通信情報保護學會誌
第3卷 第1號, 1993. 3

EDI 보안 시스템과 디지탈 서명

조광문* · 김태윤**

1. 서 론

컴퓨터의 보급과 통신 기술의 발달로 인하여 여러가지 정보 시스템이 구축되어 정보화 사회로 발전하고 있다. 이에 따라 정보 시스템의 중요성이 증가되고 있으며 이를 효율적이고 안전하게 운영하는 문제가 매우 중요한 요소로 자리잡고 있다.

정보 시스템의 보호를 위한 대책은 여러가지 측면에서 살펴볼 수 있다. 시스템이나 기타 장비에 대한 물리적인 보안 대책, 효율적인 관리와 운영을 위한 인적 자원 대책, 기술적인 측면에서의 대책, 법과 제도적인 측면에서의 대책 등이 있다. 이중에서도 가장 적은 비용으로 효율적인 보안 체계를 제공할 수 있는 것이 암호 시스템 등을 이용한 기술적인 측면의 대책이다.

EDI 시스템은 한 기업의 컴퓨터로부터 다른 기업의 컴퓨터로 표준화된 서식에 맞추어 정보를 교환하는 방법을 의미한다. EDI 시스템에 있어서도 정보의 보안 문제가 중요한 문제로 대두된다. 거래 자료의 교환 처리가 보다 자동화되고 일상적인 의사 결정에 관계될수록 이것을 사용하는 회사의 컴퓨터 시스템 및 통신망, 그리고 자료를 중계해주는 측의 신뢰성 등의 문제가 중요하게 된다.

특히 EDI 시스템에서는 기존의 다른 정보 시스템에서 요구하는 보안 요소 중에서도 전송되는 자료에 대한 신뢰성과 인증(authentication)의 문제가 매우 중요하게 고려되어야 한다.

본 연구에서는 EDI 시스템에 적용되어야 할 보안 요소를 X.435를 중심으로 분류하고, 이러한 보안 서비스 중에서 인증과 부인 봉쇄 서비스를 제공하기에 가장 적합한 디지탈 서명(digital signature)기법에 대한 내용을 제시한다. 그리고 EDI 시스템에 디지탈 서명기법을 적용하기 위한 구체적인 방안을 제시한다.

2. EDI 시스템의 보안 요소

ISO의 개방형 통신 모델에서 EDI 시스템을 사용하기 위해서 고려되어야 할 주요 보안 요소들은 다음과 같다.

- 시스템 가용성(service availability)
- 데이타 무결성(integrity)
- 대등 객체 인증(peer authentication)
- 액세스 제어(access control)
- 보안 감사 추적(security audit trail)
- 데이타 비밀성(confidentiality)

이들 서비스 요구 사항들이 서로 독립적인 것은

* 고려대학교 전산과학과 박사과정
** 고려대학교 전산과학과 교수

아니고 어느 정도 중복성이 존재한다. 이들 각각의 서비스에 대한 부분적인 개요를 정확하게 인식하는 것이 EDI 시스템을 위한 보안 서비스의 전체적인 형태를 알 수 있는 좋은 방법이다.

시스템 가용성이란 EDI 서비스가 언제 어디서나 가능하도록 하는 것으로서 매우 중요한 요구 사항이다. 시스템 가용성이 없이는 EDI 서비스 제공업자가 존재하지 못한다고도 할 수 있다. 이 서비스는 필요한 EDI 시스템 하드웨어와 소프트웨어를 중복되게 설치하여 운영하는 것으로 해결할 수 있다. 시스템을 중복으로 유지하면서 가장 신뢰할 수 있는 시스템 요소를 사용하여 EDI 서비스를 제공할 수 있게 한다.

데이타 무결성이란 다른 정보 시스템에서와 마찬가지로 EDI 시스템을 사용하여 정보를 교환하는 거래 당사자들이 원하지 않는 데이타의 손실이 발생되지 않도록 하는 것이다. 현재 발생되고 있는 데이타 무결성을 해치는 요소는 시스템 하드웨어의 장애나 소프트웨어에 대한 부하의 과중 등이다. 이러한 문제는 보다 신뢰성 있는 통신 회선과 소프트웨어를 사용함으로써 해결될 수 있다. 그러나 앞으로는 사용자에 의한 데이타의 임의적인 변경이나 조작 등의 문제가 더 심각하게 될 것이다. 이를 해결하기 위해서는 교환되는 EDI 인터체인지(interchange) 내에 데이타의 무결성을 검증할 수 있는 정보를 추가하는 방법이 있다.

대등 객체 인증이란 주로 Third Party에 의해 제공되는 서비스로서 서로의 신분이 확인된 거래 상대자만이 EDI 메시지를 교환할 수 있도록 하는 방법이다.

액세스 제어는 EDI 서비스 제공업자가 정당한 사용자에게만 통신 회선의 접근을 손쉽게 제공할 수 있도록 하는 기능이다. 일반적으로 정당한 사용자를 확인하기 위하여 간단한 패스워드를 이용하는 방법이 적용된다. 이외에 사용자들 사이에 전용 통신 회선을 설치하는 방법이 있다. 전용선을 사용함으로써 쉽게 통신 회선을 사용할 수 있을 뿐만 아니라 대량의 정보 전송시 효율적이다.

보안 감사 추적은 사용자에게 EDI 메시지의 전송 현황에 대한 정보를 제공한다. 즉, 정보 교환에 따르는 중요한 상황을 확인하는 것이다. 전송한 메시지가 수신자에게 정확하게 도착하였는지, 실제로 수신자가 메시지를 접수하였는지 등의 정보를 사용자에게 제공해 준다. EDI 서비스 제공업자에게 있어서 이 서비스는 매우 중요하다. 보안 감사 추적 정보는 EDI 시스템의 사용자들 사이에 발생하는 메시지 송수신의 부인 등에 따르는 논쟁에 대한 기록 자료가 될 수 있다.

