전자상거래와 정보보안

1999년 11월 20일

김종기
부산대학교

순 서

- 전자상거래에서의 정보보안의 필요성
- EC 보안 요구사항
- EC 보안 요소기술
- 암호기술
  - 대칭키 암호 vs. 비대칭키 암호
  - 해쉬함수
  - 디지털 서명
- 전자지불시스템
  - SET

디지털 경제의 대두

- "The Emerging Digital Economy" (미 상무성, 1997)
- 디지털 혁명의 도래
  - 가격 대비 컴퓨팅 파워의 비약적인 증가
    - 1MIPS당 1991년 $230에서 1997년 $3.42로 하락
  - 인터넷의 급격한 확산
    - 사용자가 1994년 3백만명에서 1998년 1억명으로 증가하였으며, 2005년 10억명으로 예상
    - 인터넷 통신량은 100일마다 두 배씩 증가
- 정보기술(IT) 발전은 막대한 경제적 효과를 가져옴
  - IT 산업의 성장율은 전체 경제의 두 배에 달함
  - IT 부문은1998년 GDP의 8.2% 차지하며 향후 급격한 증가가 예상됨
  - IT에 대한 투자는 전체 기업체의 장비 투자비의 45%에 이름
  - IT 제품 가격의 하락은 전반적인 인플레이션의 감소를 가져옴
    - 1997년, 1%의 인플레이션의 하락 효과

전자상거래 시장의 특징

- 시장접근의 용이성은 소비자의 인터넷 사용도와 밀접한 관련
- 기존 거래관행이나 규제와의 마찰 가능성 내포
  - 생산자와 소비자간 직거래가 이루어지고 시간과 공간을 초월하여 비대면적인 전자상거래 환경으로 변화됨에 따라 기존의 상거래와 관련된 상관행과 충돌 가능
- 다음 사항에 대한 전반적인 고려 필요
  - 정보인프라에 대한 접근 보장
  - 새로운 전자적인 환경에서 야기되는 법적인 불확실성의 최소화
  - 대금 자불 및 운송에 관련된 물류적인 문제의 해소
  - 정보시스템과 전자적인 거래에 대한 사용자와 소비자들의 신뢰 확보

EC 보안의 필요성

- INTERNET의 활용에 따른 보안 취약성 증대
  - 불특정 다수의 사용자 존재
  - Point of Entry의 다양성
- 상호운용성은 EC의 기본적인 요구사항 (Global Interoperability)
- EC의 안전성, 신뢰성 확보는 EC 활성화의 전제조건
- 개방네트워크상의 전자상거래 장애
  - 전자상거래의 확산에 가장 큰 장애요인은 개방네트워크체제로의 전환에 따른 보안문제
    - 메시지 가로채기
    - 문서의 유효성 부정
    - 개인정보의 불법적 수집
    - 해킹과 바이러스 침입에 의한 피해
- 컴퓨터 범죄 증가 추이(1998, CSI/FBI 컴퓨터범죄와 보안 설문조사)
  - 1997년에 비하여 16% 증가, 1996년에 비하여 22% 증가
  - 241개 설문 대상 기관에서 금융적 손실은 $136,822,000으로 1997년에 비하여 36% 증가
  - Exopa Terra사의 조사보고서는 컴퓨터와 관련된 범죄가 급속히 증가하고 있으며 경제적 피해액이 년간 1.2조 달러에 이른다고 발표

