인터넷 우표의 보안기술

2000. 9. 19

김광조, 이병천
한국정보통신대학원대학교
암호와 정보보안 연구실
http://caislab.icu.ac.kr

목차

1. 인터넷 우표의 개요

- 전자우표 **(E-postage, digital postage)**
  - 기존의 우표의 기능에 부가정보를 추가 수록하여 우편통합시스템 관리상의 필수 정보로 사용
  - 인터넷을 통해 우편요금을 결제한 다음 전자우표를 다운로드하여 자신의 컴퓨터에서 봉투 또는 라벨에 인쇄
  - **2**차원 바코드 형태로 인쇄

- 전자우표의 이점
  - 이용자의 편의, 사회비용 절감
  - 우편 사업의 노동 집약 형태에 의한 인건비와 비효율성 측면을 개선

- **USPS(United State Postal Service)**에서 기술개발 선도 및 적용

e-stamp

stamps.com

2. USPS 전자우표 시스템의 보안기술

IBIP(Information Based Indicia Program)

- **USPS**의 우편통합서비스의 일환으로 정보기반인증을 적용한 인터넷 우표 사업
- 집중화된 데이타관리 지원과 안정적인 요금별납처리 및 안정적인 계측지원을 위한 도구로써 활용

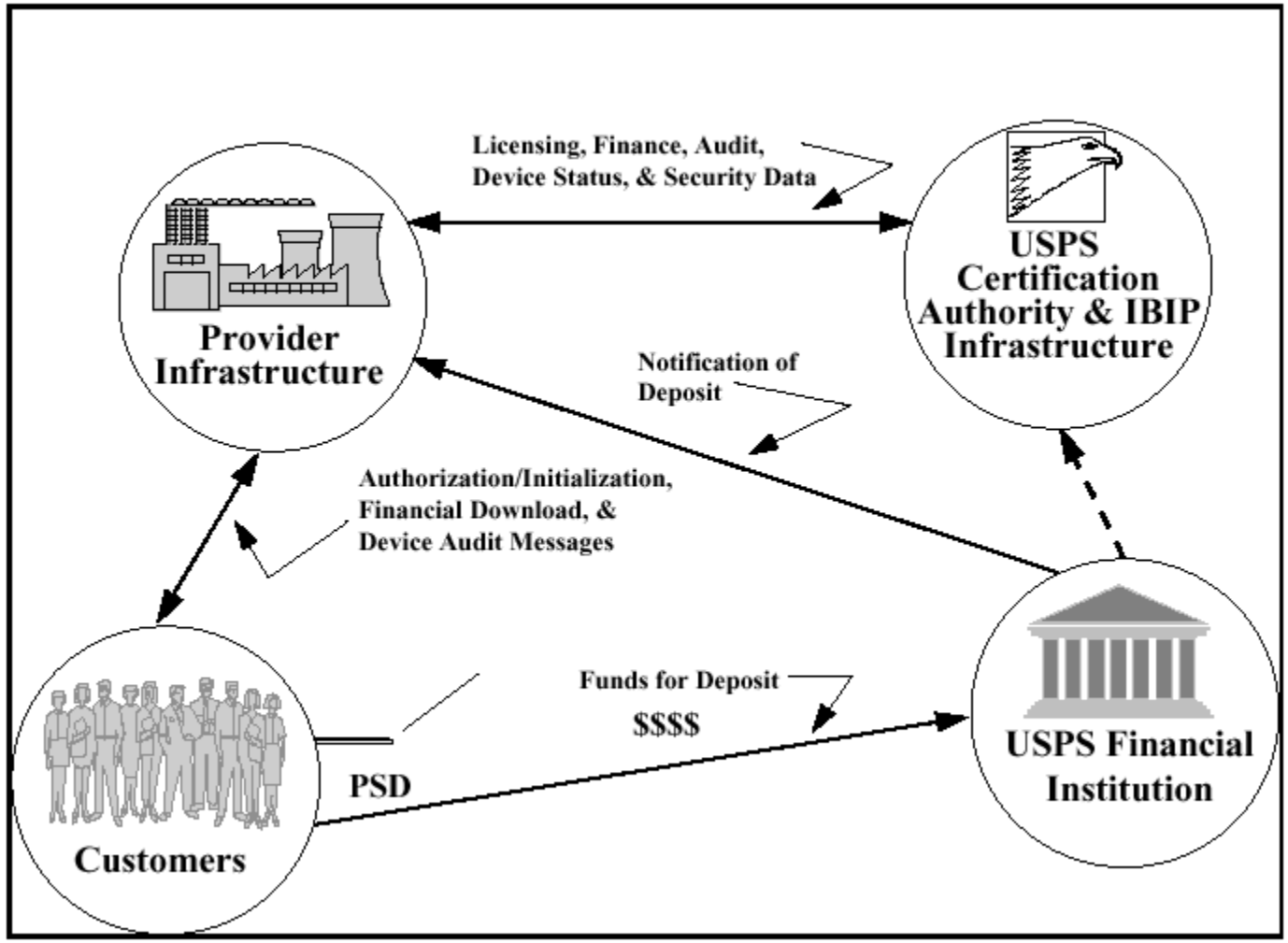
IBI(Information Based Indicia)

- 우편요금을 납부하였다는 증명을 표시하는 전자우표
- 봉투 또는 소포용 라벨에 **2**차원 바코드로 인쇄
- 수록 정보 **:** 우편번호, 발신지**/**수신지 주소, 전자인증내역, 중량, 우편요금, 발송일, 발송 장소, 고객의 **ID**, 우편요금 잔고 표시 등

PSD(Postal Security Device)

- 인터넷 우표의 위조 및 변조방지를 위한 하드웨어 장치

시스템의 전체 구조


Licensing, Finance, Audit,
Device Status, & Security Data
Provider
Infrastructure
USPS
Certification
Authority & IBIP
Infrastructure
Notification of
Deposit
Authorization/Initialization,
Financial Download, &
Device Audit Messages
Funds for Deposit
$$$$
PSD
Customers
USPS Financial
Institution

