메타-몰 구조를 갖는 전자쇼핑몰에서의 안전한 지불체계에 대한 연구

A Secure Payment Method for Meta-Malls Architecture

송 용 욱 (Yong Uk Song) 경상대학교 경영학부

이 재 규 (Jae Kyu Lee) 한국과학기술원 테크노경영대학원

목 차

Keywords: *meta mall, 전자지불, SET, 전자쇼핑몰*

Ⅰ. 서 론

전자상거래가 활성화되면서 다양한 형태의 전자쇼핑몰들이 등장하고 있다. 현재 인터넷 상에는 40만개 이상의 전자쇼핑몰이 성업 중인 것으로 알려져 있으며, 그 수는 나날이 증가하고 있다. 치열한 경쟁 하에서 전자쇼핑몰이 성공하기 위해서는 다양한 상품과 풍부한 상품정보를 제공해야 하고, 일반 사용자들이 편리하게 사용할 수 있어야 하며, 상품의 가격이 저렴해야 한다. 이와 같은 장점을 갖출 수 있는 전자쇼핑몰 구조로 제시된 것이 메타-몰 구조(Meta-Malls Architecture) (Lee 등, 1998; Keller, 1997)이다. 메타-몰은 하부의 독립적인 몰들을 통합하여 하나의 몰처럼 행동함으로써 고객에게 다양한 상품정보와 편리한 사용환경을 제공한다.

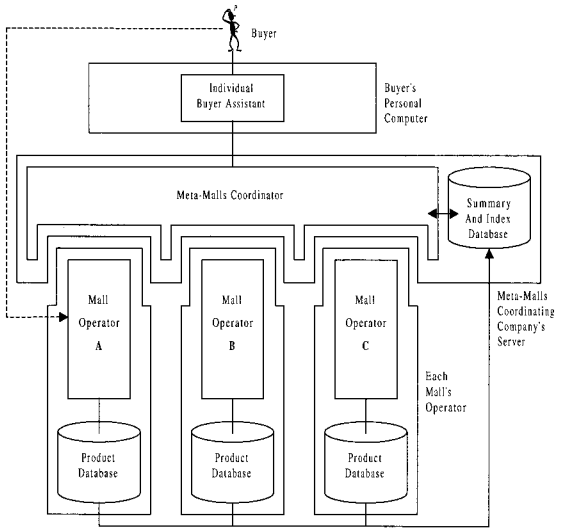
지불정보의 보안은 모든 전자쇼핑몰들이 시스템의 안전을 위해 심혈을 기울이는 분야이면서, 그 자체가 전자쇼핑몰의 중요한 선전요소 중의 하나이기도 하다. 현재 대부분의 전자쇼핑몰들이 사용하고 있는 보안 방법인 SSL(Secure Socket Layer) (Cain, 1996)의 결점이 알려지면서 그 대안으로 주목받고 있는 것이 SET(Secure Electronic Transaction) (Master Card and Visa, 1997)이다. 필적할 만한 다른 대안이 없는 상태에서 그 제안자가 신용카드 업계의 양대 산맥인 Visa와 Master Card라는 이유 때문에 SET은 현재 사실상의 표준(de facto standard)으로 자리잡고 있다.

그런데, SET 지불 보안 규정은 하나의 상인이 있는 전형적인 전자쇼핑몰을 대상으로 하고 있기 때문에 메타-몰 구조처럼 여러 상인이 있고, 따라서, 여러 상인으로부터 구매한 상품들을 한꺼번에 지불 처리해

주는 경우는 지원하지 않고 있다. 본 논문에서는 사실상의 표준인 SET를 수용하면서, 메타-몰에서 여러 상인의 상품을 구매하는 경우도 지원할 수 있는 안전한 지불방안을 제시하고자 한다. 이를 설명하기 위하여 2절에서 메타-몰 구조를 설명한 후, 3절과 4절에서 지불정보 보안 기법과 전자상거래 지불 보안 체계들을 소개한다. 그리고 5절에서 메타-몰의 지불 보안 체계를 상술하고 5절에서 요약하도록 하겠다.

Ⅱ. 메타-몰 구조

메타-몰 구조는 <그림 1>에 나타나 있다. <그림 1>에서 Mall Operator들은 독자적인 기능을 갖는 전자쇼핑몰 시스템이고, Meta-Malls Coordinator는 이들 하부 몰들을 통합하여 하나의 몰처럼 행동하는 메타-몰 시스템이다. 메타-몰은 하부의 여러 몰들을 통합함으로써 여러 몰의 상품들을 마치 한 몰의 상품인 것처럼 하나의 웹 화면에서 보여 줄 수 있기 때문에 여러 몰이 모일 경우 고객에게 다양한 상품정보를 보여줄 수 있게 된다. 또, 메타-몰은 여러 몰들을 통합하여 하나의 쇼핑몰처럼 행동하기 때문에 고객은 여러 몰에 드나드는 불편함이 없이 하나의 몰에서 쇼핑하듯이 편리하게 쇼핑을 즐길 수 있다. 이 과정에서 메타-몰은 유사상품검색이라는 기능을 통하여 여러 몰에서 판매하는 유사한 상품들을 검색하여 한 화면에서 보여주기 때문에 고객의 검색 편의성을 더 한층 높여준다. 이 유사상품검색 기능은 상인 간의 가격경쟁을 유도하는 역할도 하게 되며, 동시에 상인은 유사상품검색을 광고라는 측면에서 활용할 수도 있다.



〈그림 1〉 메타-몰의 구조

메타-몰에 들어온 고객은 메타-몰의 여러 하부 몰에서 상품들을 선택하여 구매하게 된다. 그러나, 주문 및 지불처리과정에서 고객은 하부 몰에 구애 받지 아니하고 한꺼번에 지불을 처리할 수 있어야 한다. 이것이 원-스톱 지불(One-Stop Payment)이다. 또한, 이 지불처리는 안전하게 이루어져야 한다. 즉, 지불처리과정에서 고객의 지불정보 - 신용카드 번호, 계좌번호, 비밀번호 등 - 가 제 3자에게 알려져서는 안되며, 특히, 상인에게도 알려져서는 안된다. 이러한 안전한 지불처리를 위한 보안 규정이 SET이다. 그러나, 전술한 바와 같이 SET규정은 하나의 상인이 있는 경우만을 대상으로 하고 있으므로, 메타-몰에서처럼 여러 하부 몰에서 상품을 구매하여 원-스톱으로 지불처리를 하고자 하는 경우는 지원하지 못한다.

Ⅲ. 지불정보 보안 기법

3.1 전자지불시스템의 보안 목표

인터넷은 개방형 구조(Open Architecture)를 갖는 공중망이기 때문에 보안에 대한 고려가 미약하고 이에 따라 인터넷을 이용한 지불 정보의 전송은 기본적으로 보안 취약성을 내포하고 있다. 그렇지만, 이러한 인터넷의 보안 취약성은 암호화 방법에 의해 해결할 수 있다. 그러면, 그 구체적인 해결 방법들을 살펴보기 전에 먼저 이 취약성들을 극복하기 위하여 전자지불시스템 내에 구현해야 할 보안상의 기능들이 무엇인지 정의하도록 하자. 이것들은 다음의 네 가지로 요약할 수 있다.