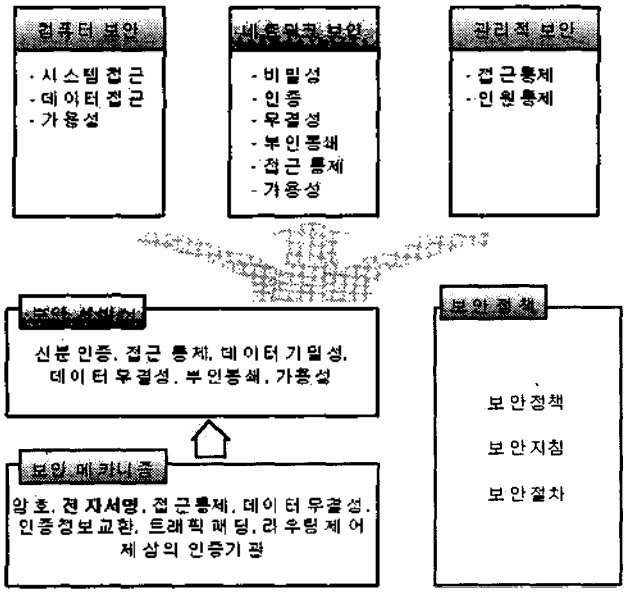
전자상거래에서의 피해유형

- 인터넷 사기
  - 인터넷을 통한 제품 및 서비스의 사기는 경매사기나 피라미드식 판매 등 다양한 형태로 나타남
- 내부자 정보 오남용
  - 내부자에 의한 정보 오남용은 컴퓨터 단말기 조작을 통한 금융사고가 주종을 이루며 내부자로부터 기밀정보를 빼내는 스파이활동 등이 있음
- 해킹
  - 외부자에 의한 해킹사고는 전산망에 침투하여 정보의 불법삽입, 변조, 유출, 파괴 등의 행위를 하여 금전적인 손실이나 정신적인 피해 등 유발
- 전자우편
  - 전자우편의 이용이 증가함에 따라 무분별한 광고성 전자우편 송신으로 인한 피해나 전자우편 폭탄이나 장난전자우편을 통한 피해 유발
- 개인정보 유출
  - 불법적인 개인정보의 유출로 인해 프라이버시의 침해를 유발하며 특히, 개인정보를 영리적으로 이용하여 심각한 피해 유발

EC 보안 요구사항

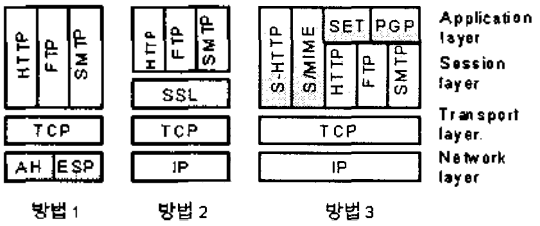
- EC 보안 위험요소
  - 통신과정에서 데이터의 도청, 불법적인 수정 및 삭제
  - 거래 참여자가 자신의 신분을 허위로 진술하거나, 송수신 행위를 부인
  - 비인가 사용자에 의한 시스템 해킹
- 판매자 요구사항
  - 구매자의 신분 확인을 위한 사용자 인증
  - 구매자의 물품구매 자격 확인
  - 공인된 인증기관에 의한 거래 확인 및 대금 지불 인증
  - 구매자의 주문 사실에 대한 부인봉쇄(nonrepudiation)
  - 대금지불을 보증하는 지불시스템
  - 판매자의 거래정보에 대한 익명성 보장
- 구매자 요구사항
  - 상품에 대한 인증
  - 판매자의 신분 확인
  - 대금지불 내용의 무결성 유지
  - 구매 사실의 확인을 위한 영수증 제공
  - 거래내역에 대한 정보의 비밀성 및 익명성 보장

