대한산업공학회/한국경영과학회 '98 춘계공동학술대회 논문집.1998 년 4 월 24-25 일. 경성대학교:Session B 15.2

메타-몰 구조를 갖는 전자쇼핑몰에서의 안전한 지불체계에 대한 연구
A Secure Payment Method for Meta-Malls Architecture

이재규*, 송용욱**
* 한국과학기술원 테크노경영대학원
** 국제전자상거래연구센터

Abstract

As electronic commerce brisks up, enormous number of and various types of internet shopping malls are open and prosperous. The Meta-Malls architecture was introduced to take the advantage of economy of scale and to allure consumers with plenty of commodities. Security of order information and payment instruction is also a buzzword in shopping malls based on the Meta-Malls architecture as in other kind of shopping malls. The security problem is, however, much more complicated in the Meta-Malls architecture due to the characteristics of the architecture. This paper suggests a security architecture which ensures the secure transmission of order information and payment instruction among customers, merchants, and financial institutes by introducing the concept of payment representative. The objectives of the security architecture are confidentiality, authentication, integrity, and linkage. To achieve the objectives, the architecture defines several additional encrypted messages between the payment representative and the shopping malls in the meta-mall based on SET (Secure Electronic Transaction), which is a *de facto* standard in the field of electronic commerce. This architecture was implemented for a Korean shopping mall which is running business.

1. 서론

전자상거래가 활성화되면서 다양한 형태의 전자쇼핑몰들이 등장하고 있다. 현재 인터넷 상에는 25 만개 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)[11]이다. 메타-몰은 하부의 독립적인 몰들을 통합하여 하나의 몰처럼 행동함으로써 고객에게 다양한 상품정보와 편리한 사용환경을 제공한다.

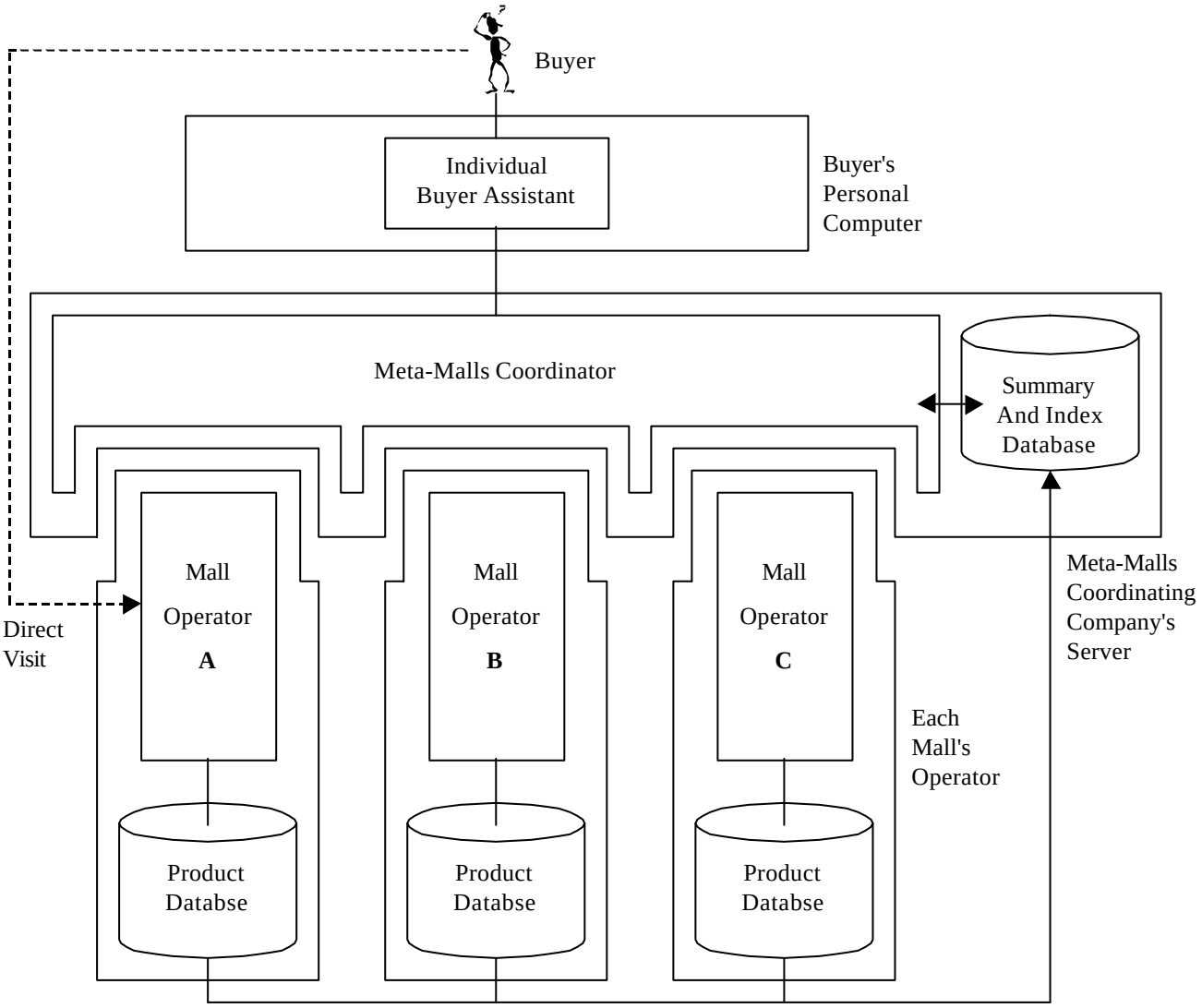
지불정보의 보안은 모든 전자쇼핑몰들이 시스템의 안전을 위해 심혈을 기울이는 분야이면서, 그 자체가 전자쇼핑몰의 중요한 선전요소 중의 하나이기도 하다. 현재 대부분의 전자쇼핑몰들이 사용하고 있는 보안 방법인 SSL(Secure Socket Layer)[2]의 결점이 알려지면서 그 대안으로 주목받고 있는 것이 SET(Secure Electronic Transaction)[12]이다. 필적할 만한 다른 대안이 없는 상태에서 그 제안자가 신용카드 업계의 양대 산맥인 Visa 와 Master Card 라는 이유 때문에 SET 은 현재 사실상의 표준(*de facto* standard)으로 자리잡고 있다.

