□ 기술해설 □

CALS 표준에 따른 EDI 보안

한국무역정보통신 이경상*

목 차

1. CALS 표준과 EDI

CALS는 세계의 모든 기업을 연결하는 네트워크이며, 표준 규격으로서의 역할을 하게 될 것이다. 각국의 기업이 상호간에 정보를 교환하기 위해서는 반드시 ISO 9000 과 같은 국제적으로 통일된 표준이 필요하며 그 역할을 CALS가 담당할 것이다. CALS는 ISO및 다양한 분야에서 제정된 규격을 많은 부분에서 채택하고 있는데, 그중에는 EDI의 데이타 표준인 EDIFACT도 있다. EDI는 정형화된 문서 중심으로 사용되고 있고 이로 인해 CAD와 같은 도면이나 비정형화된 그래픽 정보를 수용하지 못하는 제약을 가지고 있다.

초고속 정보망의 구축과 멀티미디어 급속한 보급은 EDI에도 비정형화된 그래픽이나 이미지 정보를 교환할 수 있는 기능의 제공이 요구되고 있다. CALS에서는 다양한 표준(SGML, CGM, STEP, CCITT G4 등)을 통해 비정형화된 문서의 교환을 위한 표준들을 제정하여 활용하고 있다. 따라서 CALS 표준의 한 분야로 EDI를 확대 적용하여 비정형화된 문서의 교환이 가능한 체제로 발전시킬 수 있을 것이다.

CALS에서의 보안은 EDI에서와 마찬가지로 통신망을 통해 메시지를 거래당사자간에 주고받아야 하는 만큼 전송 과정에서 발생하는 자료의 삭제, 분실, 변조를 방지하고, 컴퓨터 시스템에 저장된 데이타의 불법적인 변조 및 파괴를 방지할 수 있는 보안체계가 필요하다.

2. EDI 보안요소

EDI 메시지는 기업 또는 거래처간에 서류로 된 문서대신 교환되는 전자문서로 컴퓨터를 매개체로 송수신할 때 EDI 메시지의 송신 및 수신에 대한 확인(Confirmation of Message), 동일한 메시지를 수신했다는 증거(Receipt of an equvalent Message), 메시지 내용에 대한 부인 봉쇄(Non-Repudiation of Content), 및 법적 구속력(legal binding) 등의 보안 기능이 요구된다. 따라서 이러한 보안요구와 관련된 EDI 보안서비스를 살펴보기로 한다.

* 종신회원

2.1 EDI 네트워크 및 통신

EDI 메시지를 교환하기 위해서는 거래 당사자간에 적당한 통신 수단이 필요하다. 대부분 공중교환망을 사용해서 거래 당사간에 EDI 메시지를 직접교환 하거나, 신뢰할 수 있는 Third Party를 사용한다. Third Party는 자사의 통신망에 연결된 고객에게 보안의 적절함을 확신시켜야 한다. EDI 메시지 중계를 위해 대부분의 third party가 사용하고 있는 중계 시스템인 MHS에서 지원하는 주요 보안서비스들에 대해 살펴보기로 한다.

■ **접근제어(Access Control)**

대다수 EDI 사용자의 주요 관심은 자신의 EDI 메시지가 허가되지 않은 타인에 의해 불법적으로 노출될지도 모른다는 우려를 하고 있다. 사용자의 EDI 데이타가 보관된MAILBOX에 대한 접근제어는 고유의 사용자번호(ID)와 비밀번호를 통해서 하게되는데 이을 통해서 허가 받지 않은 사람의 불법적인 접근을 방지한다. 또한 Third Party 통신망에서의 MAILBOX간 문서의 흐름은 ID와 허가된 데이타 화일들을 사용해서 통제되며 모든 데이타는 third party에 의해 관리된다.

■ **메시지 내용의 무결성(Message content Integrity)**

송신자와 수신자간에 EDI 메시지가 교환되는 과정중에 메시지의 내용이 변조되지 않도록 하는 서비스로 주로 메시지 내부에 변조여부를 확인할 수 있는 인증코드를 삽입하는 방법을 주로 사용한다. 일반적으로 EDI 시스템에서는 메시지의 무결성을 보장하기 위한 방법으로 사용자 인증을 함께 할 수 있는 디지탈서명(Digital Signature)을 요구한다.