3.1.1 기밀성(Confidentiality)

기밀성은 전달내용을 제 3자가 획득하지 못하도록 하는 것이다. 예를 들어 전자결제를 위하여 은행 계좌번호와 그 비밀번호를 인터넷을 통하여 상인에게 전달할 때 암호화하여 전송함으로써 도청자가 도청에 의하여 암호문을 얻어 내더라도 그 내용을 알지 못하도록 할 필요가 있다.

3.1.2 인증(Authentication)

인증은 정보를 보내오는 사람의 신원을 확인하는 것이다. 예를 들어, 어떤 고객이 상품의 구매대금으로 신용카드번호를 보내왔을 때 상인은 그 고객이 그 신용카드의 실제 소유자인지를 확인할 필요가 있다.

3.1.4 무결성(Integrity)

무결성은 정보전달 도중에 정보가 훼손되지 않았는지 확인하는 것이다. 예를 들어, 신용카드 회사에 어떤 카드 사용자가 "상인 을에게 100만원을 지불하겠다"는 내용을 보내왔을 때 이 내용이 원래는 "상인 갑에게 100만원을 지불하겠다"는 내용이었던 것이 중간에 (아마도 을에 의해서) 변조된 것이 아닌지를 확인할 필요가 있다.

3.1.5 연결성(Linkage)

전자지불에서 중요한 보안 목표 중의 하나는 상인에 대하여 지불정보의 기밀성을 보장하는 데 있다. 상인 자신이 사기꾼으로 돌변하여 고객의 지불정보를 악용할 수도 있기 때문이다. 이를 위하여 SET에서는 주문정보는 상인만 볼 수 있도록 하고, 지불 정보는 금융기관만 볼 수 있도록 기밀성을 유지한다. 따라서, 상인은 고객으로부터 주문정보와 지불정보를 받아서 주문정보는 정산, 배송 등의 정보로 사용하고, 지불정보는 그 내용을 보지 못한 채 금융기관에 넘겨주어 금융기관으로부터 지불처리 결과만을 받게 된다. 이때, 상인의 관점에서는 자신이 금융기관에 넘겨주는 지불정보가 자신이 받은 주문정보에 대한 지불정보인가, 혹시 다른 사람에 의해 지불정보가 바뀌지는 않았는가를 확인할 필요가 있다. 이렇게 주문정보와 지불정보 간의 연관성을 확인하는 것이 연결성이다.

이밖에 고객이 주문사실을 부인했을 때 상인이 그에 대한 반증을 들 수 있는 부인방지(Nonrepudiation)를 전자지불시스템의 보안목표로 넣기도 하지만 부인방지를 위한 기술의 복잡성(Schneier, 1996)과 고객이 주문사실을 부인했을 때 그것을 굳이 거부할 수가 없는 마케팅 상의 필요성 등 때문에 현재 대부분의 전자지불시스템들은 부인방지를 크게 고려하지 않고 있고, 본 논문에서도 부인방지는 고려하지 않기로 한다.

3.2 암호화 기법

앞 절에서 이야기한 네 가지 기능은 인터넷의 보안 취약성을 극복하기 위하여 전자지불시스템들이 갖추어야 할 기본적인 기능이다. 본 절에서는 현대적 암호화 방법론들을 살펴봄으로써 다음 절에서 앞의 네 가지 기능을 구현하는 방법을 설명하는 데 이론적 기반을 제시하도록 하겠다. (Schneier, 1996)

암호화 알고리즘의 보안성이 그 알고리즘이 수행하는 내용의 기밀성에 의존할 때 이 알고리즘을 제한 알고리즘(Restricted Algorithm)이라고 부른다. 과거의 수많은 역사적인 암호화 알고리즘들이 제한 알고리즘이었음에도 불구하고 이러한 제한 알고리즘은 현대의 암호 알고리즘으로는 부적절하다. 많은 구성원으로 이루어진 한 그룹에서 제한 알고리즘을 쓸 수는 없다. 왜냐하면, 그 그룹 구성원의 한 사람이 그 그룹을 떠날 때마다 다른 알고리즘을 사용하여야 하며, 이를 위해서는 다른 알고리즘을 고안하여 구성원에게 다시 나누어 주어야 하는 부담이 따른다. 이를 막기 위해 구성원마다 다른 알고리즘을 쓴다면 역시 그 많은 알고리즘을 고안하고 관리해야 하는 문제가 따르며, 또 그 알고리즘을 장착한 컴퓨터 하드웨어나 소프트웨어의 대량생산이 불가능하기 때문이다. 다시 이야기 하면, 제한 알고리즘은 보안성의 유지 및 표준화를 제공하지 못하고 있다.

현대의 암호학은 이 문제를 키(Key)를 이용하여 해결하였다. 키는 매우 큰 숫자 (예를 들어 0과 2^{1024} 사이의 수) 중의 하나이며, 키가 가질 수 있는 가능한

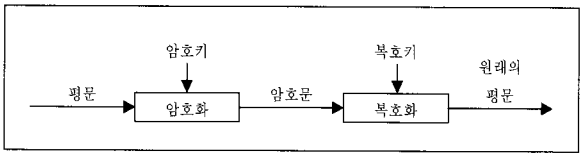
값의 범위를 Keyspace라고 부른다. 암호화와 복호화는 이 키를 이용하여 이루어지며, 키의 값을 제외하고는 모든 사용자가 동일한 암호화 및 복호화 알고리즘을 사용한다. 암호키를 K_1, 복호키를 K_2라고 하고 평문을 M, 암호문을 C, 암호화 함수를 E, 복호화 함수를 D라고 표시하면 다음과 같은 수식으로 표현할 수 있다.

$E_{K1}(M) = C$

$D_{K2}(C) = M$

$D_{K2}(E_{K1}(M)) = M$

키를 이용한 암호화와 복호화 과정을 그림으로 도시하면 <그림 2>와 같다.

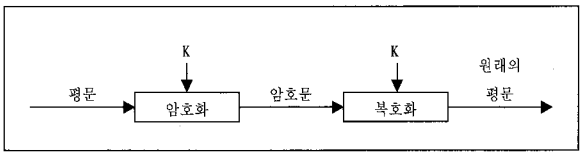


〈그림 2〉 키를 이용한 암호화와 복호와 과정

키 기반 암호화 알고리즘은 크게 두 가지로 나누어 볼 수 있다. 하나는 비밀키 암호화 방식이고 다른 하나는 공개키 암호화 방식이다. 그리고, 암호화 알고리즘은 아니지만 전달된 정보의 변경 여부(무결성)나 정보를 보낸 사람을 확인(인증)할 때 사용하는 것으로 메시지 다이제스트(Message Digest) 기법이 있다. 전자상거래 보안에서는 위의 세 가지 방법이 주로 사용된다. 이들을 각각 설명하면 다음과 같다.

3.2.1 비밀키 암호화 방식 (Symmetric Algorithm, Secret-key Algorithm, Single-key Algorithm, One-key Algorithm, 대칭형 알고리즘)

암호키로부터 복호키를 계산해 낼 수 있거나, 반대로 복호키로부터 암호키를 계산해 낼 수 있을 때 이 암호화 알고리즘을 비밀키 암호화 방식이라고 부른다. 대부분의 비밀키 암호화 방식에서는 암호키와 복호키가 동일하다. 동일한 암호키와 복호키를 K라고 했을 때, 암호화, 복호화 과정을 그림으로 도시하면 <그림 3>과 같다.

