스마트카드와 인터넷상거래의 결합구조 분석

양 철 영 cyyang@msd.kaist.ac.kr
이 재 규 jklee@msd.kaist.ac.kr

인터넷상거래 연구실
한국과학기술원

1. 연구 배경 및 목표

- 인터넷상거래에서의 전자지불 방법은 안전한 정보 저장 및 사용을 위하여 스마트카드를 활용하는 방향으로 통일되어 가고 있음.
- 인터넷 상거래의 전자지불에 있어서의 이슈
  - 전자지불의 형태를 무엇으로 정할 것인가?
    - 스마트카드를 활용하는 전자현금 프로토콜 정의
    - 스마트카드 구조, 형태 정의
    - 타 시스템과의 상호호환성 확보 방안 정의 등
  - 어떠한 비즈니스 모형을 만들 것인가?
    - 스마트카드의 적용 대상 정의
    - 비즈니스 모형에 따른 필요한 시스템 정의 등

- 목표
  : 스마트카드와 인터넷의 결합구조 분석
  - 전자지불 유형의 분류에 따른 분석: 대표적 지불 유형의 분류 및 비교
  - 비즈니스 모형에 따른 구조 분석: 사업모형에 따른 구조 정의 및 비교

스마트카드와 인터넷상거래 결합구조

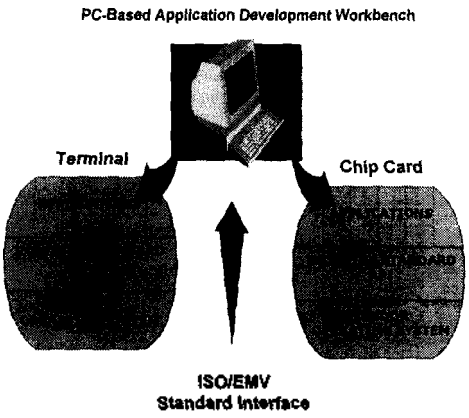
- 전자지불 유형 분류(대표적 전자지불을 위한 스마트카드 표준에 따른 분류)
  - 비자캐시 타입: Open Platform 표준안을 따르는 비자진영의 지불 유형
  - 몬덱스 타입: Multos를 따르는 마스터카드 진영의 지불 유형
  - IC-SET 타입: 자체 표준을 허용하면서도 타 표준과의 거래도 지원하는 유럽 진영의 지불 유형
  - 금결원 타입: 자체 표준을 추구하는 국내의 지불 유형

- 비즈니스 모형 분류(예시)
  - 교통카드 구조
  - 교통카드 + 인터넷 충전
  - 인터넷상에서의 전자현금 사용 구조
  - SET 기반 금융카드 구조

2. 전자지불 유형

유형		
비자캐시 타입	•가치 저장형으로 은행 정산 필요 •표준아키텍처: Open platform(Java card 2.0 기반) •예: 비자카드사의 지불시스템 유형	Smart Commerce Japan(SCJ)에서의 스마트카드와 인터넷 결합구조 예시
몬덱스 타입	•개인간 가치 이전이 허용되는 형태 •표준 아키텍처: MULTOS •예: 마스터카드사의 몬덱스 지불시스템 유형	현재 인터넷상에서의 Pilot 프로젝트 없음
IC-SET 타입	• 자체 표준을 허용하면서 상호호환성을 위해 공동의 표준을 지원하는 형태 • 표준안:Banksys, CB의 Interoperable C-SET	Interoperable C-SET(IC-SET) 프로토콜 분석
금결원 타입	• 자체 표준 지향: 자체적인 보안알고리즘, 프로토콜 • 표준안: 금융결제원 전자지갑 표준안	현 전자지갑 표준안은 인터넷 상거래 고려 안됨.