■ **메시지 순차의 무결성(Message Sequence Integrity)**

메시지 유실 또는 불법적인 복제/추가/삭제를 방지하기 위한 차원의 보안서비스로 메시지 순차번호(Message Sequence Number) 또는 Time Stamp로 해결될 수 있으며, Third Party의 메시지 전송 현황 서비스의 일환으로 제공되며 추후 거래 당사자들간의 분쟁이 발생할 경우 이를 해결할 수 있는 증거 자료로 활용이 가능하다.

■ **대등객체인증(Peer Entity Authentication)**

서로 신분이 확인된 거래상대방간에만 통신을 해주는 메시지 경로 서비스에 해당한다. 주로 Third Party에 의해 제공되는 서비스이나, 공개키 암호화 방식에 기반을 둔 디지탈 서명을 사용할 경우에는 거래당사자 시스템간에 직접 상호 신분을 확인할 수도 있다.

■ **EDI를 위해 확장이 필요한 보안서비스**

기존의 MHS가 제공하는 보안 서비스로도 EDI 메시지를 보호할 수는 있지만 많은 분야에서 MHS가 제공하는 기능에 추가적인 보안서비스 기능을 요구하는 것이 일반적인 추세이며 다음의 내용들이 추가적으로 제공되어야 한다.

- Proof of EDI Notification : EDI 통지의 수신자에게 해당 EDI 통지의 송신처에 대한 증명
- Non-Repudiation of EDI Notificaton : 송신한 메시지가 정당한 수신자에게 배달 되었는지의 여부를 알려주며, EDI 통지의 송신자가 송신 사실을 거짓으로 부인하는 것을 방지
- Proof of content received : 수신자에 의해 수신된 EDI 메시지의 내용이 송신자가 보낸 메시지의 그것과 동일하다는 증거 제공
- Non-Repudiation of content recieved : 수신자가 메시지 수신 사실을 거짓으로 부인하려는 시도를 막을 수 있는 기능을 제공
- Non-Repudiation of content originated : 수신된 메시지의 내용이 송신자에 의해 송신된 메시지의 내용과 동일다는 것을 EDI 메시지의 수신자에게 제공해야 한다. 이럴 경우 송신자에 의한 메시지 송신사실 부인을 방지할 수 있다.

2.2 EDI Application

EDI application 통제는 EDI 거래의 입력, 처리, 출력 및 내부 시스템에서 다른 시스템으로 데이타를 옮기는 interface를 관리한다. 입력에서의 통제는 데이타의 엔트리, 검증, 에러처리 등이며, 가장 적절한 통제의 예는 사용자 ID와 비밀번호를 가지고 입력의 권한이 있는지의 여부를 가리는 방법이다. 처리과정에서의

통제는 합법적인 데이타가 처리될 수 있도록 확증할 수 있는 프로그램의 형태로 구축되어야만 하며, 처리과정에서 정확하게 레코드와 화일이 읽히고 변경되도록 한다. 출력의 통제는 일반적으로 자료의 대사, 출력물의 배포, 레코드의 보존, 및 출력에러를 포함한다. 특히 EDI에서의 거래내용에 대한 대사는 모든 거래가 정상적으로 처리되었는지를 확인할 것을 요구한다.

2.3 EDI 자료보존

EDI 자료의 보존 및 유지는 보편적인 종이기반(paper-based) 시스템에서의 보존이나 유지와 유사하다. EDI에서의 주된 관심사는 보존 및 유지되는 전자 레코드(electronic record)의 신뢰성과 전자 레코드들이 존재하는 환경과 기능들이 레코드의 무결성(integrity) 이 보장되는냐 하는 것이다.

