The Journal of Korea
Institute of CALS/EC
Vol. 2, No. 1, June. 1997

SET을 기반으로 한 전자상거래 트랜잭션 모델링에 대한 연구

고영철*, 송병열*, 조현규*, 함호상*[1]

A Study on Electronic Commerce Transaction Modeling based on SET

Young-Cheol Go, Byoung-Youl Song, Hyun-Kyu Cho, Ho-Sang Ham

Abstract

Commerce activities which are free form space and time constraint using a communication network are called Electronic Commerce(EC). Because of sending a commercial information using open network such as Internet in EC, they need the security of commerce information (payment information and purchase information), checking the integrity of transferring data and certifying all parts participated in commerce for a secure commerce. Recently Visa and MasterCard Co. released the Secure Electronic Transaction (SET) Protocol for secure payment card transaction on Internet. This paper proposes a Secure Electronic Commerce Transaction Model(SECTM) using SET in order to support the secure commerce on Internet. The proposed transaction model prevents merchant from abusing the cardholder's payment information (credit-card number etc.) and enables cardholder to shop securely in Electronic Shopping Mall.

Keyword: Electronic Commerce (EC), Secure Electronic Transaction (SET),
Secure Electronic Commerce Transaction Model (SECTM)

---

[1] 시스템공학연구소 시스템공학연구부

1. 서 론

전자상거래의 범위를 기업과 소비자간의 활동으로 제한하면 인터넷상에 홈 페이지나 가상상점(Virtual Store), 가상 상점가(Virtual Shopping Mall) 등을 개설하여 일반 소비자를 대상으로 마케팅과 판매 활동을 하는 사이버 비즈니스로 정의할 수 있다. 이러한 전자상거래는 유통 채널이 짧고, 상거래에 필요한 시간과 공간의 제약이 없으며, 판매거점이 불필요하고, 고객정보 획득이 용이하며, 효율적인 마케팅이 가능하고, 고객 요구에 즉각적으로 대응할 수 있으며 소액 자본으로 사업을 전개할 수 있는 특징들을 지니고 있다.

인터넷을 통한 전자상거래의 규모는 이미 거대 시장을 형성하고 있으며, 전 세계적인 규모는 조사기관에 따라 약간의 차이가 있으나 95년 중 평균적으로 약 3천 7백 50억 달러로 집계되고 있다. 또한, 전체 구매시장에서 통신판매가 차지하는 비율은 15%정도이며 금액으로는 7천 5백억 달러에 달하는 것으로 조사되었으며, 그 중 전자상거래가 차지하는 비율은 이미 50%에 달한다. 전세계 도·소매 상거래 규모는 1994년에 총 4.7조 USD에서 2000년에는 총 8조 USD로 174% 성장할 것이며, 이 중에서 인터넷/온라인 분야는 1994년 460억 USD에서 2000년에는 8,000억 USD로 1740% 성장[Killen, 1996]함으로써 컴퓨터 네트워크 특히 인터넷을 통한 상거래의 규모는 다른 매체를 능가할 것이라는 예측이 나오고 있다.

전자상거래 시스템을 개발하는 경우에 고려할 사항은 다음과 같다.

먼저, 소비자(consumer)는 가상 쇼핑몰에서 정보유출의 위험이나 불안을 느끼지 않고 안전하게 쇼핑 하기를 원한다. 판매자(merchant)는 가상 쇼핑몰에서 일어나는 트랜잭션을 효율적이면서도 낮은 비용으로 처리하기를 원한다. 마지막으로 카드 발행사(payment card brands)는 기존 상거래에 미치는 영향을 최소화하는 방향으로 전자상거래 시스템이 개발되기를 원한다. 또한, 기존에 운영되고 있는 가상 상점들은 고객의 카드 정보 등의 지불 정보를 직접 취급하므로 상거래 정보의 전송에 대한 기술적인 보안 문제뿐만 아니라 이러한 정보를 취급하는 담당자들의 도덕적 문제나 제도적 문제가 발생하므로 소비자의 상거래 정보에 대한 보호가 필요하다. 상기의 사항들은 곧바로 SET의 개발 동기가 되었으며, 소비자의 요구, 판매자의 요구, 카드 발행사의 요구 등을 충족시키며 소비자 지불 정보를 안전하게 유지하는 프로토콜이 제안되었다.

SET은 인터넷상에서 신용카드 트랜잭션을 안전하게 처리하기 위해 Visa와 MasterCard사가 공동으로 개발한 프로토콜로써, 지불 정보 및 구매 정보의 기밀성과 전송되는 데이터의 무결성 및 상거래 참여 부문에 대한 인증을 제공하는 공개 표준으로 지불 서비스 개발자나 응용 프로그램을 개발하는 소프트웨어 벤더(vendor)가 모두 이용 가능하다.

SET은 기본적으로 이중 서명(dual signature)의 개념으로 소비자의 암호화된 주문 정보와 지불 정보에 대한 해독의 권한을 설정하고 있다. 소비자는 지불 정보를 판매자가 해독할 수 없도록 암호화하여 전송하므로,

판매자에 의해 소비자의 지불 정보가 임의로 사용되는 것을 막을 수 있으며, 소비자가 암호화한 지불 정보를 받은 은행은 지불 요청에 대하여 신뢰할 수가 있다. 따라서, 타인에 의한 소비자의 주문 정보와 지불 정보에 대한 오용을 막을 수 있다.

본 연구에서는 신용 카드의 안전한 처리와 전송되는 데이터들의 무결성 및 기밀성 등을 지원하는 SET 프로토콜을 이용하여 기존의 전자상거래 트랜잭션 모델이 지닌 보안상의 문제점을 보완한 트랜잭션 모델을 제시한다.

앞으로의 구성은 다음과 같다. 2 장에서는 전자상거래의 동향 및 기존의 전자상점에 대하여 살펴보고, 3 장에서는 SET 에 대한 고찰을 하고, 4 장에서는 SET 을 이용한 트랜잭션 모델을 제안한다. 끝으로 5 장에서는 연구의 결론 및 향후 과제에 대하여 기술한다.