그런데, SET 지불 보안 규정은 하나의 상인이 있는 전형적인 전자쇼핑몰을 대상으로 하고 있

기 때문에 메타-몰 구조처럼 여러 상인이 있고, 따라서, 여러 상인으로부터 구매한 상품들을 한꺼번에 지불 처리해 주는 경우는 지원하지 않고 있다. 본 논문에서는 사실상의 표준인 SET 를 수용하면서, 메타-몰에서 여러 상인의 상품을 구매하는 경우도 지원할 수 있는 지불방안을 제시하고자 한다. 이를 설명하기 위하여 2 절과 3 절에서는 메타-몰 구조와 SET 를 소개한 후 4 절에서 메타-몰의 지불 체계를 상술하고 5 절에서 요약하도록 하겠다.

2. 메타-몰 구조

메타-몰 구조는 [그림 1]에 나타나 있다. [그림 1]에서 Mall Operator 들은 독자적인 기능을 갖는 전자쇼핑몰 시스템이고, Meta-Malls Coordinator 는 이들 하부 몰들을 통합하여 하나의 몰처럼 행동하는 메타-몰 시스템이다. 메타-몰은 하부의 여러 몰들을 통합함으로써 여러 몰의 상품들을 마치



[그림 1] 메타-몰의 구조

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.

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, 지불처리 과정에서 고객의 지불정보 - 신용카드 번호, 계좌번호, 비밀번호 등 - 가 제 3 자에게 알려져서도 안되며, 특히, 상인에게도 알려져서는 안된다. 이러한 안전한 지불처리를 위한 보안 규정이 SET 이다. 그러나, 전술한 바와 같이 SET 규정은 하나의 상인이 있는 경우만을 대상으로 하고 있으므로, 메타-몰에서처럼 여러 하부 몰에서 상품을 구매하여 원-스톱으로 지불처리를 하고자 하는 경우는 지원하지 못한다.

