정보보호 개론

Chapter 14 전자상거래 보안

목포해양대 해양전자통신공학부

전자상거래의 개요 (1)

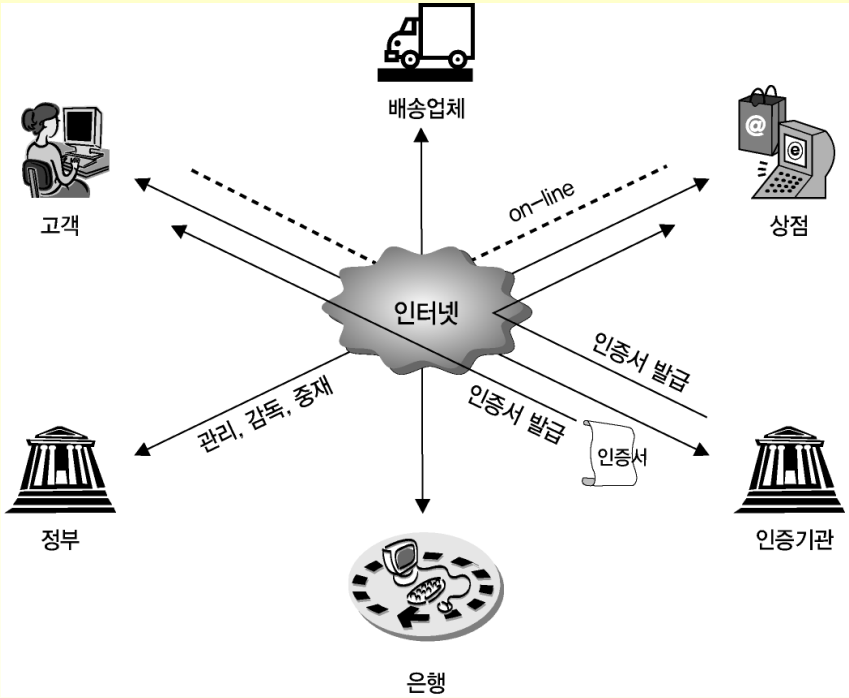
- 전자상거래
  - 인터넷 등의 개방형 네트워크를 이용하여 상품이나 서비스의 거래가 이루어 지는 것
- 전자상거래를 하는 목적
  - 상거래의 신속성과 효율성을 실현
  - 인터넷상에서 상거래와 관련된 모든 업무를 전자적으로 처리할 수 있는 환경을 실현
- 전자상거래 구분
  - B2C(Business to Customer)
  - B2B(Business to Business)
  - B2G(Business to Government)
  - BIE(Business In Enterprise)

전자상거래의 개요 (2)

- B2C
  - 기업과 개인 간에 전자상거래
  - 주로 개인과 온-라인 쇼핑몰 업체가 웹을 통해 물건을 거래하는 소매 분야에 활성화
- B2B
  - CALS (Continuous Acquisition & Life-cycle Support 또는 Commerce At Light Speed), EDI(Electronic Data Interchange)를 통한 기업간 전자상거래
  - 기업 이윤 증대
- B2G
  - 기업과 정부 간의 전자상거래
  - 조달, 행정, 인증 등 주요 공공정보 공증에 따른 정보 보호, 전자 입찰 등의 투명한 행정 구현 등의 효과를 제공
- BIE
  - 생산 관리, 기술 관리, 인원 관리, 판매 관리, 자금 관리 등 기업 내부 업무의 정보화와 관련된 전자상거래
  - 기업 내부 구조의 효율성 향상으로 기업 경쟁력을 향상하고자 제공되는 전자상거래 대상

전자상거래의 구성요소

- 고객
  - 상품이나 서비스를 구매하는 개체
- 상점
  - 상품이나 서비스를 판매하는 개체
- 은행
  - 고객과 상점 간의 결재를 중계하는 관리 기관
- 인증기관
  - 고객과 상점의 신원을 보증하는 제 3의 신뢰할 수 있는 기관