2. 기존의 연구

2.1 전자상거래의 동향

선진 각국의 전자상거래에 대한 동향 및 관련 소프트웨어의 연구개발 내용은 다음과 같다.

먼저, 미국 정부는 93 년 10 월 클링턴 대통령이 97 년부터 정부 조달을 전면 전자화하는 물자 조달 합리화 방안에 서명한 후에 국가 차원에서 전자 상거래를 단계적으로 도입하고 있다. 미국 정부의 전자상거래 도입 일정은 94 년 3 월에 전자상거래를 위한 체계 정의 및 담당 실행조직 정비, 94 년 9 월에 상품거래 전반에 해당하는 업무가 전자상거래에 의해 실시가능 하도록 실행단계에 돌입, 95 년 7 월에 전자결재·계약문서 교환 등 업무 전반을 전자화, 97 년 1 월에는 정부 전 조직 차원의 전자상거래 구축 완료로 되어 있다. 인터넷상에서 구현되어 있는 전자상거래의 형태는 현재 정보 조달시장의 전자거래화, 대기업의 구매시스템, 기업상호간의 일반 상거래, 소비자 대상의 상품 및 서비스 비지니스 등 크게 네가지 형태로 구현되어 있다.

일본의 경우는 95 년 말 통산성 주관으로 EC 실증 추진위원회를 발족하고 향후 상거래의 전자화 시대에 대비하여 보안기술 등의 기반기술을 표준화하고 전자상거래의 실증실험도 수행하고 있다. 96 년에 약 100 억엔을 투자해 전자상거래와 관련된 10 여 개의 기술과제와 20 여 개의 실증 프로젝트를 추진 중에 있다.

유럽은 ESPRIT 프로젝트의 일환으로 사용자의 비밀보장을 위한 전자결재시스템을 개발하기 위한 CAFE(Conditional Access For Europe) 프로젝트를 수행 중이며, 전자상거래를 위한 비밀자료의 암호화와 해독을 위한 운용체계로서 Smart Card Chip 을 설계 및 개발할 목적으로 SOSCARD(Secure Operating Systems Smart Card) 프로젝트를 수행하고 있다.

한국에서는 96 년 초 통상산업부와 정보통신부 산하에 각각 CALS/EC 협회와 기술협회를 발족시켜 기업간 상거래 활동 중심의 실험 프로젝트를 추진 중에 있으나 선진 수준에는 크게 못 미치고 있는 실정이다. 인터넷이 확산되면서 기업들의 관심이 높아져 대기업을 중심으로 상업활동을 위한 실험들이 시도되고 있으며, 한국과학기술원의 이재규 교수를 준비 위원장으로 하는 국제상거래연구센터와 한양대 허신 교수를 회장으로 하는

전자화폐연구회, 그리고 인터넷상의 전자상거래 활성화를 위해 결성된 국제적 컨소시엄인 커머스넷의 지원조직인 커머스넷코리아가 설립되고 있다.

인터넷상에서 가상상점가를 구축/운영하는 시스템은 오라클사의 인터넷 커머스 서버 솔루션, 마이크로소프트사의 MICS 솔루션, 넷스케이프사의 머천트 시스템(Merchant System)과 오픈 마켓사의 머천트 솔루션(Merchant Solution) 등이 있다.

2.2 가상 상점의 구축 사례

전세계적으로 인터넷상에 웹사이트를 통해 개설되어 있는 가상 상점의 수는 약 2만개가 넘는 규모이며 그 시장 규모도 계속 증가하고 있다. 본 연구에서는 인터넷에 구축되어 있는 해외 상점의 사례로 지금까지 발표된 인터넷 상점 구축 도구 중에서 가장 성능이 좋은 것으로 평가 받고 있는 오픈 마켓사의 머천트 솔루션 패키지를 이용하여 구축된 가상 쇼핑몰과 국내 사례로 데이콤에서 운영하고 있는 인터파크(Interpark)에 대하여 소개한다.

2.2.1 국외 사례(OPEN MARKET 사)

오픈 마켓사의 머천트 솔루션의 경우, 프론트 오피스 도구(Front Office Tool)와 백 오피스 도구(Back Office Tool)로 구성되어 있다[Open Market Co., 1996a]. 프론트 오피스 도구는 인터넷상에 전자상점을 구축하고 관리하기 위한 도구로써 StoreBuilder, Transaction Link, Secure WebServer 및 WebReporter로 구성되어 있다. 그리고 백 오피스 도구는 상인의 영업 행위를 지원하는 기능들로 구성되어 있다.