3. SET (Secure Electronic Transaction)

SET 은 신용카드 회사인 Visa 와 Master Card 가 전자상거래에서 신용카드를 이용한 지불처리를 안전하게 할 수 있도록 제안한 지불보안 규정이다. 이 규정은 1997 년 5 월 31 일에 버전 1.0 이 발표되었으며, 전세계 신용카드 결제금액의 80% 정도를 위 두 회사가 처리하고 있다는 이유와 SET 에 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 SET 이 목표로 하고 있는 것은 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 연결성(Linkage)이다[3]. 기밀성은 네트웍을 통해 전달되는 주문정보, 지불정보 등의 메시지를 제 3 자가 중간에서 보지 못하도록 하는 것이다. 특히, 지불정보의 경우는 상인도 보지 못하게 한 것이 특징이다. 인증은 메시지를 보내온 상대편을 확인할 수 있도록 하는 것이다. 무결성은 전달되어온 메시지가 중간에 변형되지 않았음을 확인할 수 있도록 하는 것이다. 연결성은 서로 다른 두 메시지 간의 관련성을 확인할 수 있도록 하는 것이다. 상인은 고객으로부터 주문내용을 명시한 주문정보와 지불처리를 위한 지불정보를 받아서, 이중 주문정보는 배달 및 결제를 위해 사용하고, 자신이 보지 못하도록 암호화되어있는 지불정보는 금융기관에 보내어 결제에 사용한다. 이때, 상인으로 하여금 주문정보와 함께 전달되어 온 지불정보가 주문정보에 있는 주문을 결제처리하기 위한 것이라는 것을 확인시켜주는 것이 연결성이다.

이러한 보안 목표를 달성하기 위하여 SET 에서는 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. SET 은 공개키 기반의 키 인증방

법을 사용하고 있으므로 이를 지원하기 위하여 인증기관(Certificate Authority)의 계층구조와 루트 인증기관의 키 관리 및 인증기관과 고객, 상인 및 금융기관 간의 메시지에 대해서도 규정하고 있다. 암호화의 개념과 내용에 대해서는 참고문헌 [3]를 참조하기 바라며, SET 의 자세한 내용에 대해서는 참고문헌 [1], [5], [6], [7], [8], [9], [10], [12], [13] 등을 참조하기 바란다. SET 이 정의한 메시지들의 목록은 <표 1>에 나타나 있다.

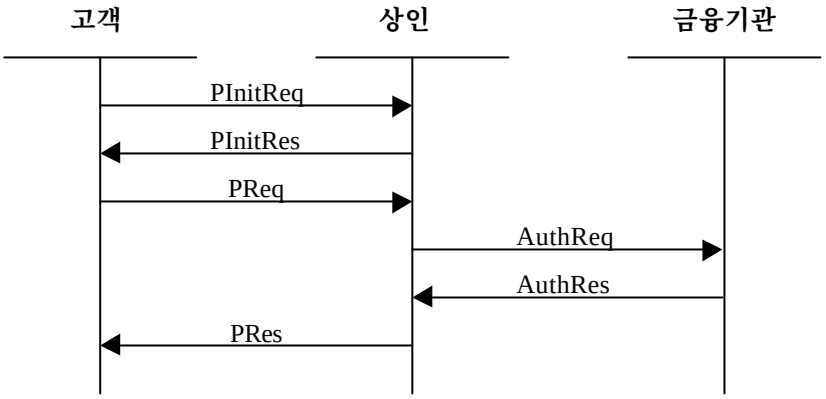
<표 1> SET 메시지의 종류

	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
21	CertInqReq / CertInqRes	PG – PCA	인증서 발급 상황 문의

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

4. 메타-몰의 지불 체계

3 절에서 설명한 SET 의 메시지들을 상인의 관점에서 살펴보면 SET 은 1 명의 상인과 다른 사람들 - 고객, 금융기관, 인증기관 - 간의 메시지만을 규정하고 있는 것을 알 수 있다. 지불 처리의 관점에서 이 부분을 좀 더 자세히 살펴보자. SET 의 지불처리 과정은 [그림 2]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 AuthReq 에 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 3 절에서 설명한 바와 같다. 금융기관