전자상거래의 실현 요구사항

- 통신 및 네트워크 기술
  - 멀티미디어 정보를 자유롭게 교환할 수 있는 컴퓨터 통신 기술과 네트워크 기술의 구축
  - 쌍방향 통신이 이루어지도록 표준화되고 합리적인 인터페이스와 소프트웨어 기준 확립
- 구조적인 체계
  - 상품 목록, 가격, 견적서 제시와 구입행위와 같은 거래내역, 부인봉쇄 기능 등을 제공하기 위한 구조적인 체계가 필요
  - 상호 신원 확인을 위한 인증구조 구축
  - 암호, 디지털 서명, 공개키 기반 구조, 인터넷 보안 기술
- 고객의 신용관리 방법 구축
  - 전자지불 결재방법, 확인방법, 청구서 수령 및 영수증 발행 등 고객의 신용 관리방법을 구축
  - SET 프로토콜, SSL 프로토콜, 전자화폐

전자상거래 보안 요구사항 (1)

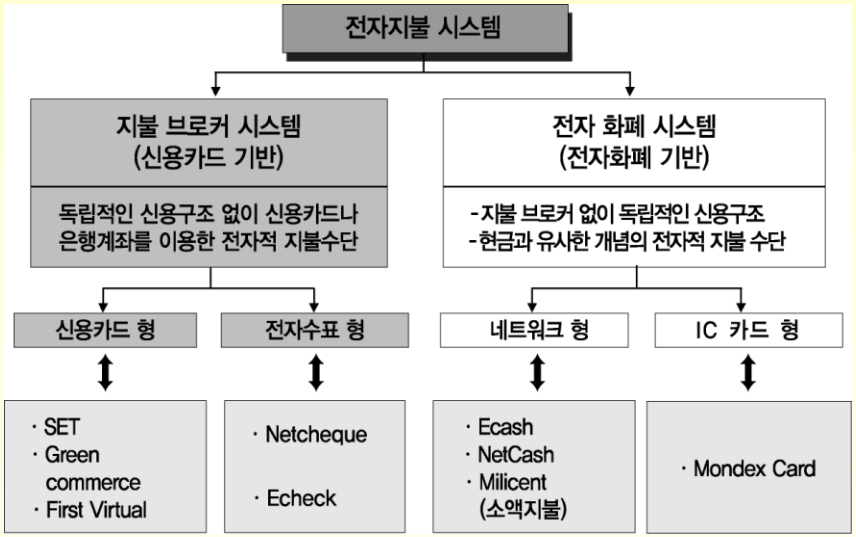
- 요구되는 정보보호 기반기술
  - 서로 간 높은 신뢰도를 가질 수 있도록 사용자인증과 메시지 인증기술로 거래 주체들 간에 상대방의 신원을 인증할 수 있어야 함
  - 무결성(Integrity) 기술로서 교환되는 전자 문서의 위·변조 여부를 확인할 수 있어야 함
  - 비밀성(Confidentiality) 유지
  - 부인방지(Non-repudiation)기능으로 거래 사실을 부인할 수 없도록 거래 사실을 증빙
- 전자상거래의 보안문제 해결
  - 전자문서의 위 , 변조 및 부인 방지를 위해서 전자서명 기술을 활용
  - 거래 상대방의 신원확인을 위하여 전자서명 인증 제도를 도입
  - 전송내용의 비밀유지를 위하여 비밀성 유지를 위한 암호화 기술 사용

전자상거래 보안 요구사항 (2)

- 전자상거래 구성 요소들에게 보안 기능을 제공하기 위한 보안 기술
  - 네트워크 계층(IP 계층)
    - IPSec이 적용
    - 종단간(end-to-end) 비밀성, 무결성과 인증 기능을 제공
  - 전송(transport) 계층
    - SSL/TLS가 적용
    - 종단간 비밀성, 무결성 및 인증 기능을 제공
  - 응용(application) 계층
    - 전자상거래 전용 SET(SET : Secure Electric Transaction) 프로토콜 개발
    - 비밀성, 무결성, 인증, 접근통제, 부인 방지 등의 서비스를 통합 제공
    - 지불 기능을 안전하게 제공

전자지불 시스템 (1)

- 신용카드나 은행거래를 이용한 전자적 지불 수단
- 별도의 인프라 구축 없이 기존의 구축된 금융 시스템을 이용하여 기존의 법과 제도 테두리 내에서 서비스의 제공 및 이용이 가능한 결재 시스템