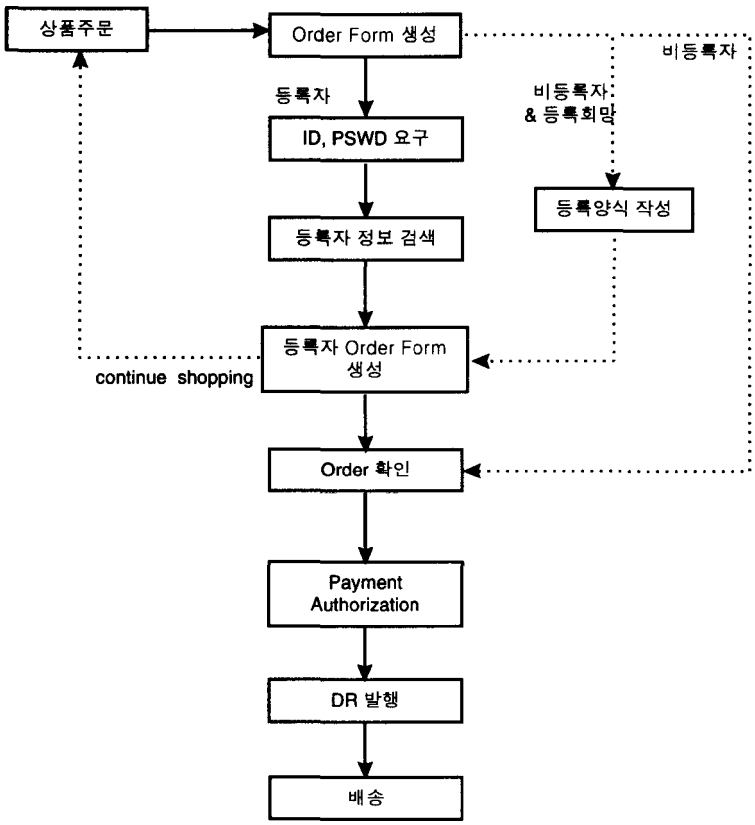
오픈 마켓사의 머천트 솔루션으로 구축된 가상 상점들은 등록자의 경우 과거 거래 내역 조회 등의 부가서비스를 제공하고 비등록자도 상점에서 원하는 상품을 구입할 수 있다. 또한, 소비자는 쇼핑 카트의 기능을 가진 주문 양식을 사용하고, 구입한 상품에 대한 지불 방법으로는 신용카드를 사용하도록 되어 있다. 그러나, 쇼핑 카트의 기능을 가진 주문 양식을 사용하므로 하나의 쇼핑 카트에는 한명의 수취인만을 지정 가능하여 구매를 원하는 상품들의 수취인이 각기 다를 경우에는 쇼핑 카트의 기능을 이용할 수 없다. 또한, 판매자가 취급 가능한 신용 카드이외의 지불 수단(판매자가 취급할 수 없는 카드 이용 거래 및 온라인 입금)을 사용하기 원하는 소비자는 상품을 구입할 수 없다는 단점이 있다. 그림 2.1)은 오픈 마켓사의 상거래 흐름을 나타낸 것이다.

2.3.1 국내 사례(INTERPARK)

국내에서 인터넷을 통해 상점을 개설하여 상거래를 하는 곳은 여러 곳이 있으며, 본 연구에서는 데이콤에서 운영하는 인터파크(Interpark)[Dacom, 1997]에 대하여 알아본다.

인터파크는 오픈 마켓사와는 달리 기본적으로 등록자 기반으로 되어 있어, 비등록자는 상품을 구입할 수 없다. 지불 수단으로 신용 카드, 온라인 입금, 쿠폰 및 상품권 개념의 사이버 캐쉬를 이용할 수 있으므로 상품 지불에 대한 제약이 적으며, 주문 양식과 쇼핑 카트의 개념을 분리하여 제공하여 각각의 상품별로 수취인을 지정할 수 있으므로 수취인이 다수인 경우에도 쇼핑 카트의 기능이 제공된다. 또한, 이용자는 과거 거래 내역을 조회할 수 있으며, 구입한 상품의 교환 및 환

불도 가능하다. 그러나, 등록자 기반이므로 비등록자는 쇼핑을 할 수 없다는 점이 가장 큰 문제점이라 할 수 있으며, 각 상품마다 수취인이 다른 경우 수취인의 주소를 직접 모두 입력해야 하는 번거러움이 있다.



[그림 2.1] 오픈 마켓사의 상거래 흐름도

3. SET

SET은 인터넷과 같은 오픈 네트워크상에서 신용카드의 처리를 안전하게 수행하기 위한 기술적인 스펙으로 특정 전송 기술 및 보안 기술에 의존하지 않으며, 암호화를 통하여 각 구성 요소들간의 전송되는 지불 정보 및 구매 정보의 기밀성 보장, 디지털 서명을 이용한 전송되는 데이터에 대한 무결성 보장, 디지털 서명과 인증서(certificate)를 이용한 소비자·판매자 인증 및 전자상거래의 합법적인 구성원을 보호할 수 있는 최상의 보안성을 제공하고 있다[Visa & MasterCard Co. 1997a].

SET은 현재 지불 수단으로 신용카드를 이용하며, 신용카드 지불의 특성상 소액 거래에는 적합하지 않다.

SET은 OSI 계층의 응용 계층에서 운영되는 프로토콜로 구성 부분은 다음과 같으며,

SET 프로토콜을 이용하기 위해서 각각의 부분은 SET을 지원하는 소프트웨어를 가지고 있어야 한다.

먼저, 카드 소유자(Cardholder, 일반 소비자)는 신용카드를 소지한 구매자로서 SET을 이용하기 위해서는 SET을 지원하는 브랜드(brand)의 카드와 소프트웨어를 가지고 있어야 한다.

판매자(Merchant, 상인)는 상품을 판매하는 당사자이며, 대형 판매자의 경우 보통 은행과 직접 전용망을 통해 거래하는 경우도 있으나 일반적으로 지불 처리를 대리하는 지불 게이트웨이(Payment Gateway)를 사용한다. SET 프로토콜을 이용하기 위해서는 SET을 지원하는 은행과 거래를 열어야 하며 SET 판매자 소프트웨어를 가지고 있어야 한다.

인증 관리국(Certificate Authority : CA)이란 각종 인증서(certificate)의 발행 및 인증을 대리하는 기관이며, 보통 제 3 기관으로 정하며 거래에서 일어나는 각종 문제를 해결할 수 있는 기관이 되는 것이 좋다. 한 예로써, 카드 발행처가 카드 소유자에 대한 CA가 될 수 있으며 판매자의 대한 CA는 판매자의 거래 은행이 될 수 있다. 각 거래 은행 및 회사간은 적당한 협정에 의해 서로 상대방의 인증서를 지니고 거래하는 상대방의 유효성을 판단하게 된다.

지불 게이트웨이란 지불 요구 및 지불 인가 등을 대리로 처리하며, 은행 전용망을 사용하지 않는 판매자를 대상으로 은행 등의 전용망과 연결하여 지불에 관계된 흐름을 제어한다.

카드 발행처(Issuer, 은행이나 카드 회사)란 소비자가 소유하고 있는 신용카드를 발행하는 은행이나 회사를 말한다.