VISA Open Platform

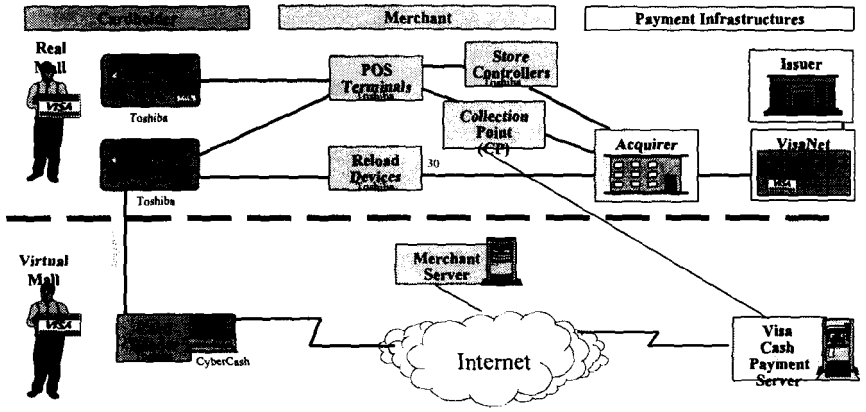


특징

- Java 기반:
  - ***Write Once, Run Anywhere***
  - Platform Independence
  - Security
  - Wide Scale Acceptance
- Scope
  - Card Specification
    : Java Card 2.0 spec.
  - Terminal Specification
  - Workbench Tools

Visa Cash + 인터넷 결합 구조

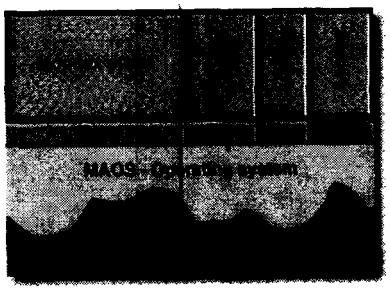
SCJ(Smart Commerce Japan) 예



Mondex

- 참여자들
  - Mondex International: 기술표준 및 Business Rule 제공
  - Originator
  - 회원사(은행/카드사)
  - 가맹점
  - 카드회원
  - 제조업체(스마트카드, 단말기, 네트워크 등)
- Mondex + 인터넷 결합 구조(계획)
  - 보안: 공개키 기반, 카드와 카드간 인증
  - 편리성: Merchant에게 별도의 하드웨어 불필요(카드간 이체)
  - EMV/SET 지원: original SET + EMV 지원 (스마트카드 지원)

Multos Architecture



- High-security Multi-Application Operating System (MAOS) for smart cards.
- Application Development Language:
  - MEL (MULTOS Enabling Language)
  - C
- Applicable to Mondex and other application

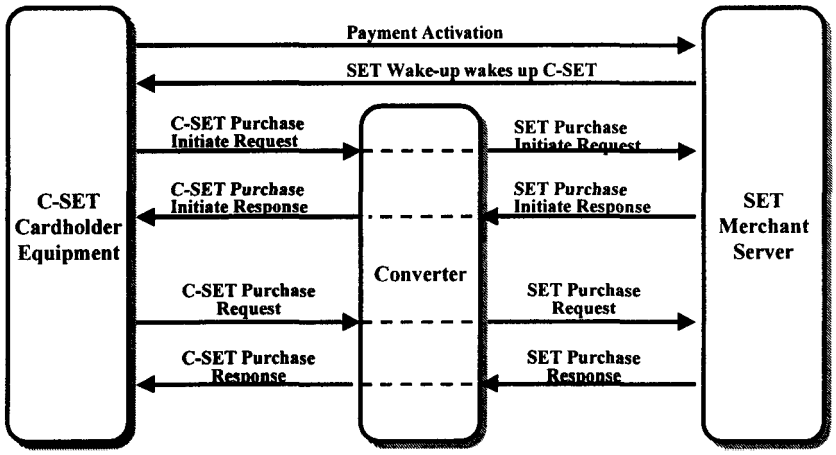
Applications
MULTOS
Firewalls
Silicon (hardware)
Interpreter and API
Application load certificate

Interoperable C-SET(IC-SET)