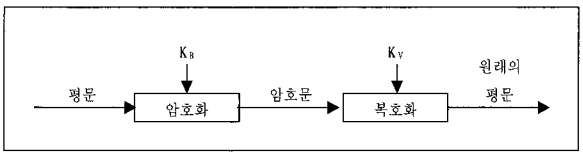


〈그림 3〉 비밀키 암호화 방법을 사용한 암호화 및 복호화

이 방법의 장점은 암호화와 복호화가 빠르다는 점과, 다양한 암호화 기법이 개발되어 있다는 것이다. 그러나, 이 방법의 단점은 복수의 사용자가 관련되어있을 때 키의 공유 문제가 발생한다는 것과 키자 체를 상대방에게 안전하게 보내는 것이 문제가 된다는 것이다.

3.2.2 공개키 암호화 방식 (Asymmetric Algorithm, Public-key Algorithm, 비대칭형 알고리즘)

이 방법에서는 암호키와 복호키가 서로 다르며, 또한 암호키로부터 복호키를 계산해낼 수 없다. 이 방법이 공개키 방법이라 불리는 이유는 암호키가 공개되어도 된다는 것 때문이다. 아무나 암호키를 이용하여 어떤 내용을 암호화 할 수 있지만, 오직 해당 복호키를 가진 사람만이 그 암호문을 복호할 수 있다. 이 때문에, 이 알고리즘에서는 암호키를 공개키(Public Key)라고 부르고, 복호키를 개인키(Private Key)라고 부르며, 비밀키 암호화 방식에서 키를 비밀키(Secret Key)라고 부르는 것과 구별한다. 공개키를 KB, 개인키를 KV라고 표시했을 때, 암호화, 복호화 과정을 그림으로 도시하면 <그림 4>와 같다.



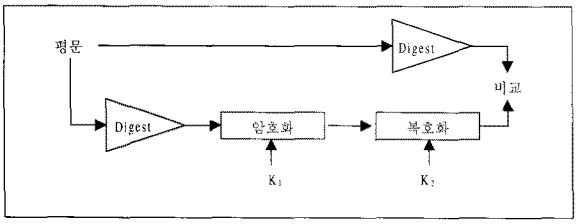
〈그림 4〉 공개키 암호화 방법을 사용한 암호화 및 복호화

이 방식의 장점은 키를 상대방에 보내는 것(키 교

환)에 보안상의 허점이 없다는 점과 정보의 기밀 유지 이외에 다른 목적(인증, 무결성 등)으로도 사용할 수 있다는 점이지만 단점으로는 암호화, 복호화 속도가 비밀키 암호화 방식에 비해 매우 느리고 많은 양의 자료를 암호화, 복호화 하기가 불편하다는 점 등이 지적된다.

3.2.3 메시지 다이제스트(Message Digest)

앞에서 이야기 한 바와 같이 메시지 다이제스트는 암호화 방법은 아니다. 이것은 일방향 해쉬(One-way hash) 함수를 이용하여 주어진 정보를 일정한 길이 내의 아주 큰 숫자(해쉬값)로 변환해 주는 것이다. 이 함수는 일방향(One-way)이기 때문에 주어진 정보로부터 해쉬값을 만들어 낼 수는 있어도, 반대로 이 해쉬값으로부터 원래의 정보를 복구해낼 수는 없다. 다만, 정보와 함께 그 정보의 해쉬값을 받은 사람은 받은 정보의 해쉬값을 구한 후, 정보와 함께 전달된 해쉬값을 비교함으로써, 그 값이 같다면 정보의 전달 중에 정보가 변경되지 않았음을 (100%는 아니지만 거의 확실하게) 확인할 수 있으며, 만약 그 값이 다르다면 정보가 전달 중에 어떻게 든 변경되었음을 알 수 있다. 물론, 이 해쉬값은 암호화 알고리즘에 의해 암호화되어 전달되어야 한다. 그렇지 않다면, 정보를 중간에서 변조하는 사람이 정보를 변조한 후 그 변조된 정보의 해쉬값과 함께 보낼 수 있기 때문에 해쉬값이 제대로 기능하지 못하게 된다. 이 과정을 그림으로 도시하면 <그림 5>와 같다.



〈그림 5〉 메시지 다이제스트를 이용한 메시지 변조 확인 (무결성)

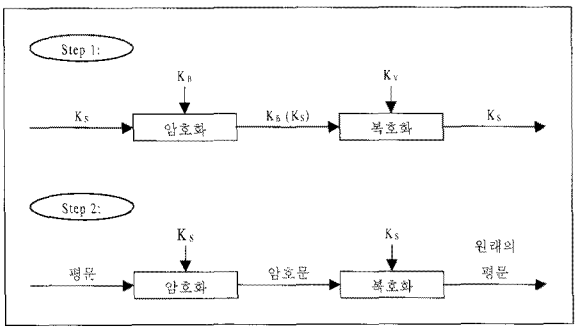
3.3 암호화 기법의 적용

3.1절에서 이야기한 전자지불시스템에서 필요한 네 가지 보안기능(기밀성, 인증, 무결성, 연결성)을 3.2절에서 이야기한 3가지 암호화 방식(비밀키 암호화 방식, 공개키 암호화 방식, 메시지 다이제스트)에 의해 구현하는 방법을 네 가지 보안기능별로 설명하도록 하겠다.

3.3.1 기밀성(Confidentiality)

기밀성은 비밀키 암호화 방식 또는 공개키 암호화 방식 모두에 의해 이룰 수 있다. 비밀키 암호화 방식을 쓴다면 보내는 사람은 미리 정해진 키를 이용하여 암호화 한 후 보내고, 받는 사람은 같은 키를 이용하여 암호문을 복호화 하면 된다. 공개키 암호화 방식을 쓴다면 보내는 사람은 받는 사람의 공개키를 이용하여 암호화 한 후 보내고, 받는 사람은 자신의 개인키를 이용하여 복호화 하면 된다.

위 두 방법은 각기 단점을 갖고 있는데 비밀키 방식의 경우 키를 미리 갖고 있어야 한다는 점이 단점이며, 공개키 방식의 경우는 암호화 및 복호화 시간이 길고 장문의 정보를 보낼 때 암호화 및 복호화가 불편하다는 것이다. 이 때문에 보통 기밀성을 위한 암호화 방법으로는 비밀키 방식과 공개키 방식을 혼용한다. 즉, 전달 정보 자체는 임의의 비밀키를 이용하여 비밀키 암호화 방식으로 암호화하고, 비밀키 자체는 받는 사람의 공개키를 이용하여 공개키 암호화 방식으로 암호화한 후 두 암호문을 보내면, 받는 사람은 자신의 개인키로 비밀키를 복호화 한 후 이 비

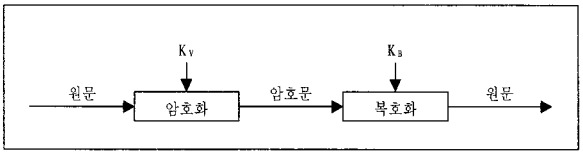


〈그림 6〉 비밀키 방식과 공개키 방식을 혼용한 기밀성 확보 방법

밀키를 이용하여 전달정보를 복호화한다. 이와 같이 비밀키를 주고받는 것을 키의 교환(Key Exchange)이라고 부른다. 위 과정을 그림으로 도시하면 <그림 6>과 같다.

