# E-Mail기반의 인터넷 EDI를 위한 수신부인방지 프로토콜

김준범*, 권혁인**, 김영찬*
* 중앙대학교 컴퓨터공학과
** 중앙대학교 경영학과

# The Protocol of receiver non-repudiation for E-mail based Internet EDI

Jun-Bum Kim*, Hyuk-in Kwon**, Young-Chan Kim*
* Dept. of Computer Science and Engineering, Chung-Ang Univ
** Dept. of Business Adminstration, Chung-Ang Univ

## 요 약

인터넷 EDI 시스템은 TCP/IP 프로토콜을 사용하여 문서를 전송하게 되는데 전송 도중 패킷 스니핑에 의하여 문서정보가 노출될 수 있다. 이러한 정보노출을 방지할 수 있는 대표적인 보안 기법에는 인터넷 EDI 보안 프로토콜로 권고되고 있는 S/MIME과 전자우편 암호화 프로그램인 PGP가 있다. S/MIME은 내부에서 사용되는 암호알고리즘의 사용제약으로 인하여 완벽한 구현이 어려우며 PGP의 경우 보안측면에 있어서 수신부인 방지 기능을 제공하지 못하고 있다. 본 논문에서는 S/MIME과 PGP에서 사용되고 있는 보안 기법을 분석하여 기밀성, 인증, 무결성, 송수신 부인방지 기능을 가지는 시스템을 제시한다. 본 시스템은 기존 암호화 알고리즘들의 문제점을 보완할 수 있는 혼합모델을 사용하여 기밀성과 무결성, 송신부인방지 기능을 구현하였고, 인증서버인 삼성 PKI 서버와의 인터페이스를 개발하여 인증을 획득하였다. 수신부인방지의 경우 암호화 메카니즘만으로 획득될 수 없기 때문에 수신자가 문서를 읽는 순간 송신자 측으로 수신자의 전자서명을 자동으로 전송해 주는 프로토콜을 통하여 구현하였다.

## 1 서론

인터넷 EDI(Internet EDI : IEDI)란 EDI 문서를 기존 VAN 망에서 전송하는 것이 아니라 인터넷망을 사용하여 EDI 문서를 전송하려는 개념이다[1]. IEDI 시스템에서는 EDI 문서를 SMTP/MIME 기반의 전자메일을 사용하여 인터넷망에 전송하게 되는데 전송 도중 제삼자가 패킷을 획득한 뒤 정보를 획득하여(Sniffing) 내용을 판독 및 변조한 뒤 재 전송 한다해도 수신측에서는 그 사실을 전혀 알 수가 없다. 이러한 정보 노출은 개방형 특성을 가지는 인터넷을 통하여 문서를 전송하기 때문에 발생하게 되는데, 정보를 암호화하여 송수신하는 보안 기법을 사용하여 방지할 수 있다. IEDI 시스템의 보안을 위하여 제시되고 있는 S/MIME은 공개키 암호화 방식의 사용제약과 구현상의 복잡성으로 인하여 구현이 어렵다. IEDI 시스템은 TCP/IP 프로토콜을 사용한 메일 기반의 문서 전송 시스템이기 때문에 문서 보안 측면에서 대표적인 메일 보안 프로그램인 PGP의 보안 기법과 비교될 수 있다. 그러나 PGP 프로그램은 수신 부인 방지를 해결하지 못하고 있으며, 인증을 해결하기 위한 기법으로 공개키 링 구조를 사용하는데 이는 확장성에 있어서 문제점을 가진다. 일반적으로 문서노출을 방지할 수 있는 보안체계가 갖추어야할 기능은 크게 네 가지로 구분된다. 첫째, 기밀성(Confidentiality)으로써 전달 내용을 제 3자가 알아내지 못하도록 하는 기능이다. 둘째, 인증(Authentication)으로써 각 거래자의 신원을 실제로 확인 및 보장해 주는 기능이다. 셋째, 무결성(Integrity)으로써 정보전달 과정에 있어서 정보의 수정 여부를 확인해 주는 기능이다. 넷째, 부인방지(Non-Repudiation)로써 문서의 송·수신 사실에 대하여 부인하는 것을 방지해 주는 기능이다[2].