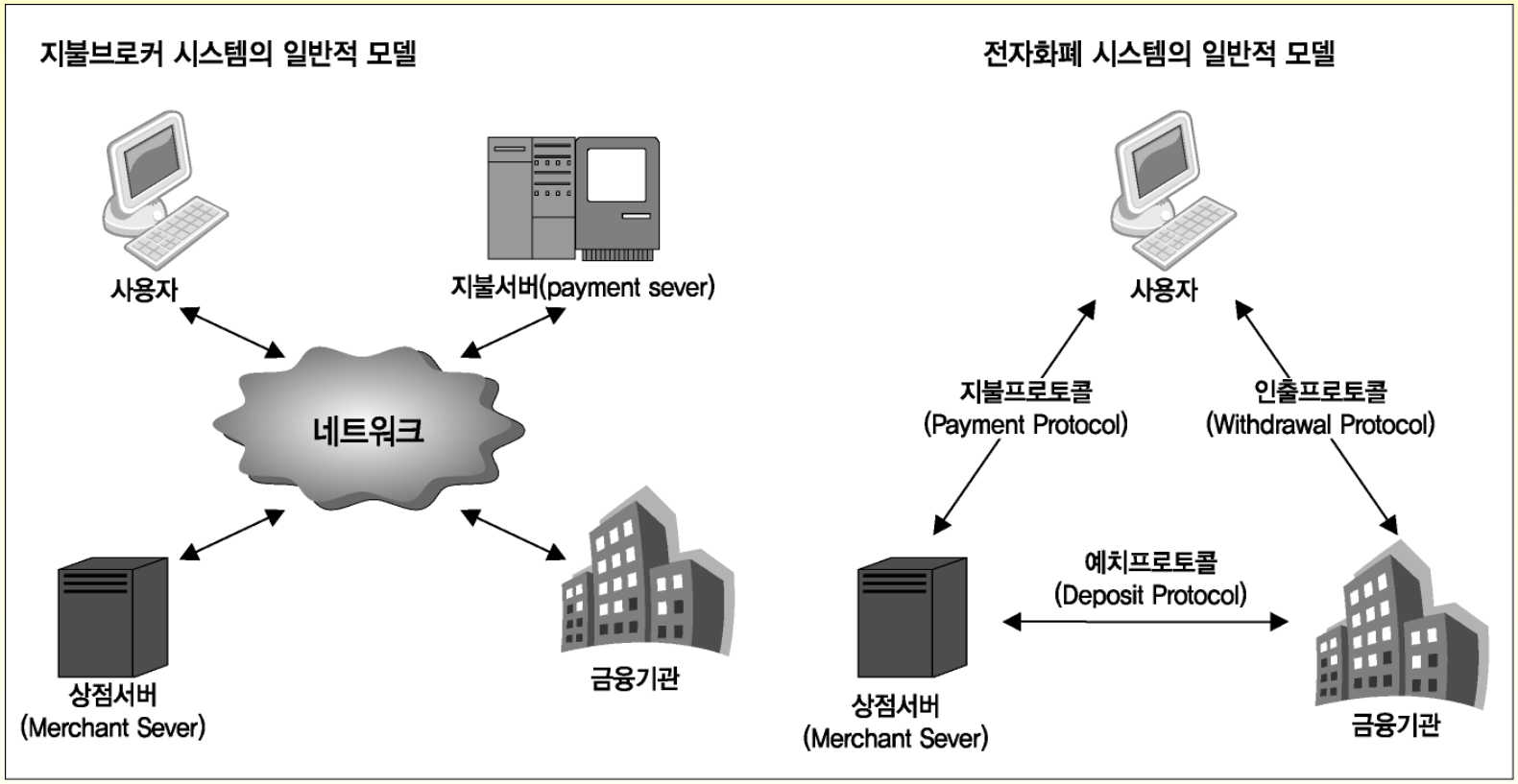


전자지불 시스템 (2)

- 지불 브로커 시스템 (신용카드 기반)
  - 장점
    - 이미 기존에 구축된 신용카드 거래나 은행거래를 채택함
    - 금융시스템의 사용이 가능하여 사용자에게 신뢰감을 제공
    - 법적, 제도적 문제의 어려움 탈피
    - 거래 방법에 대한 사용자의 친밀감
  - 단점
    - 사용자의 개인정보가 유출 및 프라이버시를 침해받을 수 있음
    - 신용카드 번호 등의 기밀정보에 대한 노출 가능성
- 전자화폐 시스템
  - 장점
    - 사용자의 프라이버시 보호
    - 실제 화폐를 대치
    - 개인 정보의 노출 위험성을 제거
    - 오프라인 방식으로도 동작가능
  - 단점
    - "돈세탁", 효율성의 문제, 법적, 행정적 제도의 지원이 필요