3.3.2 인증(Authentication)

인증은 공개키 암호화 방식에 의하여 이룰 수 있다. 전달될 내용을 보낼 사람과 받을 사람이 모두 미리 알고 있는 상황 하에서 보내는 사람이 그 내용을 자신의 개인키(Private Key)를 이용하여 공개키 방식으로 암호화하여 보내고, 받는 사람은 그것을 상대방의 공개키(Public Key)로 복호화한 후 그 내용을 확인해 보아 맞으면, 받는 사람은 그 내용을 보낸 사람을 확인할 수 있다. 왜냐하면, 미리 약속된 내용으로 복호화되도록 암호화를 할 수 있는 사람은 이 공개키의 짝이 되는 개인키를 알고 있는 사람뿐이기 때문이다. 이 과정을 그림으로 도시하면 <그림 7>과 같다.



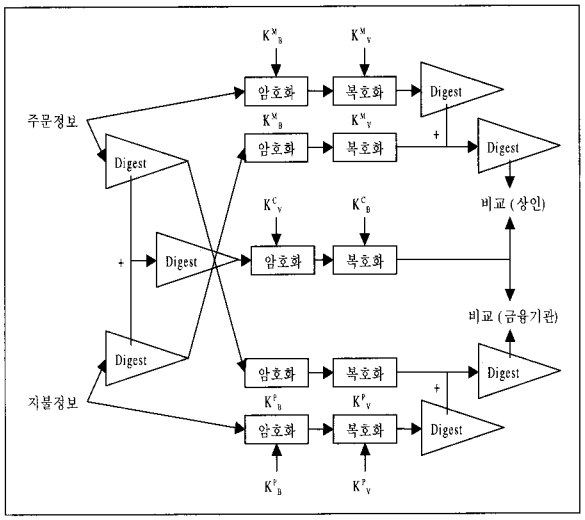
〈그림 7〉 공개키 방식에 의한 인증 방법

(1)절에서 이야기한 바와 같이 공개키 암호화 방식은 속도가 오래 걸리고 장문의 내용을 암호화, 복호화 하기 어려우므로 인증 시에도 미리 정해진 내용을 개인키로 암호화하고 공개키로 복호화 하기 보다는 그 내용을 메시지 다이제스트 한 것을 암호화하고 복호화 한다. 이것을 전자서명(Digital Signature)이라 하는데 전자서명은 인증뿐만 아니라 밑에서 이야기할 무결성도 보장하게 된다. 이에 관해서는 3.5 절에서 자세히 설명하도록 하겠다.

3.3.3 무결성(Integrity)

무결성은 메시지 다이제스트를 암호화하여 보냄으로써 이룰 수 있다. 이 부분은 3.2 절에서 메시지 다이제스트를 설명할 때 이미 설명하였으므로 생략한다.

3.3.4 연결성(Linkage)



(범례) K^C_V : 고객 개인키 K^C_B : 고객 공개키
K^M_V : 상인 개인키 K^M_B : 상인 공개키
K^P_V : 금융기관 개인키 K^P_B : 금융기관 공개키

〈그림 8〉 이중 서명에 의한 연결성 확인

연결성은 이중서명(Dual Signature)에 의해 확보할 수 있다. SET에서 고객은 상인 이외의 사람에 대해 기밀성이 보장되는 주문정보와 금융기관 이외의 사람에 대해 기밀성이 보장되는 지불정보를 만든 후 각각에 이중서명을 붙여서 상인에게 보낸다. 이중서명은 주문정보의 해쉬값과 지불정보의 해쉬값을 합(Concatenate)한 것을 다시 해쉬한 결과값을 고객의 개인키로 암호화한 일종의 전자서명이다. 동시에, 지불정보의 해쉬값은 주문정보와 함께 암호화되고, 주문정보의 해쉬값은 지불정보와 함께 암호화된다. 따라서, 상인은 암호화된 주문정보를 복호화함으로써 주문정보를 얻어내어 해쉬값을 구한 후 동봉된 지불정보의 해쉬값과 합한 것을 다시 해쉬하여 이중서명의 내용과 비교해볼 수 있다. 이때, 두 해쉬값이 동일하다면 고객이 원래 암호화했던 지불정보가 훼손되지 않았으며, 따라서 그 지불정보는 자신이 받은 주문정보에 대한 지불정보임을 확인할 수 있게 되는 것이다. 금융기관도 같은 과정을 거쳐 이중서명을 확인할 수 있다. 이 과정을 도시하면 <그림 8>과 같다.

3.4 Refreshness

전자지불시스템에서 필요한 네 가지 보안기능을 이룩하기 위하여 3.3절에서 설명한 각 메시지들은 Refreshness 특성을 가져야 한다. 이것은 재생공격(Replay Attack)을 방지하기 위한 것이다. 재생공격이란 암호화된 메시지를 도청하여 (내용은 모른 채) 저장하였다가 일정 시간 후에 그 메시지를 다시 보내는 것이다. 이때 메시지를 받은 사람이 그 메시지가 재생된 것이라는 것을 알지 못하는 한 그 메시지는 암호화 상에 전혀 문제가 없는 메시지로서 정상 처리되게 된다.

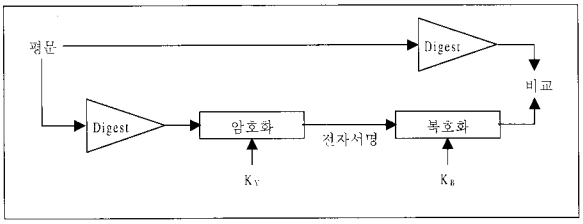
어떤 메시지를 받아야 할 사람은 재생공격을 방지하기 위해 메시지를 받기 전에 임의의 큰 정수(Challenge)를 생성한 후, 메시지를 보낼 사람에게 그 정수를 먼저 보내어, 그것을 포함한 메시지를 생성하여 보낼 것을 요구한다. 그러면, 같은 내용의 원문을 보내더라도 매번 보내는 암호 메시지는 달라지게 되며, 재생된 메시지는 사용할 수 없게 된다. 이때, 이 메시지는 Refreshness 특성을 가졌다고 한다.

3.5 전자서명 (Digital Signature)

전자서명은 인증과 무결성을 한꺼번에 해결해 준다. 전자서명이란 보내는 내용을 메시지 다이제스트 한 것을 보내는 사람의 개인키로 암호화한 것을 말한다. 전자서명은 메시지 다이제스트하기 전의 원래의 정보와 함께 전달되게 되는 데, 이 원래의 정보와 전자서명을 이용하여 인증과 무결성을 확인할 수 있다.

먼저 인증의 측면에서 설명하면, 전자서명을 받은 사람은, 보낸 사람의 공개키로 전자서명을 복호화 한 내용과 원문의 메시지 다이제스트를 비교함으로써 그것이 같다면, 그러한 전자서명을 만들 수 있는 사람은 보낸 사람뿐이라는 사실로부터 상대방을 확인할 수 있다.

둘째로, 무결성의 측면에서는 전자서명의 복호문과 원문의 메시지 다이제스트가 같다면 원문이 전달과정에서 바뀌지 않았음을 확인할 수 있다. 그리고, 혹시 중간에 다른 사람이 그 내용을 변조하려 한다 하더라도 보낸 사람의 공개키로 풀릴 수 있는 전자서명을 만들기 위해서는 보낸 사람의 개인키를 알아야 하는 데 이를 변조자가 알 수는 없으므로 문제가 없다. 전자서명을 확인하는 과정은 <그림 9>에 나타나 있다.