본 논문은 인증 기능을 획득하기 위하여 사용자 인증을 대행해주는 인증기관(Certificate Authority : CA)과의 연결 인터페이스를 구현한다. 또한 수신부인 방지를 해결하기 위하여 수신측에서 문서 수신 후에 송신측으로 수신자의 전자서명을 자동 전송해 주는 수신 부인 방지 프로토콜을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 IEDI 시스템의 보안 솔루션으로써 제시되고 있는 S/MIME과 대표적인 메일 보안 프로그램인 PGP에 대한 요소 기술을 파악하고 3장에서는 본 시스템에서 문서 전송을 위하여 구현한 암호화, 복호화 과정에 대하여 기술한다. 4장에는 본 논문이 제안하고 있는 수신자 부인 방지를 위한 수신부인 방지 프로토콜에 대하여 기술하고 마지막으로 5장은 결론으로써 본 논문의 연구 성과와 향후 연구에 대해서 기술한다.

## 2 기반연구

IEDI 시스템을 위한 보안은 S/MIME을 사용하여 구현하도록 권고되고 있다. 가장 최근에 S/MIME 3.0이 제시되었고 몇 가지 새로운 보안 요소가 추가되었다. 그러나 S/MIME을 구현하는데 필요한 공개키 암호 라이브러리의 사용제약과 구현상의 복잡성으로 인하여 S/MIME의 전기능을 구현하기 어렵다. SMTP/MIME 기반의 IEDI 시스템의 보안을 위한 또 다른 구현 방향으로써 고려될 수 있는 것이 대표적인 전자 우편 보안 프로그램인 PGP 보안 전략이다. PGP 는 현재 6.0 버전까지 개발되어 있으며 미국 암호기술의 제한에 적용되지 않는다는 장점으로 인하여 널리 사용되고 있다.

### 2.1 S/MIME

S/MIME(Secure Multipurpose Internet Mail Extensions)은 인터넷 MIME메시지에 전자서명과 암호화기능을 첨부한 프로토콜이다[3]. S/MIME 내에서 실제 문서를 암호화 해주는 대칭형 알고리즘은 DES-CBC, Triple-DES-CBC, RC2가 사용되며 대칭형 암호화 키를 암호

화하는데 사용되는 비대칭형 암호화 알고리즘에는 RSA가 있다. 인증을 위한 구현은 계층적 인증구조를 가진 베리사인사의 인증기관을 사용하며 인증서는 X.509 형식의 전자인증서를 이용한다. 메시지 다이제스트를 생성하기 위한 알고리즘은 MD5, SHA-1이 있다.

S/MIME의 장점은 PGP에 비해서 확장성과 유연성이 우수하다는 점이다. 다시 말해 작은 그룹 내에서 신뢰 구조를 쉽게 구축할 수 있을 뿐만 아니라 큰 그룹 구성 시에도 쉽게 확장할 수 있고 많은 전자우편 응용프로그램과의 접목이 용이하다. S/MIME의 암호학적 약점은 해커가 암호화된 메시지의 서명과 암호화된 메시지를 구분할 수 있으며, 또한 누가 서명했는지를 알 수가 있다는 점이다[3].