데이타 비밀성은 다른 정보 시스템에서 요구되는 서비스와 마찬가지로 정당한 사용자가 아닌 제 3 자가 전송되는 메시지의 내용을 알 수 없도록 하는 것이다. 이것은 일반적으로 암호화 기법을 적용하여 수행된다.

3. X.435 보안 서비스 및 구현 방안

EDI 시스템은 적용되는 하부 통신 프로토콜에 따라 여러가지 형태를 가질수 있다. 그중에서도 많은 시스템들이 축적 후 전송 방식을 사용하고 있는 X.400 프로토콜인 MHS(Message Handling System)에 기반하여 제공되고 있다. MHS에서 제공되어야 하는 보안 서비스는 2장에 제시된 것과 같고 이것은 X.402에 정의되어 있다. 그러나 EDI가 기본적인 보안 기능을 제공하면서 단순히 거래 문서를 전달하는 것에 그치지 않고 발생 가능한 법적인 분쟁 등을 해결할 수 있도록 하기 위해서는 추가적인 서비스 기능이 요구된다. 이에 따라 EDI를 위한 전용 프로토콜로 X.435가 제안되었다. X.435에는 EDI를 위한 보안 서비스 요소로서 EDI 메시지의 인증과 부인 봉쇄 서비스가 추가되었다. 또한 X.435 권고에는 새로운 형태의 EDI 메시지 구조를 위하여 Pedi를 규정하고 있다.

EDI 시스템을 위한 보안 서비스의 전체적 내용은 표 1과 같다.

Pedi 프로토콜은 자체 내에 몇가지의 안전성 서비스를 포함하고 있으며, 이러한 서비스들은 송수신된 EDIM(EDI Message)에 대한 안전성 서비스를 제공한다. X.435에 추가 정의된 보안 서비스는 그림 1과 같다.

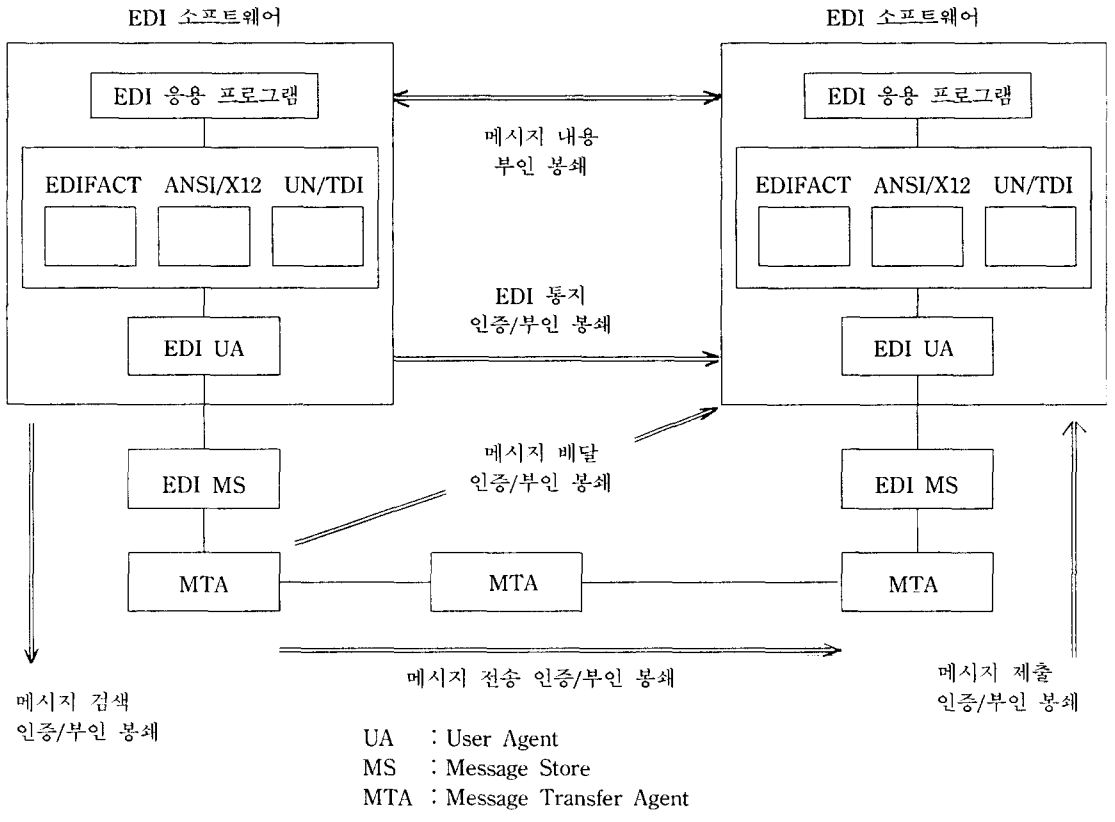


그림 1. X.435 추가 보안 서비스 내용

표 1. X.435 보안 서비스 내용

Origin authentication	X.402
EDIM responsibility authentication	X.435
Proof of EDI notification	
Proof of retrieval	
Proof of transfer	
Secure access management	X.402
Data confidentiality	X.402
Data integrity	X.402
Non-repudiation	X.402
Non-repudiation of EDIM responsibility	X.435
Non-repudiation of EDI notification	
Non-repudiation of retrieval	
Non-repudiation of transfer	
Non-repudiation of content	
Message security labelling	X.402
Security management services	X.402

X.435에 추가된 보안 서비스의 내용은 인증과 부인 봉쇄 서비스이다. 이들은 서로 상호 연관되어 제공된다. 이러한 인증/부인 봉쇄 서비스는 메시지의 제출(submission), 배달(delivery), EDI 통지(EDI notification) 등으로 구분할 수 있다.