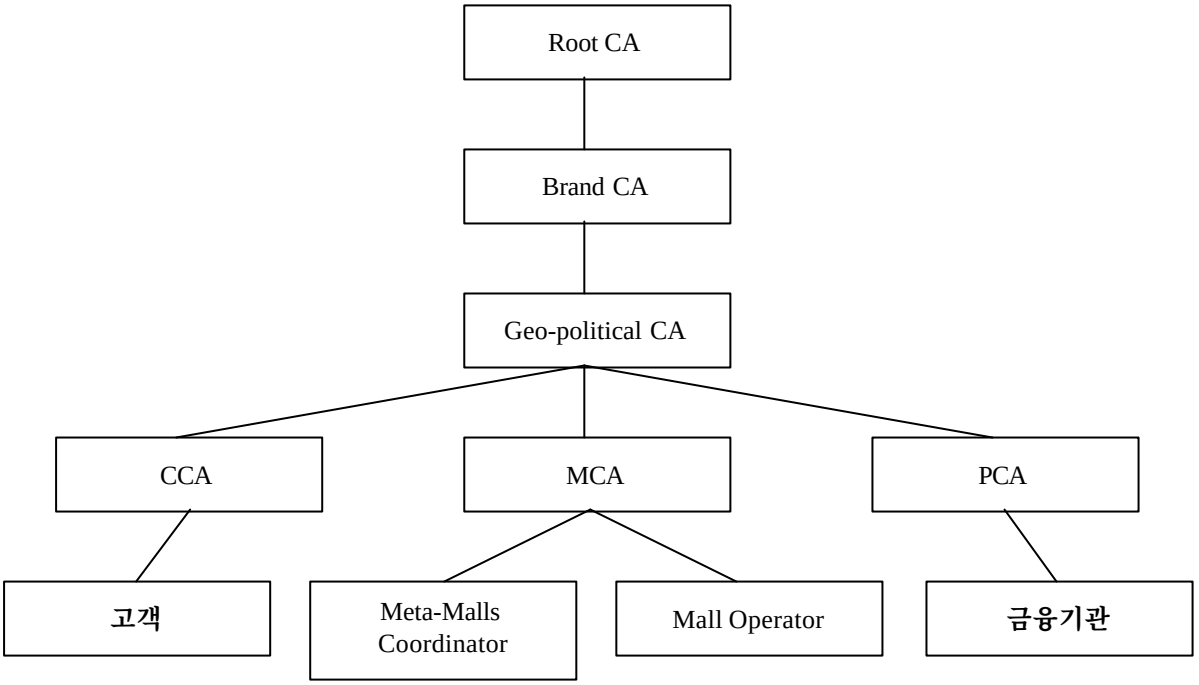
[그림 2] SET 의 지불처리 순서

은 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 PRes 에 넣어 고객에게 통보한다. 만약, 지불승인이 났으면 주문내용을 배달용 데이터베이스 등에 등록함으로써 상품을 배달할 수 있도록 한 후 그 결과를 역시 PRes 에 넣어 고객에게 통보한다.

이상의 지불 메시지 처리과정을 살펴보면 SET 규정은 1 인의 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 SET 이 정한 규정을 그대로 활용할 수 있도록 하기 위해서 본 논문에서는 "지불대표자"의 개념을 제시한다. 즉, 여러 몰을 대표하는 지불대표자가 SET 의 상인의 역할을 수행함으로써 SET 이 정한 규정을 그대로 활용할 수 있도록 하고, 승인이 난 주문에 대해서는 지불대표자가 각 몰별로 해당 주문정보를 나누어 주도록 한다는 것이다. [그림 1]의 메타-몰의 구조를 살펴보면 Meta-Malls Coordinator 가 지불대표자의 역할을 할 수 있음을 알 수 있다. 따라서, 메타-몰에서는 Meta-Malls Coordinator 가 SET 의 상인역할을 하면서 PInitReq, PInitRes, PReq, PRes, AuthReq, AuthRes 등의 메시지를 고객과 금융기관 사이에서 처리하고, AuthRes 메시지 처리 후 고객에게 PRes 메시지를 전달하기 전에 Mall-Operator 들에게 주문정보를 전달하도록 하면 된다.