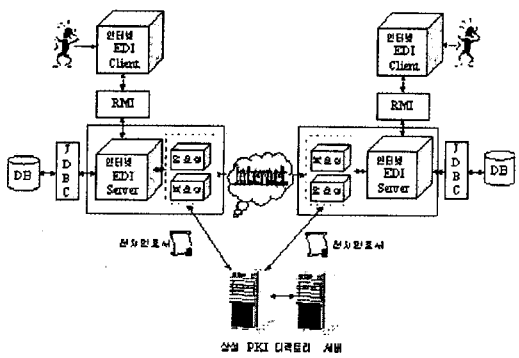
### 2.2 PGP

PGP(Pretty Good Privacy)는 표준화 기관이나 정부단체에서 개발한 것이 아닌 Phil Zimmermann이 만들어낸 전자우편 암호화에 대한 디팩토(de-facto) 표준이다[4]. PGP에서 데이터를 암호화하기 위한 대칭형 알고리즘으로는 128 비트 IDEA를 사용하며, 대칭형 암호화 키를 암호화하는데 사용되는 비대칭형 암호화 알고리즘은 RSA를 사용한다. PGP는 사용자 인증을 위해 공개키 링(Public Key Ring)구조를 사용한다. 공개키 링 구조란 자신과 다른 사람들의 공개키를 링 구조로 연결해 놓은 구조이다. 이것은 사용자들간의 신뢰도를 계산하여 그 공개키의 진위를 결정하는데 사용된다.

PGP의 장점은 단일 애플리케이션상에서 패키지화되어 암호화, 전자서명, 검증 그리고 키 관리를 수행한다는 점이다. PGP는 사용자들이 서로 키 교환을 통해서 인증을 확립하는 구조(Web of trust)를 가진다. 이 구조는 비공식적이며 따라서 작은 그룹에 적용이 용이하다. PGP의 단점은 MIME과의 통합성이 결여되어 있고, 키 관리에 있어서 시간이 많이 소모되며 상당량의 수작업을 필요로 한다는 점이다. 또한 다수 사용자 그룹에 적용하기에는 그 관리가 어렵다는 단점이 있다[4].

## 3 IEDI 시스템을 위한 보안 기법 설계 및 구현

본 논문에서 제안하고 있는 보안 기법을 적용한 SMTP/MIME 기반 IEDI 시스템의 전체적인 구조도는 다음 [그림 1]과 같다.



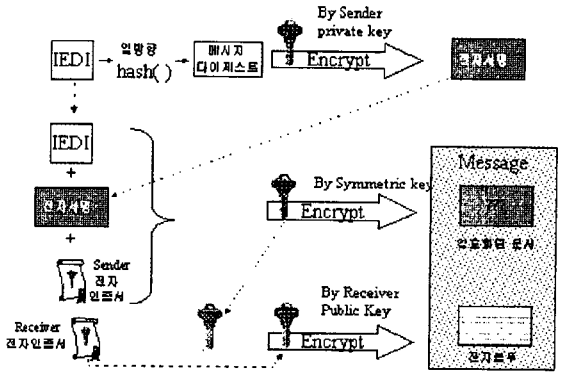

[그림 1] IEDI 시스템 구조

IEDI 문서를 주고 받고자 하는 사용자들은 IEDI 클라이언트를 이용하여 문서를 작성한 뒤 IEDI 서버를 이용하여 송수신 한다. IEDI 클라이언트와 IEDI 서버간에는 RMI를 사용하여 메시지를 주고 받는다. 송신자가 IEDI 클라이언트를 이용하여 IEDI 문서를 작성하면 이 문서는 RMI를 통해 IEDI 서버로 전달되고 IEDI 서버는 필요한 작업을 수행한 뒤 구성된 문서를 JDBC를 사용하여 데이터베이스에 저장한다. 저장된 IEDI 문서는 전송되기 전에 문서의 보안을 위해서 암호화된다. 암호화를 위해서 PKI 인증기관을 이용하여 인증을 받은 뒤 암호화 알고리즘들을 사용하여 암호화된다. 암호화된 IEDI 문서는 SMTP/MIME 전자 메일 프로토콜을 이용하여 수신자에게 전송된다. 전송된 문서는 수신자가 메일 확인을 할 때 IEDI 서버에 의해서 처리되게 된다. 우선 암호화된 IEDI 문서를 복호화하기 위해 PKI 인증기관을 이용하여 필요한 인증서를 다운받고 복호화 알고리즘을 사용하여 복호화한다. 복호화된 문서는 무결성, 기밀성 등이 체크된 뒤 필요한 변환 과정을 거친다. 처리된 IEDI 문서는 JDBC를 사용하여 데이터베이스에 저장한 뒤 다시 RMI를 사용하여 수신자에게 보여지게 된다.