3.1. 메시지 제출 인증/부인 봉쇄 서비스

메시지 제출 인증/부인 봉쇄 서비스는 EDI 시스템의 사용자와 MTA 사이에서 제공되어야 하는 것이다. 메시지 제출 인증 서비스는 메시지의 송신자가 원래 의도했던 수신자들에게 전송하고자 하는 메시지를 MTS(Message Transfer System)가 수신하였다는 것을 확인하는 것으로서 이 확인 응답을 메시지의 송신자가 확인할 수 있어야 한다. 그리고 메시지 제출

부인 봉쇄 서비스는 메시지가 MTS에 제출되었다는 사실을 송신자가 부인할 수 없게 만드는 것이다.

3.2. 메시지 배달 인증/부인 봉쇄 서비스

메시지 배달 인증/부인 봉쇄 서비스는 EDI 시스템을 사용하여 메시지를 전송한 사용자와 이 메시지를 수신할 사용자를 담당한 MTA 사이에서 제공되어야 하는 서비스이다. 메시지 배달 인증 서비스는 MTS에 의해서 메시지 전송자가 의도한대로 정당한 수신자들에게 메시지가 전달되었다는 확인 응답을 얻기 위한 것이다. 그리고 메시지 배달 부인 봉쇄 서비스는 메시지 배달 인증 서비스를 이용하여 메시지 헤더에 명시된 메시지 수신자들에게 배달을 했다는 사실을 해당 MTA가 부인할 수 없도록 해주는 서비스이다.

3.3. EDI 통지 인증/부인 봉쇄 서비스

EDI 시스템의 MS와 UA 사이의 EDI 통지 인증 서비스는 메시지의 송신자가 전송한 메시지가 정당한 수신자에게 배달되었는지 확인한다. 그리고 EDI 메시지에 대한 책임이 수용(accepted) 되었는지, 회송(forwarded) 되었는지, 또는 거부(refused) 되었는지를 확인하기 위한 것으로서 수신한 메시지에 대한 서명을 생성하여 메시지 송신자에게 다시 돌려보내는 방식이다. 이러한 과정은 X.435에 정의된 EDI 통지(notification)를 사용하여 수행된다.

EDI 통지 인증 서비스를 요구하기 위해서는 메시지 송신자가 EDIM 헤딩의 edi-notification-requests 항목에 통지 요구 사항을 명시하고, edi-notification-security 항목을 "proof"로 표시한다. edi-notification-requests 항목에 명시될 수 있는 요구 사항으로는 PN(Positive Notification), NN(Negative Notification), FN(Forwarded Notification) 등이 있다. EDIM 헤딩의 주요 구조는 그림 2와 같다.

이 메시지를 수신한 사용자가 EDIN을 생성하게 된다. EDIN은 수신한 메시지에 대한 서명을 생성하여 만들게 된다. 이것을 원래 EDIM을 전송한 사용자에게 전송하게 되고, 이를 수신한 원래의 EDIM 송신자는 EDIN 송신자의 신분을 확인하여 EDIM이

```
EDIM Heading : : =SEQUENCE {
        this-EDIM
        originator
        recipients : : =SEQUENCE {
            recipient
            action-request
            edi-notification-requests-field : : =SEQUENCE {
                edi-notification-requests
                edi-notification-security
                edi-reception-security
            }
            responsibility-passing-allowed
            .
            .
            .
        }
        edin-receiver
        .
        .
        .
}
```

그림 2. EDIM 헤딩의 주요 구조

안전하게 전송되고 수신되었는지를 확인하게 된다.

그리고 EDI 통지 부인 봉쇄 서비스는 EDIM 헤딩의 edi-notification-security 항목과 edi-reception-security 항목을 "non-repudiation"으로 표시하고, 그외의 과정은 EDI 통지 인증 서비스와 거의 같은 방식으로 수행된다.

4. EDI 사용자 인증과 디지탈 서명

4.1. EDI 사용자 인증

EDI 메시지에 대한 사용자 인증이란 서로 정보를 교환하는 거래 상대방이 올바르게 승인된 거래처이며, 교환되는 정보도 정당한 자료라는 것을 확인해 주는 작업이다. EDI 시스템을 활용하여 업무를 처리하게 되면 더이상 종이 문서에 서명된 서류를 사용할 수 없게 되기 때문에 사용자에 대한 인증 작업은 반드시 필요로 되는 중요한 일이 된다.

이러한 인증 작업이 없이 단순히 기존의 종이 서류의 사용에 의한 업무를 EDI 시스템과 같은 컴퓨터 통신망을 이용하여 처리하게 되면, 메시지의 송수신시 상대방의 신분을 확인하거나 사용자의 정당성을 인정하고 송수신자 사이에 발생할 수 있는 분쟁을 비롯한 여러가지 문제를 해결할 수 없게 된다. 따라서 기존에 사람의 자필 서명이나 도장과 같은 역할을 수행할 수 있는 새로운 제도나 절차가 반드시 필요하게 된다.

이러한 절차나 과정에서도 기존의 문서 처리와 마찬가지로 임의의 사용자가 EDI 시스템을 통하여 메시지를 전송하였을 때, 수신자가 고의적으로 메시지의 내용을 자신있게 유리하도록 변경할 수도 있고, 메시지 송신자가 메시지의 전송 사실을 부인하거나 자신이 원래 전송한 메시지와 그 내용이 다르다고 주장하는 경우가 발생하게 된다. 결과적으로 송수신자 사이에 분쟁이 발생하고 경우에 따라서는 법적인 처리 절차까지 거쳐야 한다. 그리고 거래 당사자 간의 법적인 책임을 입증할 수 없고, 불완전한 자료나 인증되지 않은 자료의 유입이 발생한다.

EDI 메시지와 사용자에 대한 인증 기법을 적용하게 되면, 메시지의 수신자가 메시지를 수신하였을 때 그 내용의 변조 여부를 확인할 수 있게 된다.