전자지불 시스템 (3)

- 지불 브로커 시스템, 전자화폐시스템 비교



전자지불 시스템 (4)

- 일련의 전자상거래 대금 지불 과정을 수행하는 하드웨어 및 소프트웨어를 포함
- 고객, 금융기관, 상점 서버, 지불 서버 등으로 구성
  - 고객
    - 상점 서버로부터 물건을 구입
    - 결재 서버에게 결재 대행을 요청
  - 지불 서버
    - 은행, 신용카드 회사 등의 금융기관에게 계좌이체 또는 신용카드 결제를 의뢰하여 결재를 수행

전자지불 시스템 (5)

- 전자지불 시스템 분류
  - 지불시점에 따른 분류
    - 선불
    - 직불
    - 후불
  - 인증방법에 따른 분류
    - 온라인
    - 오프라인
  - 인증방법에 의한 분류
    - 무암호
    - 공개키 암호/전자서명 시스템
    - 대칭키 암호 시스템
  - 거래 액수에 따른 분류
    - 소액
    - 고액
  - 지불방식에 따른 분류
    - 지불 브로커
    - 전자화폐

전자화폐 시스템 (1)

- 네트워크를 통해 전자적으로 구현된 화폐가치를 교환하여 결재를 수행하는 시스템
- 결재 방법과 사용 방법에 따라 IC카드형과 네트워크형으로 분류
- IC카드형 전자화폐
  - IC칩을 포함하고 있는 플라스틱 카드에 화폐가치를 저장한 후 결재 시에 이를 인출하여 사용하는 방식
  - 외형상 신용카드와 동일
  - 사용자는 네트워크나 은행의 ATM 기기를 통하여 자신의 계좌로부터 일정 금액을 인출한 후 이를 IC칩에 저장하여 사용
  - 장점
    - 휴대가 간편하고 다양한 용도로 사용이 가능
  - 단점
    - 시스템 구축 비용이 많이 들고 호환성에 문제
- 네트워크형 전자화폐
  - 은행의 계좌로부터 인출된 현금에 상응하는 화폐가치를 네트워크를 통해 다운로드 하여 사용자의 컴퓨터에 저장하거나 인터넷상의 가상은행에 저장한 후 결재 시에 이를 인출하여 사용하는 방식
  - 장점
    - 초기 구축 비용이 저렴
  - 단점
    - 휴대가 어려움

전자화폐 시스템 (2)

- 전자화폐
  - 액면 가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치 정보
  - 유통성, 양도가능성, 범용성, 익명성 등의 현금 기능
  - 원격송금성, 수송상의 비용 절감, 금액의 분할 및 통합의 유연성, 전자성 등의 특징으로 현금의 단점 보완
  - 익명성 해결이 관건
    - 불법적인 돈세탁, 밀수거래, 조세 회피 수단으로 악용 가능성
    - 적절한 감사 기능과 사용자 프라이버시와 익명성을 보장하는 유연한 시스템 구축이 난점
- 전자화폐시스템
  - 전자지불 시스템의 지불 서버와 같은 지불 브로커 없이 독립적인 구조로 결재를 수행하는 신용 기반
  - 사이버 공간에서 현금 개념으로 통용되는 전자적 지불 수단 제공

전자화폐 시스템 (3)

- 다양한 공격을 방지하고 화폐 가치를 유지 하기 위해 전자화폐의 안전성 확보 필요
- 안정성 대책
  - 사전조치
    - 암호기술, 인증기술, 임시 저항(tamper resistant)장치, 제한 한도액 규제, 인증제도 등
  - 중간조치
    - 추적가능성과 모니터링, 중앙시스템과의 조회, 거래이력의 보존과 온라인 검증, 정보개시 등
  - 사후조치
    - 핫 리스트와 장치의 사용거부, 시스템의 정지 등

전자화폐 시스템 (4)

- 전자화폐의 정보보호 요구조건
  - 디지털 정보의 완전 독립성(independence)
    - 디지털 자체로서 완벽한 화폐 가치를 가져야
    - 화폐의 정당성을 인증받기 위한 은행의 서명, 복사방지를 위한 기술 등
  - 전자화폐의 재사용 불가능
    - 이는 복사 및 위조 등으로 인한 부정사용을 할 수 없도록 하기 위함
    - 보완 대책
      - 위, 변조 방지를 위한 마이크로칩을 이용한 안전장치를 내장
      - 고성능 암호처리 프로토콜 설치
      - 전자화폐 발행 은행의 지속적인 모니터링
      - 전자화폐 거래 관련 기록 유지
  - 전자화폐의 익명성
    - 정당한 사용자의 화폐 사용 내역은 알려져서는 안 됨
    - 사용자의 사생활은 보호되어야 할 뿐만 아니라 사용자의 구매내역 등이 추적 불가능해야 함