EC 보안구조



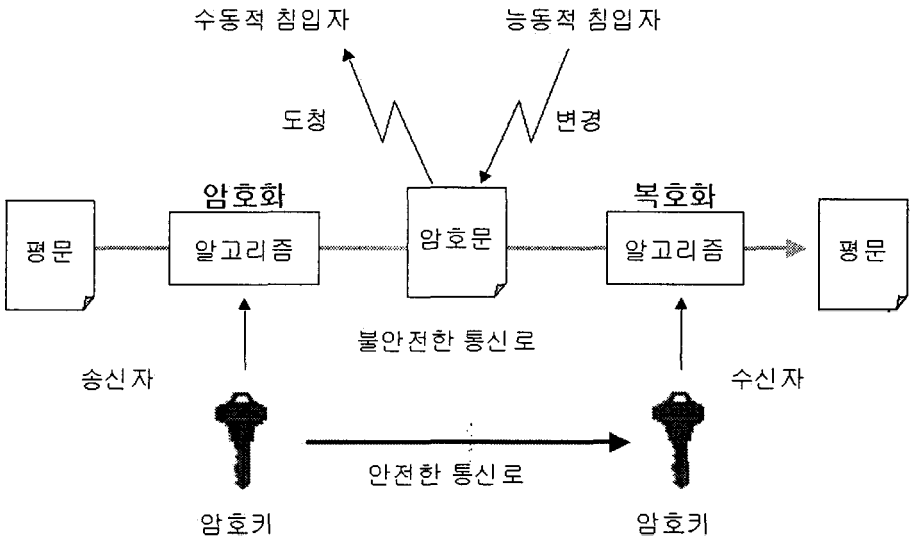
Internet 정보보안 기술

네트워크에서의
보안 표준 사용방법



표준	기능	어플리케이션
Secure HTTP(S-HTTP)	Secure Web transactions	Browsers, Web servers, Internet applications
Secure Sockets Layer(SSL)	Secure data packets at the network layer	Browsers, Web servers, Internet applications
Secure MIME(S/MIME)	Secure e-mail attachments across multiple platforms	E-mail packages with RSA encrytion and digital signature
Secure Wide-area Nets (S/WAN)	Point-to-Point encryption between firewalls and routers	Virtual private networking
Secure Electronic Transaction(SET)	Secure credit card transactions	Smart cards, transaction secure electronic commerce

암호의 기본 개념



암호 알고리즘

- 평문을 암호문으로 변환하는 일련의 규칙
- 대치 (Substitution)
  - 하나의 문자를 다른 문자로 바꾸는 것
  - CaesarCipher

$$c_i = E(p_i) = p_i + 3$$

treaty impossible → wuhdwb lpsrvvleoh

- 치환 (Transposition, Permutation)
  - 메시지 내의 문자의 순서를 재배치하는 것
  - columnar transposition

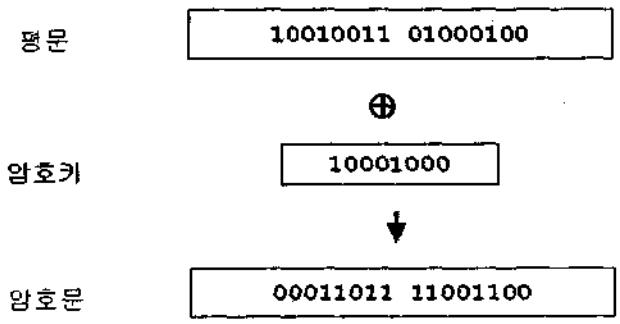
c_1	c_2	c_3	c_4	c_5
c_6	c_7	c_8	c_9	c_{10}
c_{11}	c_{12}	c_{13}	c_{14}	c_{15}

↓

$c_1c_6c_{11}\ c_2c_7c_{12}\ \cdots\ c_5c_{10}c_{15}$

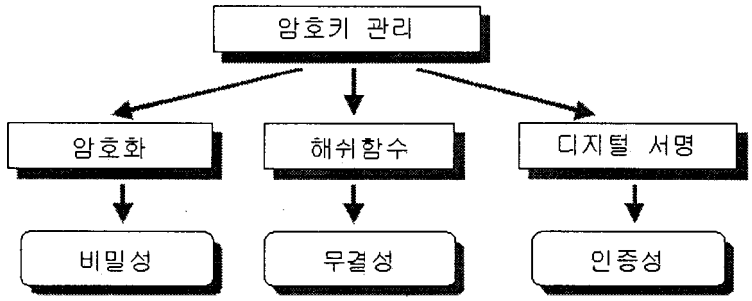
암호키

- 암호키를 변경함으로써 동일한 평문에 대해 상이한 암호문 생성 가능
- 암호 알고리즘은 공개하고 암호키의 보안성을 유지하여 암호의 안전성 도모
- 암호키의 길이는 암호 안전성의 주요 요소