은행(Acquirer)은 판매자가 거래를 하는 은행으로 지불 게이트웨이를 통하여 지불 요청에 대한 인가여부를 결정한다.

SET 스펙에는 전자상거래에 필요한 모든 사항이 정의된 것이 아니라, 지불 흐름과 관련하여 정보의 전달 및 보안에 대한 사항과 상거래에 참여하는 각 부분의 역할에 대하여 주로 정의하고 있다. 다음은 SET 스펙에서 정의된 사항들이다.

- 암호화 알고리즘(RSA, DES 등)의 적용 방법
- 인증 메시지와 메시지 형식
- 구매 메시지와 메시지 형식
- 인가 메시지와 메시지 형식
- 대금결제(Capture) 메시지와 메시지 형식
- 구성 요소들간의 메시지 프로토콜

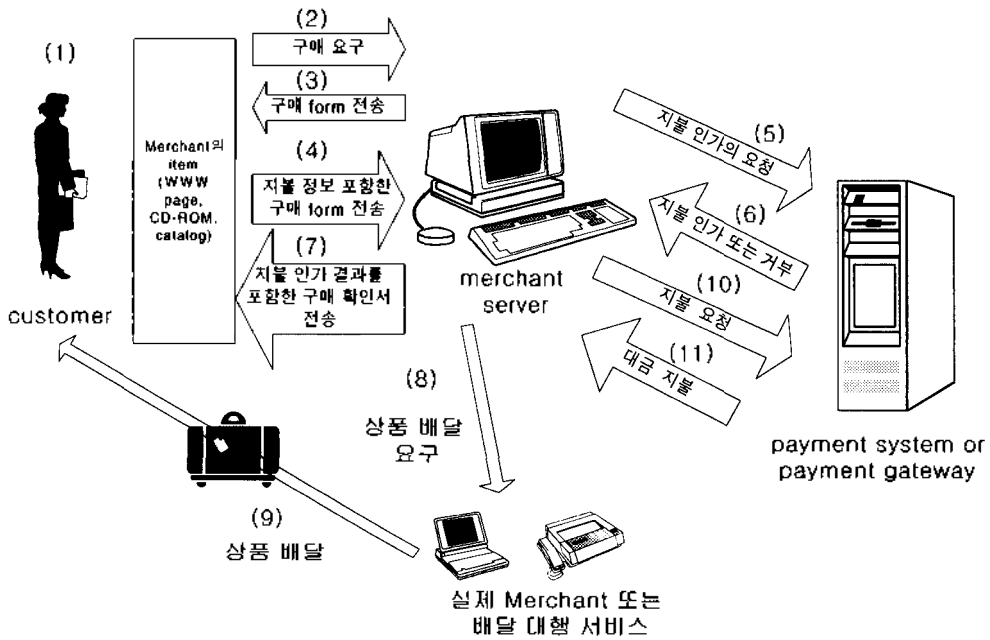
다음은 SET 스펙에서 정의되지 않은 사항들로 SET을 기반으로 한 전자상거래 시스템을 개발하려는 개발자들이 정의할 사항들이다.

- 상품 전시, 상품 배달 등의 메시지 프로토콜
- 인증서 발행시 각 은행별로 고려되는 세부 사항
- 판매자에 의해 표현되는 부분(상품 전시 내용, 상품 전시 방법, 주문 양식 등)
- 신용카드이외의 지불방법(전자현금이나 현금 거래)
- 메시지 전달시 오류에 대한 처리(전송 중인 메시지가 손실되는 경우)

SET을 지원하는 전자상점을 이용하고자 하는 사용자는 SET을 지원하는 소프트웨어를 기반으로 하여 다음의 과정에 따라 안전하게 쇼핑을 할 수가 있다.

1.고객이 상품을 검색(WWW Page, CD-ROM, 혹은 카탈로그 이용)
2.고객이 구매할 상품을 선택
3.고객은 선택한 상품의 리스트, 가격 등이 포함된 구매형식을 받음(상인이 고객에게 전송)
4.고객이 신용카드를 선택
5.고객이 상인에게 지불 방법을 포함한 완전한 구매 요구서 전송
6.상인은 고객의 거래 은행에 지불 인가 요청
7.상인이 고객에게 구매 확인서 전송
8.구매가 확인된 경우에 상인은 배달 또는 서비스 수행
9.상인은 상품 배달이나 서비스 수행 후 고객의 거래 은행에 지불 요구

그림 3.1)은 이러한 상거래 흐름을 나타내고 있다.