전자화폐 시스템 (5)

- 전자화폐의 정보보호 요구조건 (계속)
  - 거래의 오프라인 처리
    - 사용자와 상점 사이에서의 거래는 오프라인 방식으로 처리가 이루어 져야 함
  - 타인에게 양도 가능
    - 전자화폐를 받은 상점이나 사용자는 다시 해당 전자화폐를 다른 상점이나 제 3의 사용자에게 사용이 가능해야 함
  - 분할 이용 가능성
    - 일정한 가치를 가지고 있는 전자화폐는 그 금액의 크기만큼 자유롭게 분할되어 사용될 수 있어야 함
    - 분할되어 사용하고 남은 나머지 한도의 전자화폐에 대한 안전성도 분할되기 전의 전자화폐와 같은 안전성을 유지
  - 부정적인 사용자의 경우 익명성 취소
    - 부정적인 사용자의 경우 익명성 취소가 요구
    - 부정적 사용
      - 돈세탁, 돈 약탈, 마약구매, 무기구매 등
    - 익명성 취소
      - 전자화폐의 소유자를 식별하는 소유자 추적
      - 은행으로부터의 화폐인출을 식별하기 위한 화폐 추적

전자화폐 지불시스템 (1)

- IC 카드 기반 전자화폐 지불시스템
  - VISA Cash Card
  - Mondex Card
  - E-Cash
  - NetCash
  - CyberCoin
  - EMV 현금카드

전자화폐 지불시스템 (2)

- 신용카드 기반 전자화폐 지불시스템
  - First Virtual
  - CARI(Collect All Relevant Information)
  - SSL(Secure Socket Layer)
  - Cyber Cash
  - iKP
  - SEPP(Secure Electronic Payment Protocol)
  - SET(Secure Electronic Transactions)

전자화폐 지불시스템 (3)

- 전자 수표
  - FSTC 전자수표
  - NetBill
  - NetCheque
- 소액지불시스템
  - Millicent
  - SubScrip
  - PayWord
  - Micro Mint

전자지불 보안 기술

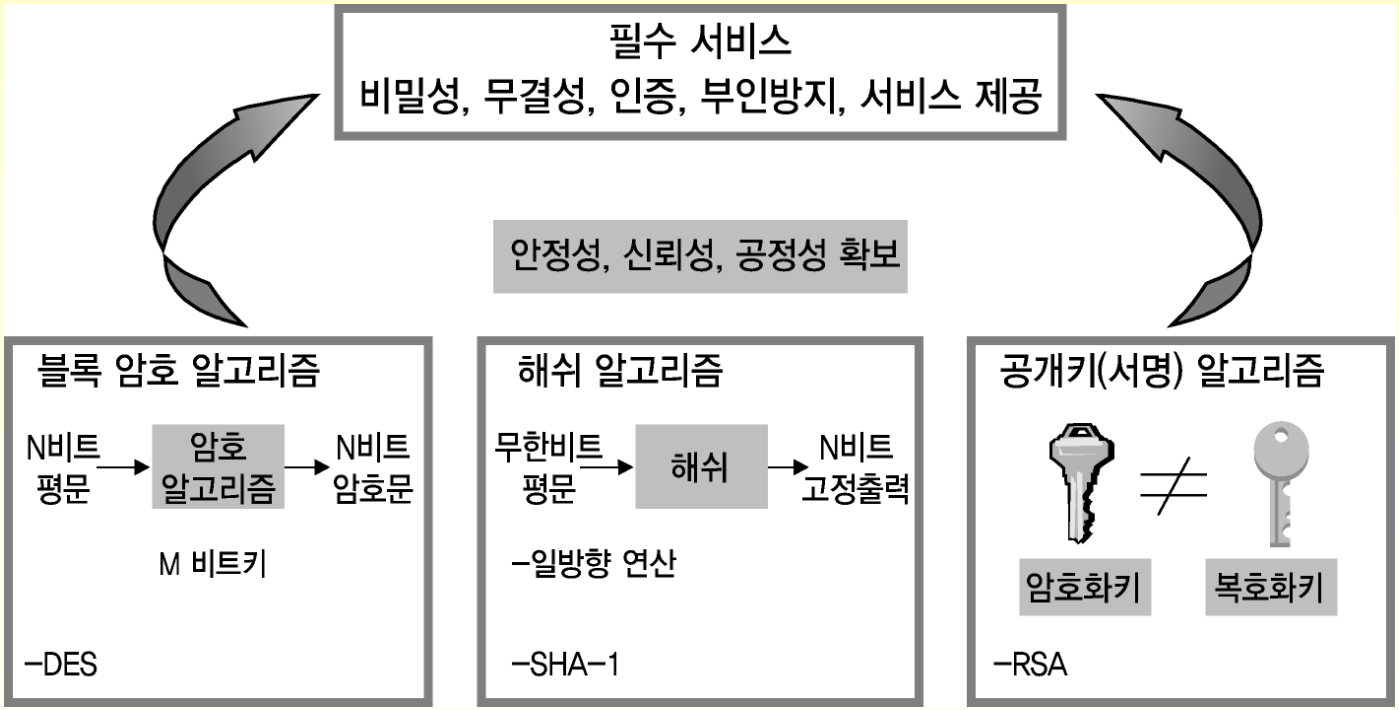
- SHTTP(Secure HyperText Transfer Protocol)
  - HTTP 연장선상에서 보안 기능을 제공하는 응용 계층 보안 프로토콜
- SSL(Secure Socket Layer)
  - 전송 계층에서 인증, 무결성, 비밀성, 압축 등 보안 서비스 제공
- SET(Secure Electronic Transaction)

