The Journal of Korean
Institute of CALS/EC
Vol. 3, No. 2, Dec. 1998

UN/EDIFACT레벨에서의 정보보호

염용섭*

The Security on UN/EDIFACT message level

Yong-Seop Yeom

요 약

컴퓨터 통신망을 통한 자료교환이 증가되고 있는 요즘 정보보호 위협요소 역시 비례하여 증가되고 있다. 거래 상대방과 중요한 상역 거래문서를 전자문서 형태로 주고받는 EDI(Electronic Data Interchange) 는 부당한 행위자에 의한 불법적인 전자문서의 내용 변조 및 누출 그리고 송수신사실에 대한 부인(Repudiation) 등의 여러 위협들에 대항할 수 있는 정보보호 기능을 필수 서비스로 제공해야 한다.

본 고에서는 KT-EDI 시스템의 실제 운영환경을 기반으로하여 시스템이 제공하는 정보보호 서비스 중에서 기본적인 메세지출처인증(Message Origin Authentication) 서비스와 내용 기밀성(Content Confidentiality) 서비스를 중심으로 UN/EDIFACT 전자문서 레벨에서의 구현에 관하여 다룬다.

* 한국통신 멀티미디어 연구소 EDI 연구실

1. 서론

EDI란 기업간 거래 문서를 컴퓨터가 인식할 수 있는 약속된 표준 전자문서 형태로 변환하여 통신망을 통해 거래 당사자간 교환하는 전자문서 교환시스템이다[11]. 이를 위해 KT-EDI시스템에서는 교환대상이 되는 전자문서의 표준으로 현재 국제 표준 전자문서 규격으로 되어있는 UN/EDIFACT 표준을 따르며, 그러한 전자문서를 유통시킬 통신표준은 EDI 국제 통신표준인 ITU-T X.435 표준과 정보보호를 위해 ITU-T X.509/X.500 표준을 준거하고 있다[6][7][8].

컴퓨터 통신망을 통한 자료교환이 증가되고 있는 요즘 정보보호 위협요소 역시 비례하여 증가되고 있다. 거래 상대방과 중요한 상역 거래문서를 전자문서 형태로 주고받는 EDI(Electronic Data Interchange) 는 부당한 행위자에 의한 불법적인 전자문서의 내용 변조 및 누출 그리고 송수신사실에 대한 부인(Repudiation) 등의 여러 위협들에 대항할 수 있는 정보보호 기능을 필수 서비스로 제공해야 한다.

증가하고 있는 많은 정보보호 위협 요소로부터 정보를 보호하는 문제에 대한 해결책 없이는 통신망을 통한 전자상거래의 실현은 현실적으로 불가능하다.

KT-EDI 시스템에서는 가입자시스템과 중계시스템이 공중망을 매개로하여 전자문서를 송수신하는 운영환경에서 정보보호를 구현하기 위하여 UN/EDIFACT 메세지 레벨과 ITU-T X.435 레벨에서 각각 적합한 정보보호 기능을 구현하였다.

본 논문에서는 한국통신에서 개발한 KT-EDI 정보보호 시스템의 정보보호 서비스 구현 방법 중 UN/EDIFACT 메세지 레벨에서의 기본적인 메세지출처인증 서비스와 내용 기밀성 서비스를 중심으로 구현 기술을 제시함으로써 통신망을 통한 자료교환에서의 보안문제에 대한 하나의 해결책을 제시하고자 한다

2. KT-EDI 정보보호시스템

원격지 송수신자가 컴퓨터 통신망을 이용하여 EDI 데이타를 주고 받을 때 가장 보편적으로 직면할 수 있는 정보보호 위협요소에는, 어떤 실체가 마치 다른 실체인 것처럼 행하는 위장(Masquerade)위협요소, 정보의 내용을 부당하게 손실하거나 부당한 목적으로 변조하는 위협요소, 자신이 정보를 송수신한 행위를 부당하게 부인하는 위협요소, 또한 정보를 전송과정에서 부당하게 입수하여 손실이나 변조를 가하지 않으면서 정보의 내용을 누출하는 위협요소, 기능 수행의 부당한 방해위협요소 등이 있다.

전술한 정보보호 위협들에 효율적으로 대응하고 안전한 정보교환을 이루기 위해 EDI 국제통신표준인 ITU-T X.435에서는 EDI시스템의 정보보호를 위해 28종의 정보보호 서비스가 정의되어 있다[6]. 정의된 서비스들은 다양한 시스템 환경 및 정보보호 정책을 반영한 결과로 광범위하게 정의되어 있다. KT-EDI정보보호 시스템에서는 권고된 28종 서비스를 모두 구현하지는 않고, EDI 시스템의 용도 및 특성에 맞게 선

택 기준을 설정하여 이에따라 선정된 서비스를 대상을 시스템을 설계, 구현하였다. KT-EDI 시스템에서는 구현할 정보보호 서비스 요소의 선택기준을 아래와 같이 다섯 가지로 결정하였다.

