特輯

EDI 보호(Security)

鄭 鎭 旭
成均館大學校 情報工學科

Ⅰ. 서 론

EDI는 기업간 거래에 필요한 정형화된 자료를 규격화된 양식으로 네트워크를 통해 컴퓨터 또는 응용프로그램간에 데이타를 교환하는 것을 의미한다. 즉, EDI란 기업 및 관련기관의 거래당사자가 의도하는 거래를 수행할 수 있도록 "표준 포맷"으로 된 "표준화된 기업간 거래문서"를 컴퓨터 대 컴퓨터 통신방식으로 교환하는 것을 말한다. 그래서 EDI는 CCITT 메시지 통신처리시스템인 X.400 프로토콜을 이용해서도 어느 정도 EDI서비스를 지원할 수 있지만 메시지의 책임(responsibility), 책임회송(forwarding), 보안(security) 등의 서비스는 X.400 프로토콜만으로는 지원할 수가 없다. 따라서 CCITT에서는 1990년 그림1과 같은 EDI 메시지 환경에 관련된 EDI서비스 지원규약인 X.435와 F.435 권고안을 발표하였다. CCITT의 EDI 메시징시스템(EDIMS:EDI Messaging System) 표준규약인 X.435 권고안에서는 새로운 형태의 메시지, 즉, EDI메시지 구조를 위한 프로토콜로 Pedi를 규정하였고, F.435에서는 EDI서비스를 규정하고 있다.

무역, 유통, 운송 등 각 분야에서 EDI를 이용함에 있어서 반드시 해결해야 될 과제가 보안문제이다. 즉, 어떤 물량이 주문되었을 때, 그 주문에 대한 진위 여부의 확인이나 전달과정에서의 변조 및 누락이 없었는지, 또는 주문자가 나중에 주문사실을 부인하지 못하게 하는 조치라든가 중요한 거래 내용의 제3자로의 누설 방지 등의 보안이 해결되지 않으면 EDI의 광범위한 이용은 불가능하게 될 것이다. 왜냐하면, EDI상에서 거래되는 모든 문서는 실제 각 기업의 이익과 바로 직결되는 중요한 서류들이기 때문이다.

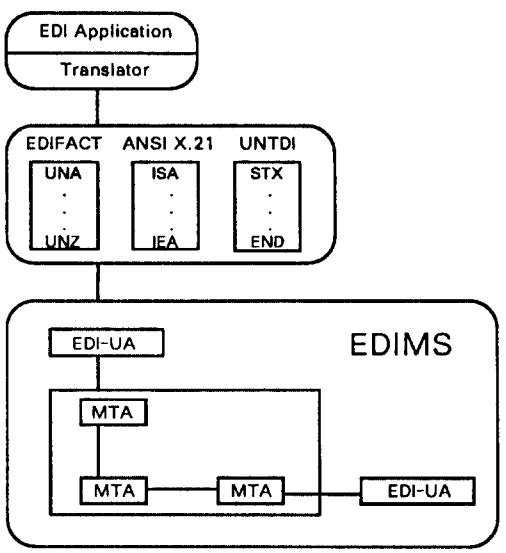


그림 1. EDI 메시지 환경

본 고에서는 EDI 보안의 위협요소와 이에 대한 대응책인 EDI 보안서비스 중 시급히 구현되어야 할 서비스에 대해 그 메카니즘을 분석하고 이를 구현한 결과를 살펴봄으로써, 향후 본격적인 EDI 보안서비스 구현시 참고모델로서 이용할 수 있도록 하였다.

Ⅱ. EDI 보안구조

1. 보안구조 모델

보안구조는 특정한 개방형 시스템 구조의 문맥에

각 영역의 기능들이 어떻게 적용될 수 있는가를 다루며, 개방형 시스템의 보안에 대하여 통일된 관점 제공을 목적으로 개발되고 있다. 또한 시스템과 시스템의 객체들을 보호하는 방법의 정의와 시스템간의 상호작용에 관련된다. 즉, 특정한 보안서비스를 제공하기 위한 데이타요소와 동작의 순서를 다룬다.