비효율적인 레코도들의 보존으로 부터 초래된 노출(Exposure)은 단순히 기억용량에 따른 비용 이상의 많은 의미를 내포한다. 연산에 치명적인 화일들을 잃어버렸을 때, 그 결과는 반드시 조직에서 임시적인 shut-down과 같이 간단하지만은 않다. 그 손실은 그 화일을 기다리는 거래상대방의 연산에 또한 영향을 미칠 것이다. 사실상 전체적인 EDI 사업 싸이클이 분열될 수도 있다. 모든 정보 시스템들은 치명적인 정보의 불승인된 조작, 손실, 폭로등이 초래될 수 있는 취약한 부분을 가지고 있다. 노출이 가지는 특별한 위험은 EDI 레코드의 관리를 third party에 위임하는데 있다.

2.4 EDI Audit

조직에서 제3자에게 독립된 견해를 제공하는 의무를 수행할때 감사자들은 특별히 EDI와 관련된 몇가지 문제와 직면하게 되는데, 종이없는 환경하에서 실명적인 접근이 여전히 적절한가? 내장된 audit 모듈이 통제기능을 위해 계속적으로 필요한가? 어떤 EDI 레코드가 보관되고, 어떤 형태로 보관되는가? 거래상대방끼리는 단지 상호신뢰에만 의존해야 하는가? 감사자들이 예외 리포트만 조사하고 간단한 거래에 대해 컴퓨터와 수작업의 계산 결과만 비교한다는 것은 충분치 않으므로 EDI환경하에서 감사자들은 다음의 몇가지 요소를 고려해야 한다.

■ EDI 통제 고려사항

- computer 전체를 감사한다는 것은 더이상 효과적이지 않다.
- 좋은 시스템은 실제적인 테스트 보다는 효과적인 통제에 좌우된다.
- 통제 실패는 접근할 수 없는 결과를 초래한다.
- 우발적 사고에 대한 계획이 가장 높은 우선순위를 가져야 한다.
- 보존 정책과 법률적 요구사항이 고려되어야 한다.

■ 통제에 따른 EDI 영향

- EDI는 전통적인 audit trail을 변화시킨다.
- 보다 적은 인력 투입은 전자레코드의 100 % 검사를 허용하는 자동화된 audit program을 요구한다.
- 시스템의 정지는 비지니스 순환에서 모든 거래상대방에게 영향을 미칠수 있다.
- EDI시스템은 회사의 우발적인 재난 대비 계획에 포함되어야 한다.
- 전자서류는 반드시 보호되어져야 한다.

3. EDI 관련 암호화 방법

EDI 보안은 암호학이라는 자연과학의 한분야로 부터 얻어진 기술을 사용해서 구현하고 있다. 암호화 기술을 사용하는 시스템은 송신자가 메시지를 암호화해서 수신자에게 메시지를 전송할 수 있으며, 수신자만이 수신한 메시지를 복호화 할 수 있도록 확신할 수 있어야 한다. 그러한 과정은 그림 1에 자세히 나타난다.

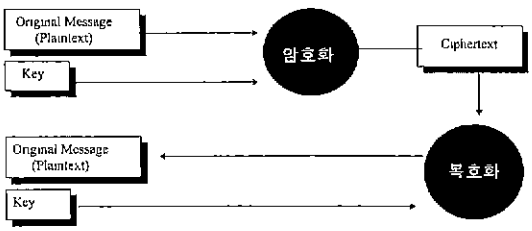

그림 1 암호화시스템

송신자는 cipher 또는 알고리즘이라 불리는 특정 방법을 사용하며, 키와 평문(plaintext)을 결합해서 ciphertext를 만들어 낸다. Ciphertext는 그용어가 나타내는 바와 같이 알아볼 수 없도록 되어 있으며 Third Party도 그 내용을 알 수 없다. 수신자는 송신자의 정반대 과정을 거쳐 본래 메시지를 재생해 낸다.