〈그림 9〉 전자서명에 의한 인증 및 무결성 확보

3.6 전자인증서 (Digital Certificate)

앞 절에서 전자서명의 기능을 설명할 때 인증, 무결성, 연결성 등을 확인하기 위해 중요한 역할을 한 것이 정보를 확인하는 데 쓰인 공개키였다. 전자서명을 받은 사람은 그것을 보낸 사람의 공개키로 복호화함으로써 그러한 내용들을 확인할 수 있었던 것이다. 그런데, 상호 확인이 원칙적으로 불가능한 가상공간 내에서 다른 사람의 공개키를 어떻게 알 수 있는가 하는 것이 문제가 된다.

이를 위하여 제시된 것이 인증기관(CA, Certificate Authority)이다. 인증기관은 한 사람의 공개키를 자신의 개인키로 암호화함으로써 그 사람의 공개키를 인증한다. 물론, 인증기관은 인증하기 전에 그 사람을 실제로 확인한 후 그 사람이 제시한 공개키를 인증하여야 한다. 인증기관의 개인키로 암호화한 공개키를 전자인증서(Digital Certificate)라고 부른다. 이 전자인증서를 받은 사람은 인증기관의 공개키로 전자인증서를 풀어서 나온 공개키를 상대방의 공개키라고 믿을 수 있다. 왜냐하면, 그러한 전자인증서를 만들 수 있는 사람은 그 개인키를 알고 있는 인증기관뿐이며, 인증기관은 믿을 수 있기 때문이다. 물론, 이 확인을 위한 전제조건은 그 인증기관의 공개키는 미리 널리 유포되어 모두가 알고 있어야 하며, 그 공개키는 누군가에 의해 조작되어 있지 않아야 한다. 그렇지 않

다면 전자인증서의 확인은 틀린 것이 되기 때문이다.

A라는 사람이 B라는 사람의 전자인증서를 받았는데 그 인증을 한 것은 C라는 인증기관이라고 하자. 이때, A가 C의 공개키를 미리 알고 있고, 또 C를 믿는다면 B의 공개키를 믿을 수 있다. 그러나, 만약 C가 A에게 처음 보는 인증기관이라면 어떻게 할 것인가? 일반적으로 오직 한 개의 인증기관이 전세계, 전 가상공간의 인증기관 역할을 할 수는 없을 것이다. 수 많은 자료를 저장, 관리해야 할 뿐만 아니라, 지구상의 다른 편에 있는 사람도 일일이 확인하여야만 하기 때문이다. 따라서, 한 CA는 특정지역의 사람들에 대해 인증을 하고, 이 CA 자체는 그보다 상위의 지역의 CA가 다시 인증을 하고, 또 그 CA는 더 상위의 CA가 인증을 하는 등의 CA 계층구조(CA Hierarchy)를 생각해 볼 수 있다.

CA 계층구조의 한 예로 SET에서는 각 계좌별로 전자인증서를 발행하고, 이 전자인증서 발행기관은 해당 국가의 신용카드 발급사가 되도록 하며, 그 상위에서는 국가가 인증기관이 되고, 다시 그 위에 카드상표사(VISA, Master Card)와 최상위 인증기관(Root CA)을 두는 CA 계층구조를 제시하고 있다.

Ⅳ. 전자상거래 지불 보안 체계

본 절에서는 현재 제안되었거나 사용 중인 전자상거래 지불 체계들을 소개한다. 이를 위하여 4.1 절에서 각종 전자상거래 관련 지불 체계들을 소개한 후, 4.2 절에서는 본 논문이 기본 지불 체계로 사용한 SET에 대하여 좀 더 상세한 설명을 하도록 한다.

4.1 전자상거래 지불 보안 체계와 사용 현황

현재까지 업계에서 제시(de facto standard)한 전자상거래 관련 지불 체계로는 SSL, SET, OBI, OFX, OTP 등을 들 수 있다.

SSL(Secure Socket Layer) (Freier 등, 1996)은 원래 웹 브라우저와 웹 서버 간에 전달되는 메시지의 보안을 위한 보안 체계로서, 원칙적으로 전자상거래 지불 보안 체계라고 부를 수는 없다. 다만, 전자쇼핑몰에서 쓰일 때 고객의 웹 브라우저와 상인의 웹 서버 간의 지불정보의 보안을 제공해 줄 수 있고, 특히 구현 및 사용이 용이하기 때문에 고객과 상인 간 지불 정보의 보안 목적으로 현존 대부분의 쇼핑몰들이 사용하고 있다. 그렇지만, 지불 정보가 상인에게 노출된다는 점과 고객이 정당한 카드소지자인지를 엄밀하게 확인할 수 없다는 점 등이 문제가 되고 있다.(http://home.netscape.com/eng/ssl3/index.html)

SET(Secure Electronic Transaction)은 SSL을 이용한 지불 체계의 문제점을 해결하고 좀 더 강력한 지불 정보 보안을 지원하기 위하여 제안된 것이다. 웹 서버와 웹 브라우저 간의 보안 체계만을 명시한 SSL과 달리, SET은 전자상거래 지불 관련 당사자(고객, 상인, 금융기관, 인증기관) 간의 지불 및 보안 관련 정보의 전달 순서 및 전달 내용 등 지불 체계 전반에 대하여 규정하고 있는 B-to-C 전자상거래 전용 지불 보안 체계이다. (http://www.setco.org/)

OBI(Open Buying on the Internet) (OBI Consortium, 1999)는 인터넷을 통한 저가, 대량의 일용품 구매에 관한 개방된 표준이다. 원래 American Express와 Supply Works가 처음 개발할 때는 인터넷을 통한 사무용 비품 구입에 이용하도록 설계되었으나, 현재는 일반적인 B-to-B환경에서 사용될 수 있는 인터넷 상거래용 표준 보안 체계로서 받아들여지고 있다.(http://www.openbuy.org/)

OFX(Open Financial Exchange) (CheckFree Corp. 등, 1998)는 온라인 금융서비스 서버와 클라이언트 소프트웨어 간에 교환되는 금융정보의 보안을 위한 보안 체계이다. 이 체계에서는 제 3자를 거치지 않고 금융기관과 고객이 직접 금융정보를 주고 받도록 한다. 따라서, 원칙적으로 이 체계는 전자계좌이체, 거래내역 조회 등 전자금융서비스를 지원하기 위한 것이지만, 계좌이체 결과가 상인에게 전달될 수 있는 통로가 추가되면 B-to-B 또는 B-to-C 환경에서 지불 보안 체계로 사용될 수도 있다. (http://www.ofx.net/)

OTP(Open Trading Protocol) (The Open Trading Proto-

col Consortium, 1998)는 기존의 또는 신규의 거래 모델(Trading Model)들을 지원하기 위한 기반 구조이다. 따라서, OTP는 특정한 지불체계가 아니라 기존의 또는 앞으로 새로 나올 지불체계를 포함한 인터넷 상거래의 전 과정(Trading Model)을 지원할 수 있는 환경을 제공하는 데 그 목적이 있다. 현재 OTP Specification Version 0.9.9가 IETF에 표준 제정을 위해 신청 중에 있다. (http://www.otp.org/)

지금까지 살펴본 바와 같이 B-to-C 전자쇼핑몰에서 현재 사용할 수 있는 지불 보안 체계는 SSL과 SET이다. 이미 지적한 바와 같이 SSL을 이용한 지불 보안 체계는 그것의 구현 용이성 및 사용자(고객)의 편리성 때문에 보안상의 문제점에도 불구하고 거의 대부분의 전자쇼핑몰들이 사용하고 있다. 그렇지만, 점차 인터넷 지불 정보 보안의 중요성이 강조됨에 따라 SET 또는 이에 필적할 만한 새로운 지불 정보 보안 체계의 도입이 절실한 실정이다. 1999년 12월 현재 국내에서 SET 기반 지불 체계를 실질적으로 운영하고 있는 전자쇼핑몰로는 본 논문의 연구결과를 적용한 메타랜드(http://www.metaland.com/)와 현대백화점(http://www.hyundaidept.com/) 등이 있는 것으로 알려져 있다.