현재 보안 서비스들은 OSI 보안 구조에서 제안된 두 세개의 일반적인 보안서비스로 제한되어 있으며, 이들은 각각의 SASE마다 구현되어 있음으로 인해 보안서비스의 중복이 발생한다. 그래서 이런 중복성을 제거하자는 의미에서 제안된 것이 SCSE(Secure Communication Service Element) 모델이었다. SCSE 모델은 응용계층에서 공통적으로 요구되는 보안서비스를 하나의 SCSE로 만들어 놓은 것이다.

1) SCSE의 구성도

SCSE 모델은 공통적으로 요구되는 보안서비스를 제공하기 위한 세개의 Facility 즉, 인증서비스를 제공하는 AF(Authentication Facility), 데이타 무결성 서비스를 제공하는 IF(Integrity Facility), 그리고 데이타 비밀성 서비스를 제공하는 CF(Confidentiality Facility)와 이 모듈에 관련된 정보를 유지하는 SMIB로 구성되었다. 그림 2는 이러한 SCSE의 내부 구조를 도시하고 있다.

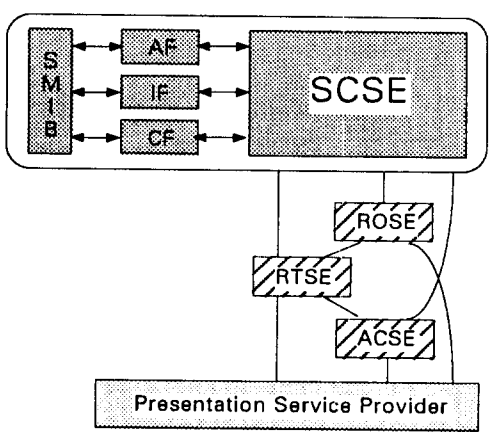


그림 2. SCSE 내부구조

2) SCSE 구성요소의 기능

① AF(Authentication Facility)

접속지향 통신에서 통신관련자에 대한 인증을 하고 해당 통신에 참여할 자격을 검사하는 Facility이다. 동위실체의 신뢰성있는 접속의 확립이나 데이타전송의 과정에서 수행되는 동위실체 인증서비스를 제공해주는 부분으로서 식별검사나 암호화기능을 수행한다. 즉, 동위실체인증과 같은 서비스요소를 지원할 수 있다.

② IF(Integrity Facility)

전송되는 데이타의 무결성을 점검하는 무결성 서비스를 제공하는 Facility로서 메시지인증코드를 이용하여 무결성을 검사하고 데이타의 순서를 검사한다. 무결성은 내용의 무결성을 점검하는 내용무결성(Content Integrity)과 전송되는 전문의 순서를 점검하는 순서무결성(Sequence Integrity)으로 나누어진다. 즉, 접속 무결성과 같은 서비스요소를 지원할 수 있다.

③ CF(Confidentiality Facility)

통신되는 데이타가 불법적으로 내용이 노출되는 것을 방지하는 데이타 비밀성 서비스를 제공하는 Facility로서 암호화 메카니즘을 사용하여 전송되는 데이타의 내용을 감출 수 있다. 즉, 접속 비밀성과 같은 서비스요소를 지원할 수 있다.

④ SMIB(Secure Management Information Base)

SMIB(Secure Management Information Base)는 보안구조에서 Facility들이 각각의 해당되는 서비스를 제공하기 위해 필요한 암호화 알고리즘, 암호화 동작 모드, 암호화 키이, 초기벡터 등의 정보를 유지하는데 사용되도록 국부시스템에 위치시켰다. SMIB에 저장된 정보들은 문맥(Context)단위로 처리되는데 이를 PRC(Protection Context)라 하며 각각의 PRC ID에 의하여 구분되고 관리된다. 이러한 정보들은 각각의 시스템에 있는 국부 SMIB에 동일하게 저장되어야 하므로 OSI 보안관리 프로토콜 등에 의해 관리되어야 한다.