전자우표에 포함되는 데이터

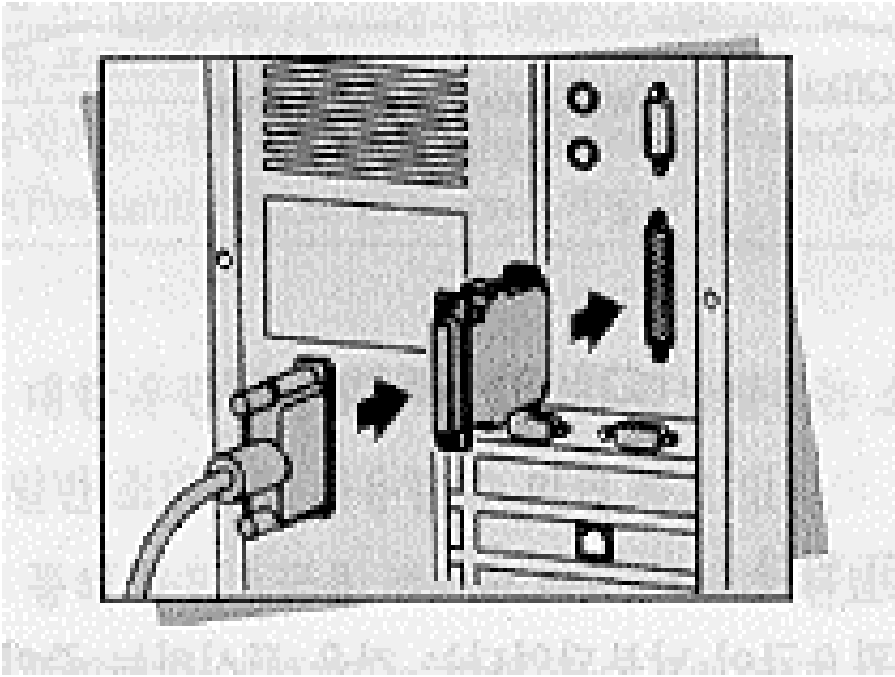
Data Elements	Barcode Data	Human-Readable Data	Length (bytes)	Field Number
Indicia Version Number	Yes	No	1	1
Algorithm ID	Yes	No	1	2
Certificate Serial Number	Yes	No	4	3
Device ID				
- PSD Manufacturer ID	Yes	Yes	2	4
- PSD Model ID	Yes	Yes	2	5
- PSD Serial Number	Yes	Yes	4	6
Ascending Register	Yes	No	5	7
Postage	Yes	Yes	3	8
Date of Mailing	Yes	Yes	4	9
Originating Address:				
- City, State, ZIP Code	No	Yes	---	---
- Licensing ZIP Code	Yes	No	4	10
Reserved Field 1	Yes	No	5	11
Software ID	Yes	No	6	12
Descending Register	Yes	No	4	13
Rate Category	Yes	No	4	14
Digital Signature	Yes	No	DSA 40 / RSA 128 / ECDSA 40	15
Reserve Field 2	Yes	No	Variable Size	16

전자서명을 이용한 신분인증, 부인방지 서비스

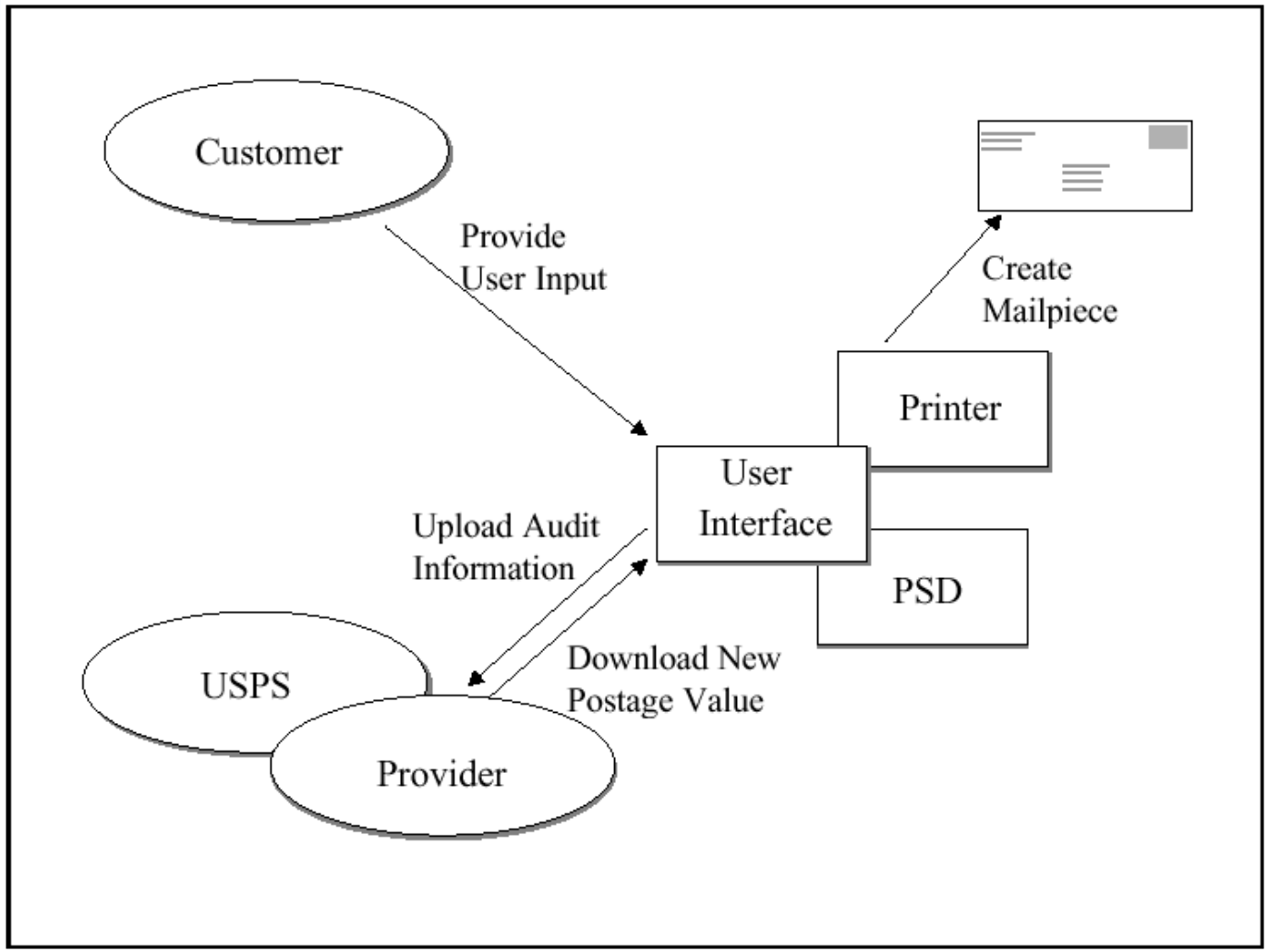
PSD (Postal Security Device)

PSD란?