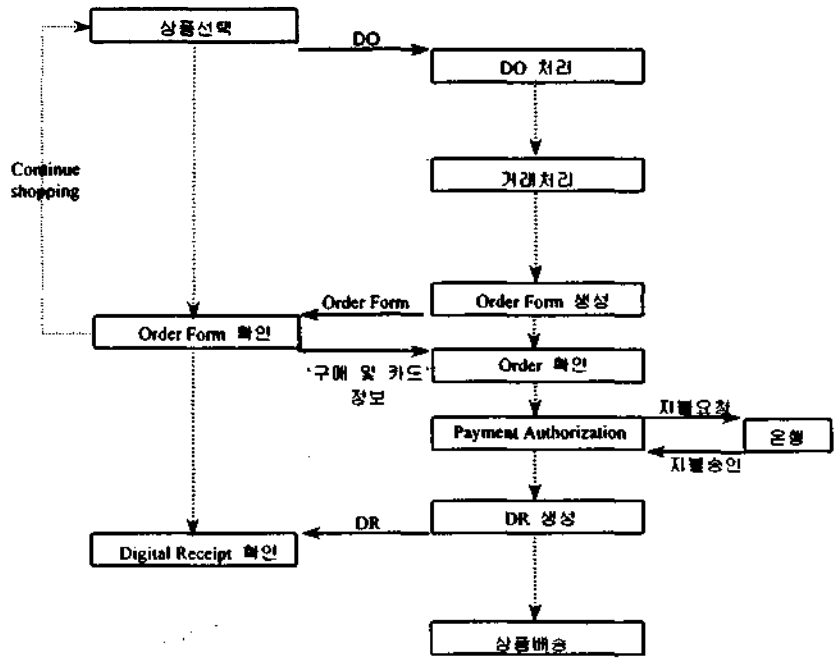
[그림 3.1] SET 쇼핑 시나리오

4. SET 을 기반으로 한 트랜잭션 모델

4.1 기존의 전자상거래 트랜잭션 모델

기존의 트랜잭션 모델은 소비자의 신용카드에 대한 정보를 판매자에게 전달하여 지불 처리가 이루어진다. 소비자가 지불을 위해 판매자에게 보내는 지불 정보는 인터넷상에서 전송 중에는 암호화되어 전송되지만 판매자는 암호가 풀린 평문으로 수신하게 된다. 이러한 것은 소비자가 소유한 카드의 사용을 판매자에게 위임한 것과 같으며, 악의가 있는 판매자는 소비자가 전달한 카드 정보를 오용할 수 있으므로 소비자는 카드 정보 전달을 주저하게 되며 판매자에게 전달되어 저장된 카드 정보는 인터넷 상점에 침투한 해커에 의해 정보가 유출되어 금융 사고가 발생될 수도 있다. 또한, 은행은 판매자가 소비자의 동의를 얻고 지불 요청을 하는지를 알 수 없으므로 판매자의 지불 요청을 신뢰할 수 없으며 지불 요청을 거절할 수 있다. 이러한 문제의 근본적인 원인은 소비자의 카드 정보를 판매자가 취급할 수 있다는 것과 서로에 대한 신용을 인증할 방법이 없기 때문에 발생한다. 따라서, 소비자·판매자 및 은행 등 상거래에 관련된 모든 부분들이 먼저 인증 기관에 등록하여 상거래 전에 서로의 신용을 확인하고, 소비자가 보낸 지불정보(카드 정보 및 지불 금액)는 은행만이 해독할 수 있도록 암호화하여 은행에 전달하고 전달된 지불정보에 따라서 판매자에게 결제가 이루어지면 상기의 문제점들이 해결될 수 있다.

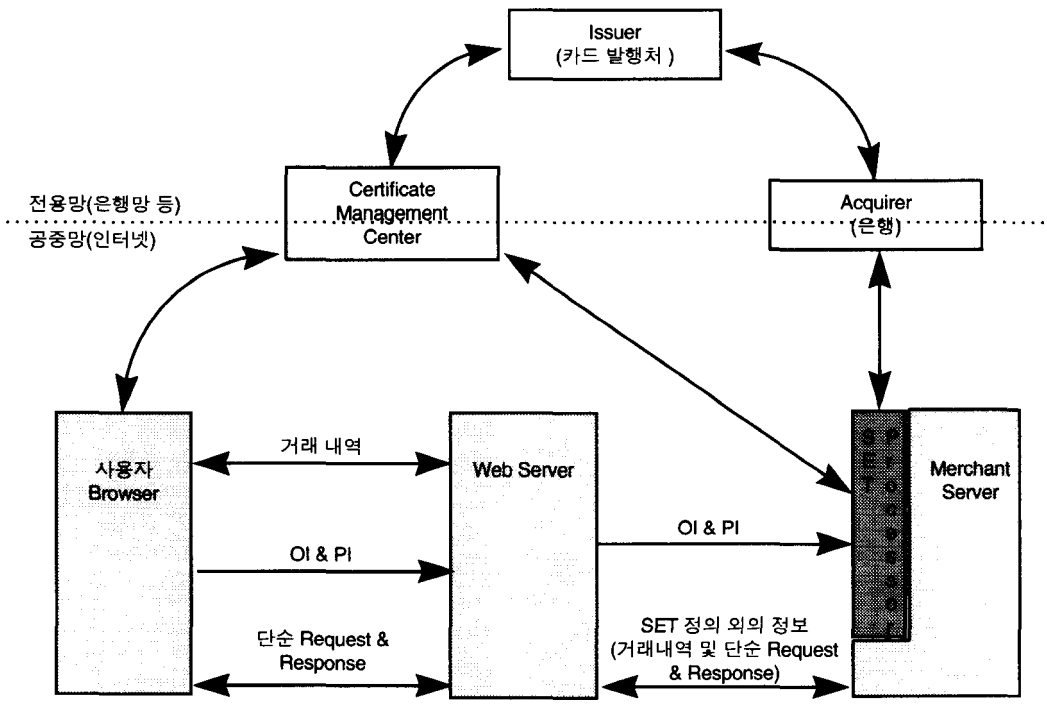
그림 4.1)은 기존의 트랜잭션을 간략하게 도시한 것이다.



[그림 4.1] 기존의 트랜잭션 모델

4.2 제안 SET 기반의 트랜잭션 모델

SET을 기반으로 한 전자상거래에서는 소비자와 판매자는 모두 인증 관리국인 CA에 등록하여 상거래 전에 서로의 인증서(certificate)를 확인하며, SET을 지원하는 소프트웨어를 이용하여 상거래를 한다. 다음에 제시하는 그림 4.2)는 SET 기반의 일반적인 시스템 구조도를 나타내고 있다. 은행과 카드 발행처간의 통신은 은행망 등의 전용망을 이용하며, 소비자와 판매자 사이의 상거래는 공중망인 인터넷을 사용한다. 기본적으로 소비자 및 판매자는 각각 CA를 이용하여 서로의 인증을 확인한다. 시스템간에 전송되는 정보 중에서 주문정보(Order Information, OI)와 지불정보(Payment Information, PI) 등은 기밀성과 무결성이 요구되므로 SET에서 정의한 암호화 방법 및 디지털 서명을 이용하여 전송되며, 상품 카탈로그, 상품 배달, 단순 정보 제공 등과 같이 기밀성 및 무결성을 요하지 않는 정보는 SET 규격을 따르지 않는다.