2. EDI보안구조를 위한 방향

응용계층에서는 모든 보안서비스들을 제공해 줄 수 있고 몇몇 특정 서비스는 그 성격상 응용계층에서만 제공가능하므로 현재 보안 표준화 동향을 분석해 볼 때 응용계층에 보안기능을 위치시키는 경향이 있다. EDI는 컴퓨터 네트워크를 통한 전자문서교환 시스템이므로 SCSE의 보안요소들은 기본으로 만족되어야 하며, SCSE 모델에서 처럼 EDI보안을 위한 SE를 SCSE의 상위에 위치시킴으로써 구성할 수 있다. 즉, SCSE 모델을 기반으로 하는 EDI보안 SE는 SCSE

에 포함된 Facility이외에 EDI보안에 특이한 Facility를 추가함으로써 구성할 수도 있다. EDI 보안서비스 중 부인불능에 해당하는 서비스들 즉, 발신지부인불능, 제출부인불능, 배달부인불능, 수신부인불능, 검색부인불능, 전송부인불능, 내용부인불능을 지원하기 위한 Facility 등을 추가하고 이런 Facility를 이용할 수 있는 절차들, 그리고 EDI 보안서비스를 지원하는데 필요한 여러가지 알고리즘이나 메카니즘을 SMIB에 추가하는 방향으로 구성할 수 있을 것이다.

3. EDI 보안 위협요소(Security threats)

EDI는 MHS 환경을 흡수한 시스템으로서 기존의 MHS 시스템이 갖고 있는 위협요소들에 EDI 시스템에서만 발생할 수 있는 특이한 위협요소가 추가되었다. EDI 보안위협요소로는 위장(Masquerade), 메시지 시퀀싱(Message Sequencing), 메시지 분실(Message loss), 정보의 변경(Modification of Information), 서비스의 거절(Denial of Service), 부인(Repudiation), 정보의 누설(Leakage of Information), EDIMG 사용자에 의한 정보의 조작(Manipulation of information by EDIMG user), 그밖의 위협들(Other Threats)이 존재한다. 이러한 위협들은 고의적 혹은 사고에 의해서 일어날 수 있고, 능동적(Active) 또는 수동적(Passive)일 수 있다.

표 1 EDI 보안서비스

서 비 스	
Origin Authentication	Message Origin Authentication Probe Origin Authentication Report Origin Authentication Proof Of Submission Proof Of Delivery
EDIM Responsibility Authentication	Proof of EDI Notification proof of Retrieval Proof of Transfer
Secure Access Management	Peer Entity Authentication Security Context
Data Confidentiality	Connection Confidentiality Content Confidentiality Message Flow Confidentiality
Data Integrity	Connection Integrity Content Integrity Message Sequence Integrity
Non-Repudiation of EDIM Responsibility	Non-repudiation of EDI Notification Non-repudiation of EDI Retrieval Non-repudiation of EDI transfer Non-repudiation of EDI Content
Non-repudiation	Non-repudiation of Origin Non-repudiation of Submission Non-repudiation of EDI Delivery
Message Security Labelling	Message Security Labelling
Security Management	Change Credentails Register MS-Register

또한 둘 이상의 위협들이 복합되어서 일어날 수도 있다. 이러한 위협요소들을 방어하기 의한 보안서비스들은 표1과 같다.

4. EDI 보안서비스(Security Service)

1) 발신처 인증(Origin Authentiction) 보안서비스

발신처 인증보안서비스는 데이타의 발신처와 통신 대등실체의 인증을 제공한다. 일반적으로 EDI 에서의 인증 보안서비스들은 위장(Masquerade)의 위협으로부터 보호하기 위해서 제공되어 질 수 있다. 이러한 위장의 위협을 방지하기 위해 제공되어지는 보안서비스들은 메시지 발신처 인증(Message Origin Authentication), 프로브 발신처 인증(Probe Origin Authentication), 리포트 발신처 인증(Report Origin Authentication), 안전한 접근 관리(Secure Access Management), 배달증명(Proof of Delivery), 제출증명(Proof of Submission) 서비스들이 있다.