암호에 의한 보안 서비스

- 비밀성 (Confidentiality)
  - 비인가자가 정보를 해독 불가능하게 하는 기능
- 인증성 (Authenticity)
  - 메시지 인증성 (Integrity, Message Authenticity)
    - 정보의 무결성 (Integrity)을 확인하고 보장
  - 개체 인증성 (Entity Authentication)
    - 상대 개체의 신원을 확인하고 보장
      - 개체 A가 개체 B에게 자신의 신분을 증명
      - 제3자가 개체 A로 위장 불가능



암호체계의 분류

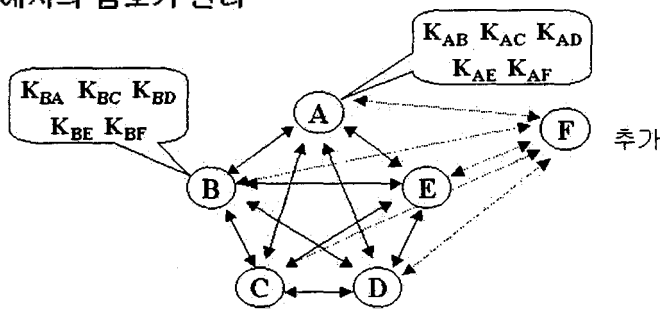
- 대칭 암호체계
  - (Symmetric Cryptosystem, Secret Key Cryptosysytem, Conventional Cryptosystem)
  - 암호화 및 복호화 암호키가 동일 (One Key)
  - 암호화와 복호화 과정이 동일 (Symmetric)
  - 암호키를 비밀로 유지 (Secret Key)
- 비대칭 암호체계
  - (Asymmetric Cryptosystem, Public Key Cryptosystem)
  - 암호화 및 복호화 암호키가 상이 (Two Keys)
  - 암호화와 복호화 과정이 상이 (Asymmetric)
  - 암호화 암호키는 공개 (Public Key), 복호화 암호키는 비밀로 보유 (Secret Key)

DES (Data Encryption Standard)

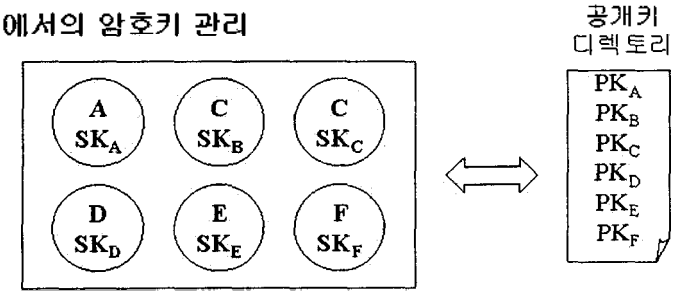
- IBM의 Lucifer암호를 수정하고 단순화 함
- 미국 NBS가 1977년 연방표준으로 채택
  - FIPS PUB 46, 74, 81, 112, 113, ANSIX3.92 (DEA: Data Encryption Algorithm)
  - 미국의 금융정보보호 표준
- 연방정부의 비밀이 아닌 민감한 정보 보호용으로 개발
- 민간부문에서 가장 잘 알려지고 널리 사용되는 블럭 암호 알고리즘
- NIST에 의하여 2번 재인증됨 (1997년 까지 인증되었으며, 현재는 AES 선정 작업이 진행 중)
- 구현속도
  - H/W : 1G bit/sec
  - S/W : 2.56 M bit/sec (80486, 33MHz)
- DES의 적용사례
  - 전자자금이체
    - 현금자동입출력기 (ATM) : 미국에서 매일 4000억$ 처리
  - UNIX 시스템 패스워드 암호화
  - EDI/CALS/EC에서 널리 활용