### 3.1 암호화 구현

본 시스템에서는 사용되는 인증기관이 전 세계적으로 공신력있는 인증기관임을 가정하고 IEDI 문서를 주고 받기 위해서 송수신인은 모두 새 사용자 신청 과정을 통해서 인증기관에 등록을 하고 실제 확인작업을 거쳐 합법적인 사용자로 인증을 받는 과정이 선행되어야 함을 전제로 한다. 암호화는 다음과 같은 단계를 거쳐서 수행된다.

첫째, 인증서버에 접속하여 송신자와 수신자의 전자 인증서를 다운받는다. 둘째, IEDI 문서에 대한 전자서명을 만든다. IEDI 문서를 일방향 해쉬함수인 MD5를 사용하여 메시지 다이제스트를 생성한다. 생성된 메시지 다이제스트는 송신자의 개인키를 사용하여 공개키 암호화 방식인 RSA 암호화 알고리즘으로 암호화한다. 셋째, 수신자의 공개키를 획득한다. 다운 받은 수신자의 전자인증서를 인증기관의 공개키로 복호화하여 수신자의 공개키를 획득한다. 넷째, 전송하기 위한 최종 암호 메시지를 만들어 낸다. 전송할 IEDI 문서와 전자서명 그리고 송신자의 전자 인증서를 하나의 메시지로 구성한 뒤 대칭형 암호화 알고리즘인 Triple-DES-CBC 암호화 알고리즘을 사용하여 암호화된 문서를 만든다. Triple-DSE-CBC 암호화에 사용된 암호화 키는 수신자의 공개키를 가지고 공개키 암호화 알고리즘인 RSA 암호화 알고리즘을 사용하여 암호화한다. 이렇게 수신자의 공개키로 암호화된 대칭형 암호키를 전자봉투(Digital Envelop)라 한다. 생성된 암호화 문서와 전자봉투를 하나의 메시지로 구성하면 전송을 위한 최종 암호 메시지가 생성된다. 암호화 과정은 다음 [그림 2]와 같다.



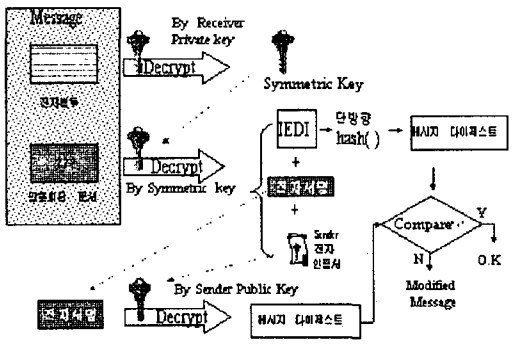

[그림 2] 암호화 과정

### 3.2 복호화 구현

복호화는 다음과 같은 단계를 거쳐서 수행된다.

첫째, 수신된 암호화 메시지를 전자봉투와 암호화된 문서로 분리한 뒤 복호화를 거쳐 필요한 복호키와 문서들을 얻어낸다. 전자봉투를 수신자의 개인키를 가지고 공개키 암호화 알고리즘인 RSA를 사용하여 복호화한다. 이 복호화의 결과로 암호화된 문서를 복호화하는데 필요한 복호키를 얻어낸다. 암호화된 문서를 복호키를 가지고 대칭형 암호화 알고리즘인 Triple-DES-CBC를 사용하여 복호화한다. 이 복호화의 결과로 IEDI 문서와 전자서명 그리고 송신자의 전자인증서가 연결된 메시지를 얻어낸다. 이 메시지를 각각 분리하여 IEDI 문서, 전자서명 그리고 송신자의 전자인증서를 얻어낸다. 둘째, 무결

