디지털 케이블방송 인증 기술

2002. 10. 5

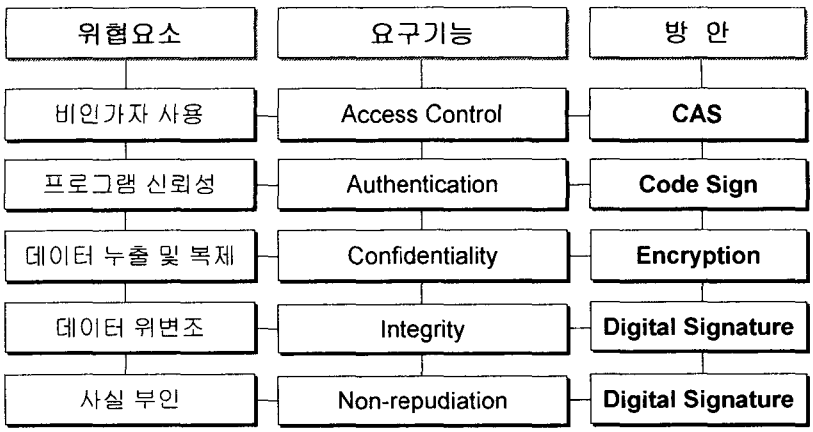
김 중 신
jskim@signgate.com

제1호 공인인증기관 KICA 한국정보인증
Korea Information Certificate Authority Inc

DCTV Security Needs

- **Service Provider**
  - 외부의 공격이나 비인가자의 서비스 접속 방지
  - Network을 통한 악의적인 소프트웨어 배포 방지
  - 효율적인 Damage Control
- **Content Provider**
  - 컨텐츠 불법 복제 및 도용 방지
  - Contents 보안등급
- **User**
  - 안전한 소프트웨어 다운로드(protect virus/worm/Trojans)
  - 개인정보 보호

Security Measures



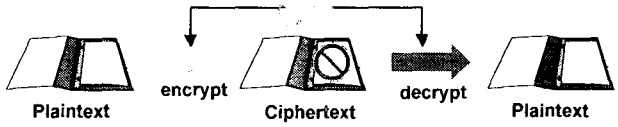
PKI Introduction

- **PKI : Public Key Infrastructure**
  - Authentication
    - Identification certified by TTP(Trusted Third Party)
    - Digital Signature : DSA, RSA, EC, KCDSA
  - Encryption
    - Symmetric encryption : DES, RC2/4/5, IDEA, SEED, etc
    - Public Key encryption : RSA, DH, ElGamal, EC, etc
  - Integrity
    - Hash Funtion : SHA-1, MD5, etc
    - Massage Authentication Code : HMAC-SHA, etc
    - Digital Signature : RSA, ECDSA, ElGamal, etc
  - Non-repudiation
    - Digital Signature : RSA, ECDSA, ElGamal, etc

Encryption

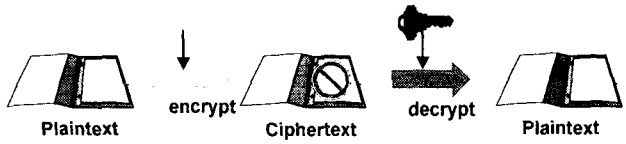
❑ Conventional : Fast but tough key management