암호키 관리

- 대칭암호에서의 암호키 관리



- 비대칭 암호에서의 암호키 관리



비대칭 암호체계 개요

- Diffie-Hellman "New Directions in Cryptography," (1976)
- 특징
  - 암호키 분배 문제가 단순
  - 암호화와 복호화를 분리
- 기능
  - 암호화
  - 암호키 분배
  - 인증
  - 디지털서명
- 비대칭 암호체계의 구분
  - 정수론 문제에 근거
    - 소인수분해문제에 근거 (RSA(1978), Rabin(1979), Williams(1980)
    - 이산로그(Discrete Logarithm)문제에 근거 (Diffie-Hellman(1976), ElGamal(1985))
    - 평방잉여(Quadratic Residue)문제에 근거
  - NP 문제에 근거 : Merkle-Hellman(1978)
  - 부호이론에 근거 : ErrorCorrecting Code
    - McEliece(1978)
  - 타원곡선 (Elliptic Curve) 암호체계

RSA

- 대표적인 비대칭 암호체계
- Rivest, Shamir, Adleman (1978)
- 큰 합성수(예: 512비트)를 인수분해하는 문제의 어려움에 안전성이 근거
- 구성 : $n = pq$ (p,q는 소수)
  - 공개키 : n, e
  - 비밀키 : $d = e^{-1} \bmod (p-1)(q-1)$
  - 암호화 : $E(m) = m^e \bmod n$
  - 복호화 : $D(c) = c^d \bmod n$
- 예)
  - p=47, q=71, n=3347,
  - 평문 및 암호문 공간 [1,...,3346]
  - e=79, d= 1019
  - $E(688) = 688^{79} = 1570 \bmod 3347$,
  - $D(1570) = 1570^{1019} = 688 \bmod 3347$
- 미국 내에만 특허 (2000년 9월 만료)
- 구현속도 (512비트 RSA)
  - H/W (Chip) 64K bps (DES보다 1000배 느림)
  - S/W 1K bps 미만 (DES보다 100배 느림)

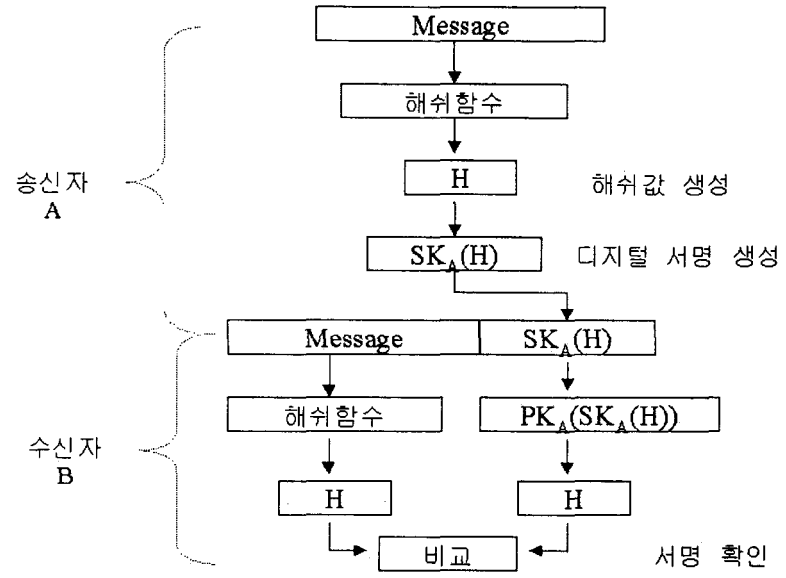
해쉬함수

- 임의의 길이를 갖는 입력값에 대하여 고정된 길이의 값을 출력
- 해쉬함수의 특성
  - 일방향성 (One Wayness)
  - 충돌회피성 (Collision Free)
  - 계산효율이 높아야 함
- 해쉬함수 사용목적
  - 메시지 인증
    - (암호화된 메시지) + (메시지에 대한 해쉬값)
  - 디지털 서명의 기본 요소
  - 컴퓨터 바이러스 점검
- 해쉬함수의 종류
    - 블럭암호 사용
      - ISO 표준안
    - 전용 해쉬함수
      - MD4 (Rivest, 1992)
      - MD5 (Rivest, 1992)
      - Snefru (Merkle, 1990)
      - N-Hash (NTT, 1990)
      - SHA (Secure Hash Algorithm)