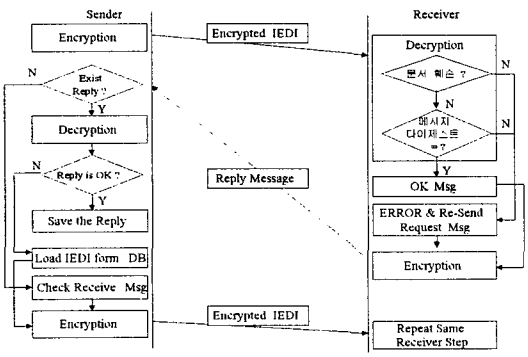
성 확인을 위해 수신측에서 메시지 다이제스트를 생성한다. 얻어진 IEDI 문서를 일방향 해시함수를 사용하여 수신자 측에서 메시지 다이제스트를 생성한다. 셋째, 송신자의 공개키를 획득한다. 송신자의 전자인증서를 인증기관의 공개키로 복호화하여 결과로 송신자의 공개키를 획득한다. 넷째, 송신자가 생성한 메시지 다이제스트를 얻어낸다. 전자 서명을 송신자의 공개키와 공개키 암호화 알고리즘인 RSA로 복호화하여 송신자가 생성한 메시지 다이제스트를 얻는다. 다섯째, 무결성 확인을 위해 메시지 다이제스트를 비교한다. 수신측에서 수신받은 문서로부터 생성된 메시지다이제스트와 송신측에서 생성된 메시지다이제스트를 비교한다. 두 개의 메시지 다이제스트가 같은 경우 문서가 변경되지 않았음을 의미하고 비교 결과가 다른 경우 메시지가 수정되었음을 의미한다. 복호화 과정은 다음 [그림 3]과 같다.




[그림 3] 복호화 과정

## 4 수신 부인 방지 프로토콜

본 논문에서 제안하고 있는 수신 부인 방지 프로토콜은 다음 [그림 4]와 같다.




[그림 4] 수신부인방지 프로토콜

IEDI 문서의 송수신을 위해서 클라이언트와 서버간의 메시지 교환 프로토콜을 정의해야 한다. 네트워크를 통해서 전송되기 때문에 다음 세 가지 경우가 발생한다. 에러 없이 메시지가 정상적으로 전송되는 경우, 전송과정에서 메시지가 유실되는 경우, 해커에 의해서 메시지가 수정되어 보내지는 경우이다. 본 시스템에서는 수신측 클라이언트가 문서를 수신한 경우 응답 메시지를 송신측으로 자동 전송하게 한다. 이 응답 메시지를 통해서 수신자가 문서 수신 사실을 부인할 경우 증거를 제시할 수 있도록 하는 수신부인방지 기능을 획득한다. 에러 없이 정상적으로 메시지가 전송되는 경우는 수신측에서 메일 확인을 통해서 문서를 복호화하고 무결성 체크를 하여 아무 이상이 없는 경우이다. 이 경우는 송신측에 "수신자 ID, 이상무, IEDI 문서 번호, IEDI 문서 수신 성공"이라는 메시지를 암호화하여 발송하게 한다. 이 응답 메시지는 수신자가 수신부인시에 송신측에서 제시할 수 있는 증거가 된다. 전송과정에서 메시지가 유실되는 경우는 전자봉투가 유실되거나 훼손되는 경우와 암호화된 문서의 일부가 유실되거나 훼손되는 경우로 나뉜다. 이는 복호화시에 암호화된 문서를 복호화할 수 없기 때문에 복호화 단계에서 에러를 발생시키고 "수신자 ID, 복호화 불가능, IEDI 문서 번호, 문서 재전송 필요"라는 메시지를 생성한다. 이 메시지를 암호화하여 문서를 보낸 송신측에 전송한다. 송신자가 이 요구 메시지를 받으면 해당 IEDI문서를 데이터 베이스로부터 읽어온 뒤 재 전송한다. 해커에 의해서 메시지가 수정되어 보내지는 경우는 수신측에서 메일 확인 후 복호화 한 뒤 메시지 다이제스트 비교 과정에서 체크된다. 수정된 문서의 메시지 다이제스트와 원래 문서에 대한 메시지 다이제스트 값은 절대 같을 수 없다. 이 경우는 "수신자 ID, 문서의 무결성 오류, IEDI 문서 번호, 문서 재 전송 필요" 메시지를 생성한 뒤 이 메세지를 암호화하여 문서를 보낸 송신측에 전송한다. 송신자가 이 요구 메시지를 받으면 해당 IEDI문서를 데이터 베이스로부터 읽어온 뒤 재 전송한다.