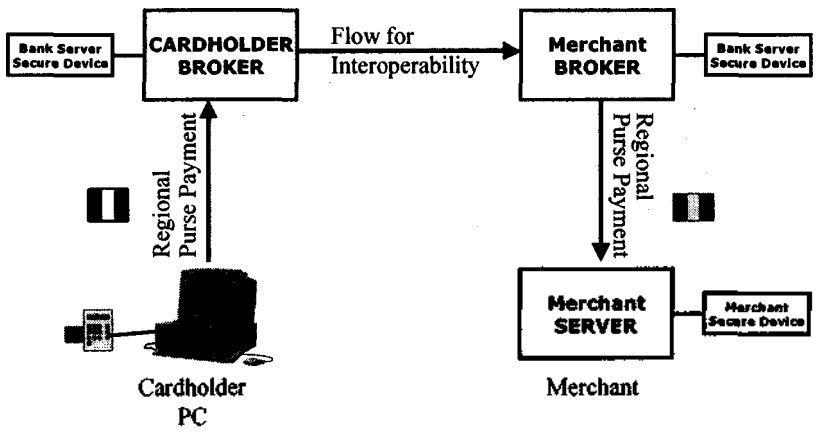
- Debit and Credit Card Payments
  - 국내: C-SET 표준(기존의 EMV 카드 지원)
  - 국제 상호운용성: SET 사용
  - 특징:
    - Converter를 두어 C-SET과 SET 메시지 호환
    - SET용 인증서는 Converter에서 고객 혹은 머천트의 정보를 바탕으로 생성
    - Converter가 안전한 시스템이어야 함.
- Internet Purse Payments
  - 타 시스템간(국제간) 호환을 위해 Broker 이용
    - Cardholder Broker, Merchant Broker
  - 지불 프로토콜:two-phase protocol
    - Agreement Phase + Payment Phase
  - 스마트카드: 대칭키 방식 통신
  - Cardholder S/W: 공개키 방식 통신(Cardholder의 개인키 보관)

IC-SET: Credit/Debit Card Payment

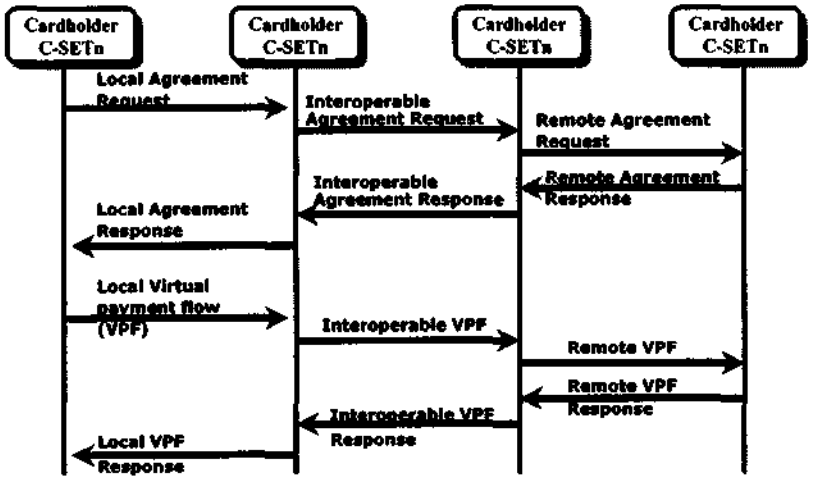
Debit and Credit Card Payment Transactions
with a non-domestic Merchant



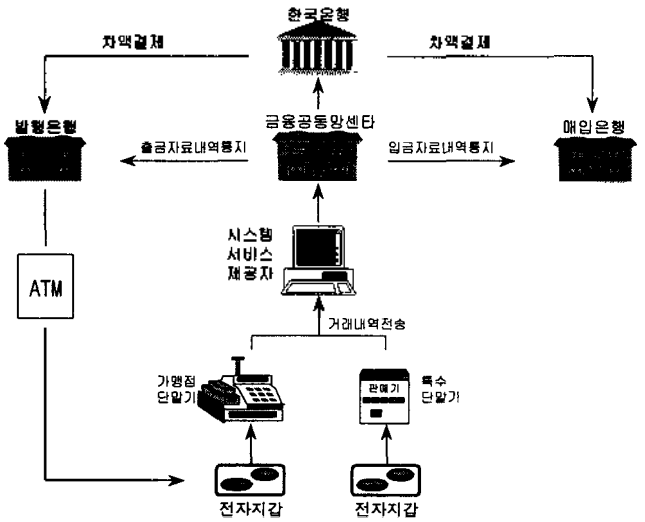
IC-SET: Internet Purse Payment



IC-SET: Purse Payment Transactions



금융결제원 전자지갑 표준안(1)