2) 안전한 접근 관리(Secure Access Management) 보안서비스

안전한 접근 관리 보안서비스는 자원에 대한 불법적인 사용으로 부터의 보호(Protection)와 관련되고, 대등실체 인증과 보안문맥(Security Context) 보안서비스의 두 개의 요소(Components)로 나누어 질 수 있다. 이 서비스는 위장, 정보의 누설, 그 밖의 위협으로 부터 보호하기 위해서 제공되어진다.

3) 데이타 비밀성(Data Confidentiality) 보안서비스

이 서비스는 불법적인 누설로 부터 데이타를 보호하기 위해서 제공되어진다. 이러한 데이타 비밀성 보안서비스들은 MHS의 정보누설 위협(Leakage of Information Treats)으로 부터 보호하기 위해서 제공되어질 수 있으며, 이러한 정보의 누설 위협으로 부터 보호하기 위해 제공되어지는 보안서비스들은 접속 비밀성(Connection Confidentiality), 내용 비밀성(Content Confidentiality), 메시지 흐름 비밀성(Message Flow Confidentiality), 안전한 접근 관리(Secure Access Management) 서비스들이 있다.

4) 데이타 무결성(Data Integrity) 보안서비스

데이타 무결성 보안서비스는 MHS에 대해서 능동적인 위협을 방지하기 위해서 제공되어진다. 이러한 데이타 무결성 보안서비스들은 메시지 시퀀싱(Message Sequencing), 정보의 변경(Modifi-

cation of Information)위협으로 부터 보호하기 위해 제공되어질 수 있으며, 이 서비스에는 접속 무결성(Connection Integrity), 내용 무결성(Content Integrity), 메시지 순서 무결성(Message Sequence Integrity) 서비스들이 있다.

5) 부인불능 보안서비스(Non-repudiation)

부인불능 보안서비스는 메시지가 제출, 전송, 배달된 후, 제삼자에게 그 메시지의 제출, 전송, 수신한 사실에 대한 부인할 수 없는 증명을 제공한다. 이러한 부인불능 보안서비스는 부인(Repudiation)의 위협으로 부터 보호하기 위해서 제공되어지며, 제공되는 서비스는 발신처 부인불능(Non-repudiation of Origin), 제출 부인불능(Non-repudiation of Submission), 배달 부인불능(Non-repudiation of Delivery) 서비스들이 있다.

6) 메시지 보안 레이블링(Message Security Labelling) 보안서비스

이 서비스는 보안 레이블이 MHS(MTA들과 MTS 사용자)의 모든 실체와 연계되도록 해주고, 메시지 보안 레이블 보안요소에 의해서 제공되어진다. 레이블의 무결성과 비밀성은 메시지 인자 무결성 보안요소와 메시지 인자 비밀성 보안요소에 의해서 제공되어진다.

7) 보안 관리 서비스(Security Management Service)

EDI는 많은 보안 관리 서비스를 필요로 하지만, 여기서는 크리덴셜의 변경과 MTS사용자 보안 레이블링의 등록에만 관계된다. 이러한 보안 관리 서비스는 위장(Masquerade), 정보의 누설(Leakage of Information), 그리고 그밖의 위협들로 부터 보호하기 위해서 제공되어질 수 있고, 이러한 보안 관리 서비스에는 크리덴셜 변경 보안서비스, 등록 보안서비스, MS 등록 보안서비스들이 있다.

8) EDIM 책임 인증/부인불능(EDIM responsibility authentication/Non-Repudiation)

EDIMG 환경내에서 부인(Repudiation)에 대응하는 보호장치를 제공하는 서비스로, EDIM 책임 회송을 형식화(Formalizing)하는 것과 관계된다. 이러한 보안관련 서비스는 다음과 같다.

(1) EDI통지 증명/부인불능(Proof/Nonrepudiation of EDI Notification)

(2) 검색 증명/부인불능(Proof/Non-repudiation of retrieval)

(3) 전송 증명/부인불능(Proof/Non-repudiation of transfer)

Ⅲ. EDI 보안서비스의 설계 및 구현

EDI를 구현하기 위한 통신 수단으로서 주로 MHS 시스템을 사용하고 있으므로 여기서도 1988년의 X.400과 1990년에 EDI를 위해 보완된 X.435를 위주로 하여 보안서비스를 분석하였다.