4.2. 디지탈 서명

EDI 시스템을 통하여 전송되는 메시지에 전자적인 기법의 디지탈 서명을 한다는 것은 메시지의 수신자가 송신자를 확인할 수 있다는 것이고, 송신자가 후에 이 메시지의 전송 사실을 부인할 수 없어야 한다는 것이다. 즉, 디지탈 서명이란 EDI 시스템의 사용자 각각을 확인할 수 있고, 교환되는 메시지에 대한 인증과 송수신자 사이에 발생하는 분쟁 등의 문제를 해결할 수 있어야 한다. 이러한 목적을 달성하기 위하여 임의의 사용자가 디지탈 서명된 EDI 메시지를 거래 상대자에게 전송하였다고 할때, 다음의 조건을 만족하여야 한다.

- 수신자는 서명을 보고 메시지의 송신자를 확인할 수 있다.
- 수신자를 비롯한 어느 누구도 메시지의 내용을 변경하거나 송신자가 작성한 서명을 위조할 수 없다.
- 송신자가 서명이나 메시지의 내용 자체를 부인했을 때, 중재자가 송수신자 사이의 분쟁을 해결할 수 있어야 된다.

인증을 위한 서명 기법으로의 디지탈 서명과 기존에 사람의 손에 의한 자필 서명의 차이점은 다음과 같다. 사람의 자필 서명은 그것이 아무리 복잡하다 하더라도 비교적 손쉽게 위조해 낼 수 있다. 반면에 디지탈 서명은 그 기법을 적용하는 방법에 따라 위조의 확률을 최소로 줄일 수 있다. 또한 자필 서명은 사람에 따라 거의 일정하여 모든 서류에 동일하게 사용되지만 디지탈 서명은 사용하는 서류마다 각각 다른 서명을 할 수 있다는 점이다.

디지탈 서명기법에는 공통키(Private key) 암호 시스템을 이용한 방법과 공개키(Public key) 암호 시스템을 이용한 방법이 있다. 일반적인 암호화기법으로 공개키 시스템이 널리 사용되는 것과 같이 디지탈 서명기법에도 공개키 암호 시스템을 주로 사용한다.

공통키 암호 시스템을 이용한 디지탈 서명기법에

서는 메시지의 송수신자가 키를 안전하게 보관하여야 됨은 물론 신뢰성 있고 안전하며 보다 강력한 역할을 수행하는 중재자가 필요하다. 이 기법에서는 송수신자 사이의 서명 확인을 중재자를 통하여 수행하게 된다. 따라서 전송 데이타량이 증가되어 통신 효율이 매우 저하되거나, 메시지의 변경이나 서명의 변경 주장에 대하여 명확한 판단을 내리지 못할 경우도 발생할 수 있다.

4.3. 공개키 암호 시스템에 의한 디지탈 서명

공개키 암호 시스템에서는 각각의 사용자가 공개키와 비밀키를 사용하여 암호화와 복호화 과정을 수행한다. 각 사용자의 공개키는 누구나 알 수 있고 쉽게 얻을 수 있도록 공개된 장소에 보관되고, 비밀키는 해당 사용자만이 보관하게 된다.

메시지의 송신자가 수신자에게 메시지를 전송하는 가장 간단한 방법은 수신자의 공개키로 메시지를 암호화하여 전송하고 수신자는 수신된 암호문을 자신의 비밀키로 복호화하는 방법이다. 메시지의 송신자를 A라 하고, 수신자를 B라고 하면 다음과 같은 과정을 통하여 메시지를 암호화할 수 있다.

$$C=E_B(M)$$
$$M=D_B(C)$$

이 경우에는 메시지의 비밀성을 보장할 수 있으나 특정 송신자가 메시지를 전송하였다는 사실은 증명할 수 없게 된다. 왜냐하면 누구나 수신자의 공개키를 쉽게 알아낼 수 있기 때문에 메시지를 암호화하여 전송할 수 있기 때문이다.

반면에 특정한 송신자가 메시지를 전송하였다는 것을 확인하기 위해서는 송신자의 비밀키를 이용하여 메시지를 암호화한 후 전송하고, 수신자는 수신된 암호문을 송신자의 공개키로 복호화하여 메시지를 얻을 수 있다. 이 과정은 다음과 같다.

$$C=D_A(M)$$
$$M=E_A(C)$$

그러나 이 경우에 있어서는 특정한 송신자가 수신자에게 메시지를 전송하였다는 사실은 인증할 수 있으나, 송신자의 공개키를 알고 있는 모든 사용자가 암호문을 해독할 수 있게 되어 메시지의 비밀성이 보장되지 못하는 결과가 된다.

따라서 메시지의 비밀성과 인증을 보장할 수 있도록 하기 위해서는 송신자가 메시지를 자신의 비밀키로 암호화하고, 이를 수신자의 공개키로 다시 한번 더 암호화한 결과의 암호문을 전송한다. 수신자는 수신된 암호문을 자신의 비밀키로 복호화하고, 송신자의 공개키로 재복호화하여 원래의 메시지를 구할 수 있게 된다. 이러한 공개키 암호 시스템을 이용하여 제공되는 디지탈 서명기법의 수행 과정을 다음 그림 3과 같이 나타낼 수 있다.