3.1 비밀키 암호화(Secret Key Cryptosystem)

비밀키 시스템은 송신자와 수신자 모두가 동일키를 가지며, 가장 일반적으로 사용되고 가장 안전한 방법은 DES(Data Encryption Standard)알고리즘이다. 비밀키는 반드시 유일해야 하며, 반드시 송신자와 수신자만 알고 있어야 한다. 그리고 이 비밀키는 모든 거래상대방간에 필요하다. 이것은 두 가지의 문제를 안고 있는데, 첫째는 거래상대방의 수가 매우 많은 경우 수많은 키를 안전하게 보관해야 하는 문제가 발생하게 된다. 둘째로 거래 관계가 성립될 때, 생성된 키를 거래상대방에게 안전하게 전달하는 방법을 찾아야만 하는 문제가 있다.

3.2 공개키 암호화(Public Key Cryptosystem)

공개키 또는 비대칭형 암호화 시스템에서 각 거래상대방은 한쌍으로 된 키를 가지며, 하나의 키는 한쪽 상대방에게는 비밀키로 그리고 또 다른 키는 공개키로 모든 다른 거래상대방에게 공개된다.

송신자는 수신자의 공개키를 사용하여 한 메시지를 암호화 한다음 그것을 전송한다. 많은 상대방이 수신자의 공개키를 알고 있을 지도 모른다. 그중에는 수신자의 공개키를 공격하려는 의도를 가진 자도 있을 수 있다. 공개키 알고리즘에서 하나의 키는 메시지를 암호화 하기 위해 일단 사용되면 동일키를 해당 메시지를 복호화 하기 위해 사용될 수 없다. 해당 메시지를 복호화 할 수 있는 유일한 키는 암호화 하기 위해 사용한 키와 관련된 키가 된다. RSA(Rivest Shamir Adleman) 알고리즘이 가장 일반적으로 사용되는 비대칭형 알고리즘이며 EDI 공개키 보안을 위한 사실상의 표준이 되어 왔다.

RSA 알고리즘은 많은 컴퓨터 계산을 요구하며 이런 이유로 인해 해쉬라 불리는 부가적인 단계가 수행되며, 해쉬는 짧고 고정된 길이의 값을 갖는 메시지 내용을 변환한다. RSA 알고리즘을 사용하는 전자서명과 검증과정은 그림 2와 같다.

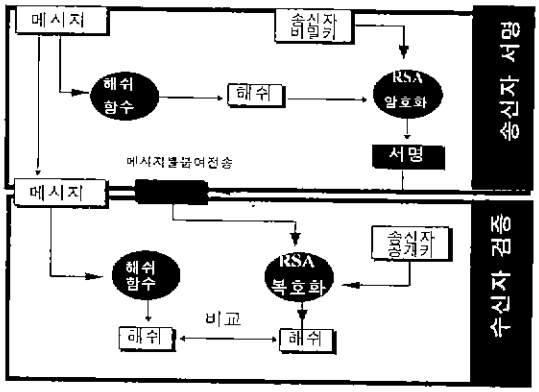

그림 2 RSA의 서명 및 검증과정

3.3 키관리(Key Management)

보안 시스템은 키의 관리를 통해서 시스템의 안전을 보증할 수 있다. 따라서 안전하게 키를 생성하고 보관하고 분배하는 것이 필요한 데 이것이 키관리이다. 키는 랜덤한 방법으로 생성되며 한 거래상대방에게 동일키가 주어질 확률은 거의 없다. 일단 키가 생성되면 키는 안전하게 보관되어야만 하며 이것은 마스타 키를 가지고 키 자체를 암호화 함으로써 달성된다.

대칭키 암호화 시스템에서 키는 거래상대방에게 가장 안전한 방법으로 전달되어야 하는데, 키를 전달 받는 거래상대방은 키의 송신자와 그것의 무결성이 보장되어야 하며, 키는 전송중에 기밀성이 유지되어야 한다. 비대칭키 암호화 시스템에서 비밀키는 이느 누구에게도 노출해서는 안되며 각 거래상대방에게 공개키를 전송해야만 한다. 그림3은 키관리의 과정을 보여준다.