- **IBIP**를 위해 정보보안 기능을 수행하는 하드웨어 장치
- 유일성을 가지는 하드웨어



전자우표 생성을 위한 **PSD**의 역할



PSD의 보안기능과 IBIP 함수의 관계

- **PSD**의 보안기능
  - **PSD** 초기화
  - 전자서명 생성 및 검증
  - 레지스터의 안전한 관리 : 금액관리 및 전자우표 관리
- **IBIP**의 기능
  - 장치 인증
  - 전자지불
  - 전자우표 생성
  - 감사**(audit)** 기능

PSD Security Functions	IBIP Device Authorization	IBIP Financial Functions	IBIP Indicium Creation	IBIP Device Audit
Initialization	✓			
Digital Signature*	✓*	✓*	✓	✓*
Register Management		✓	✓	

3. 인터넷 우표에 사용되는 암호기술

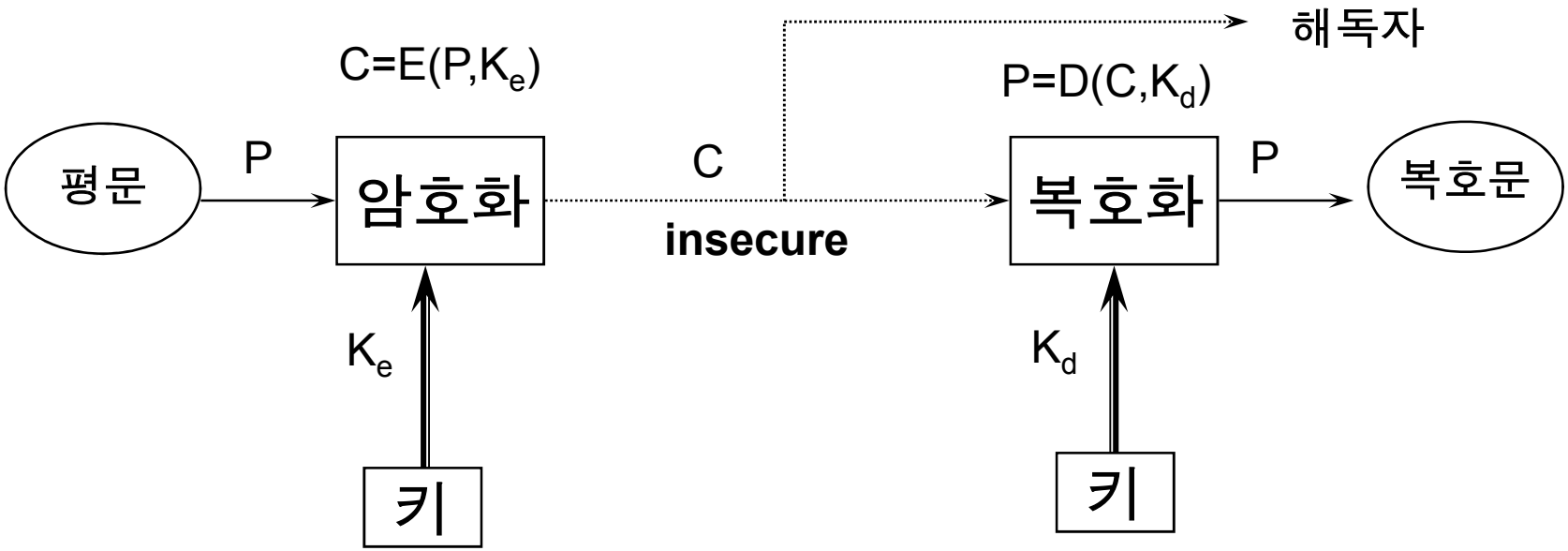
- **DSA (Digital Signature Algorithm)**
  - 미국의 전자서명 표준(**DSS**), **FIPS PUB 186**
- **RSA**
  - **PKCS #1: RSA Encryption Standard version 2.0**
- **ECDSA (Elliptic Curve Digital Signature Algorithm)**
  - **DSA**의 타원곡선 암호 버전
  - **ANSI X9.62 Standard (Working Draft), Elliptic Curve Digital Signature Algorithm.**
- **SHA-1(Secure Hash Algorithm)**
  - 전자서명에 사용되는 해쉬 암고리즘

암호기술이 제공하는 정보보호 서비스

- **Privacy (or confidentiality)** (기밀성)
  - 적법자만이 비밀정보를 보유
- **Data integrity**(무결성)
  - 불법적인 수단에 의해 정보의 변질되지 않음
- **Entity authentication (or identification,** 실체인증)
  - 실체의 **identity**를 확인
- **Message authentication** (메시지 인증)
  - 정보의 출처를 확인
- **Signature**(전자서명)
  - 정보와 실체를 연결하는 수단
- **Access control**(접근 제어)
  - 권한자에게만 재원의 접근을 허가
- **Non-repudiation**(부인봉쇄)
  - 사전의 행위나 동작을 부인 못하게 하는 수단

공개키 암호의 개념

- 두개의 비대칭 키를 이용하는 암호시스템
  - K_e : 공개키, 암호화 및 서명검증에 사용
  - K_d : 비밀키, 복호화 및 서명생성에 사용
- 기밀성과 인증성을 제공



전자서명의 요구조건

- 효율성 **(Efficiency) :** 서명문을 효율적으로 생성
- 위조불가**(Unforgeability):** 서명자만이 서명문 생성
- 서명자 인증**(Authentic):** 서명자를 확인가능
- 재사용 불가**(Not reusable):** 타문서의 서명으로 사용 불가
- 변조 불가능 **(Unalterable):** 서명된 문서의 변조 불가능
- 부인 봉쇄 **(Non-repudiation) :** 서명 후, 서명 사실 부인불가