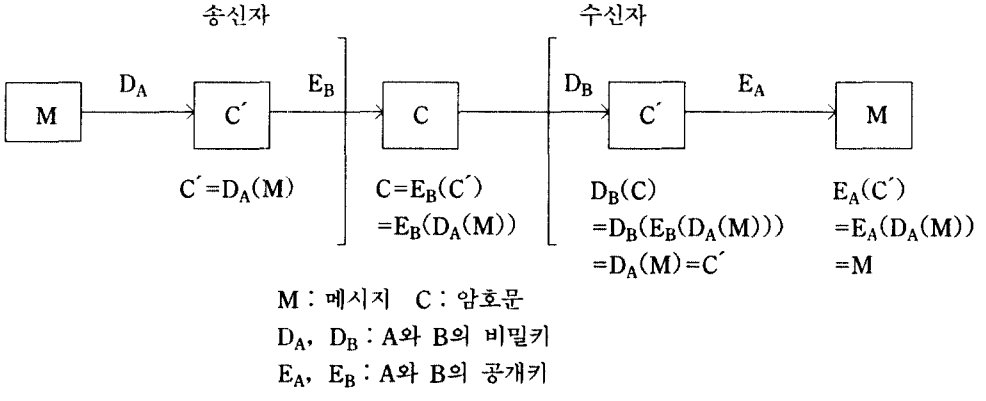


그림 3. 공개키 암호 시스템을 이용한 디지탈 서명 과정

이러한 체계를 갖는 시스템에서 수신자는 C나 C′을 디지탈 서명으로 보관하면 된다. 송신자가 자신의 비밀키를 이용하여 암호화 과정을 수행한다는 것은 송신자 이외에는 수행할 수 없는 작업이다. 따라서 이것을 송신자의 서명이라고 볼 수 있다. 이렇게 생성된 디지탈 서명은 아무도 위조해 낼 수 없게 된다. 메시지의 수신자가 수신된 암호문에 대하여 자신의 비밀키와 송신자의 공개키를 이용하여 복호화하게 되는데 이때 송신자의 공개키를 사용한다는 사실 자체가 송신자의 서명을 확인하는 작업이 된다. 따라서 메시지의 수신자가 암호문을 보관하고 있으면, 추후 발생될 수 있는 모든 상황에 대한 해결을 할 수 있다. 따라서 디지탈 서명을 이용한 인증 작업이 수행되는 것이다.

공개키 암호 시스템을 이용한 디지탈 서명 기법을 적용하려면 반드시 암호화와 복호화가 역과정이 되어야 한다. 이러한 암호 시스템의 대표적인 것으로 RSA 시스템이 있다. RSA 시스템은 매우 큰 수의 정수 연산이 필요로 되는 시간적인 단점을 갖고 있지만 현재 공개키 암호 시스템으로 널리 사용되고 있다.

5. EDI 시스템에의 적용

여기에서는 EDI 시스템에서 디지탈 서명을 이용하여 메시지의 전송과 수신을 확인할 수 있는 방법에 대한 내용을 X.435의 메시지 구조인 EDIM과 EDIN을 중심으로 제시한다.

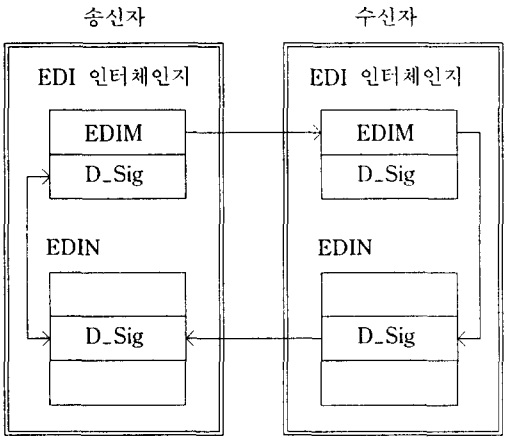


그림 4. EDI 시스템에서의 메시지 수신 확인 과정

5.1. EDI 메시지에 대한 수신 확인 기본 과정

EDI 시스템에서의 메시지의 전송과 수신을 확인하기 위한 기본적인 과정은 그림 4와 같다.

그림 4에서 메시지의 송신자는 우선 전송하고자 하는 메시지 EDIM에 대하여 적절한 해쉬 함수를 적용한다. 이 결과에 대하여 자신의 비밀키를 적용하여 D_Sig(Digital Signature)를 발생시킨다. 메

```
EDIN CommonFields : : =SEQUENCE {
        subject-edim
        edin-originator
        first-recipient
        notification-time
        notification-security-elements : : =SEQUENCE {
            original-content
            original-content-integrity-check
            edi-application-security-elements
            security-extensions
        }
        edin-initiator
        notifications-extensions
```

그림 5. EDIN 공통 항목 구조

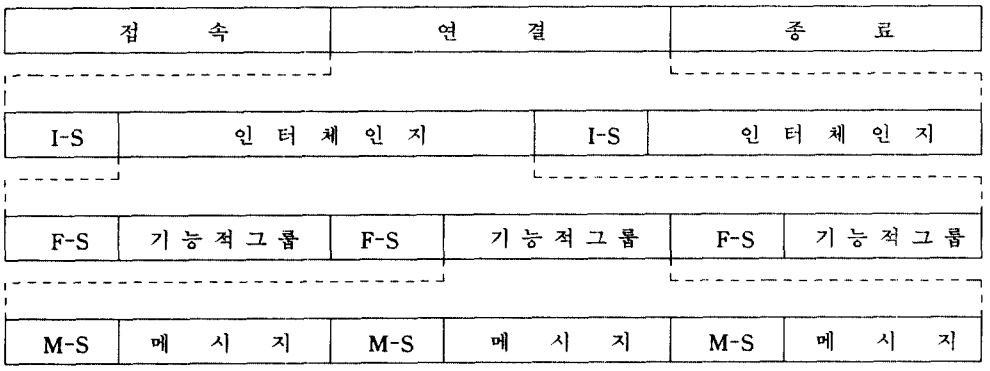
시지 송신자는 EDIM과 D_Sig가 함께 포함된 EDI 인터체인지를 EDI 시스템을 이용하여 전송하게 된다. EDI 인터체인지의 수신자는 인터체인지 내에서 EDI과 D_Sig 항목을 분리한다. EDI의 내용은 적절한 절차에 따라서 처리하고, D_Sig 항목 부분을 EDIN의 해당 항목에 복사한다. EDIN의 공통 항목 부분 중에서 notification-security-elements 항목의 부항목인 original-content-integrity-check 항목에 복사한다. EDIN 공통 항목 부분의 구조는 그림 5와 같다.