디지털 서명

- 서류에 대한 친필 서명의 기능을 전자적인 정보에 구현
- 디지털 서명의 요건
  - 위조 불가능
  - 3자가 서명자의 서명을 검증 가능
  - 분쟁시 진위 확인 가능
- 디지털 서명의 종류
  - 인수분해문제에 근거
    - RSA (1978)
    - Feige-Fiat-Shamir (1986)
    - Guillou-Quisquater (1988)
    - ESIGN (1985)
  - 이산로그문제에 근거
    - ElGamal (1985)
    - Schnorr (1989)
    - DSA (Digital Signature Algorithm) (1991)
      - NIST의 디지털 서명표준에서 사용하는 디지털 서명 알고리즘

해쉬함수를 이용한 디지털 서명



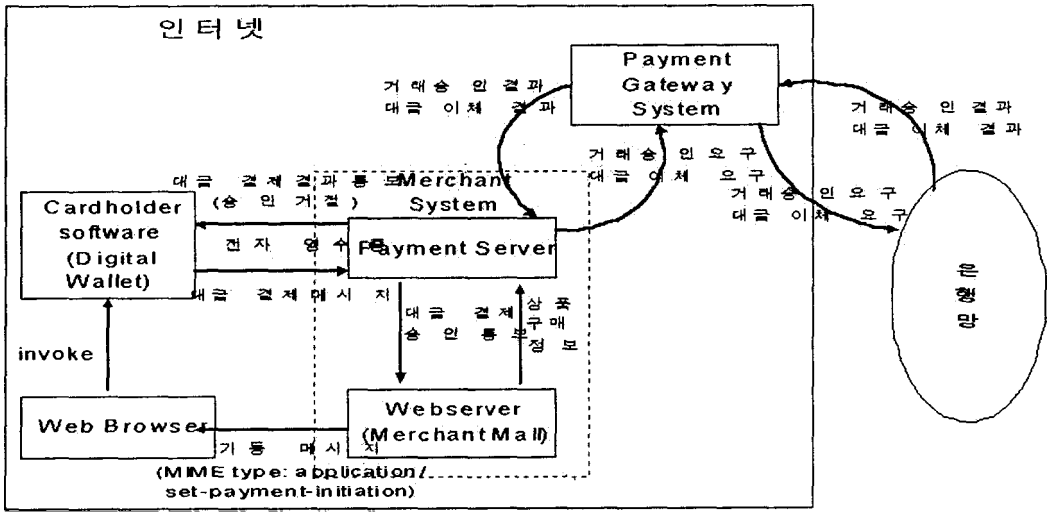
전자지불시스템

- 전자지불시스템의 필요성
  - 기존의 대금결제수단의 문제점은 새로운/개선된 지불수단을 요구함
    - 거래처리의 지연
    - 소액거래에 있어서 대금이체 비용의 과다
    - 결제정보의 유출
  - 안전한 지불수단은 전자상거래 확산의 전제조건
- 지불시스템의 유형
  - 전자화폐
    - Mondex (영국 Mondex International), CAFE (EU), NetCash (미국 Netbank), NTT 신전자현금 (일본 NTT), Millicent (DEC), Europay (EU)
  - 전자수표
    - NetCheque (미국 USC), NetBill (미국 CMU), CheckFree (미국), Red-Check (미국)
  - 신용카드 형
    - iKP (IBM), SET (Secure Electronic Transaction)