3.1 DSA

▣ 키 생성

$$y = g^x \bmod p$$

공개키 : ***p, q, g, y***
비밀키 : ***x***

▣ 서명 생성

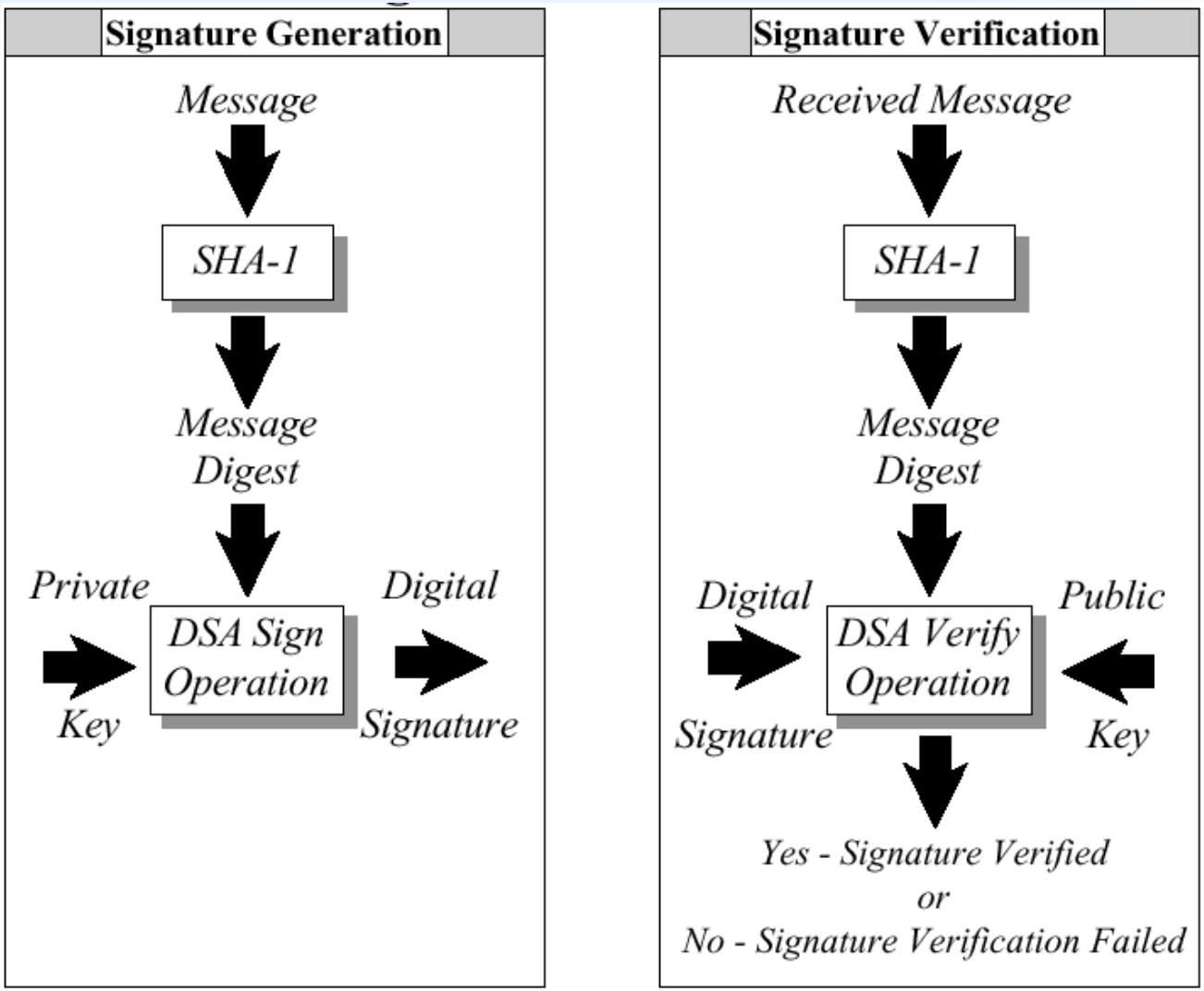
$$k \in_R Z_q$$
$$r = g^k \bmod p$$
$$s = k^{-1}(h(m) + xr) \bmod q$$

서명값 : **(*r, s*)**

▣ 서명 검증

$$r \overset{?}{=} g^{h(m)/s} y^{r/s}$$

3.1 DSA


Signature Generation
Message
SHA-1
Message Digest
Private
Key
DSA Sign Operation
Digital
Signature
Signature Verification
Received Message
SHA-1
Message Digest
Digital
Signature
DSA Verify Operation
Public
Key
Yes - Signature Verified
or
No - Signature Verification Failed

3.2 RSA 전자서명

▣ 키 생성

- **For large 2 primes *p,q, n=pq* ,$\phi(n)=(p-1)(q-1)$. : Euler phi 함수**
- **Select random e s.t. gcd($\phi(n)$, e) = 1**
- **Compute *ed* = 1 mod $\phi(n)$ -> $ed = k\phi(n) + 1$**
- **Public key = {e, n}, secret key = {d, {n}}**