[그림 4.2] SET의 일반적인 구조도

제안된 트랜잭션 모델은 SET을 기반으로 하여 모든 지불 처리가 이루어진다. 소비자는 구매할 물품에 대한 지불 처리를 위해, 판매자는 해독할 수 없지만 은행은 해독할 수 있도록 암호화된 지불정보를 판매자에게 전송하고, 판매자는 전송된 정보를 단지 은행

에 보내는 것으로 지불 인가 요청을 은행에 할 수 있다. 이러한 일련의 과정에서 소비자의 암호화된 지불정보를 판매자는 해독할 수 없으므로 판매자 임의의 카드 사용을 막을 수 있으며, 소비자의 카드 정보를 판매자의 시스템에 저장하고 있지 않으므로 시스템에 침투한 해커 등에 의한 금융사고를 막을 수 있다. 또한, 은행은 소비자가 보낸 정보를 통해 지불인가 요청을 한 판매자는 소비자의 동의를 얻었음을 확인 할 수 있으므로 지불 요청에 대한 결제를 할 수 있다. 따라서, 기존 전자상거래 트랜잭션이 지닌 소비자 지불 정보 유실 가능성과 은행의 지불 거부 등의 문제점을 해결 할 수 있다.

본 논문에서 제안한 시스템을 이용하여 상거래를 하기 위해서는, 먼저 상거래에 관련된 부분들은 모두 인증 기관인 CA에 등록하여 신용에 대한 인증서를 받는다. 상거래가 이루어지면 상대방이 소지한 인증서를 통하여 서로의 인증을 확인하게 된다. 시스템의 특징으로는 쇼핑 카트 기능을 지원하여 여러 품목을 구입하고 한 번에 지불할 수 있으며, 시스템에 등록하지 않은 비등록자들도 원하는 상품을 선택하여 구매 할 수 있으며, 시스템에 등록한 사용자는 부가서비스(할인 및 구매 내역 조회 등) 지원 등의 특징을 가지고 있다. 그림 4.3)은 소비자와 판매자를 중심으로 한 트랜잭션을 나타내고 있으며, 소비자가 상품을 선택하는 '쇼핑 및 거래처리' 단계와 상품의 구매와 지불을 위한 '구매 및 지불처리' 단계로 구성된다.

4.2.1 쇼핑 및 거래처리

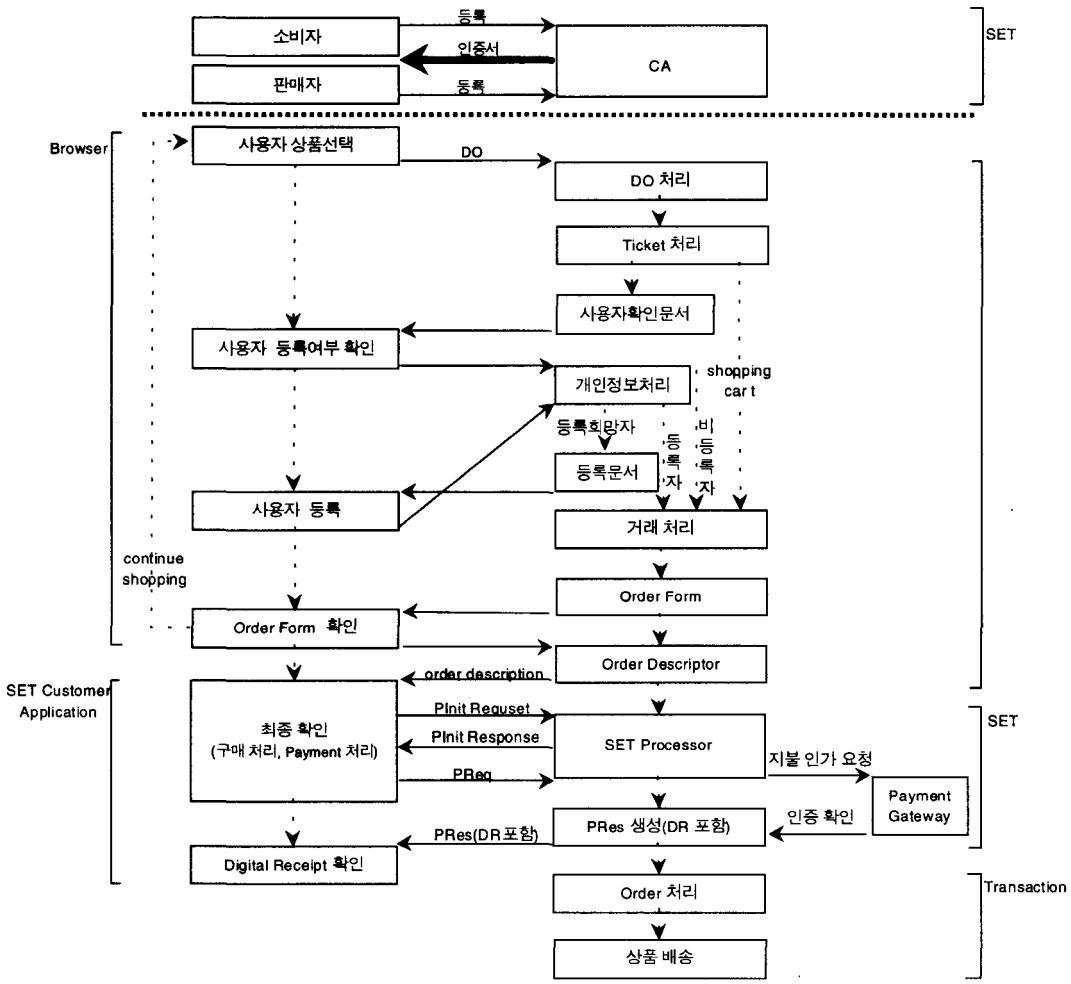
'쇼핑 및 거래처리' 단계는 상점에 접속한 소비자가 원하는 상품을 선택하여 구매를 결정하는 과정과 판매자가 소비자의 구매결정에 대하여 거래정보를 처리하는 과정으로 구성되며, 각 모듈별 기능을 살펴보면 다음과 같다.