메시지의 수신자는 이외에도 필요한 내용을 추가하여 EDIN을 생성하고 이를 원래의 EDIM 송신자에게로 전송한다. EDIN을 수신한 EDIM 송신자는 EDIN에서 분리한 D_Sig와 원래 자신이 처음에 생성한 D_Sig를 비교하게 된다. 이러한 과정을 거쳐서 메시지의 전송과 수신이 정확하게 이루어졌다는 사실을 확인하게 된다. 만약 메시지의 송신자가 적절한 해쉬함수와 암호화 방법을 갖추지 못하고 있을 때도 이 확인 과정을 수행할 수 있다. 이때에는 EDIN의 생성자 측에서 D_Sig를 위한 original-content-integrity-check 항목을 사용하지 않고, original-content 항목을 사용하여 수신한 EDIM 전체를 복사하여 전송함으로써 확인 과정을 수행한다.

5.2. 보안 서비스 세그먼트를 추가한 UN/EDIFACT

EDIM에 대한 수신 확인을 위한 디지탈 서명을 적용하는 방법과 같이 EDI 시스템을 통하여 전송되는 메시지인 EDIM의 전체 내용에 대한 서명을 생성하여 사용할 수도 있으나, EDI 메시지가 갖는 특성을 활용하여 다단계의 보안 서비스를 위한 서명기법을 적용할 수도 있다.

EDI 시스템을 통하여 송수신되는 메시지의 단위를 EDI 인터체인지라고 한다. 특히 EDI의 국제 표준으로 사용되고 있는 UN/EDIFACT의 구조에서는 EDI 인터체인지가 엔벨로프(envelope)라는 개념으로 이루어져 있다. 이 엔벨로프는 인터체인지, 기능적 그룹(functional group), 메시지의 3단계로 구성된다. 이때 각 엔벨로프 단계에 포함되는 표준 서식들이 같은 수준의 보안성 요구를 가질 수도 있으나, 일반적으로 서로 다른 수준의 보안성 요구를 갖는다. 즉, 하나의 송수신 메시지 단위 내에 포함되는 문제들에 대하여 메시지별 또는 기능적 그룹별로 선택적인 보안성의 적용이 가능하고, 또한 적용을 원하는 서비스의 종류도 지정할 수 있도록 하



I-S : 인터체인지 보안 세그먼트(Interchange Security Segment)
F-S : 기능적 그룹 보안 세그먼트(Functional Group Security Segment)
M-S : 메시지 보안 세그먼트(Message Security Segment)

그림 6. 보안 서비스 세그먼트가 추가된 UN/EDIFACT 구조

여야 한다는 것이다. 또한 메시지의 특정한 항목에 대한 보안 서비스를 적용할 수 있고, 같은 서비스에 대해서도 적용되는 보안 서비스의 강도를 다르게 할 수도 있다.

이러한 서비스를 제공하기 위하여 디지탈 서명 시스템을 적용할 수 있다. EDI 표준 서식인 UN/EDIFACT 구조에서 각 인터체인지와 기능적 그룹, 메시지 사이에 보안 서비스를 적용하기 위한 새로운 세그먼트를 추가하는 방법이다. 이러한 추가 세그먼트는 모두 선택적으로 사용할 수 있다. 추가된 세그먼트를 포함한 UN/EDIFACT 메시지 구조를 그림 6과 같이 그려볼 수 있다.

보안 서비스 세그먼트에 포함될 수 있는 내용으로는 적용된 보안 서비스 기능에 대한 내용과 이에 관련된 사항, 사용자의 암호화 키에 대한 정보, 그리고 직접적으로 보안 서비스에 관련된 디지탈 서명이나 메시지 인증코드(MAC : Message Authentication code) 등이 있다. 이러한 방법을 사용함으로써 각 메시지에 대하여 필요한 직접적인 보안 서비스를 적용할 수 있고, 또한 선택적 부분에 대한 서비스도 제공하여 보안 서비스 적용에 따른 오버헤드 문제도 어느 정도 해결할 수 있게 된다.

5.3. 디지탈 다중 서명 방식

지금까지의 디지탈 서명 기법으로 EDI 시스템을 사용하여 각 기업간에 문서를 교환하는데 있어서 필요로 되는 상대방 신분의 인증과 송수신되는 메시지의 내용에 대한 인증을 수행할 수 있다. 이러한 디지탈 서명 기법을 단순 서명(single signature) 방식이라 한다. 그러나 일반적으로 대부분의 기업에서 하나의 문서를 대외적으로 제출하기까지는 여러 단계의 필요한 사람들에 의한 문서의 내용의 확인과 서명을 거쳐야 한다. 이러한 개념을 디지탈 서명의 개념에도 포함시키고자 하는 것이 디지탈 다중서명 방식(digital multisignature)이다. 즉, 메시지의 원래 작성자에 의한 디지탈 서명과 이 내용을 확인하기 위한 상급자의 결재 서명 등 여러명의 사용자에 의한 디지탈 서명의 개념을 나타낸다.

디지탈 다중서명 방식은 크게 순차 다중 서명(sequential multisignature) 방식과 동시 다중서명(simultaneous multisignature) 방식의 두가지 종류로 구분된다. 순차 다중 서명방식은 하나의 같은 메시지에 대하여 여러명의 서명자들이 차례대로 서명하는 방식이고, 동시 다중서명 방식은 한 메시지에 대하여 여러 서명자들이 동시에 서명하는 방식이다.

다중서명을 위한 여러가지 기법들이 개발되어 사용되어 왔다. 그중 가장 간단한 방법은 한가지의 단순 서명방식을 같은 메시지에 대해 여러번 반복 적용함으로써 수행된다. 그러나 이 방법은 단순서명 방법을 적용하는 횟수만큼 문서의 길이가 늘어나게 된다는 단점을 갖는다. 공개키 암호시스템과 단방향 함수를 이용한 다중서명 방식이 있는데, 이 방법은 다중 서명 메시지의 길이가 거의 증가하지 않고 서명의 순서에 대한 제약을 받지 않는다는 장점이 있다. 그러나 RSA 방식과 같은 공개키 암호 시스템에 근거하기 때문에 계산량이 많아져 서명 처리 속도가 떨어지는 단점이 있다. 이외에도 각 사용자의 ID를 이용하여 서명하는 방식이 있다. 이 방법은 고속처리와 ID에 근거하여 RSA 방식 보다는 효율적이라 할 수 있다.