4. EDI 보안의 취약점

현재 적용되고 있는 EDI보안체계 및 제어시

거래당사자 A	거래당사자 B
Generate DES local master key(LMK)	Generate DES LMK
Generate RSA key pair	Generate RSA key pair
Encrypt key pair with LMK and store	Encrypt key pair with LMK and store
Generate DES key encrypting key(KEK) for 거래당사자 B	
Encrypt KEK with LMK and store	
Transport KEK to B by secure route	Receive KEK, encrypt with LMK and store
Transmit public key to B encrypted with KEK	Decrypt A's public key, encrypt with LMK and store
Encrypt B's public key, encrypt with LMK and store	Transmit public key to A, encrypted with KEK
	Generate key pair for additional authoring user
	Encrypt with LMK and store
Receive public key of B's new user, decrypt. encrypt with LMK and store	
	Transmit public key of new user to A, encrypt with KEK

그림 3 키관리 절차

스템은 매우 취약하며, 특히 Third Party를 통해 EDI 메시지를 거래하는 거래상대방은 서로 어느정도의 정보노출 위험을 가지고 있다. 이러한 위험은 EDI시스템간에 존재하는 제어결핍(Major Control Deficiency)을 의미한다. 이는 기술적인 문제이거나 부주의한 사업방법 또는 관리방법에 기인한다. 특히 보안정보를 한곳에서 집중적으로 관리하는 통신망은 주요 해킹의 대상이 될 수 있기 때문에 매우 심각한 고려가 있어야 한다. 가까운 장래에 없어질 것이라 생각되지만, 이런 형태로 관리되는 Third Party 통신망 중에서도 EDI를 사용하는 통신망은 사용을 재고해 볼만한 가치가 충분히 있다.

4.1 불확실한 법적 제문제

일반적으로 EDI라고 하면 표준화된 기업간 거래서식(주문서,송장 등)또는 기업과 행정관청사이의 행정서식(수출신고서 등)을 합의된 통신표준에 따라 컴퓨터간에 교환하는 전자문서 교환방식을 말한다. 즉 일정한 형태로 포맷된 명료한 내용의 상거래/행정 관련정보를 당사자 전체가 합의한 문법(protocol)에 맞추어 상호전송하는 시스템을 의미한다.

종이서류가 가지고 있는 내용확인 및 증거 또는 권리의 유통성(유가증권의 경우)등의 기능을 전자적으로 처리하게 되는 것이며, 한번 입력한 내용이 권한 있는 자에 의해 특별히 바뀌어지지 않는 한 모든 과정에서 두루 쓰이므로 재입력할 필요도 없게된다. 그러나 종래의 종이서류를 전자문서로 그 형태를 전환함에 따라 법적 효력을 부여키 위한 기존의 인증(도장이나 서명) 방법은 EDI에서는 그 기능을 상실하게 되는데, 전자문서에서는 어떻게 이 인증문제를 해결할 것인지가 의문시된다. 기존 상거래 관련 법령에서 종이로 된 서류를 요구할 경우에는 이를 어떻게 받아들일 것인가의 문제, 즉 전자문서에도 기존의 종이서류와 같은 법적 구속력이 인정될 것인지도 살펴보아야 한다.

또 당사자들간에 분쟁이 발생하여 소송이 진

행되었을 때에 전자문서가 증거법상 그 증거능력이 인정될 수 있을 것인가도 중요한 문제이다. 당사자들이 텔렉스나 우편제도 또는 전자매체를 활용해 오던 종래의 거래와는 달리 EDI 방식에서는 통신도중 에러가 발생할 수 있는데, 이 경우 손해가 발생하였다면 누구의 책임으로 할 것인가도 중요한 문제이다. 또 계약과 관련하여 의사표시의 효력 발생시기 등을 증명해야 할 필요성이 있을 경우 이를 어떻게 정해야 할 것인가도 고려해야 한다.

4.2 EDI 보안구조의 한계

4.2.1 MAC(Message Authentication Coding)의 한계

MAC은 주로 메시지의 송신자를 확인하기 위하여 사용된다. 그러나 원래 MAC은 메시지의 Integrity를 보장하기 위한 목적으로 설계된 것이고 메시지의 송신자 확인용이 아니다. 따라서 이는 명백하게 잘못 적용한 것이라고 할 수 있을 것이다.