4.2 SET (Secure Electronic Transaction)

SET은 신용카드 회사인 Visa와 Master Card가 전자상거래에서 신용카드를 이용한 지불처리를 안전하게 할 수 있도록 제안한 지불보안 규정이다. 이 규정은

〈표 1〉 SET 메시지의 종류

	메시지 이름	참여자	용도
1	PInitReq / PinitRes	C - M	구매/지불 요구 상호 초기화
2	PRes / PRes	C M	구매/지불 요구 처리
3	InqReq / InqRes	C M	구매/지불 처리 상황 문의
4	AuthReq / AuthRes	M PG	지불승인 처리
5	CapReq / CapRes	M PG	지불전표 처리
6	AuthRevReq / AuthRevRes	M PG	승인 취소 처리
7	CapRevReq / CapRevRes	M PG	전표 취소 처리
8	CredReq / CredRes	M PG	환불 처리
9	CredRevReq / CredRevRes	M PG	환불 취소 처리
10	PCertReq / PcertRes	M PG	인증서 처리
11	BatchAdminReq / BatchAdminRes	M PG	복수 메시지 처리
12	CardCInitReq / CardCInitRes	C CCA	인증서 발급 상호 초기화
13	RegFormReg / RegFormRes	C CCA	인증서 양식 받기
14	CertReq / CertRes	C CCA	인증서 발급 처리
15	CertInqRes / CertInqRes	C CCA	인증서 발급 상황 문의
16	Me-AqCInitReq / Me-AqCInitRes	M MCA	인증서 발급 상호 초기화
17	CertReq / CertRes	M MCA	인증서 발급 처리
18	CertInqReq / CertInqRes	M MCA	인증서 발급 상황 문의
19	Me-AqCInitReq / Me-AqCInitRes	PG PCA	인증서 발급 상호 초기화
20	CertReq / CertRes	PG PCA	인증서 발급 처리

(범례) C - 고객, M - 상인, PG - 금융기관,
CCA - 고객용 인증기관, MCA - 상인용 인증기관, PCA - 금융기관용 인증기관

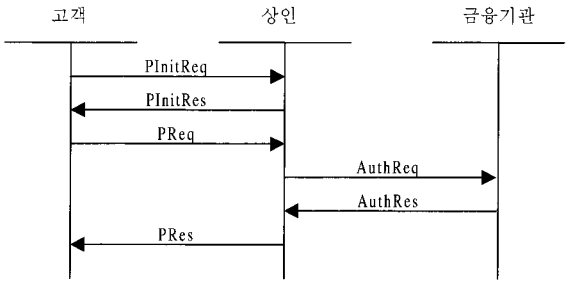
1997년 5월 31일에 버전 1.0이 발표되었으며, 전세계 신용카드 결제금액의 80% 정도를 위 두 회사가 처리하고 있다는 이유와 SET에 필적할 만한 다른 대안이 없다는 이유 때문에 개인 대 기업 간(Business-to-Consumer)의 전자상거래에서 사실상의 표준(*de facto standard*)으로 받아들여지고 있다.

보안 측면에서 SET이 목표로 하고 있는 것은 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 연결성(Linkage)이다. (Master Card and Visa, 1997) 이러한 보안 목표를 달성하기 위하여 SET에서는 고객, 상인, 금융기관 간에 어떤 내용의 메시지들이 어떻게 암호화 되어 어떤 순서로 전달되는지를 명시하고 있다. 암호화 방법으로는 현대 암호학에서 가장 보편적으로 사용하고 있는 전자봉투(Digital Envelope), 전자서명(Digital Signature)과 함께 연결성을 위하여 이중서명(Dual Signature)을 사용하고 있다. SET은 공개키 기반의 키 인증방법을 사용하고 있으므로 이를 지원하기 위하여 인증기관(Certificate Authority)의 계층구조와 루트 인증기관의 키 관리 및 인증기관과 고객, 상인 및 금융기관 간의 인증서 발급을 위한 메시지에 대해서도 규정하고 있다. SET의 자세한 내용에 대해서는 참고문헌 송용욱(1997), International Telecommunication Union(1994a, 1994b, 1994c, 1994d, 1994e, 1994f), Master Card and Visa(1998), RSA Data Security Inc.(1993) 등을 참조하기 바란다. SET이 정의한 메시지들의 목록은 <표 1>에 나타나 있다.

V. 메타-몰의 지불 체계

5.1 지불대표자를 통한 지불 정보 처리

4절에서 설명한 SET의 메시지들을 상인의 관점에서 살펴보면 SET은 1명의 상인과 다른 사람들 - 고객, 금융기관, 인증기관 - 간의 메시지만을 규정하고 있는 것을 알 수 있다. 지불 처리의 관점에서 이 부분을 좀 더 자세히 살펴보자. SET의 지불처리 과정은 <그림 10>에 나타나 있다. 지불처리 초기화를 위하여 PInitReq 메시지와 PInitRes 메시지를 고객과 상인이 주고 받은 후 본격적으로 주문정보와 지불정보가 들어있는 PReq 메시지가 고객으로부터 상인에게 전달된다. 상인은 이중에서 지불정보를 AuthReq에 넣어서 금융기관에 보내어 지불승인을 의뢰한다. 지불정보는 금융기관만 볼 수 있도록 기밀성이 보장되어 있기 때문에 상인은 보지 못하며, 다만 이중서명에 의하여 지불정보와 주문정보 간의 연결성만 확인할 수 있음은 3절에서 설명한 바 있다. 금융기관은 지불정보에 포함되어 있는 신용카드번호와 비밀번호 등을 바탕으로 신용조회를 수행한 후 그 결과를 AuthRes 메시지에 넣어 상인에게 통보한다. 상인은 AuthRes 메시지를 읽어서 지불승인이 나지 않았으면 그 결과를 PRes에 넣어 고객에게 통보한다. 만약, 지불승인이 났으면 주문내용을 배달용 데이터베이스 등에 등록함으로써 상품을 배달할 수 있도록 한 후 그 결과를 역시 PRes에 넣어 고객에게 통보한다.