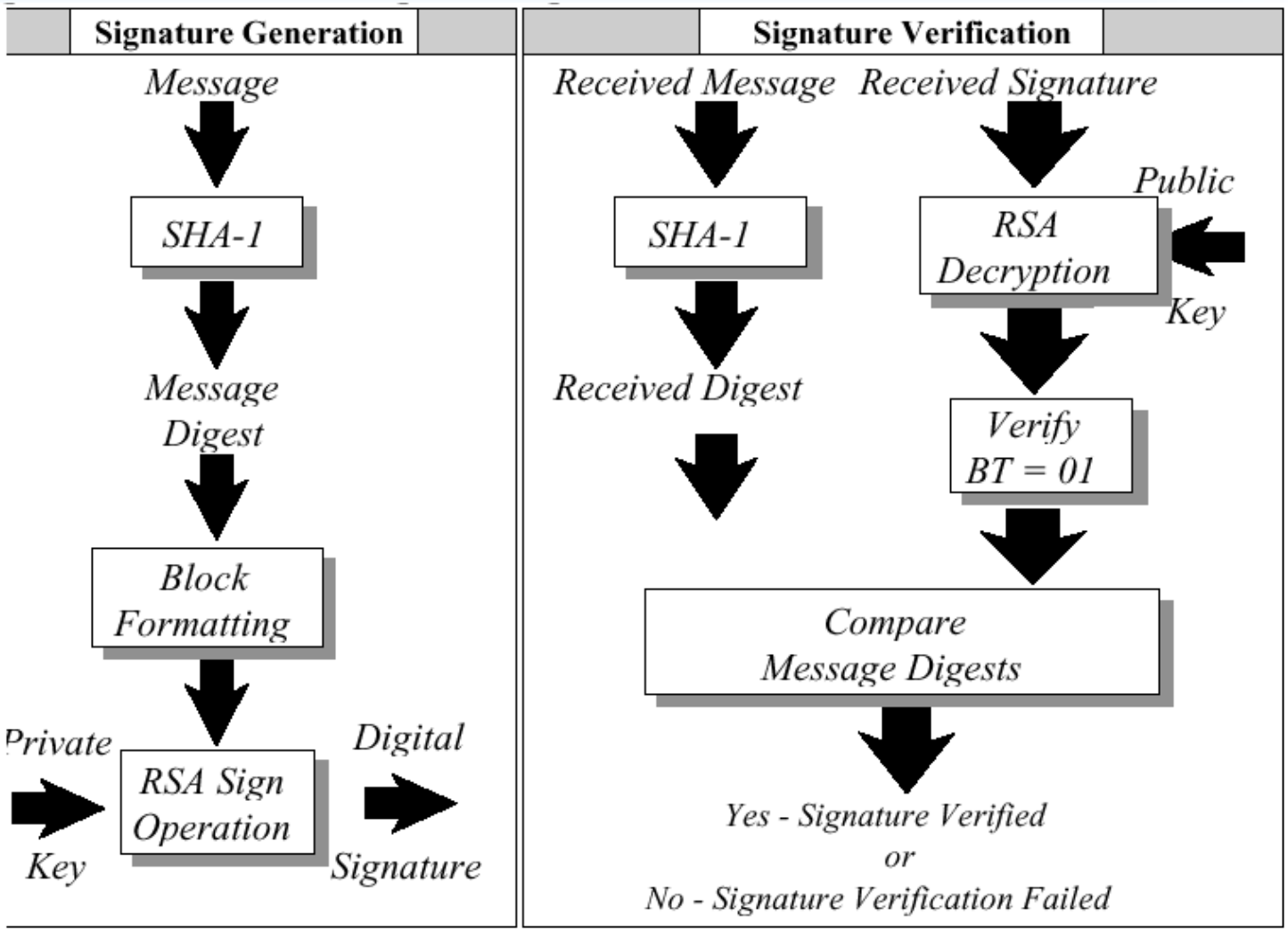
▣ 서명생성

$$s = h(m)^d \bmod n$$

▣ 서명 검증

$$h(m) \overset{?}{=} s^e \bmod n$$

3.2 RSA 전자서명


Signature Generation
Message
SHA-1
Message Digest
Block Formatting
Private Key
RSA Sign Operation
Digital Signature
Signature Verification
Received Message
Received Signature
SHA-1
Public Key
RSA Decryption
Received Digest
Verify BT = 01
Compare Message Digests
Yes - Signature Verified
or
No - Signature Verification Failed

3.3 ECDSA

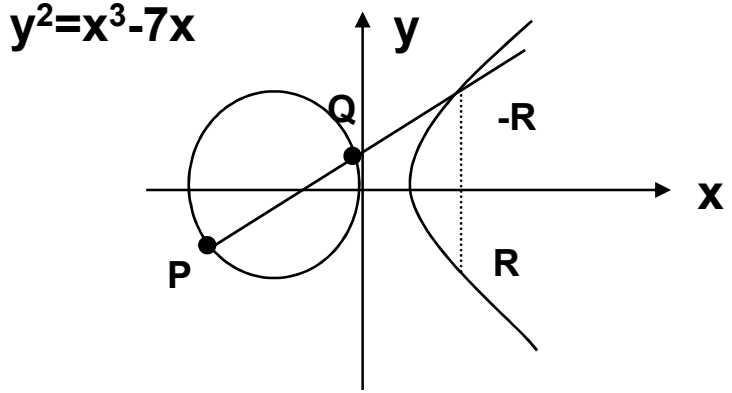
▣ 타원곡선

- 대수기하학적으로 **basepoint**를 가진 **genus(鐘數)**가 **1**인 **smooth** (편미분값이 **0**이 아닐 때) **curve**

$$E(K) = \{(x, y) \in K \times K : y_2 + a_1 xy + a_3 = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\vartheta\}$$

▣ 타원곡선 암호

- 타원곡선상의 덧셈군의 특성을 이용하여 이산대수문제의 어려움에 기반하는 공개키 암호 시스템



P=(-2.35,-1.86)
Q=(-0.1,0.836)
-R=(3.89,5.62)
R=P+Q=(3.89,-5.62)

유한체 Z_p^* 와 타원곡선 $E(F_p)$ 의 비교

Group	Z_p^*	$E(\mathbb{F}_p)$
Group Integers elements	{ 1, 2, . . ., p -1 }	Points (x, y) on E plus $\mathcal{O}$
Group operation	Multiplication modulo p	Addition of points
Notation	Elements: g, h	Elements: P, Q
	Multiplication: $g \bullet h$	Addition: $P + Q$
	Inverse: g^{-1}	Negative: $-P$
	Division: g / h	Subtraction: $P - Q$
	Exponentiation: g^a	Multiple: aP
Discrete Logarithm Problem,	Given $g \in Z_p^*$ and $h = g^a \bmod p$ find a	Given $P \in E(\mathbb{Z}_p)$ and $Q = aP$, find a

3.3 ECDSA

▣ 키 생성

$P \in E(Z_P)$ of order q 공개키 : E, P, Q, q

$Q = dP$ 비밀키 : d

▣ 서명 생성

$k \in_R Z_q$

$R = (x_1, y_1) = kP$

$r = x_1 \bmod q$

$s = k^{-1}(h(m) + dr) \bmod q$ 서명값 : (r, s)