소비자 측 브라우저는 다음의 기능을 수행한다.

- •상품 검색 및 선택
- •사용자(등록자 여부) 확인
- •비등록 사용자의 등록
- •주문품 확인

판매자 측의 트랜잭션은 다음의 기능을 수행한다.

- •전자 주문서(Digital Offer, DO) 및 티켓 처리
- •사용자(등록자 여부) 확인 및 등록 양식 제공
- •개인정보처리
- •거래처리
- •주문 내역서 생성 및 전송



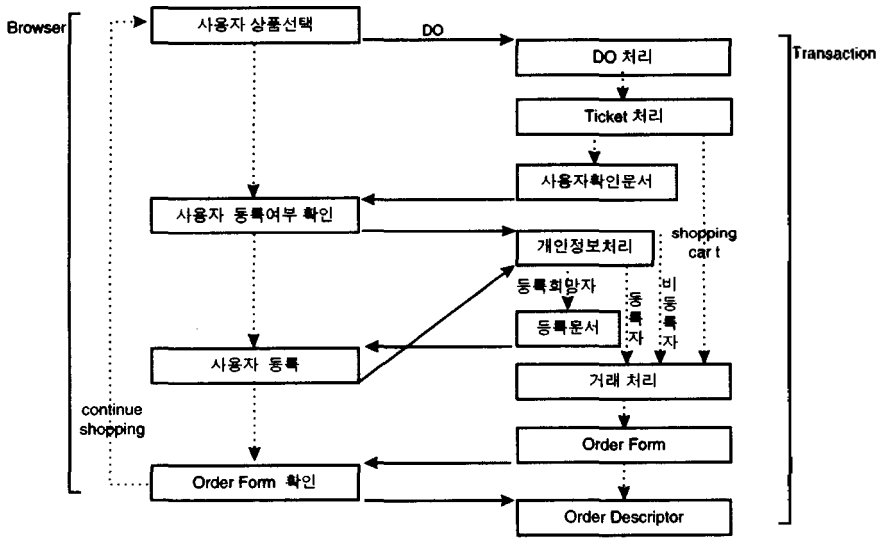
[그림 4.3] SET 기반의 트랜잭션

소비자(cardholder)는 브라우저를 이용하여 인터넷상의 상점에 접속하여 원하는 상품을 선택하고 DO를 판매자에게 전송한다. 판매자는 소비자가 전송한 DO를 처리하고 DO를 발송한 소비자의 인식과 쇼핑 유형(첫 거래 및 쇼핑 카트 이용)을 티켓의 유무로 확인한다.

티켓이 없는 소비자는 첫 거래자이므로 사용자 인식과 상태관리를 위한 티켓을 발행해 주며, 티켓을 소지한 사람은 쇼핑중(쇼핑 카트 이용)인 소비자이므로 소지한 티켓의 유효성(티켓의 무결성 및 유효 기간)을 검사한다. 티켓이 처리되면, 판매자는 소비자가 시스템 등록자인지 여부를 판단하기 위하여 사용자

확인 양식을 전송하고 사용자가 반환한 사용자 ID와 비밀번호를 통하여 등록자 여부를 확인하며, 등록을 원하는 비등록자에게는 등록 양식을 전송하고 비등록자는 등록 양식을 작성하여 등록을 한다. 소비자가 전송한 DO는 거래처리를 위하여 DB에 저장되고, 최종적으로 소비자가 원하는 상품을 모두 선택하여 구매를 원하는 경우, 판매자는 소비자측의 SET 응용프로그램 구동 메시지인 MIME 형의 주문 내역서(order description)를 생성(소비자가 선택한 상품들의 리스트를 포함)하여 소비자에게 전송한다.

다음의 그림 4.4)는 '쇼핑 및 거래처리' 단계를 도시한 것이다.



[그림 4.4] 쇼핑 및 거래처리

4.2.2 구매 및 지불 처리

'구매 및 지불처리' 단계는 소비자가 상품의 구매를 선택한 경우 발생하는 구매에 대한 지불처리가 이루어지는 과정이며, 각 모듈별 기능을 살펴보면 다음과 같다.

소비자 측 SET 응용프로그램(SET Helper)은 다음의 기능을 수행한다.

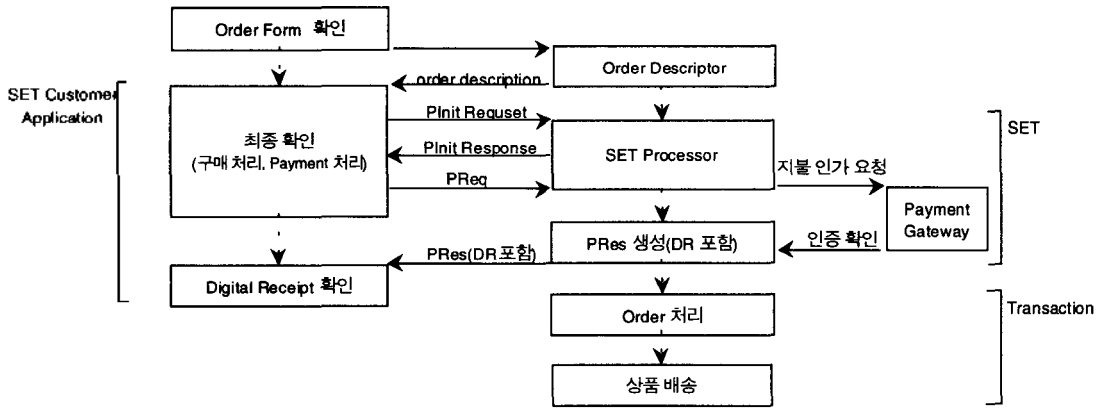
- SET 관련 부분 처리(암호화·복화화 및 디지털 서명 등)
- 구매 및 지불 처리(거래 초기화 및 구매 정보·지불 정보 전송)
- DR(Digital Receipt) 확인

판매자 측의 SET 응용프로그램인 SET 프로세서(Processor)는 다음의 기능을 수행한다.