〈그림 10〉 SET의 지불처리 순서

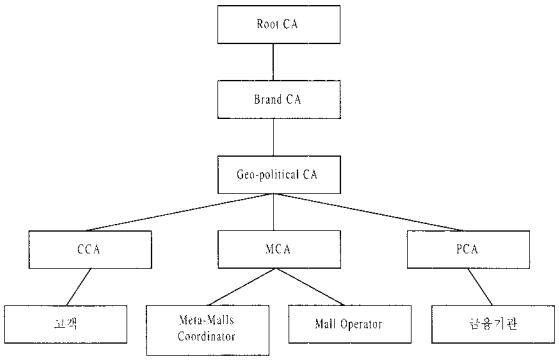
이상의 지불 메시지 처리과정을 살펴보면 SET 규정은 1인의 상인이 있는 경우만을 대상으로 하고 있음을 알 수 있다. 그러나, 전술한 바와 같이 메타-몰에는 여러 몰이 있고, 따라서 지불처리는 여러 상인과 이루어져야 한다. 원-스톱 지불처리를 수행하되 SET이 정한 규정을 그대로 활용할 수 있도록 하기 위해서 본 논문에서는 "지불대표자"의 개념을 사용한다. 즉, 여러 몰을 대표하는 지불대표자가 SET의 상인의 역할을 수행함으로써 SET이 정한 규정을 그대로 활용할 수 있도록 하고, 승인이 난 주문에 대해서

는 지불대표자가 각 몰별로 해당 주문정보를 나누어 주도록 한다. <그림 1>의 메타-몰의 구조를 살펴보면 Meta-Malls Coordinator가 지불대표자의 역할을 할 수 있음을 알 수 있다. 따라서, 메타-몰에서는 Meta-Malls Coordinator가 SET의 상인역할을 하면서 PInitReq, PInitRes, PReq, PRes, AuthReq, AuthRes 등의 메시지를 고객과 금융기관 사이에서 처리하고, AuthRes 메시지 처리 후 고객에게 PRes 메시지를 전달하기 전에 Mall-Operator들에게 주문정보를 전달하도록 하면 된다.

5.2 인증 및 무결성의 확보

Meta-Malls Coordinator와 Mall-Operator 사이에 전달되는 주문정보는 인증과 무결성을 갖도록 암호화되어야 한다. 기밀성은 본 방법론에서는 고려하지 않는다. 만약, 주문정보의 인증과 무결성이 확보되지 않는다면, 악의의 제 3자가 Meta-Malls Coordinator를 사칭하고서 주문정보를 Mall Operator에게 보내거나, 또는 Meta-Malls Coordinator에서 Mall Operator로 전달되는 메시지를 가로채어 배달지 정보 등을 바꾼 후 바뀐 메지지를 Mall Operator에게 보낼 수 있다. 이때, Mall Operator는 그 주문정보대로 상품을 배달하게 되고, 따라서, 그 제 3자는 경제적 이득을 취할 수 있게 된다. 주문정보의 인증과 무결성을 확보하기 위해서는 주문정보에 전자서명을 붙이면 된다.

전자서명을 사용하기 위해서는 두 가지 문제가 해결되어야 한다. 하나는 정보전달 상대방의 키 인증이고 다른 하나는 전자서명의 refreshness이다. 고객, 상인, 금융기관 간의 키 인증은 SET이 정한 인증기관 계층에 의해 해결되어 있다. 메타-몰의 새로운 지불체계에서 문제가 되는 것은 Meta-Malls Coordinator와 Mall-Operator 간의 키 인증이다. SET 규정을 최대한 활용하고 새로운 추가사항을 최소화하기 위하여 메타-몰 구조에서는 Meta-Malls Coordinator와 Mall-Operator 모두 상인용 인증기관으로부터 인증을 받도록 한다. <그림 11>에 메타-몰의 인증기관 계층구조가 나타나 있다. 이 그림은 Meta-Malls Coordinator와 Mall Operator 부분이 상인이었던 것을 제외하고는 SET이 정한 인증기관 계층구조와 동일하다.



〈그림 11〉 메타-몰의 인증기관 계층구조

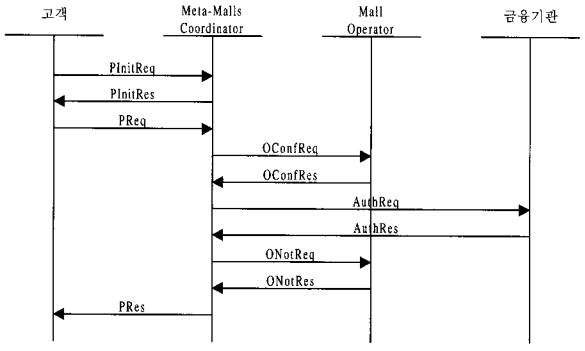
5.3 메시지 암호화 방법

3.4절에서 설명한 바와 같이 전자서명의 Refreshness란 전자서명이 되어 전달되는 메시지에 임의의 값을 갖는 바이트들을 추가하여 동일한 상품주문에 대해서도 전자서명이 달라지게 함으로써 악의의 제 3자가 과거의 전자서명을 녹음해 두었다가 다시 사용하는 재생 공격(Replay Attack)을 방지하기 위한 것이다. 이를 위해서는 Meta-Malls Coordinator와 Mall Operator 간에 Challenge - 임의의 값을 갖는 바이트들 - 를 주고받는 과정이 추가되어야 한다. 사실, SET에서 고객과 상인 간에 전달되는 PInitReq와 PInitRes 메시지의 역할 중의 하나가 바로 이것이다. Meta-Malls Coordinator와 Mall Operator 간에도 이를 위한 메시지를 추가하되 다른 용도로도 활용할 수 있기 위하여 메타-몰의 지불체계에서는 Meta-Malls Coordinator와 Mall Operator 간에 전달되는 두 번의 메시지를 다음과 같이 정의하였다.

OConfReq = S(M, { OI, Chall-S })
OConfRes = S(S, { Answer, OID, Chall-S, Chall-M })
ONotReq = S(M, { OID, Chall-M, Chall-S2 })
ONotRes = S(S, { Answer, OID, Chall-S2 })

S(P, C)는 P라는 사람이 C의 내용에 전자서명을

붙인 것을 말한다. 위 메시지에서 M은 Meta-Malls Coordinator를 나타내고 S는 Mall Operator를 나타낸다. OConfReq와 OConfRes 메시지는 주문확인(Order Confirmation)을 위한 메시지이고 ONotReq와 ONotRes는 주문통지(Order Notification)를 위한 메시지이다. 주문확인 메시지는 Mall Operator에게 고객이 주문한 상품을 판매할 수 있는가를 확인하기 위한 메시지이다. 상품의 재고부족이나 가격의 변동 등의 이유 때문에 Mall Operator가 상품을 판매할 수 없는 상황이 있을 수도 있기 때문이다. OConfReq메시지의 내용은 주문정보(OI)와 Challenge(Chall-S)이다. 주문정보는 주문확인을 위한 것이고, Chall-S는 Refreshness를 위한 것이다. OConfRes 메시지의 내용은 주문확인에 대한 대답(Answer)과, 대답이 '예'일 때 그 주문에 대해 Mall Operator가 부여한 주문번호(OID), Chall-S에 대한 응답, 그리고, 새로운 Challenge Chall-M이다. 주문통지 메시지는 Meta-Malls Coordinator가 Mall Operator에게 최종적으로 주문을 통지하여 상품의 배달 및 추후 정산을 결정짓는 메시지이다. ONotReq 메시지의 내용은 OConfRes에서 받았던 주문번호(OID), Chall-M에 대한 응답, 그리고, 새로운 Challenge Chall-S2이다. ONotRes 메시지의 내용은 주문통지를 받았다는 확인(Answer, OID)과 Chall-S2에 대한 응답이다.



