, Sun, IBM, HP 등
- 다양한 응용 인증 방법 적용
  - 지문 인식 기능 내장
  - 다른 생체 인식 분야와 연동

결 론

- 기존 IC카드 시스템을 대체할 수 있는 차세대 IC카드 제품
- 휴대와 사용이 간편하며 국제 및 국내 표준 준수
- 현재 다수 은행 및 증권사와 구축 협의 중
- 타 회사에서 인터넷 전자상거래 응용에 접목을 지원하기 위한 개발 키트 보급
- 다양한 응용과 기존 시스템에 접목 필요

참고 문헌

- Internet Security Co., Ltd., SECUREKEY™ *API Reference*, Aug. 2000
- Internet Security Co., Ltd., *SecureCenter® Administrator's Manual*, Oct. 1998
- Microsoft Development Network, Jul. 2000
- Chris Cant, *Writing Windows WDM Device Drivers*, R&D Books, 1999
- Dekker & Newcomer, *Developing Windows NT Device Drivers: A Programmer's Handbook*, Addison Wesley, 1999
- Richard Grimes, *Professional DCOM Programming*, WROX, 1997
- Sun Microsystems, Java Cryptography Environment documents
- RSA Security Co., PKCS documents
- IETF, ISO, RFC Standard documents
- William Stallings, *Cryptography and Network Security: Principles and Practice 2nd ed.*, Prentice-Hall, 1995
- A. J. Menezes, P. C.van. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997
- Intel, Motorola, Zilog, Dallas, Microchips, Pairchild, Atmel, Samsung, Hyundai Databooks

Q & A

SECUREKEY™

INTERNET SECURITY
http://www.security.co.kr
internet@security.co.kr

http://www.security.re.kr (기술연구소)

25 / 25