4.2.2 대칭키 암호화(Symmetrical Key Cryptography)의 한계

현재 EDI에서는 주로 대칭키 암호화 방법이 사용되고 있다. 대칭키 암호화란 언제 어디서라도 같은 키를 가지고 암호화하면 같은 암호문서가 작성되는 암호기법이다. 이러한 경우에는 충분한 시간만 가지고 있다면 암호화된 문서를 어렵지 않게 해독할 수 있다. DEA(Data Encryption Algorithm)은 ANSI의 DES (Data Encryption Standard)에 기반한 것이며 현재 EDI분야에서 널리 사용되는 알고리즘이다. 여기서는 64bit 키를 사용하는데 이는 70년대 중반에 만들어진 것이며, 그때의 컴퓨팅 파워로는 64bit를 모두 테스트하는 데 엄청난 시간이 걸렸지만 지금은 값싸고, 빠른 마이크로프로세서의 등장으로 그 해독시간이 매우 크게 단축되었다. 따라서 128bit키를 사용하는 방법등이 고려되어야 한다.

4.2.3 공개키 암호화(Public-Key Cryptography)의 한계

EDI에서 사용되는 MAC는 비밀키 암호화(Secret-Key Cryptocraphy)를 이루는 한 요소이다. 이 비밀키 암호화는 매우 한정된 수의 거래자와의 자료거래에 사용되는 것이며, EDI가 무역정보를 공용화 하려는 야심을 가지고 있는한 계속 사용되기에는 어려운 점이 있다. 공개키 암호화의 방법으로는 RSA가 많이 사용되는데, 이러한 알고리즘은 아직까지의 컴퓨팅 환경에서는 관리적인 부분과 프로세서의 성능부족등의 문제를 가지고 있다. 또한 대량의 메시를 교환해야 하는 환경에서는 전통적인 DEA-protected 메시지의 처리를 RSA가 쉽게 대치할 수 없을 것이다.

4.3 공유되는 표준들의 한계

표준이라는 것은 위험을 줄이고 불확실성을 없애기 위하여 만들어진다. 그러나 EDI표준에서는 꼭 그렇다고 볼 수 만은 없다. 표준을 정하는 데는 유연성과 확실성을 동시에 추구하기 때문에 모순이 있고, 또한 많은 이견과 불일치가 존재한다. 이러한 표준화의 장벽 때문에 EDI 거래자들은 다음과 같은 위험에 항상 노출되어 있다.

- 표준화기구가 새로운 표준을 정하여, 거래자들간의 합의가 위험에 처할 수 있다.
- 비용이 많이드는 표준변환 작업이 필요하며, 이는 피할 수 있는 것이 아니다.
- 계속 변화하는 표준은 상호운용성(Interoperability)를 보장하지 못한다.
- 국제표준은 특정한 국가의 특정한 사업에서 나타나는 다양성을 반영하기 어렵다.

5. EDI Interchange에서의 보안

5.1 UN/EDIFACT

UN/EDIFACT을 위한 보안 표준은 현재 개발중이며, 접근 방법은 대략 다음과 같다. EDIFACT에서 전송 단위는 interchange이며 이것은 하나 이상의 메시지를, 즉 functional group을 포함한다. 메시지는 segment로 구성되며, 특별한 segment가 interchange, functional group 및 메시지를 구별한다. 보안은 Header와 Trailer segmant 전후에 위치한 보안 segment에 의해 제공된다. 그림 4는

보 안 요 구	해 결 방 법
기밀성(Confidentiality)	RSA의 암호화된 키를 사용한 DES함호화 알고리즘
메시지 내용 무결성 (Message content Integrity)	DES 기반의 MAC 또는 RSA 전자서명
메시지 순차 무결성 (Messaage sequence Integrity)	일련번호 및 Time Stemp 사용 MAC 및 전자서명, ACK 사용
송신자의 인증 (Authentication of Origin)	MAC 또는 전자서명
송신자의 부인봉쇄 (Non-Repudiation of Origin)	전자서명
수신자의 부인봉쇄 (Non-Repudiation of recipt)	전자서명
사용자 인증 (Authenticaion of users)	PIN-secured 스마트카드(사용자관련 정보 및 암호화 키등 포함)