본 고에서는 향후 국내에서 발생될 위협요소 중 우선적인 보호가 요구되는 것으로서 메시지 노출로 인한 프라이버시 침해 및 중요 내용의 노출 문제와 메시지 수정 문제 및 발신처 인증 문제, 그리고 수신자의 수신사실에 대한 부인을 위협요소로 선정하였다. 또한, 이를 막기 위한 보안서비스로 메시지 발신처 인증(Message Origin Au-thentication)서비스, 내용 비밀성(Content Confidentiality) 서비스, 내용 무결성(Content Integrity) 서비스, EDI 내용 부인불능(Non-repudiation of EDI Content) 서비스를 구현하였다.

1. 구현 메카니즘

1)비밀보장 메카니즘

이 기능은 메시지의 불법 노출로 부터 데이타를 보호하기 위한 것으로, 사용되는 암호 알고리즘은 처리속도를 고려하여 대칭키 암호시스템으로 가장 널리 알려진 DES(Data Encryption Standard) 알고리즘을 채택하였다. 또한 그림 3과 같이 자체 난수(random number)를 발생하여 이 난수를 사용자키(UK)로 이용하도록 하였으며 메시지 전체를 암호화하게 된다.

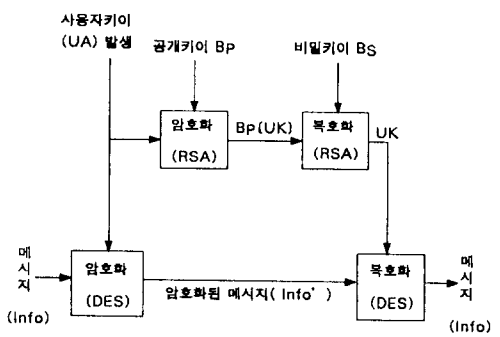


그림 3. 비밀보장 메카니즘

DES와 같은 대칭키 시스템은 비밀키(사용자키)를 반드시 상대방도 가져야 하므로 여기서는 키 관리를 간편하게 하기 위해 송신측에서 사용한 키를 수신측의 공개키를 사용하여 암호화시켜 전송하게 함으로서 수신측에서는 메시지를 암호화한 키를 알거나 보관할 필요가 없게 하였다. 즉, 사용자 키는 수신측 공개키에 의해 암호화되어 전송되며 수신측은 수신측의 비밀키를 이용하여 사용자키를 복호화한 후 이 키를 이용하여 메시지를 복호화하게 한다.

2) 인증 및 무결성 서비스

발신처 인증 서비스는 메시지의 발신자로 부터 보내진다는 것을 보장할 수 있게 한다. 즉, 발신자는 자기만이 알고 있는 비밀키를 사용하여 암호화하는데 이때 다른 어떤 사람도 발신자의 비밀키를 알 수 없다. 그리고 수신측에서는 공개키로서 복호화시킴으로써 발신처를 증명할 수 있게 된다. 그리고 메시지 무결성 서비스는 발신자가 제출한 메시지가 수신자가 수신하기 전 불법 수정이나 변경이 없었다는 것을 보장하기 위한 것이다.이 두 서비스는 X.509의 디지탈서명 메카니즘으로 해결할 수 있다. 이 때 암호화해야 할 메시지의 길이(N)가 클 때 처리 시간이 많이 소요되므로 메시지 길이가 짧은 블럭단위의 길이로 hashing 함수를 수행하여야 하는데 X.509에서는 square-modular 방식을 제시하고 있으나 여기서는 32비트 머신상에서의 효율성과 안전성이 고려된 Rivest의 MD5 Message Digest 메카니즘을 사용하였다. 여기에 사용된 암호 알고리즘은 RSA알고리즘을 이용하였다. 이의 적용 처리 절차는 그림 4와 같다.