Use the same Key to encrypt/decrypt



❑ Public Key : less fast but better key exchenge

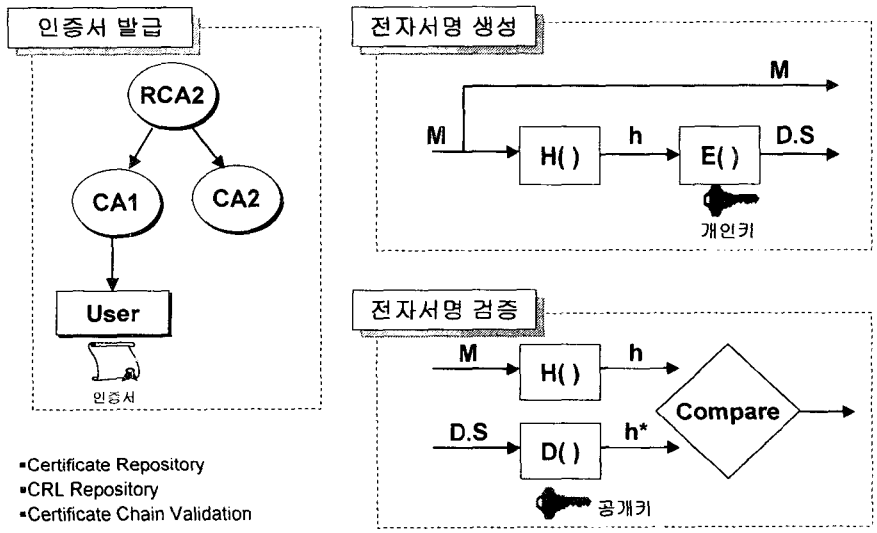
Use different key to encrypt/decrypt



4

KICA 한국정보인증주식회사

Digital Signature



- Certificate Repository
- CRL Repository
- Certificate Chain Validation

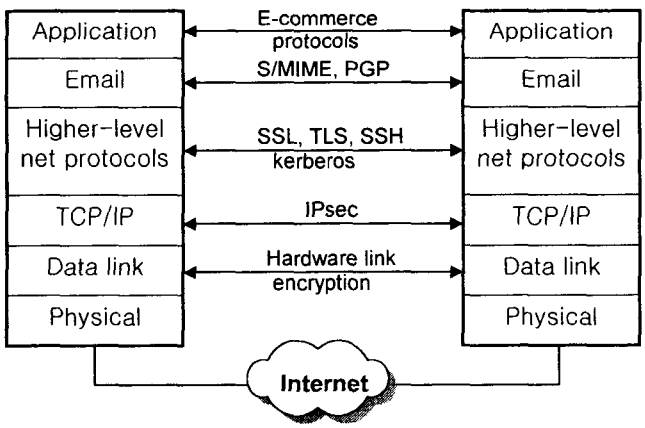
5

KICA 한국정보인증주식회사

Digital Signature(cont')

- **NIST, FIPS186-1 DSS(Sigital Signature Standard)**
  - **DSA(Digital Signature Agorithm)**
    - **Sign only**
  - **RSA(Rivest, Shamir, Adleman)**
    - **RSA Security**
    - **Sign and Encryption**
  - **EC(Elliptic Curve)**
    - **Shorter key length**
    - **Sign and Encryption**
    - **Fast computation**
    - **@Wireless PKI**
- **Related Hash function**
  - FIPS 180-1(Secure Hash Standard) : SHA-1

Security Protocol Layers

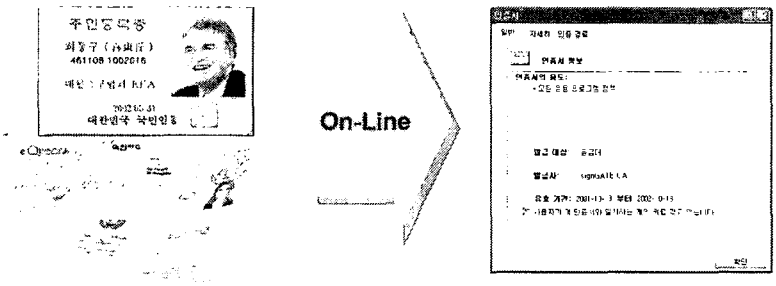


The further down you go, the more transparent it is.
The further up you go, the easier it is to deploy

Digital Certificate

- 동사무소, 대사관
- 면허시험장, **etc**

- Certificate Authority



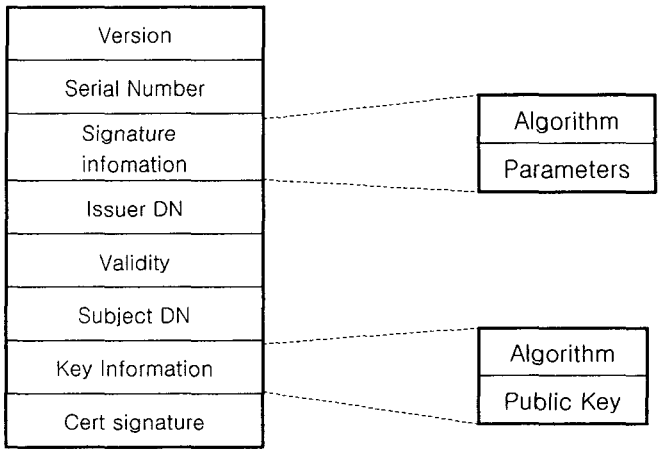
- SSN/Picture
- Finger Print
- Authority Stamping