금결원 전자지갑 표준안(2)

- 개요
  - 전자지갑소지자, 단말운영자, 시스템서비스제공자, 금융공동망센타, 발행은행, 매입 은행간의 관계 정의
  - 오프라인 거래 기준
  - 1997. 2월 전자지갑표준 발표
- 특징
  - 자체적인 스마트카드 및 지불 표준안
    - 자체적인 보안 알고리즘 탑재 계획
    - 인터넷 환경을 위한 표준안은 아직 포함되어 있지 않음
  - 대칭키 방식의 키 관리 체계
  - 국제간 결제가 아직 지원되지 않음

전자지불 유형 비교(기술/표준 관점)

유형	비자캐시 방식	모넥스 방식	IC-SET 방식	금융용 타입
카드 표준안 (Architecture)	•Open Platform	•MULTOS	•Interoperable C-SET	•금융전산업무표준 (IC 카드)
인터넷 지불 표준	•SET(ver2.0에서 지원)	•SET(ver2.0에서 지원)	• DEBIT/CREDIT: SET • Purse system: 자체표준	•지원하지 않음
스마트카드 지불표준	•EMV 3.0 기반	•EMV 3.0 기반	• EMV 3.0 기반	•CEN 기반 자체 표준개발
Multi Application 지원 체계	•Open Platform에 정의	•Multos에 정의	•지원체계가 따로 정의 되어 있지 않음	•지원체계가 따로 정의 되어 있지 않음
응용프로그램 인터넷 다운로드	•자바 Applet 이용 인터넷 다운로드	•MULTOS에 정의	• 정의되어 있지 않음	•정의되어 있지 않음
SET 인증서	현재버전: 인증서 없음 가능 옵션 - 카드에 인증서 저장 - PC에 인증서 저장	•향후 지원 계획	카드 브로커 혹은 컨버터에서 인증서 생성.	•인증서 없음
보안 (암호화 알고리즘)	•대칭키 방식 •공개키 방식	•향후 공개키 방식 지원	•대칭키 방식과 공개키 방식 혼용	•대칭키 방식

전자지불 유형 비교(비즈니스 관점)

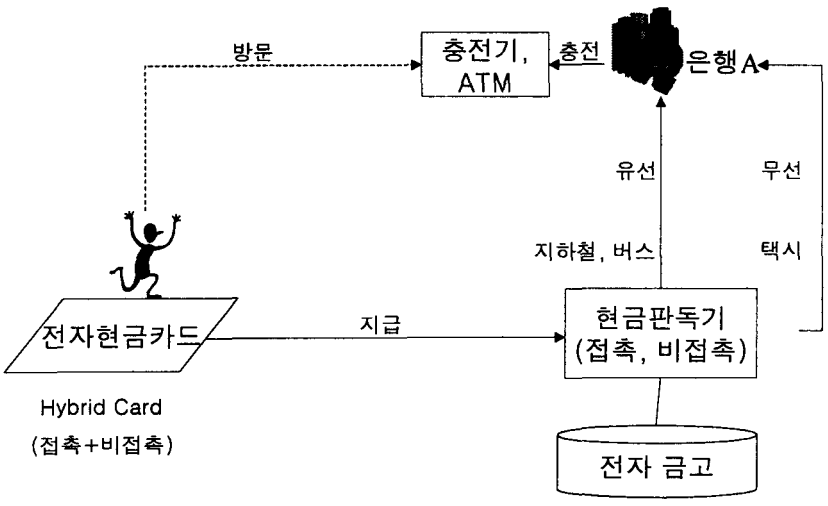
유형	비자캐시 방식	모넥스 방식	IC-SET 방식	금융용 타입
정산 기능	정산	정산 기능 없음 (개인간 이체 가능)	정산	정산
감사기능 (Auditability)	감사 가능	감사 불가능	감사 가능	감사 가능
익명성 (사생활 보호)	불완전한 익명성	익명성 지원	불완전한 익명성	익명성 지원 않음
편리성	Critical Mass 확보가 관건 개인간 이체는 불가능	고객간 이체 가능 머천트간 이체 가능	Critical Mass 확보가 관건 개인간 이체 불가능	한정된 사용 범위 - 국내용
비용 (개발비용/운영비용)	운영비용이 상대적으로 크나 초기 개발비용은 기존 시스템의 활용으로 상대적으로 적음	정산기능이 없으므로 운영비용이 상대적으로 작으나 초기 투자비용은 상대적으로 큼	정산비용, 호환을 위한 시스템 개발, 유지 비용 등으로 인해서 상대적으로 비용이 많이 듦	바자캐시형과 유사
법적 문제	•기존 은행 시스템의 모방으로 법적 문제 작음 •인터넷 거래에 따른 조세 문제 발생	•개인간 이체 허용 문제 •인터넷 거래에 따른 조세 문제 발생	•기존 은행 시스템의 모방으로 법적 문제 작음 •인터넷 거래에 따른 조세 문제 발생	•기존 은행 시스템의 모방으로 법적 문제 작음 • 조세 문제 없음