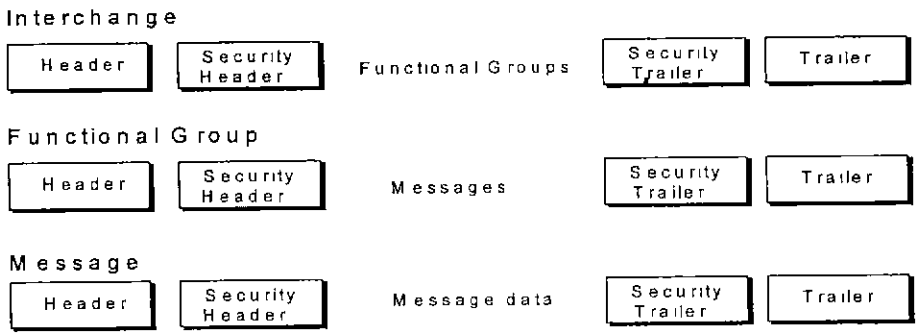

그림 4 EDIFACT에서의 보안

EDIFACT에서의 보안요구 및 해결방법을 나타낸다.

5.2 ANSI X12

ANSI X12 interchange format표준은 복잡한 보안구조를 가지는 방법으로 이끌어져 왔다. ANSI X12 interchange는 이중으로 끼워진 구조로 그림 5에 보여진 바와 같이 연속된 일련의 데이타 segment들로 구성되어 있다. 하나의 interchange는 하나 이상의 기능군을 포함하며, 각각은 관련된 상업서식의 집합을 대표한다. 하나의 기능군은 하나 이상의 Transaction set을 포함하고 있으며, 각각은 하나의 상업서식을 나타낸다.

ANSI X12.58표준은 functional group 및 transaction set 모두에서 보안기능이 어떻게 제공되어질 수 있는지 기술하고 있다. 제공된 보안 서비스는 데이타 송신자 인증(Data Origin Authentication), 기밀성(Confidentiality), 및 무결성(Integrity)이며, 이를 지원하는 보안 기술은ANSI X9.9 및 ANSI X9.23에서 도입된 DES를 기반으로 하는 암호화 기법이나 MAC (Message Authentication Code)를 사용한다.

ANSI X12.58은 functional group 및 transaction group에 삽입될 보안 segment를 정의한다. 그림 5에서 나타난 바와 같이 이들 보안 segment는 키 구분자와 초기 벡터 및 MAC 같은 데이타를 연결한다. 또한 ANSI X12.58은 Time Stamp 및 전자서명(Digital Signature)와 같은 요소를 포함하는 assurance seg-

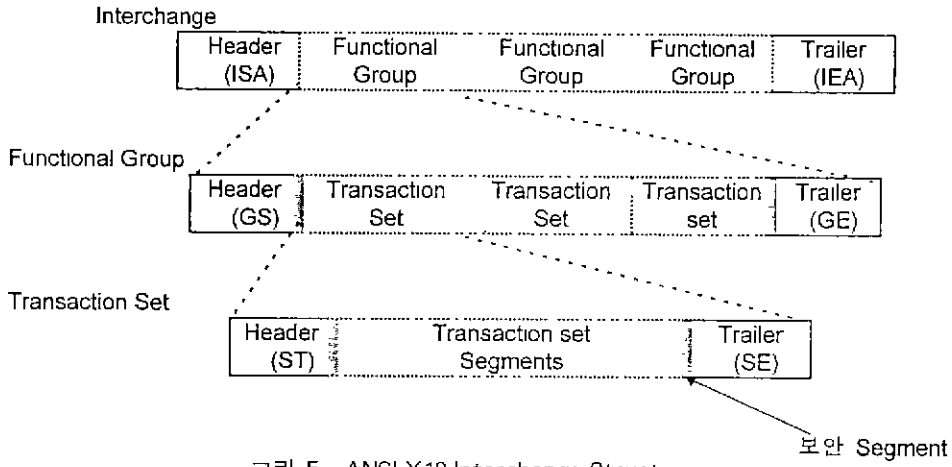

그림 5 ANSI X12 Interchange Structure

ment를 포함하도록 확장된다.