SET (1)

- SET의 개요
  - 전자상거래 당사자들에게 신뢰성과 안전성을 제공하기 위하여 인증, 비밀성 등의 보안 기능과 지불 기능을 제공하는 전자상거래 전용 프로토콜
  - 사용자와 상점이 상품을 안전하고 편리하게 주문하거나 배송할 수 있도록 지원
  - 사용자, 상점, 금융기관 사이의 지불이 원활하게 실시간으로 처리될 수 있도록 실용적이고 안정적인 지불 서비스 인프라 구조를 제공 함
  - 1996년 2월, MsterCard와 Visa사는 “인터넷상의 안전한 신용카드 거래를 위한 기술적 표준” 제정에 합의

SET (2)

- SET의 정보보호 서비스

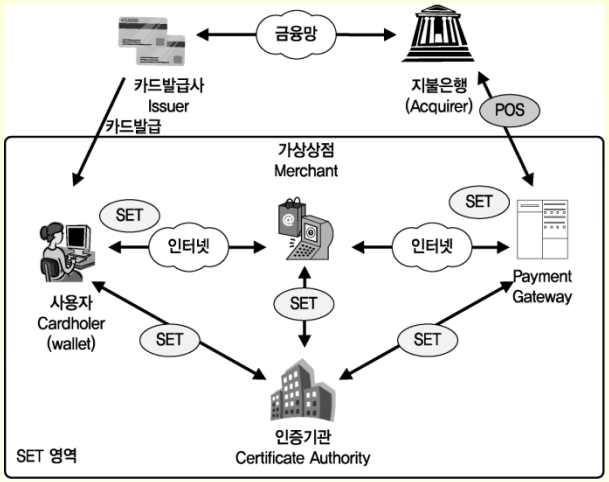


SET (3)

- SET의 기능 및 특징
  - 사용자 및 상점의 신원 인증
  - 거래 정보의 비밀성 보장
  - 지불 데이터 무결성 보장
  - 지불 데이터의 부인 방지
  - 상호 운용성 지원
  - SET의 장점
    - 안전한 전자거래 환경을 제공
    - 기존 신용카드 기반 환경에 그대로 적용 가능
    - 인증, 비밀성, 부인 불가 등의 보안 기능을 제공
    - 전자거래의 표준으로서 이질적인 전자거래 환경에서 상호 운용성을 제공
  - SET의 단점
    - 카드 소지자에게 전자지갑 S/W의 사용을 요구하여 불편을 초래할 수 있음
    - 지불 서버에 의한 결제로 인하여 별도의 H/W와 S/W의 구비를 요구함
    - 암호 프로토콜이 다소 복잡함
    - 판매자에게 SET 관련 S/W 사용을 요구하여 불편을 초래할 수 있음
    - 공개키 암호 알고리즘의 경우 프로토콜의 속도를 저하시킬 수 있음