- Digital File
- Authority Digital Signature

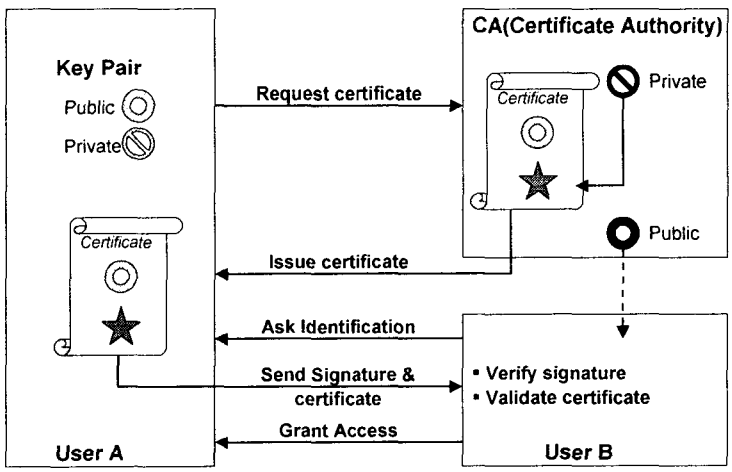
X.509 Certificate

- **ITU-T standard for providing the certification service based on the PKI**
- **Security service at application level**
  - Lower layer : SSL/TLS, Ipsec
- **Description**
  - Certificate Profile
  - Procedure and structure
  - Certificate Management Protocol
  - Certificate Request Message Format
  - Certificate Revocation List(CRL) definition, etc
  - Online Certificate Status Protocol
- **Related : IETF PKIX**
  - RFC2459, RFC2259/2260/2285/2287, RFC2510/2511, etc