▣ 서명 검증

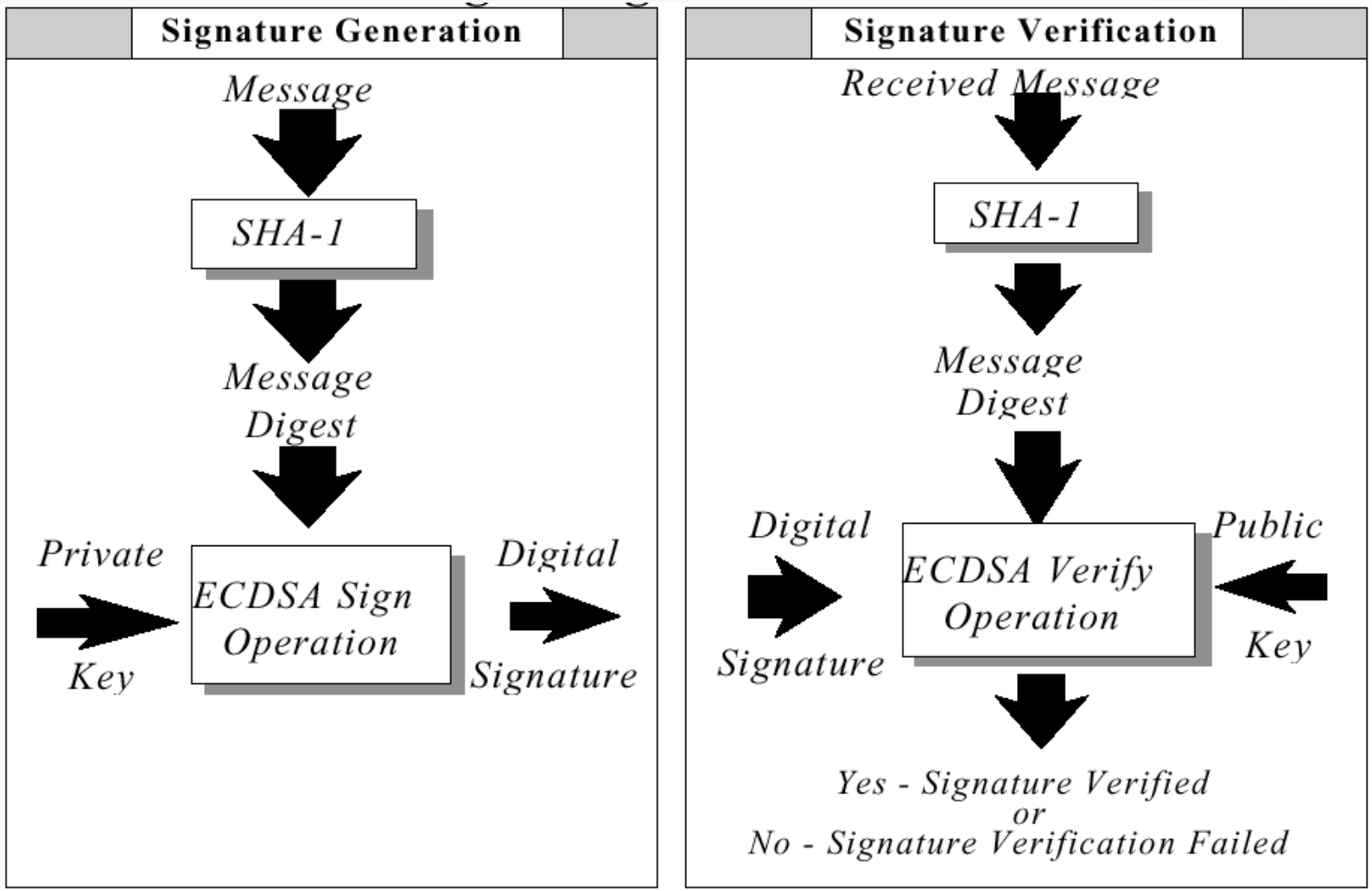
$u_1 = h(m)/s \bmod q, u_2 = r/s \bmod q$

$u_1 P + u_2 Q = (x_0, y_0)$

$v = x_0 \bmod q$

$v \overset{?}{=} r$

3.3 ECDSA


Signature Generation
Message
SHA-1
Message
Digest
Private
Key
ECDSA Sign
Operation
Digital
Signature
Signature Verification
Received Message
SHA-1
Message
Digest
Digital
Signature
ECDSA Verify
Operation
Public
Key
Yes - Signature Verified
or
No - Signature Verification Failed

ECC와 RSA 암호 비교

ECC 키크기	RSA 키크기	Time to break MIPS/Year	RSA/ECC 키크기
106	512	104	4.83:1
132	768	108	5.82:1
160	1024	1012	6.40:1
211	2048	1020	9.71:1
600	21000	1078	35.0:1

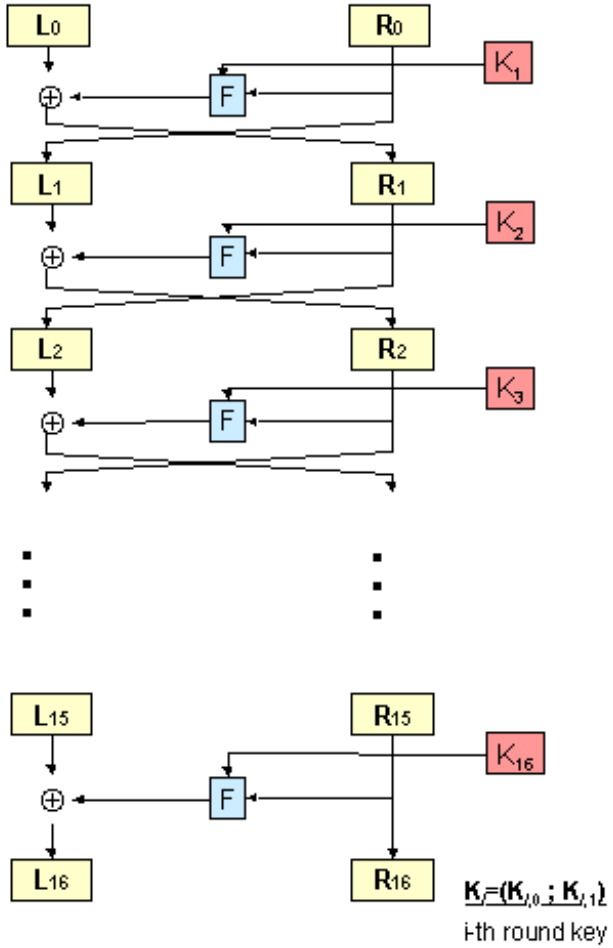
4. 국내 표준 암호 기술

- **SEED (Korean Data Encryption Standard)**
  - 128-bit symmetric block cipher
  - developed by ETRI, KISA, ADD + Academic
- **KCDSA (Korean Certificate-based Digital Signature Algorithm)**
  - developed by KCDSA Task Force Team
  - Financial support : KISA (Korea Information Security Agency), ETRI (Electronics and Telecommunications Research Institute)
- **HAS-160 (Hash Algorithm Standard)**
  - Financial support : KISA (Korea Information Security Agency), NCA (National Computerization Agency)
- **Reference**
  - KRyptoGate (Korean cRYPTOgraphers' GATEway) http://www.cryptogate.com
  - http://dosan.skku.ac.kr/~sjkim/Kr-Standard.html

4.1 SEED (대칭키 암호 표준)

- **SEED**
  - Symmetric Block Cipher
  - Block size, key size : 128-bit
  - Feistel structure
  - 16 rounds

- **Design criteria**
  - Provide security proof
  - Secure against DC, LC, Higher order DC, Related key attack
  - Faster than 3-DES in software
  - Use nonlinear function for round-key generation



4.2 KCDSA (전자서명 표준)

KCDSA (Korean Certificate-based Digital Signature Algorithm)

Domain Parameters

- ***p*** **: a large prime s.t.** $L_p = |\, p \,| = 512 + 256i \;\; \text{for } i = 0,1,...,6$
- ***q*** **: a prime factor of *p-1* s.t** $L_q = |\, q \,| = 128 + 32j \;\; \text{for } j = 0,1,...,4$

  Further, *(p-1)/2q* should be a prime or at least all its prime factors should be greater than *q*
- ***g*** **: a generator of order *q* mod *p***

User Parameters

- ***x*** **: signer's private signature key s.t.** $x \in_r Z_q$
- ***y*** **: signer's public verification key computed by** $y = g^{x^{-1}} \bmod p$
- ***z*** **: a hash value of *Cert_Data*, I.e., *z=h(Cert_Data)* where *Cert_Data* denotes the signer's certification data**