•SET 관련 부분 처리(암호화·복화화 및 디지털 서명 등)
•지불 처리(거래 초기화 및 거래 은행에 지불 인가 의뢰)
•DR 전송

소비자는 판매자의 SET 구동메시지를 수신하여 SET 소비자 응용프로그램을 구동시키고, 판매자의 신용도와 소비자가 소지한 카드를 판매자가 취급할 수 있는가 등을 확인하는 구매 초기화(PInit Request·Response)를 한 후에 구매정보(OI)와 지불정보(PI)를 암호화와 디지털 서명을 통하여 취급 권한을 설정하고 판매자에게 보낸다(PReq 메시지). 판매자는 소비자의 디지털 서명과 OI와 PI의 이중 서명을 확인하고, 소비자의 인증에 문제가 없으면 지불 게이트웨이에 지불 인증을 얻기 위해 PI를 포함한 인증 요구를 한다. 전송된 데이터들을 이용하여 지불 게이트웨이는 소비자의 신용도를 판단하여 지불 인증 여부를 판매자에게 전송하며, 인증이 이루어지면 판매자는 디지털 영수증(DR)을 포함한 구매 응답(PRes 메시지)을 소비자에게 전송하고 배송처리를 한다. 지불 인증이 실패하였을 경우에는 해당 메시지를 전송하며, 소비자는 전송된 메시지를 확인하게 된다.

다음의 그림 4.5)는 '구매 및 지불처리' 단계를 도시한 것이다.



[그림 4.5] 구매 및 지불처리

5. 결론 및 향후 과제

인터넷을 이용하는 사용자의 증가로 인한 여러 제반 사항들이 변화하고 있으며, 이에 따라 전자상거래에 대한 수요도 증가하고 있다. 현실적으로 안전하게 인터넷을 통해 상거래를 한다는 것은 보안 등의 어려운 점이 있으며, 이러한 점을 해결하기 위해 SET 프로토콜이 제안되었다. 본 연구에서는 SET을 이용하여 안전하게 상거래를 할 수 있도록 트랜잭션 모델을 제안하였다. 제안된 모델을 이용하면 CA에 등록된 소비자와 판매자들은 서로를 신용할 수 있으며, 소비자는 카드 정보의 유출에 대한 불안 없이 안전하게 쇼핑을 할 수 있다.

제안된 시스템은 신용카드 기반의 SET을 이용하므로 온라인 게임 및 전자신문 구독 등과 같은 서비스 비용이 소액인 경우에는 적합하지 않다. 따라서, 제안된 트랜잭션 모델의 기능을 확장하여 소액거래도 지원하는 전자상거래 시스템을 개발하고자 한다.

현실적으로 완전하게 SET을 지원하기 위해서는 카드 발행 회사, 은행 및 정부 기관 등의 관계 기관들의 충분한 협의를 통해 관계 법령 등 제반 사항들이 지원되어야만 한다. 또한 일반 소비자들의 전자상거래에 대한 인식의 변화도 필요하다.

참고문헌

[Killen, 1996] Killen, "Payments on the Internet : Opportunities in EC", 1996

[Dacom, 1997] "Interpark Mall & Malls", http://www.interpark.com/shop/home.htm

[Open Market Co., 1996a] Open Market Co., "Open Market's Products : A Technical Overview", http://www.openmarket.com/wp/, 1996

[Open Market Co., 1996b] Open Market Co., "The SET Protocol in Open Market's Commerce Products", Open Market Technical White Paper, September 6, 1996

[Visa & MasterCard Co., 1997a] Visa & MasterCard Co., "Secure Electronic Transaction(SET) Specification Book 1: Business Description", SET version 1.0, May 31, 1997

[Visa & MasterCard Co., 1997b] "Secure Electronic Transaction(SET) Specification Book 2: Programmer's Guide", SET version 1.0, May 31, 1997

[Visa & MasterCard Co., 1997c] "Secure Electronic Transaction(SET) Specification Book 3: Technical Specifications", SET version 1.0, May 31, 1997

저자소개

고 영 철
1995년 아주대학교 산업공학과 졸업
1997년 아주대학교 대학원 산업공학과 졸업(석사)
1997~ 현재 시스템공학연구소/시스템통합연구부 연구원
관심분야 : CALS/EC, ERP(Enterprise Resource Planning), Neural Network, CIM,

송 병 열
1995년 전북대학교 전자공학과 졸업
1997년 전북대학교 대학원 전자공학과 졸업(석사)
1997~ 현재 시스템공학연구소/시스템통합연구부 연구원
관심분야 : Electronic Commerce System, Network Security, 인공지능, 분산컴퓨팅

조 현 규
1988년 한국외국어대학교 독일어학과 졸업
1990년 고려대학교 대학원 경영학과 졸업(석사)
1997년 한남대학교 대학원 경영학과 졸업(박사)
1988~1990년 현대해상 정보시스템부
1990~ 현재 시스템공학연구소/시스템통합연구부 선임연구원
관심분야 : Electronic Commerce System, Dynamic & Real-Time Scheduling System,
System Simulation 및 Shop Floor Control System

함 호 상
1977년 고려대학교 산업공학과 졸업
1983년 고려대학교 대학원 산업공학과 졸업(석사)
1995년 고려대학교 대학원 산업공학과 졸업(박사)
1982~ 현재 시스템공학연구소/시스템통합연구부 책임연구원
관심분야 : CALS/EC, 객체지향 분석 및 설계, 시스템통합방법론

대전광역시 유성구 어은동 1번지 시스템공학연구소 시스템통합연구부
Tel: 042-869-1848 Fax: 042-869-1549 E-mail: Gycmh@seri.re.kr