## 5 결론 및 향후 연구 과제

본 논문은 SMTP/MIME 기반 IEDI 시스템의 안전한 문서 전송을 위하여 IEDI 시스템의 보안 솔루션으로 알려진 S/MIME과 대표적인 메일 보안 프로그램인 PGP의 보안 기법을 분석하여 보안 측면에서 기밀성, 무결성, 인증, 송수신 부인방지의 네가지 기능을 가지는 시스템을 구현하였다. 기밀성은 대칭형 암호화 알고리즘과 공개키 암호화 알고리즘을 혼합한 방법을 사용함으로써 서로의 단점을 보완하고 각각의 장점을 획득하였다. 사용자 인증은 삼성 PKI 인증서버가 발행해 주는 전자 인증서를 이용하여 획득하였다. 인증서버를 사용한 인증은 S/MIME에서 베리사인을 사용한 것과 동일한 개념이며, PGP에서 사용되는 공개키 링 구조에 비해 큰 그룹으로 용이하게 확장시킬 수 있다. 무결성은 일방향 해시 함수를 사용하는 메시지 다이제스트와 전자서명 기법을 사용하여 획득하였다. 송신부인방지는 전자 인증서와 전자서명기법을 사용하여 전송하는 메시지에 송신자의 전자서명을 첨부함으로써 획득하였다. 수신부인방지는 본 논문에서 제안된 수신부인방지 프로토콜을 사용함으로써 획득하였다.

다음표는 S/MIME과 PGP 그리고 제안된 보안 기법을 비교한 표이다.

| Security Elements | S/MIME | PGP | 제안 알고리즘 |
|---|---|---|---|
| 기밀성 | DES-CBC, RC2 Triple-DES-CBC | IDEA, RSA | Triple-DES-CBC RSA |
| 무결성 | RSA,MD5,SHA-1 | RSA,MD5 | RSA, MD5 |
| 인증 | Verisign CA | Public Key Ring | Samsung PKI |
| 송신부인방지 | Digital Signature | Digital Signature | Digital Signature |
| 수신부인방지 | Digital Signature (version 3.0) | Not support | Auto transfer Digital Signature |

[표 3] S/MIME, PGP, 제안된 보안 기법 비교

구현된 보안 기법은 일대일 문서 송수신에 대한 보안 기능을 제공하지만 다수의 사용자에게 동시 전송하는 경우는 고려하지 않았다. 따라서 다수의 수신자에 대해서 동시 전송하는 경우에 대한 향후 연구가 필요하다.

## 참고 문헌

1) 이진용, 권혁인, 김영찬, "인터넷 EDI 설계 및 구현", 98 가을 학술발표 논문집(III), 한국정보과학회, 1998

2) IETF, Archived EDIINT Working Group E-mail Listings, January, 1997, http://www.imc.org/ietf-ediint/mail-archive

3) Blake Ramsdell, "S/MIME Version 3 Message Specification", August 6, 1998

4) Simson Garfinkel, "Pretty Good Privacy", O'Reilly & Associates Inc, 1995