서명 생성 및 검증

Signature generation

- Generate a signature *(r,s)* for a message *m*
- Precomputation can be used for generating *r*

$$r = h(g^k \bmod p) \quad \text{with } k \in_r Z_q^*$$

$$s = x(k - r \oplus h(z \| m)) \bmod q$$

Signature verification

- On receiving *(m,r,s)*, check the validity of the signature

$$e = r \oplus h(z \| m)$$

$$r \stackrel{?}{=} h(y^s g^e \bmod p)$$

DSA, GOST, KCDSA의 비교

Schemes	$\|p\|$	$\|q\|$
DSA	$512 + 64i$ $(i = 0, 1, \cdots, 8)$	160
GOST	512 or 1024	256
KCDSA	$512 + 256i$ $(i = 0, 1, \cdots, 6)$	$128 + 32i$ $(i = 0, 1, \cdots, 4)$

Schemes	Signature Generation	Signature Verification
DSA [19]	private Key : $x \in_r \mathbf{Z}_q$	public key : $y = g^x \bmod p$
	$k \in_r \mathbf{Z}_q^*$ $r = (g^k \bmod p) \bmod q$ $s = k^{-1}(rx + h(m)) \bmod q$	$(y^{s^{-1}r} g^{s^{-1}h(m)} \bmod p) \bmod q = r$?
GOST [10]	$k \in_r \mathbf{Z}_q$ $r = (g^k \bmod p) \bmod q$ $s = rx + kh(m) \bmod q$	$(y^{-rh(m)^{-1}} g^{sh(m)^{-1}} \bmod p) \bmod q = r$?
KCDSA	private Key : $x \in_r \mathbf{Z}_q$	public key : $y = g^{x^{-1}} \bmod p$
	$k \in_r \mathbf{Z}_q^*$ $r = h(g^k \bmod p)$ $s = x(k - r \oplus h(z\|m)) \bmod q$	$h(y^s g^{r \oplus h(z\|m)} \bmod p) = r$?

4.3 Elliptic Curve KCDSA

Elliptic Curve Cryptosystem

- Stronger security and higher speed with smaller key size
- EC-KCDSA is under the standardization process

Signature Generation

$$r = h(kG) \quad \text{with } k \in_r Z_q^*$$

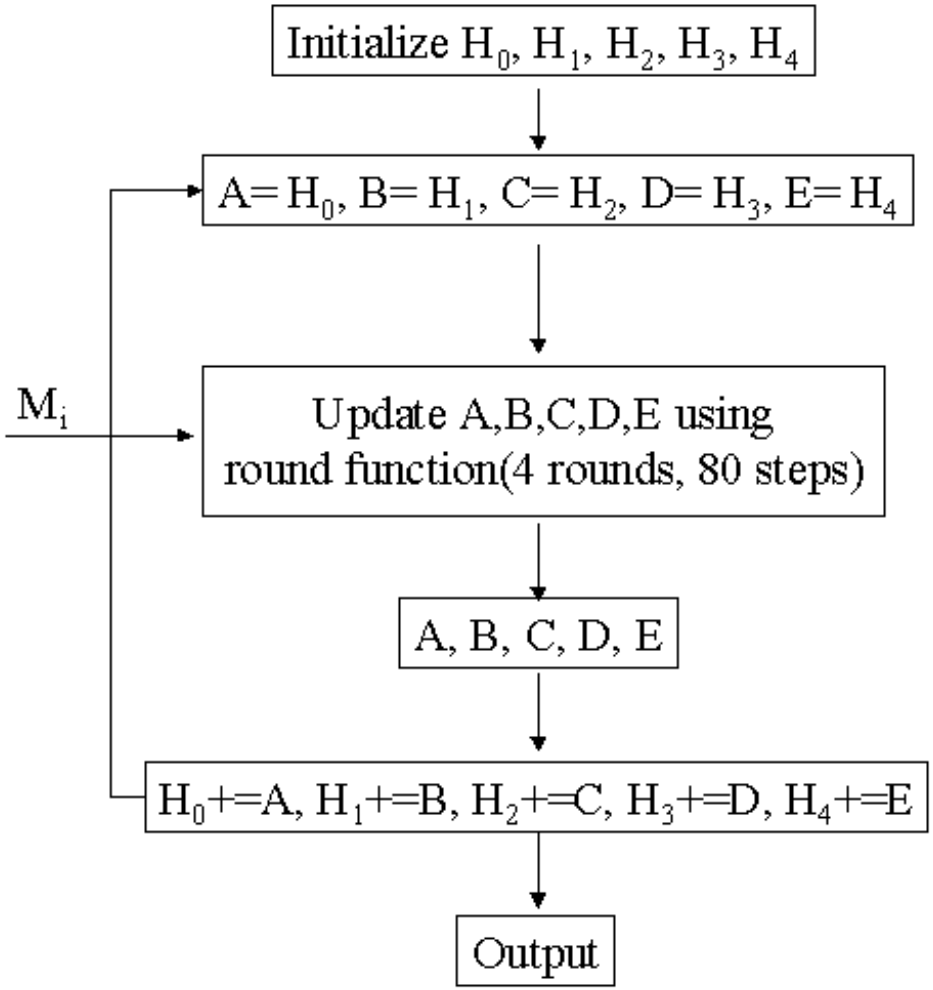
$$s = x(k - r \oplus h(z \,||\, m)) \bmod q$$

Signature Verification

$$e = r \oplus h(z \,||\, m)$$

$$r \overset{?}{=} h(sY + eG)$$

4.4 HAS-160 (해쉬함수 표준)



- **Input message block : 512 bit**
- **Output : 160 bit**
- **Compression function : 4 rounds, 80 steps**
- **5 chaining variables**
- **20 message variables**
- **Using little-endian convention**