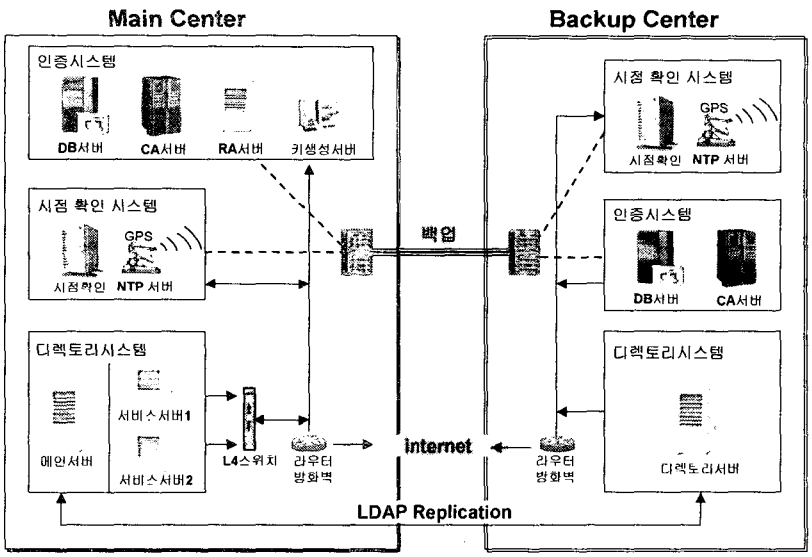
X.509 version3 Profile



X.509 Issue and Chain

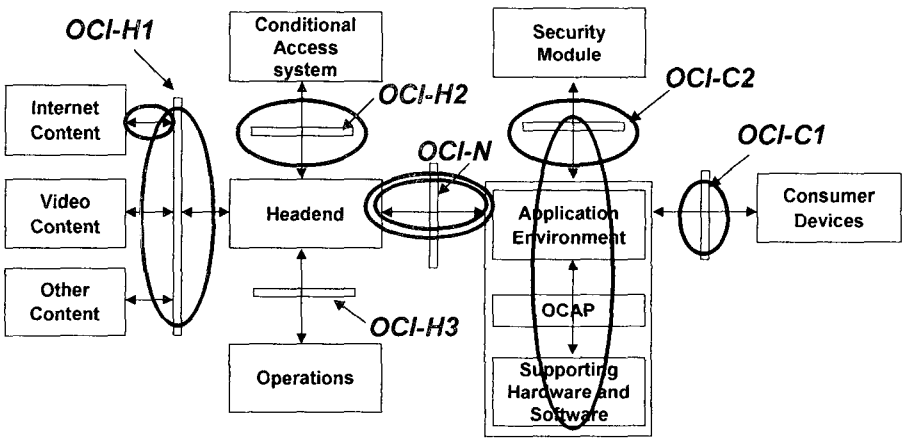


Certificate Authority System



KICA 한국정보인증주식회사

OpenCable Architecture

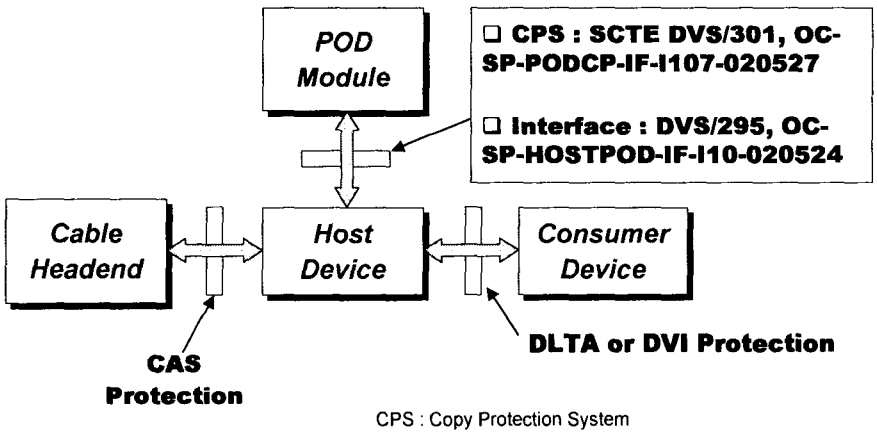


KICA 한국정보인증주식회사

Download Software Authentication

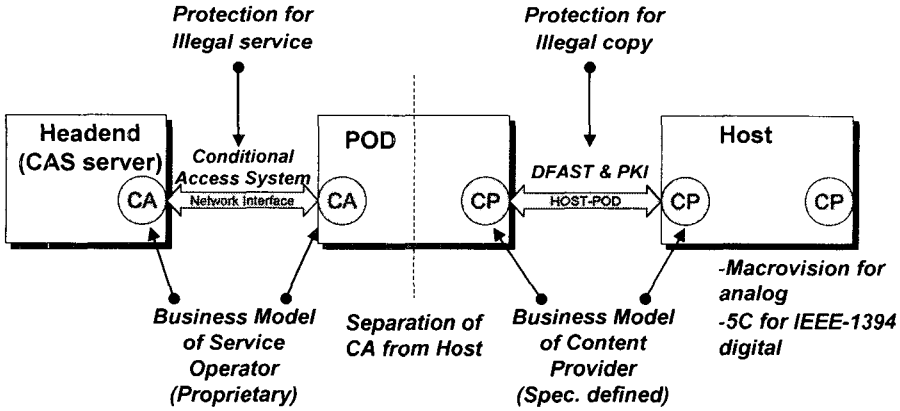
- **Acess privilege control with Digital Signing**
  - Grant Limited access of Platform resources to unsigned application
- **Code Signing**
  - Digital signing with distributor's certificate issued by Trusted Third Party
  - MicroSoft Signed Cabinet Authentication
  - Sun Microsystem Signed Applet
- **Contents Signing**
  - Insure integrity of contents
  - Prevent hackers to tamper with their contents in any place of the distribution chain