〈그림 12〉 메타-몰의 주문 및 지불저보 처리 순서

위와 같이 두 번의 메시지를 정의한 이유의 하나는 Challenge를 주고 받기 위한 것이고, 다른 하나는 Mall Operator가 주문상품을 실제로 판매할 수 있는 지를 확인하는 과정을 덧붙이기 위한 것이다. 즉, 지불승인 이전에 주문확인을 함으로써 주문확인이 실패로 끝날 경우 - 예를 들어, 한 Mall Operator가 재고부족으로 판매할 수 없다고 할 경우 - 불필요하게 주문승인을 받는 과정을 제거할 수 있기 때문이다. 따라서, 메타-몰의 지불처리 순서는 <그림 12>와 같이 된다.

Ⅵ. 요 약

지금까지 메타-몰에서의 지불처리 보안 방안을 살펴보았다. 사실상의 표준인 SET이 1인의 상인만을 대상으로 하고 있으므로, 여러 하부 몰을 거느리고 원-스톱 지불을 지원하는 메타-몰에는 그대로 적용할 수 없었다. 따라서, 메타-몰에서는 지불대표자의 개념을 도입하여 Meta-Malls Coordinator가 SET에서의 상인 역할을 하면서 Mall Operator들에 대해 주문정보를 전달하도록 하였다. 고객, Meta-Malls Coordinator, 금융기관 간에는 SET 규정을 따름으로써, 메시지의 기밀성, 인증, 무결성, 연결성을 확보하였다. 그리고, Meta-Malls Coordinator와 Mall Operator 간의 주문정보에 대한 인증과 무결성을 위하여 주문정보에 전자서명을 하도록 하였으며, 전자서명의 Refreshness를 위하여 Challenge를 주고 받을 수 있도록 주문확인과 주문통지의 두 번의 메시지 전달단계를 정의하였다. 동시에, 주문확인 메시지는 재고확인 등의 판매 가능성 여부를 확인하는 절차를 겸하도록 하였다. 본 방법론은 SET을 메타-몰에 적용하는 방안으로서 구현되었으나, SET이외의 지불방법론에 대해서도 동일하게 적용될 수 있다. 현재 ㈜메타랜드(http://www.meta-land.com)가 실제 고객들을 대상으로 이러한 지불정보 보안체계를 갖는 메타-몰 구조의 전자쇼핑몰을 운영 중에 있다.

참 고 문 헌

송용욱, "전자상거래와 SET 프로토콜", *컴퓨터월드*,

1997.11, pp. 248-252.

Cain, Adam, "Web Security: Technologies for Security, Authentication, and Privacy on the World-Wide Web", *5th International World Wide Web Conference Tutorial Notes*, pp. 1-31, May 1996.

CheckFree Corp., Intuit Inc., and Microsoft Corp., *Open Financial Exchange, Specification 1.5*, June 29, 1998.

Freier A. O., P. Karlton, and P. C. Kocher, *The SSL Protocol, Version 3.0*, Nov. 18, 1996.

International Telecommunication Union, *Abstract Syntax Notation One (ASN.1): Constraint Specification, ITU-T Recommendation X.682*, July 1994a.

International Telecommunication Union, *Abstract Syntax Notation One (ASN.1): Information Object Specification, ITU-T Recommendation X.681*, July 1994b.

International Telecommunication Union, *Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications, ITU-T Recommendation X.683*, July 1994c.

International Telecommunication Union, *Abstract Syntax Notation One (ASN.1): Specification of Basic Notation, ITU-T Recommendation X.680*, July 1994d.

International Telecommunication Union, *ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), ITU-T Recommendation X.690*, July 1994e.

International Telecommunication Union, *Authentication Framework, ITU-T Recommendation X.509*, November 1993f.

Keller, A. M., "Smart Catalogs and Virtual Catalogs", Kalakota R., and A. B. Whinston (eds.), *Readings in Electronic Commerce*, Addison-wesley, 1997, pp. 259-271.

Lee, J. K., Y. U. Song, and J. W. Lee, "A Comparison Shopping Architecture over Multiple Malls: The Meta-Malls Architecture", *Proceedings of International Conference on Electronic Commerce '98*, April 1998.

Master Card and Visa, *Secure Electronic Transaction Specification Version 1.0*, May 1997.

OBI Consortium, *Open Buying on the Internet (OBI)TM Technical Specifications, Release V2.0*, 1999.

RSA Data Security Inc., *PKCS #7: Cryptographic Message Syntax Standard, Version 1.5*, 1993.

Schneier, Bruce, *Applied Cryptography, 2nd Edition*, John Wiley & Sons Inc., 1996.

The Open Trading Protocol Consortium, *Internet Open Trading Protocol, Version 0.9*, Draft for Public Comment, 12 Jan. 1998.

메타랜드 URL → http://www.metaland.com

현대백화점 URL → http://www.hyundaidept.com/

OBI URL → http://www.openbuy.org/

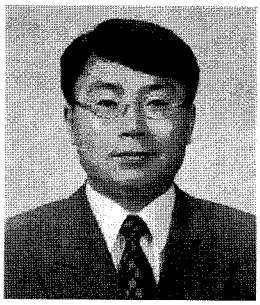
OFX URL → http://www.ofx.net/

OTP URL → http://www.otp.org/

SET URL → http://www.setco.org/

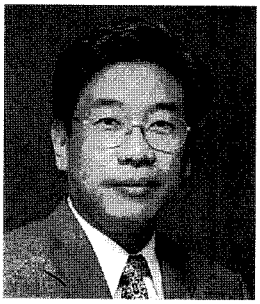
SSL URL → http://home.netscape.com/eng/ssl3/index.html

◐ 저 자 소 개 ◑



송 용 욱 (yusong@nongae.gsnu.ac.kr)

송용욱은 한국과학기술원에서 1990년도와 1995년도에 각각 석사 및 박사학위를 취득하였으며, 현재 국립경상대학교 경영학부 교수로 재직하고 있다. 그의 연구분야는 전자상거래, 전자결제 및 보안, 전문가시스템 및 수리계획법과 전자상거래의 통합 등이다. 그의 연구논문들은 Management Science, Annals of Operations Research 등에 게재되었다. 그는 "UNIK을 이용한 전문가시스템의 개발"이라는 전문가시스템 책을 공동 저술하였으며, 전문가시스템 개발도구인 UNIK의 핵심부분을 개발하였다. 또한 1998년까지 (사)국제전자상거래연구센터의 책임연구원으로 있으면서 메타랜드 전자쇼핑몰과 SET 기반 전자지불 시스템을 개발한 바 있다.



이 재 규 (jklee@msd.kaist.ac.kr)

서울대 산업공학과 학사, 한국과학기술원 산업공학과 석사, The Wharton School, University of Pennsylvania 박사를 취득하였다. 현재 한국과학기술원 테크노경영대학원 교수 및 (사) 국제전자상거래연구센타 소장으로 재직중이며, 한국지능정보시스템학회, 학회장, The 3rd World Congress on Expert Systems(1996년) 학술대회장 International Conference on Electronic Commerce('98, 2000 학술대회장 역임), Decision Support Systems, International Journal of Electronic Commerce, Expert Systems with Application 등 다수의 국제학술지 편집위원, 최근 Electronic Commerce: Managerial Perspective (Prentice Hall 2000) 및 전자상거래 원론(법영사, 1999) 출간, 주요 연구 분야는 전자상거래와 지능정보시스템이다.