비즈니스 유형에 따른 결합구조 분석

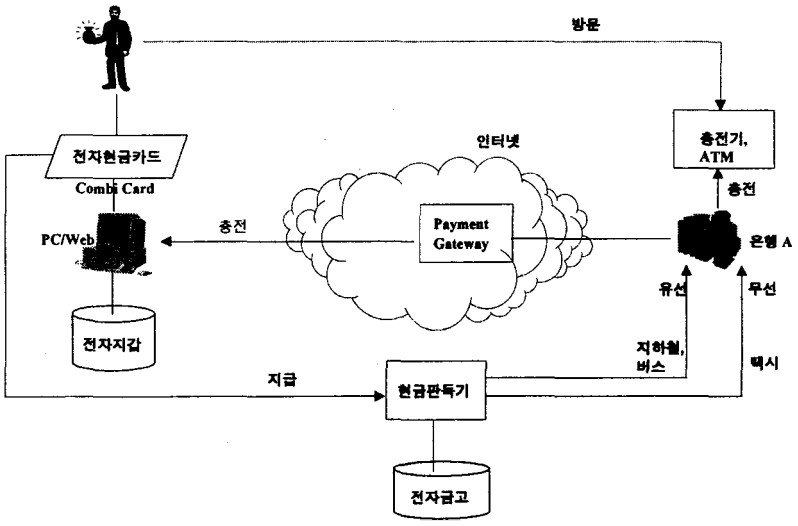
- 비즈니스 유형의 제시와 그에 따른 스마트카드와 인터넷의 결합 구조 분석
- 비즈니스 유형은 사용자 관점에서 단계적으로 접근할 수 있는 모형을 예시
- 비즈니스 유형 분류 (예시)
  - 단순 교통카드 모형
  - 인터넷상에서 교통카드 재충전 모형
  - 인터넷상에서의 전자현금 사용 모형
  - SET 기반 통합 금융카드 모형

- 유형에 따른 비교 기준
  - 스마트 카드 용도
  - 스마트 카드 타입: 접촉식, Hybrid Card, Combi-Card 등
  - 인터넷에 필요한 기능
  - 기타
- 비즈니스 유형에 따른 전자지불 형태의 결정에 대한 부분은 앞에서 다룬 것으로 대체함.