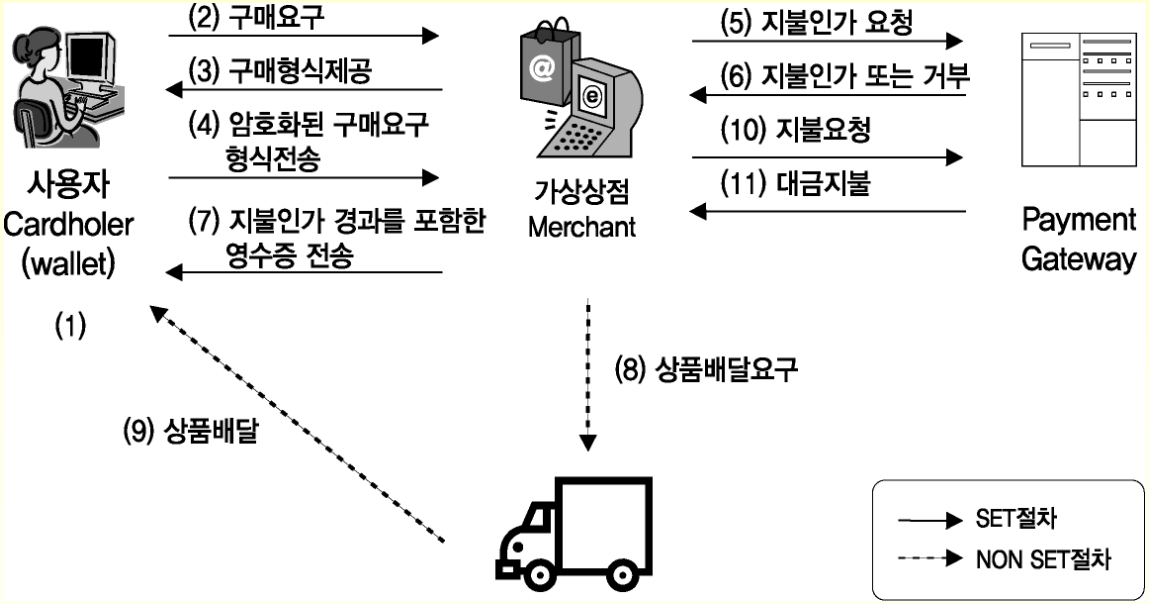
SET (4)

- SET의 구성 요소
  - 지불 게이트웨이(Payment Gateways)
    - 매입사 또는 제삼자에 의해 운영되는 장치
    - 상점이 요청한 카드소지자의 지급 정보를 이용하여 해당 금융기관에 승인 및 결재를 요청하는 기관
  - 인증기관(CA : Certification Authority)
    - SET 참여자에게 공개키 인증서를 발행하는 기관
  - 브랜드(Brand)
    - 은행카드 연합
  - 사용자와 가상상점
    - 물품의 직접적인 구매와 판매를 담당
  - 은행과 지불서버, 카드사
    - SET을 통한 물품의 대금에 대한 지불을 담당
  - 인증기관
    - 구성 요소들의 인증서 발급과 인증서 실시간 조회 서비스 등을 제공



SET (5)

- SET을 통한 전자상거래 과정
  - 인증서 관리 과정
    - 사용자, 가상상점, 지불서버의 인증서 관리를 의미
  - 거래 및 지불 과정
    - 사용자, 가상상점, 지불서버의 물품 구매와 지불 과정을 의미



SET (6)

- SET의 보안 기능
  - SET 암호 알고리즘
    - 공개키 암호화 알고리즘
    - 대칭키 암호 알고리즘
  - 이중 서명(dual signature)
    - 물품에 대한 구매 정보와 구매자의 결재 정보에 대한 서명(signature)을 각각 생성하고 두 서명을 합친 정보에 대한 서명을 다시 생성하여 수신 측에서 개별적인 서명과 합쳐진 서명에 대한 검증을 이중으로 수행
    - 결제 정보가 검증 과정에서 판매자에게 노출되는 것을 방지하고 판매자가 결제 정보를 위·변조하는 것을 막기 위해 고안된 전자서명(digital signature) 방식
  - SET 인증서