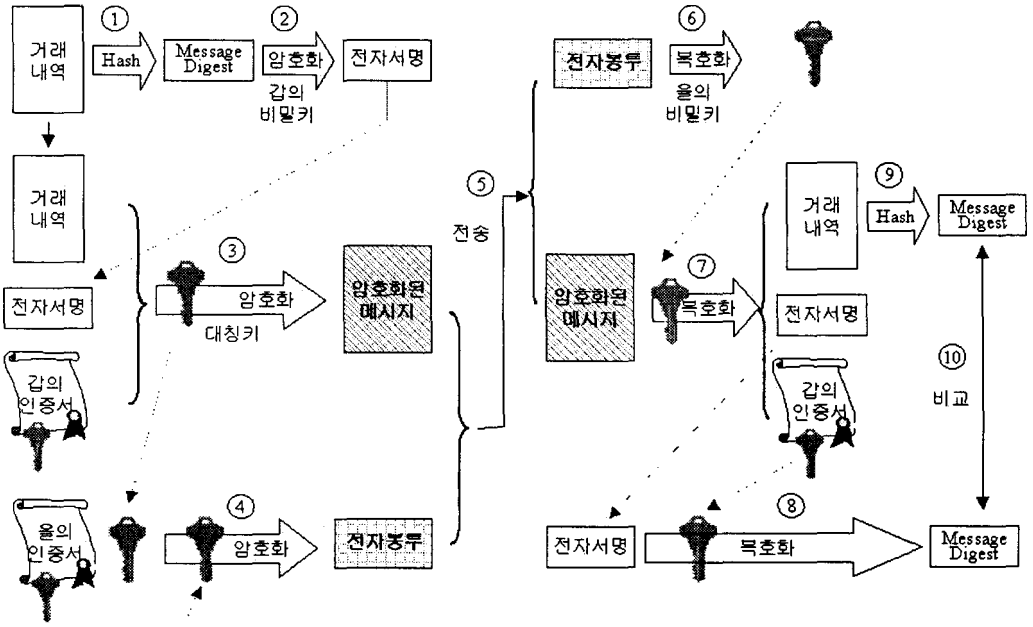
신용카드 기반 지불시스템

- 요구사항
  - 지불정보에 대한 비밀성 보장
  - 거래 당사자 신분의 인증
  - 전송 데이터의 무결성 보장
  - 암호 알고리즘 및 프로토콜의 정의
  - 응용 프로그램 간의 상호운용성 보장
  - 수용성
- SET Protocol
  - VISA와 MasterCard社 제안 (97년 7월 Version 1.0 발표)
  - de facto standard
    - GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa, VeriSign 등이 참여하고, American Express도 수용
  - 제공되는 Protocol명세
    - 고객등록, 상점등록, 구매요구, 지불허가, 지불확인
  - SET 참여자
    - 소비자 (카드 소유자), 발급기관, 상인, 상인측 금융기관 (Acquirer), 지불 Gateway, 카드 상표 (Brand)

SET 거래처리 흐름도

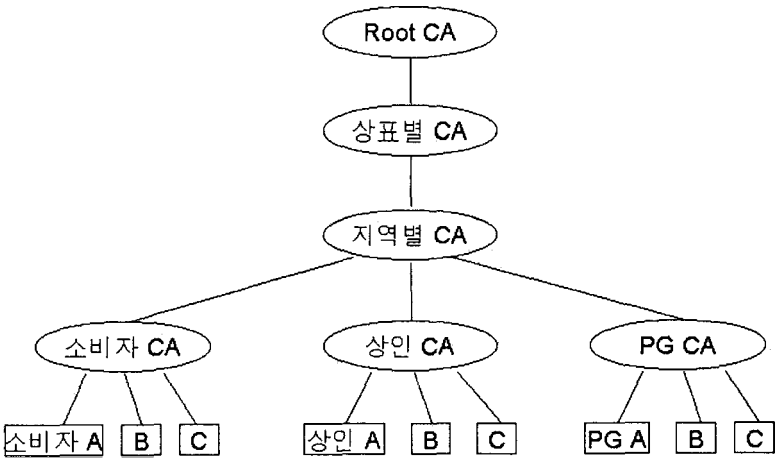


SET의 전자서명 처리 과정



25

SET 인증구조



26