그런데, Meta-Malls Coordinator 와 Mall-Operator 사이에 전달되는 주문정보는 인증과 무결성을 갖도록 암호화되어야 한다. 만약, 주문정보의 인증과 무결성이 확보되지 않는다면, 악의의 제 3 자가 Meta-Malls Coordinator 를 사칭하고서 주문정보를 Mall Operator 에게 보내거나, 또는 Meta-Malls Coordinator 에서 Mall Operator 로 전달되는 메시지를 가로채어 배달지 정보 등을 바꾼 후 바뀐 메지지를 Mall Operator 에게 보낼 수 있다. 이때, Mall Operator 는 그 주문정보대로 상품을 배달하게 되고, 따라서, 그 제 3 자는 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 refreshness 이다. 고객, 상인, 금융기관 간의 키 인증은 SET 이 정한 인증기관 계층에 의해 해결되어 있다. 메타-몰의 새로운 지불체계에서 문제가 되는 것은 Meta-Malls Coordinator 와 Mall-Operator 간의 키 인증이다. SET 규정을 최대한 활용하고 새로운 추



[그림 3] 메타-몰의 인증기관 계층구조

가사항을 최소화하기 위하여 메타-몰 구조에서는 Meta-Malls Coordinator 와 Mall-Operator 모두 상인용 인증기관으로부터 인증을 받도록 한다. [그림 3]에 메타-몰의 인증기관 계층구조가 나타나 있다. 이 그림은 Meta-Malls Coordinator 와 Mall Operator 부분이 상인이었던 것을 제외하고는 SET 이 정한 인증기관 계층구조와 동일하다.

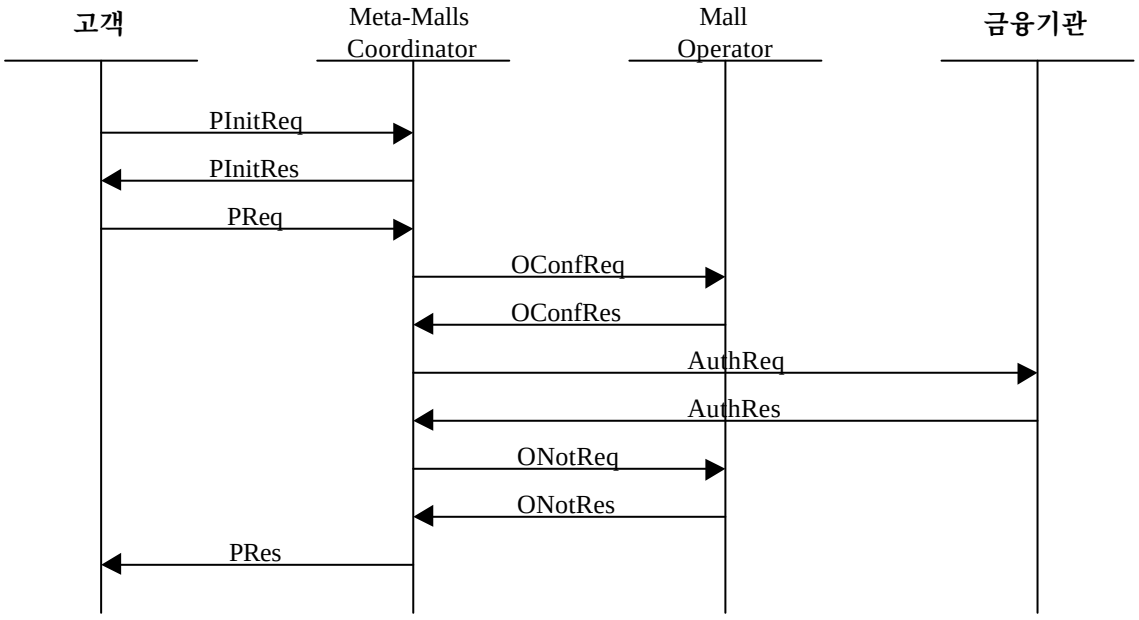
전자서명의 refreshness 란 전자서명이 되어 전달되는 메시지에 임의의 값을 갖는 바이트들을 추가하여 동일한 상품주문에 대해서도 전자서명이 달라지게 함으로써 악의의 제 3 자가 과거의 전자서명을 녹음해 두었다가 다시 사용하는 재생 공격(Replay Attack)을 방지하기 위한 것이다. 이를 위해서는 Meta-Malls Coordinator 와 Mall Operator 간에 Challenge - 임의의 값을 갖는 바이트들 - 를 주고받는 과정이 추가되어야 한다. 사실, 고객과 상인 간에 전달되는 PInitReq 와 PInitRes 메시지의 역할 중의 하나가 바로 이것이다. Meta-Malls Coordinator 와 Mall Operator 간에도 이를 위한 메시지를 추가하되 다른 용도로도 활용할 수 있기 위하여 메타-몰의 지불체계에서는 Meta-Malls Coordinator 와 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 P 라는 사람이 C 의 내용에 전자서명을 붙인 것을 말한다. 위 메시지에서 M 은 Meta-Malls Coordinator 를 나타내고 S 는 Mall Operator 를 나타낸다. OConfReq 와 OConfRes 메시지는