CPS Device Specification



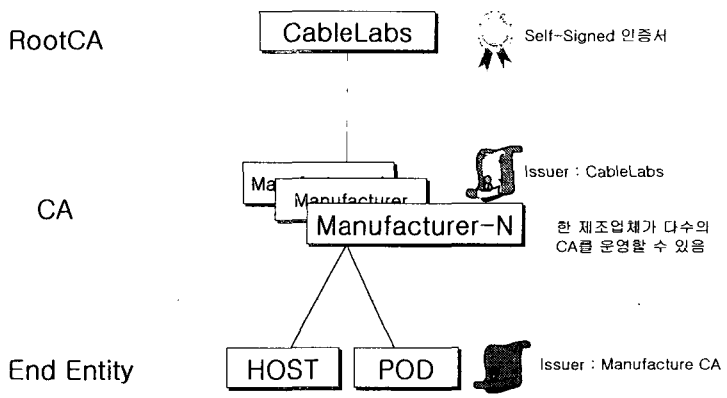
CPS : Copy Protection System
DTLA : Digital Transmission Licensing Administrator
DVI : Digital Visual Interface
CAS : Conditional Access System
POD : Point Of Deployment

Device Authentication



"Authentication based on PKI Certification"

OpenCable CA Hierarchy

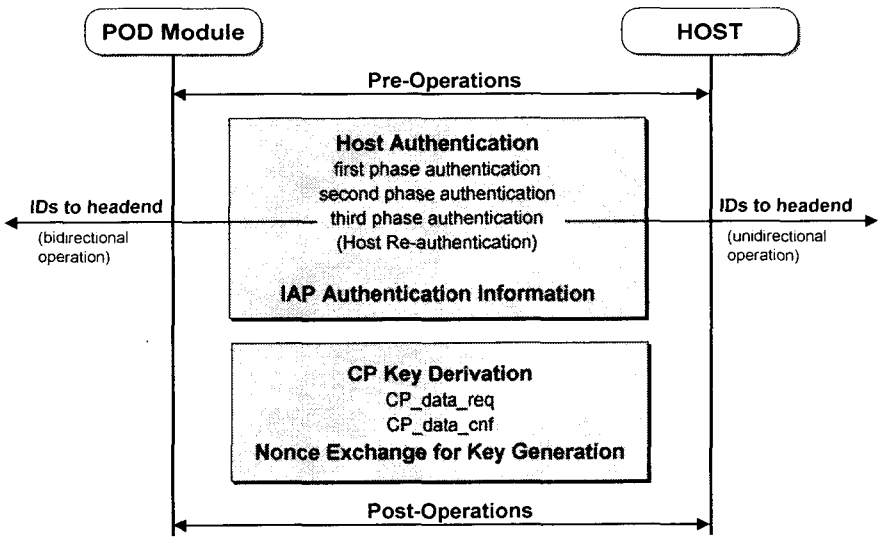


※ 인증서 발급 프로토콜 및 SO에 대한 CRL 배포방법은 명시적으로 지정되어 있지 않음

Components

- **Host**
  - CP decryption
  - CCI controlled content output
- **POD**
  - CA decryption & CP Encryption
  - CAS message termination and control
- **Headend**
  - CAS message generation
  - Authentication validity check
- **Root Certificate Authority(Root CA)**
  - Root and manufacture certificate issue
  - CRL(Certificate Revocation List) gerneration and handling

Overall Protocol



PKI Application

- Data channel protection
  - MPEG2 Transport Encryption
  - Copy Control Handling
- Key Derivation
  - DH key exchange
  - Authentication key and CP key generation
- Authentication
  - X.509 certificate
  - ID report-back
- Key management and Revocation
  - Key Refresh and CRL

ID Report-back

- Two-way system : Automatic report-back
  - 모뎀이나 리턴 채널이 지원될 경우
  - Host_DevCert/ POD_DevCert
  - Host/POD serial number
  - Host/POD Manufacture CA Name
- One-way system : Manual return
  - One-way 시스템 또는 unidirectinal host
  - Host_DevCert/ POD_DevCert
  - Host/POD serial number
  - Host/POD Manufacture CA Name
- Multiple hosts

X.509 v3 in OpenCable

구 분	규 격
인증서 형식	X.509 version 3
인증서 검증	RFC2459 except validity period
RDN 표기순서	C-O-[S]-[L]-OU-[OU]-CN
인증서 유효기간	- RootCA : 20 년이상 - CA & Device: 20 년
Key Length	- RootCA&CA : 2048 - Device : 1024
Algorithm	SHA-1withRSA

Host Authentication Parameters

❑ Device parameters

Keys	Size	Usage
DH keys(DH_pubKey_H, DH_pubKey_P)	1024 bits	D.S. Verify
Authentication Key($AuthKey_H$, $AuthKey_P$)	160 bits	CP Key generation