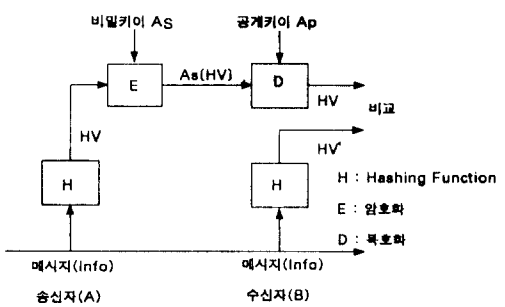


그림 4. 인증 및 무결성 메카니즘

먼저 송신측(A)에서 hashing 함수의 수행에 의해 얻어진 HV를 송신측의 비밀키 As로 서명된 정보(X=As(HV))를 메시지 헤더(header)에 부가하여 수신측에 보내면, 수신측(B)은 서명된 X를 송신측의 공개키 Ap로 복호화시켜 HV를 얻게 된다. 그 다음, 송신측으로 부터 수신된 메시지를 동일한 hashing 함수를 이용하여 HV'를 구하여 송신측으로 부터 수신된 HV의 값을 비교한다. 만약 이 값이 같다면 정당한 발신자에게서 온 것을 보장함과 동시에 변경없이 보내졌다는 것을 보장할 수 있게 된다.

3) 수신내용 부인불능 메카니즘

일상적인 상거래시 성공적인 송신시에도 통신당사자의 부인에 따른 잠재적인 위협요소가 있다. 그 중 하나로서 청구서 및 대금지불 등과 같은 메시지를 받은 수신자가 수신 자체를 부인하고 미수신 claim을 제기하는 행위이다. 이런 위협을 메시지 발신자가 봉쇄하기 위한 것이 바로 수신내용 부인불능(Non-repudiation of receipt) 메카니즘이다. 이 메카니즘을 앞에서 설명한 디지탈서명 메카니즘과 메시지의 사본을 발신자에게 되돌려 보내는 행위를 함께 사용함으로써 해결할 수 있다.

이 수신내용 부인불능은 디지탈서명을 하기 전 송신측의 EDIM(EDI Message) 내 Notification Request 필드에 PN 또는 NN을 요청하고 Notification Security 필드를 proof로 set시키는 제어과정을 먼저 거치게 된다. 그리고 난 다음 그림 5와 같은 디지탈서명 과정을 거친다. 즉, 메시지 내용이 해싱 함수를 거친 후 그 값을 서명하여 자체 로그 화일(Audit)에 수록한 다음 수신측으로 전송한다.

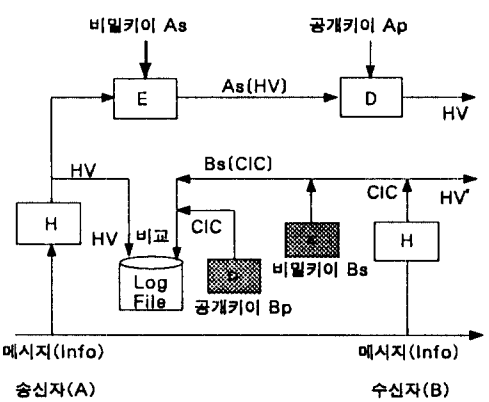


그림 5. 수신내용 부인불능 메카니즘

수신측에서는 수신된 EDIM이 PN 또는 NN으로 set되어 있으면 EDIN을 생성하기 위해 메시지 내용

을 해싱한 결과 값(CIC)을 수신측의 비밀키로 암호화하여 EDIN에 Bs(CIC)를 붙여 발신처로 보낸다. 발신측에서는 수신된 Bs(CIC)를 B측의 공개키로서 복호화시켜 이 메시지 내의 CIC와 이미 로그(Audit) 화일에 수록된 HV의 값을 비교하여 성공적으로 수행되었을 경우 수신측이 내용을 받았다는 것을 확인한 후 로그화일에 이 EDIN을 저장시켜 두고 나중에 문제가 발생시 수신자의 수신 사실에 대한 부인을 봉쇄하는 근거자료로 제시한다.