기업표준인 ANSI X12.42는 암호화 서비스 메시지 transaction set을 정의하고, EDI 시스템간에 키 정보의 전송을 지원할 수 있도록 설계되었다. ANSI X12.42는 ANSI X9.17을 기반으로 하며 ANSI X12 구문에서의 X9.17 암호화 서비스 메시지를 연결하는 표준수단을 효과적으로 지원한다.

6. EDI가 지향하는 보안서비스

EDI는 다양한 통신기술-전용선, Dial-UP, Packet 교환, ATM, Frame Relay-서비스를 전자문서의 거래를 위해 사용할 수 있다. MHS는 EDI를 위한 적합한 통신 기술중의 하나이며, 중요한 보안 기능들을 제공하고 있으나, 데이타에 대한 위장접근, 메시지의 분실, 메시지 내용의 변조, 거래사실의 부인등에 대한 대처가 미흡한 것이 사실이다.

1990년에 ITU-T 권고안인 F.435 및 X.435이 발표되었고 권고안은 MHS 백본 위에 EDI interchange를 전송할 수 있는 MHS 표준을 확장한 내용을 담고 있다. 확장된 권고안은 기존 MHS 프로토콜(p1, p3, p7)을 변경하지 않고 새로운 프로토콜인 P35 및 P_{edi}를 추가로 정의하였다.

Application으로서 EDI는 E-MAIL등의 데이타보다는 더욱 엄격한 보안이 유지되고 보호되어야만 한다. 불법적이거나 사고에 의한 거래내용의 변조, 거래사실에 대한 부인으로부터의 보호는 종이를 기반으로 하는 시스템을 대체하는 EDI 시스템의 가장 기본적인 기능이다. 따라서 EDI가 지향해야할 보안서비스는 X.435를 기반으로 이루어져야 할 것으로 생각된다.

참고문헌

[1] Ian Walden and Ashley Braganaza, DI Audit and Control pp 102-111, NCC Blackwell,1993.

[2] Warwick Ford, Computer Communications Security, Principles Standard Protocols and Techniques, pp 359-365, Prentice Hall PTR, 1994.

[3] Albert J. Marcella, Jr. and Sally Chan, EDI Security Control and Audit, pp43-55, 95-102, 123-125, Artech House, 1993.

[4] 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] Peter Landrock, Protecting Your EDI Message, Proceedings of the 3rd International Congress of EDI Users, 1991.

[6] 윤성현, 부인봉쇄 기능을 강화한 EDI 메시지

디지탈 다중 서명 방식, 한국정보과학회 논문지, VOL 21, NO. 6, 1994.
[7] 김은상, 전략경영 & EDI, 매일경제신문사, pp 129-131, 1994.
[8] 김철환, 김규수. 21세기정보화 산업혁명 CALS, 도서출판 문원, pp 47-60, 1995.

이 경 상

1976 미국 웨인 주립대학 전기공학 (학사)
1980 미국 웨인 주립대학 전산학 (석사)
1977～1983 Michigan Bell Telephone Co. 선임연구원
1983～1985 Ameritech Service Inc. 선임연구원
1985～1987 한국데이타통신(현 데이콤) 부장
1987～1989 대신전신센타 대표이사
1989～1992 일진전지/전기 이사(연구소장겸임)
1992～현 재 한국무역정보통신 이사(EDI 시스템연구소 소장)
기타 : 1981～1983 미국 웨인 주립대학 전산학 강사
1985 Central Texas College 전산학 교수
1987～1989 고려대학 전산학 강사
1990～1991 서강대학 전산학 강사
1995～현재 건설공제조합 전산고문