주문확인(Order Confirmation)을 위한 메시지이고 ONotReq 와 ONotRes 는 주문통지(Order Notification)를 위한 메시지이다. 주문확인 메시지는 Mall Operator 에게 고객이 주문한 상품을 판매할 수 있는가를 확인하기 위한 메시지이다. 상품의 재고부족이나 가격의 변동 등의 이유 때문에 Mall Operator 가 상품을 판매할 수 없는 상황이 있을 수도 있기 때문이다. OConfReq 메시지의 내용은 주문정보(OI)와 Challenge(Chall-S)이다. 주문정보는 주문확인을 위한 것이고, Chall-S 는 Refreshness 를 위한 것이다. OConfRes 메시지의 내용은 주문확인에 대한 대답(Answer)과, 대답이 '예'일 때 그 주문에 대해 Mall Operator 가 부여한 주문번호(OID), Chall-S 에 대한 응답, 그리고, 새로운 Challenge Chall-M 이다. 주문통지 메시지는 Meta-Malls Coordinator 가 Mall Operator 에게 최종적으로 주문을 통지하여 상품의 배달 및 추후 정산을 결정짓는 메시지이다. ONotReq 메시지의 내용은 OConfRes 에서 받았던 주문번호(OID), Chall-M 에 대한 응답, 그리고, 새로운 Challenge Chall-S2 이다. ONotRes 메시지의 내용은 주문통지를 받았다는 확인(Answer, OID)과 Chall-S2 에 대한 응답이다.

위와 같이 두 번의 메시지를 정의한 이유의 하나는 Challenge 를 주고 받기 위한 것이고, 다른 하나는 Mall Operator 가 주문상품을 실제로 판매할 수 있는 지를 확인하는 과정을 덧붙이기 위한 것이다. 즉, 지불승인 이전에 주문확인을 함으로써 주문확인이 실패로 끝날 경우 - 예를 들어, 한 Mall Operator 가 재고부족으로 판매할 수 없다고 할 경우 - 불필요하게 주문승인을 받는 과정을 제거할 수 있기 때문이다. 따라서, 메타-몰의 지불처리 순서는 [그림 4]와 같이 된다.



[그림 4] 메타-몰의 주문 및 지불정보 처리 순서

5. 요약

지금까지 메타-몰에서의 지불처리 보안 방안을 살펴보았다. 사실상의 표준인 SET 이 1 인의 상

인만을 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. 현재 ㈜메타랜드가 실제 고객들을 대상으로 이러한 지불정보 보안체계를 갖는 메타-몰 구조의 전자쇼핑몰을 운영 중에 있다.[4]

참고문헌

[1] 송용욱, "전자상거래와 SET 프로토콜",「컴퓨터월드」, 1997.11, pp. 248-252.

[2] Adam Cain, "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.

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

[4] http://www.metaland.com

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

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

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

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

[9] 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 1994.

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

[11] Jae Kyu Lee, Yong Uk Song, and Jae Won Lee, "A Comparison Shopping Architecture over Multiple Malls: The Meta-Malls Architecture", *Proceedings of International Conference on Electronic Commerce '98*, April 1998.

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

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