2. 보안서비스의 구현

앞에서 제시된 보안서비스 구현 메카니즘의 처리 절차를 이용하여 송수신측 사용자들 간에 메시지를 안전하게 주고 받기 위한 4가지 보안서비스를 수행하는 SEP프로토콜을 다음과 같이 정의하였다.(단, 여기서 notification 요청 및 생성과정은 이미 셋팅되어 있다고 가정하였음) 수신 부인불능 서비스시 EDI Notification 요청에 따라 PN과 NN EDIN이 셋팅되어야 하므로 이 서비스를 수행하도록 Control 문을 구현하였다.

1) 송신측 (A)

단계 1 : 일방향 hashing함수를 사용하여 hashing값(HV)을 계산하여 HV 사본을 수신 부인불능 서비스의 지원을 위하여 자신의 로그화일에 저장하고, HV를 A의 비밀키(As)로 다음과 같이 전자서명을 수행한 후,

HV = H(Info)

X = As(HV)

디렉토리시스템내의 CA에게 A와 B의 공개키 certificate를 요청한다.

단계 2 : CA는 CA의 비밀키(CAs)로 서명을 한 certificate를 A에게 보낸다.

CA⟨⟨B⟩⟩ = CAs(AI, CA, T_A, B, Bp)

CA⟨⟨A⟩⟩ = CAs(AI, CA, T_B, A, Ap)

단계 3 : A는 미리 알고 있던 CA의 공개키로서 복호화하여 시간을 조사한 후, B의 공개키(Bp)를 얻는다.

AI, CA, T_A, B, Bp = CAp(CA⟨⟨B⟩⟩)

단계 4 : 난수(UK)를 발생시켜 메시지의 내용을 암호화시킨 후 이 UK를 B의 공개키로 암호화한다.

C = UK(Info)

G = Bp(UK)

단계 5 : 보안에 필요한 데이타를 메시지 내용 위의 Header에 부가시킨 후 MTS로 보냄으로써 송신절차를 완료한다.

단계 6 : 〈수신증명서의 수신 및 부인불능 절차〉

송신자는 자신이 보낸 메시지에 대한 응답으로 수신측에서 송신측으로 보낸 수신증명서내의 Y를 수신자의 공개키 B_P로 복호화하여 B의 CIC를 얻는다.

CIC = Bs(Y)

A는 이 CIC(Content Integrity Check)와 단계 1에서 생성한 HV와 동일하면, 수신측이 내용을 받았다는것을 보장할 수 있고, 후일 B의 수신 사실에 대한 부인을 막기위한 증거물로서 자신의 로그화일에 저장한다.

2) 수신측

단계 1 : 수신측(B)은 미리 알고 있던 CA의 공개키로 A의 certificate를 복호화한다.

AI, CA, T_B, A, Ap = CAp(CA⟨⟨A⟩⟩)

여기서 시간 T_B를 조사하여 이상이 없다면 A의 공개키를 취한다.

단계 2 : A의 공개키를 이용하여 된 X를 복호화한다.

HV = Ap(X)

단계 3 : B의 비밀키로서 암호화된 사용자키 정보(G)를 복호화하고,

UK = Bs(G)

이 UK를 이용하여 암호화된 메시지 내용을 복호화한다.

Info′= UK(C)

단계 4 : 복호화된 메시지 내용(Info′)에 Hashing 함수를 수행하여 HV′를 구하고,

HV′ = H(Info′)

이 HV′를 단계 2에서의 HV와 비교하여 같다면 메시지 무결성과 발신처 인증이 입증된다.

단계 5 : 〈수신증명서의 발급〉

단계 4에서 나온 HV′를 CIC로 복사한 후 B의 비밀키이로 서명한다.

Y = Bs(CIC′)

이를 EDIN에 첨가시켜 원래의 메시지 발신자 A에게 전송한다.