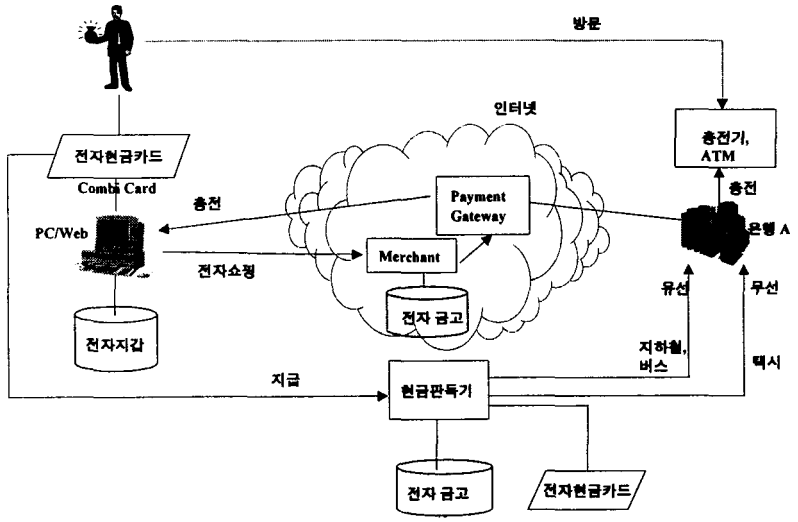
단순 교통카드 모형(하나로카드 모형)



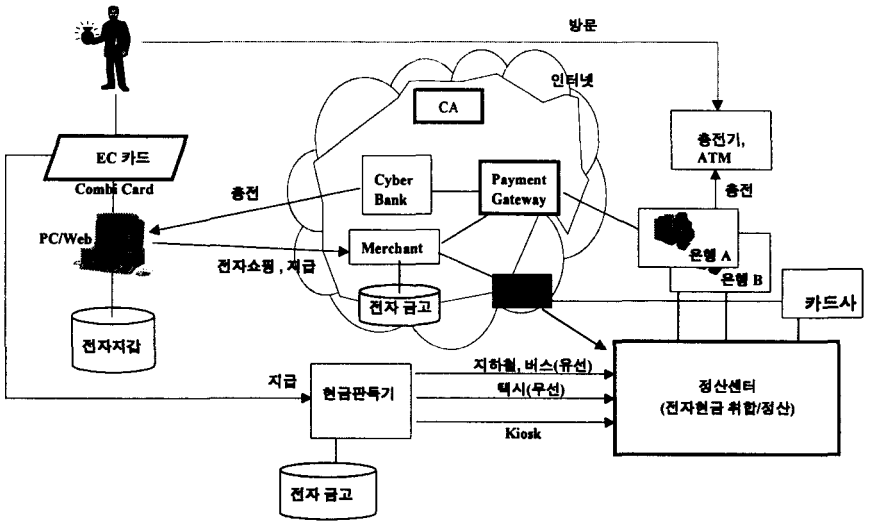
인터넷상에서 교통카드 재충전 모형



인터넷상의 전자현금 사용 모형



SET 기반 통합 금융카드 모형



비즈니스 유형에 따른 결합구조 비교

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
스마트카드 기본 용도	전자 현금	전자현금	전자현금	전자현금, 금융정보 저장 인증서 저장
스마트카드 타입	하이브리드 카드	Combi 카드	Combi 카드	Combi 카드
인터넷에 필요 기능	없음	Payment Gateway 전자지갑(PC) 전자현금 프로토콜	Payment Gateway 전자지갑(PC) 전자현금 프로토콜 머천트의 Payment Server	PG, 전자지갑(PC) 전자현금 프로토콜 머천트 PS 가상은행,CA SET 프로토콜
기타 특징	사업주체: Issuer Bank 비접촉식 판독기 비용 高	현금충전 - 인터넷 접속 PC - Combi 카드 필요 (비용문제)	인터넷 상에서 지불 쇼핑몰과 연계	•KIOSK, 여러 은행 지원 체계 •계좌이체 지원

결론

- 스마트카드와 인터넷의 결합 구조를 두 가지 관점으로 정리
  - 전자지불 유형의 분류에 따른 분석: 대표적 지불 유형의 분류 및 비교
  - 비즈니스 모형에 따른 구조 분석: 사업모형에 따른 구조 정의 및 비교
- 금융기관 등에서 스마트카드를 도입하고자 하는 경우에 비즈니스 모형의 정의를 도와주고 모형에 따른 스마트카드의 특성 및 전자지불 타입을 결정하는데 도움이 될 것으로 기대.