이 논문에서는 EDI 메시지에 대한 디지탈 서명 기법으로 각 사용자의 ID를 이용한 방식을 기본으로 하여 순차 다중서명 방식과 동시다중 서명방식 기법을 제시한다. 먼저 각 서명자의 서명 발생을 위한 키를 키분배 센터로부터 발급받고 일정한 절차에 따라 서명을 수행해 나가며, 이를 최종 인증자가 검증할 수 있어야 한다.

(1) 키 발생 및 분배

메시지에 서명을 할 각 서명자들은 키분배 센터로부터 서명에 사용할 키를 분배받아야 한다. 이를 위하여 먼저 각 서명자 i는 각자의 ID_i를 키분배 센터로 전송한다. ID로는 서명자의 이름이나 주민등록번호 등이 사용될 수 있으며, 각 서명자를 식별할 수 있는 것이어야 한다. 키분배 센터에서는 각 사용자들의 ID를 근거로 키를 생성하여 분배한다. 이 과정은 그림 7과 같이 나타낼 수 있다.

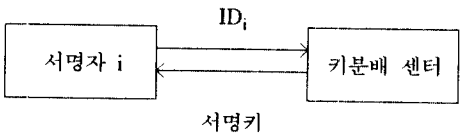
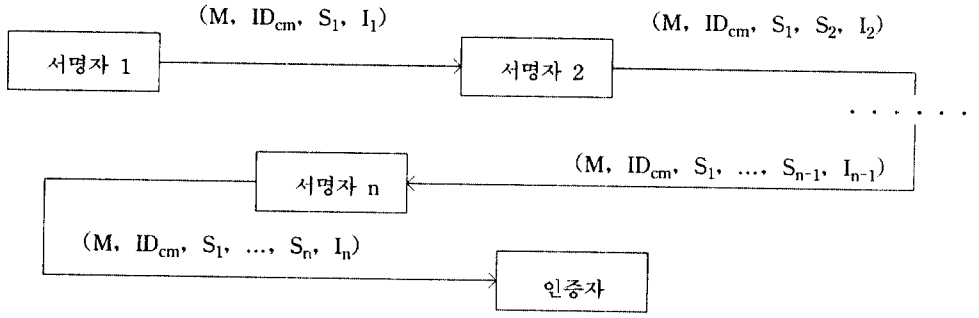


그림 7. 각 서명자에 대한 키 분배 과정

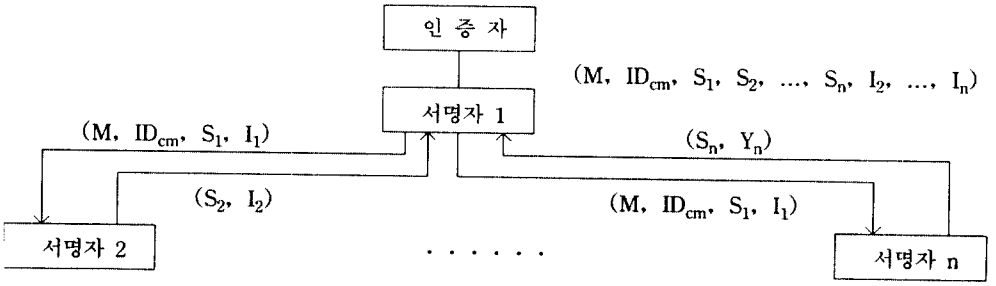
(2) 순차 다중 서명 방식

순차 다중 서명 방식에서는 하나의 메시지에 대하여 여러명의 서명자가 차례로 서명을 하는 방식이다. EDI 메시지에 대한 서명 작업을 수행하기 전에 각 서명자는 키분배 센터로부터 적절한 서명키를 분배 받아야 한다. 가장 먼저 EDI 메시지를 작성한 사용자가 그 메시지에 대한 서명을 하고, 필요한 순서에 따라 메시지를 전송하면서 서명을 하는 방법이다. 이때 메시지의 원래 작성자가 서명할 사람들의 순서를 결정하고, 각 서명자들의 ID를 함께 전송한다. 그러면 각 서명자는 공개된 단방향 함수 f, g를 사용하여 바로 앞 서명자까지의 서명을 검증한다. 그리고 자신의 서명을 추가한다. 이 과정은 그림 8과 같다.



M : EDI 메시지
ID$_{cm}$: 서명자들의 ID 결합(=ID$_1$‖ID$_2$‖...‖ID$_n$)
Si : 서명자 i의 서명
Ii : 중간 서명자가 앞 서명자들을 검증하기 위한 인증값

그림 8. 순차 다중 서명 과정



M : EDI 메시지
ID$_{cm}$: 서명자들의 ID 결합(=ID$_1$‖ID$_2$‖...‖ID$_n$)
Si : 서명자 i의 서명
Ii : 인증자가 서명자들을 검증하기 위한 인증값

그림 9. 동시 다중 서명 과정

(3) 동시 다중 서명 방식

만약 서명이 필요한 EDI 메시지가 적절한 통신 시스템에 의하여 동시에 여러 서명자들에게 전송될 수 있다면 동시 다중 서명 방식을 적용할 수 있다. 동시 다중 서명 방식에서도 순차 다중 서명 방식에서와 같이 키분배 센터로 부터 각자의 서명키를 분배 받는다.

동시 다중 서명 방식은 그림 9와 같은 과정으로 수행된다.

동시 다중서명 방식에서는 각 서명자들이 최초로 EDI 메시지를 작성한 서명자의 서명을 인증값 I_1을 이용하여 검증할 수 있고, 순차 다중서명 방식에서와 같이 다른 서명자들의 서명을 검증할 수는 없다. 최종 인증자는 각 서명자들이 생성한 인증값 I_i를 이용하여 EDI 메시지를 검증할 수 있게 된다.