❑ System Parameters

Keys	Size	Usage
Host_ID	40 bits	Authentication
POD_ID	64 bits	Authentication
DH prime	1024 bits	publicKey generation
DH base	1024 bits	publicKey generation
RSA public signing key expoenent	0 bits	Signing and verify

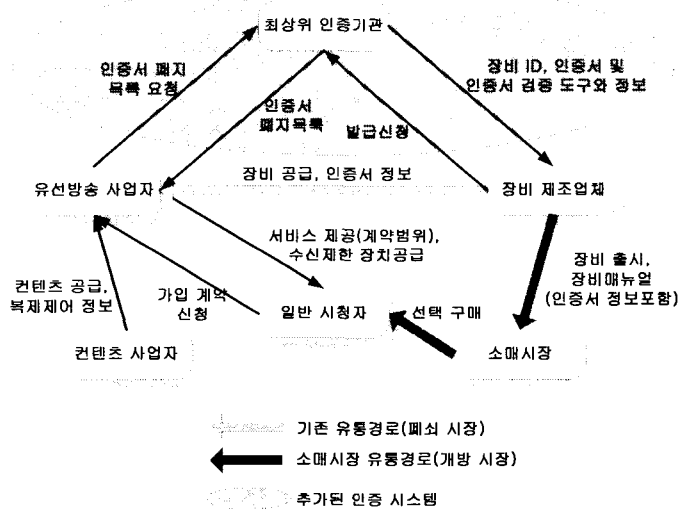
Keys and Parameters

Key or parameters	Size(bits)	Generation	Description
DHKey	408lsb for AuthKey, 224lsb for Ks	Public key exchange Function of [p,g] FIPS PUB 186-1, 140-1	408lsb of 1024 bits shared DH secret information. Long-term key, stored in NVM
AuthKey	160	SHA-1 digest with[DHKey, Host_ID, POD_ID] FIPS PUB 180-1	Result of Host authentication. Long-term key, stored in NVM
N_Host, N_module	64	FIPS PUB 186-1, 140-1	Temporary information for CP_key refresh
Ks	128	SHA-1 digest with [AuthKey, DHKey(lsb224), N_Host, N_module] FIPS PUB 180-1	128lsb of 160 bits SHA-1 digest. Session key
Ks_dfast (CP_Key)	56	DFAST[Ks]	MPEG2 TS DES-ECB key

Legal Commerce over DTV

- 관련 법.제도
  - 전자서명법 : **1999.7**월, **2002.4**월 개정
    - 인감날일과 동일한 법적 효력 부여
  - 전자거래기본법 : **1999.7**월
    - 전자서명을 통한 거래의 법적 효력 인증
- **PKI** 기반의 **e-Commerce** 인프라 구축
  - 인터넷뱅킹/사이버트레이딩등 공인인증서 사용 의무화
  - **G4C/G2B/**국세납부 등의 전자정부 프로젝트 구축
- **DTV**를 통한 **PKI** 기반의 **T-commerce** 환경 도래
  - 거래 사실에 대한 법적 효력 부여가 가능한 인증기반 도모

Device Certification System



Consideration

- ❑ 표준 규격 최대한 준용하되 국내 실정에 따라 일부 수정 적용
- ❑ 수신기 산업에 대한 국제적 유통 시장에서의 대응력을 고려
- ❑ 컨텐츠 공급자와 방송 사업자의 권익 보장
- ❑ 방송 수신자에 대한 인증 시스템에 따른 부담 최소화
- ❑ 디지털 유선방송 수신장치의 소매 시장 유통 구조 지향
- ❑ 수신장치에서의 인증 시스템 구현에 따른 부담 최소화
- ❑ 국내 유선방송 사업자간의 연대를 통한 통한 체계 구축
- ❑ 체계성을 고려하여 단일화된 인증 시스템 구축을 지향함
- ❑ 향후 확장성과 다른 시스템과의 연계를 고려하여 구성함

Q&A

Thank You !

한국정보인증 주식회사
100-791, 서울 중구 중림동 441
한국경제신문사 빌딩 9층
Tel : 02)360-3000
Fax : 02)3147-2684
http://www.signgate.com
kica@signgate.com