5. 국내 PKI 구축 현황

▣ 전자서명법의 발효 : **1999. 8.**

▣ 전자서명법 제정의 목적

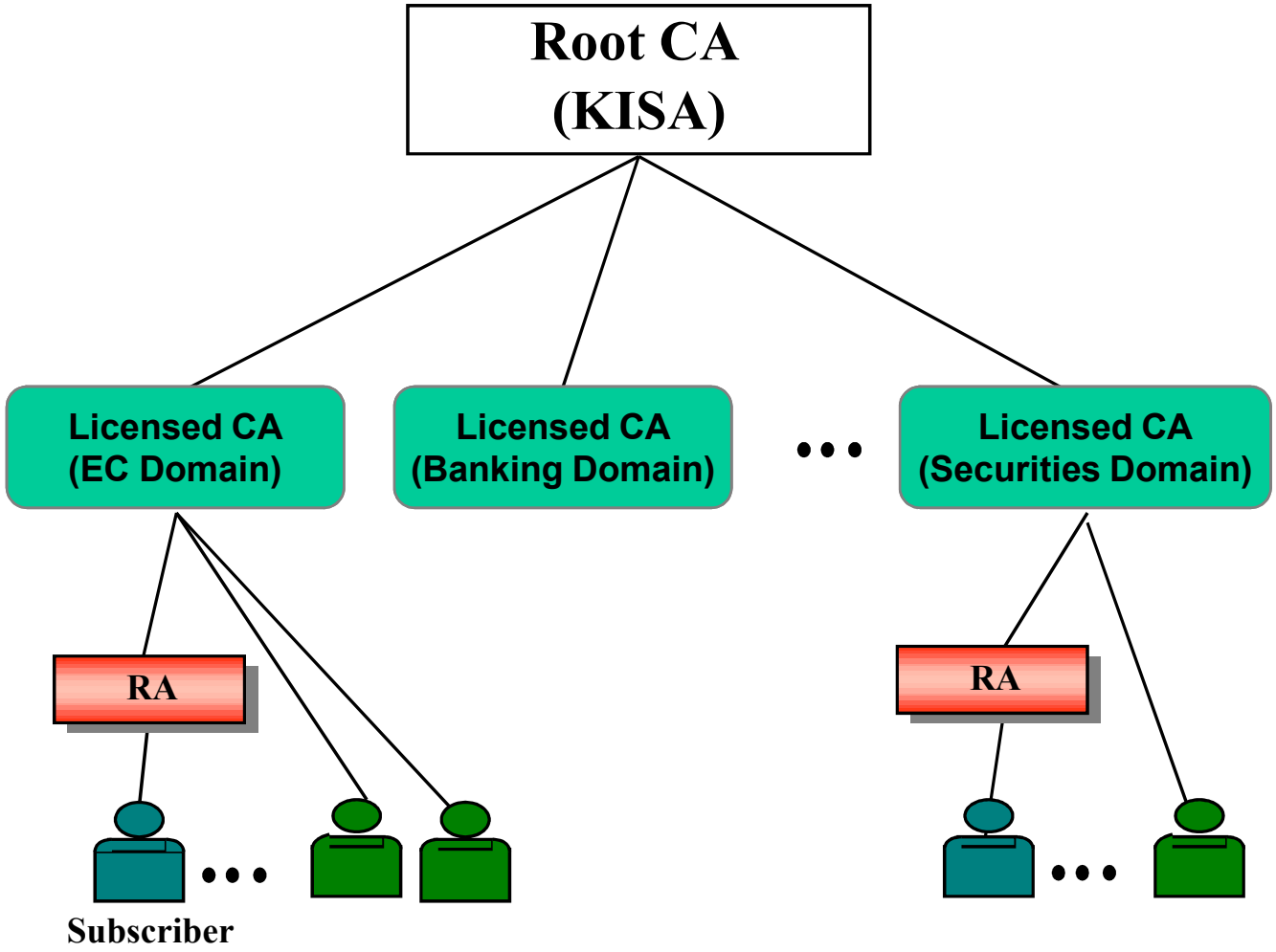
- 전자문서의 보안성 및 인증성 제공, 법적 책임 부여
- 전자상거래의 활성화
- 국내 **PKI(Public Key Infrastructure)** 구축

▣ 전자서명법안 **(1999. 2.** 제출**)**

1. KISA as Root CA

2. Operation of Licensed CA under KISA's Root CA

국내 PKI의 구조


Root CA
(KISA)
Licensed CA
(EC Domain)
Licensed CA
(Banking Domain)
Licensed CA
(Securities Domain)
RA
RA
Subscriber

Root CA의 역할

- **Operation of Digital Signature & Certification Scheme(PKI)**
  1. Issuance and Management of Certificates for Licensed CA
  2. Issuance and Management of CRLs for Licensed CA
  3. Time Stamp Service
  4. Development of CPS and Security Guidelines, etc.

     ※ CPS : Certification Practice Statement

- **Evaluation for Licensing CA**
  1. Security and Reliability of CA System Components
  2. Security and Reliability of Digital Signature Mechanism
  3. Physical and Personnel Security
  4. Network Security, etc.

Root CA의 역할

- Cross-Certification with Foreign Root CAs
- R&D of Digital Signature & Certification Technology
- Standardization for National PKI
  1. KCDSA/HAS-160(Korea Standard : October, 1998)
     - ※ KCDSA : Korean Certificate-based Digital Signature Algorithm(TTA.KO-12.0001)
     - ※ HAS-160 : Hash Algorithm Standard(TTA.IS-10118)
     - ※ TTA : Telecommunication and Technology Association
  2. RSA/SHA-1 (PKCS #1)
  3. SEED(Korea Standard : October, 1999)
     - ※ SEED : 128-bits Block cipher algorithm
- Cert/CRL profile(X.509 v.3 Cert, X.509 v.2 CRL)

PKI 구축 현황

▣ Root CA(KISA)

1. Root CA : Established on July 1999.
2. CPS of Root CA : Published on Aug. 1999.
   ※ CPS : Certification Practice Statement
3. Evaluation Criteria & Evaluation Manual : Oct. 1999.

http://www.rootca.or.kr

▣ Three Organizations preparing for Licensed CA

1. KICA for Electronic Commerce
   ※ KICA : Korea Information Certificate Authority
2. KFTCI for Banking
   ※ KFTCI : Korea Financial Telecommunications & Clearings Institute
3. KOSCOM for Securities
   ※ KOSCOM : Korea Securities Computer Corp.

6. 결론 및 향후 과제

- 보안기술의 역할 및 중요성
  - 이중사용 및 복제 등 불법 행위에 대한 대비책
  - 과금 수입의 감소 등 경제적인 손실 방지
  - 사용자와 운용자 등 모든 사람에게 보안에 관한 신뢰감 구축

- 기 확보된 보안 기술
  - 공개키 기반 구조**(PKI)**
  - 국내 표준 알고리즘**(SEED, KCDSA, EC-KCDSA, HAS-160)**의 이용
    - 향후 국제적인 호환을 고려해야 함
  - **RSA** 알고리즘은 호환 가능

- 필요한 보안 기술
  - 과금 정보 관리를 위한 전자 지불 프로토콜
  - **Tamper proof device(**예 **: Smart card, USB** 이용**)**의 제공 방법
  - 기술적 보안 기술 외의 총체적인 보안 대책 **(**관리적**,** 절차적**,** 법**/**제도 적**,** 물리적**)**