6. 결 론

컴퓨터와 통신 기술이 발전해 나감으로써 정보 시스템의 중요성이 증가되고 있으며 이를 효율적이고 안전하게 운영하는 문제가 매우 중요한 요소로 자리잡고 있다.

한 기업의 컴퓨터로부터 다른 기업의 컴퓨터로 표준화된 서식에 맞추어 정보를 교환하는 형태의 정보 교환 방식인 EDI 시스템에 있어서도 정보의 보안 문제가 중요한 문제로 대두된다. 거래 자료의 교환 처리가 보다 자동화되고 일상적인 의사결정에 관계될수록 이것을 사용하는 회사의 컴퓨터 시스템 및 통신망, 그리고 자료를 중계해주는 측의 신뢰성 등의 문제가 중요하게 된다.

특히 EDI 시스템에서는 기존의 다른 정보 시스템에서 요구하는 보안 요소 중에서도 전송되는 자료에 대한 신뢰성과 인증의 문제가 매우 중요하게 고려되어야 한다.

본 연구에서는 EDI 시스템의 보안 서비스를 위한 요소를 X.435를 중심으로 분류하고 이에 대한 구현 방안을 제시하였다. 특히 EDI를 위하여 요구되는 보안 서비스 요소인 사용자와 메시지에 대한 인증과 부인 봉쇄 서비스를 제공하기 위하여 디지탈 서명 기법을 적용하는 구체적인 방안들을 제시하였다.

앞으로의 연구 과제로는 본 연구에서 제시한 디지탈 서명기법을 구체적으로 구현하기 위한 방법을 개발하여 실제 시스템 모델로 개발하는 것이다. 디지탈 서명 생성을 위한 새로운 형태의 해쉬 함수를 개발하여야 한다. 그리고 서명 생성에 사용되는 RSA 암호 시스템 또는 ID를 사용하는 방법에서의 몇가지 문제점들을 해결할 수 있는 새로운 방법을 개발한다. 그리고 EDI 메시지의 구조에 맞는 보안 서비스 세그먼트의 표준을 규정하여 이에 적용시킬 수 있어야 한다.

기술적인 면에서의 문제외에도 디지탈 서명을 실제로 사용할 수 있는 법적, 제도적 환경과 함께 사용자들에 대한 인식의 확산이 이루어져야 한다. 이러한 제반 여건이 마련되어야지만 보다 효과적이고 안전한 EDI 시스템을 구축할 수 있다.

참 고 문 헌

1. E.J.Humphreys, "Confidence in Your Trading Partners Certificates", Proceedings of the 7th International Conference and Exhibition on Information Security, pp.273-282, 1991. 5.

2. Fred Piper, "Digital Signatures", Proceedings of the 7th International Conference and Exhibition on Information Security, pp.62-71, 1991. 5.

3. J.Williamson, J.E.Draper, "EDI Security-Today and Tomorrow", Proceedings of the 7th International Conference and Exhibition on Information Security, pp.355-368, 1991. 5.

4. Peter Landrock, "Protecting Your EDI Message", Proceedings of the 3rd International Congress of EDI Users, pp.464-473, 1991. 9.

5. R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM. Vol.21, No. 2, pp.120-126, 1978.

6. Selim G.Akl, "Digital Signatures : A Tutorial Survey", IEEE Computer, pp.15-24, 1983. 2.

7. 김대영, "디지틀 다중서명 방식", 데이타 보호

기반 기술 WORKSHOP 논문집, pp.83-94, 1992.

8. 김정희, 김태윤, "전자식 문서 교환(EDI)의 보안과 통제관리", 통신정보보호학회지, 제 1 권, 제 3 호, pp.99-108, 1991.

9. 남길현, "암호시스템을 이용한 디지탈 서명 시스템", 통신정보보호학회지, 제 1 권, 제 1 호, pp. 64-71, 1991.

10. 임용진, 이강무, 고홍기, 나종근, 김동규, "EDI 시스템의 안전성 서비스 구현 방안에 관한 연구", 통신정보보호학회 학술발표논문집, pp.153-164, 1992.

□ 著者紹介

趙 光 門

고려대학교 전산과학과 졸업(학사)
고려대학교 전산과학과 석사
현 재 : 고려대학교 전산과학과 박사과정
관심분야 : 컴퓨터 통신 보안, 이동 통신, EDI

金 泰 潤

고려대학교 산업공학과 졸업(학사)
미국 Wayne State University 석사
미국 Auburn University 박사
현 재 : 고려대학교 전산과학과 교수
관심분야 : 컴퓨터 통신, ISDN, 위성 통신, EDI

기반 기술 WORKSHOP 논문집, pp.83-94, 1992.

8. 김정회, 김태윤, "전자식 문서 교환(EDI)의 보안과 통제관리", 통신정보보호학회지, 제 1 권, 제 3 호, pp.99-108, 1991.

9. 남길현, "암호시스템을 이용한 디지탈 서명 시스템", 통신정보보호학회지, 제 1 권, 제 1 호, pp. 64-71, 1991.

10. 임용진, 이강무, 고홍기, 나종근, 김동규, "EDI 시스템의 안전성 서비스 구현 방안에 관한 연구", 통신정보보호학회 학술발표논문집, pp.153-164, 1992.

□ 著者紹介

趙 光 門

고려대학교 전산과학과 졸업(학사)
고려대학교 전산과학과 석사
현 재 : 고려대학교 전산과학과 박사과정
관심분야 : 컴퓨터 통신 보안, 이동 통신, EDI

金 泰 潤

고려대학교 산업공학과 졸업(학사)
미국 Wayne State University 석사
미국 Auburn University 박사
현 재 : 고려대학교 전산과학과 교수
관심분야 : 컴퓨터 통신, ISDN, 위성 통신, EDI