Ⅳ. 결 론

현재 세계적인 흐름을 볼 때 향후 EDI는 기업 경

영을 영위하기 위해 필수적인 요소가 될 것이며 EDI를 사용하지 않는 기업은 경쟁력에서 열세를 면치 못할 것이다. 그리고 국내에서도 외국과 거래시 EDI를 이용한 거래를 요구하는 시점에 있다. 이러한 흐름에 따라 국내에서도 EDI의 개발 및 서비스가 진행 중이다. 그러나 이런 EDI 서비스는 일종의 계약행위와 관련되므로 안전성의 확보가 EDI서비스의 성공에 직결되는 중요성을 가진다.

이러한 중요성과 시급성을 반영하여 X.435에 기인한 EDI 위협요소와 대응서비스, 보안 요구사항, 보안 메카니즘을 분석한 후, 국내에서 시급히 제공해야 할 보안서비스로서 메시지 비밀성, 메시지 무결성, 발신처 인증, 수신 부인봉쇄 서비스를 자체적으로 선정하였다. 그리고 선정된 서비스를 설계 및 구현한 결과를 살펴봄으로써 향후 국내 EDI 시스템에서의 안전한 메시지 송수신에 대한 가능성을 제시하였다.

參 考 文 獻

[1] ISO, "ISO 7498/2 Security Architecture. Information Processing System - Open Systen Interconnection Reference Model", 1984.

[2] CCITT Recommendation X.400 - X.430, "Data Communication Networks Message Handling Systems", 1989.

[3] CCITT Recommendation X.435, "Message Handling Systems : EDI Messaging Systems", 1990.9.

[4] CCITT Recommendation F.435, "Message Handling Systems : EDI Messging Systems", 1990.9.

[5] CCITT, "Recommendation X.509, The Directory-Authentication Framework", 1989.

[6] Rivest,R., "The MD4 Message-Digest algorithm(RFC 1186)", 1990.

[7] Rivest,R., "The MD5 Message-Digest algorithm", July, 1991.

[8] Kent,S., Linn,J., "Privacy Enhancement for Internet Electronic Mail", Internet Activities Board Privacy Task Force, 1989.8.

[8] Richard Hill, "EDI and X.400 using Pedi : "The guide for implementation and users", Technology Apprasals LTD, 1990.12.

[10] Suzki,K., Nakao,K. "Proposals on a Secure Communication Service Element(SCSE) in the OSI Application Layer", IEEE Journal on Selected Areas in Communication, Vol.7, No.4, 1989.

[11] Christopher Mitchell, Michael Walker, David rush, "CCITT/ISO Standards for Secure Message Handling", IEEE Journal on Selected Areas in Communication, Vol.7, No.4, 1989.

[12] Thomas Beth, Dieter Gollman, "Algorithm Engineering for Public Key Algorithms", IEEE Journal on Selected Areas in Communication, Vol.7, No.4, 1989.

[13] Man Young Rhee, "Cryptography and Secure Communications", 1993.

[14] Ashok K.Agrawala, Bijendra N.Jain, "Open Systems Interconnection : Its Architecture and Protocols", 1990.

[15] Albert J.Marcella, Jr.and Sally Chan, "EDI Security, control, and audit", 1993.

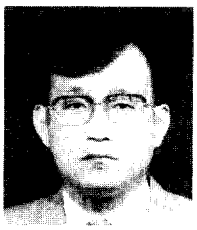
[16] Cemil Betanov, "Introduction to X.400", 1993.

[17] D.W.Davies, W.L.Price, "Security for Computer Networks", 1989.

[18] 한국전산원, "개방형 EDI의 표준화에 관한 연구", 1992.

[19] 한국전산원, "국가기간전산망 EDI 메시지 통신 기능표준(안), 1992.

筆 者 紹 介



鄭 鎭 旭

1946年 6月 20日生
1974年 2月 성균관대학교 전기공학과졸업(공학사)
1979年 2月 성균관대학교 전자공학과(공학석사)
1991年 2月 서울대학교 계산통계학과(이학박사)

1973年 ~ 1985年 한국과학기술연구소(데이타통신 실장)
1981年 ~ 1982年 Racal-Milgo 객원연구소
1992年 ~ 1993年 Maryland대학교 교환교수
1985年 ~ 현재 성균관대학교 교수

주관심 분야 : 네트워크 관리, 네트워크 보안, 고속 통신망