첫째, 현실성 기준- EDI시스템 특성상 현실적으로 구현 가능한 서비스 인지 여부

둘째, 실용성 기준- 사용환경 측면에서의 서비스 요구도가 있는가 여부

세째, 효율성 기준- 서비스 제공으로 인한 추가적인 시스템 복잡도가 없는가 여부

네째, 실질성 기준- 정보보호 서비스의 실질적인 수혜자가 사용자인가 여부

다섯째, 이익성 기준- 서비스 제공댓가로 수익(사용료)창출의 대상이 되는가 여부

KT-EDI 시스템에서는 위와 같은 정보보호 서비스 요소의 선택기준에 따라 ITU-T X.435 에 있는 28 종의 정보보호 서비스중 10 개의 서비스 만을 우선적으로 구현하였다.

10 개의 서비스 종류와 내용은 다음과 같다.

- 메세지출처인증 : 지정된 송신자가 보낸 원본 메세지임을 수신자에게 보장하는 서비스
- 메세지제출 증명: 메세지를 지정된 수신자에 전송하기 위하여 메세지를 제출하였음 송신자에게 보장하는 서비스
- 메세지배달증명: 수신자에게 메세지를 배달하였음을 송신자에게 보장하는 서비스
- 내용기밀성 : 메세지 내용이 부당하게 노출되지 않도록 암호화하는 서비스
- 내용무결성 : 메세지 내용변조를 막기 위한 전자서명 서비스
- 송신부인봉쇄 : 송신자가 발송한 메세지임을 수신자에게 증명해 주는 서비스
- 수신증명 : 수신자가 정상적으로 메세지를 수신하였음을 송신자에 통지(Notification)하는 서비스
- 내용증명 : 수신자가 원본 메세지를 수신한 증거를 송신자에게 제공하는 서비스
- 통지부인봉쇄 : 수신자가 수신통지 발송사실을 부인하지 못하도록 송신자에게 보장하는 서비스
- 수신부인봉쇄 : 수신자의 메시지 수신 사실에 대한 증거(Proof)를 송신자에게 제공하는 서비스

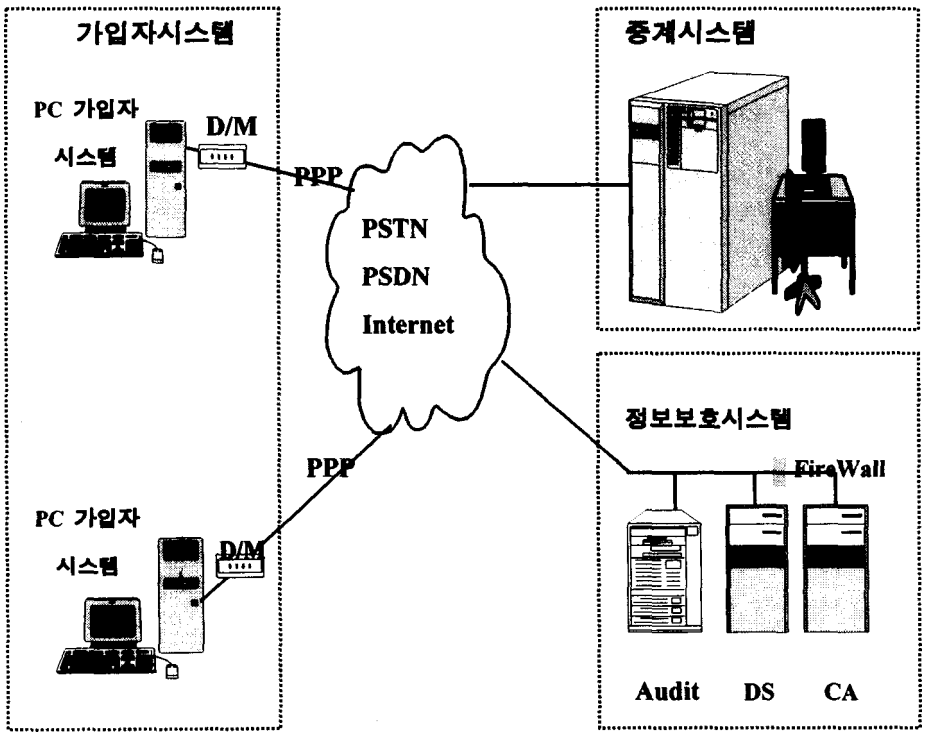
KT-EDI시스템은 EDI의 국제표준 통신 규약인 X.435와 국제 EDI문서표준인 UN/EDIFACT에 준거하여 개발된 국제표준 공중 서비스용 EDI시스템이며, 표준 메세지의 생성, 변환 및 전송기능과 망간 연동서비스를 제공하는 ADMD(ADministration Management Domain) 기능을 수행할 수 있는 개방형 시스템으로서 국내는 물론 국외의 타 EDI서비스 시스템간에도 상호연동성을 보장하는 본격 EDI시스템이다. 여기에 추가하여 유통 메세지들에 대한 정보보호를 실행하기 위해서 ITU-T X.500/509 프로토콜에 따라 구현한 정보보호시스템이 결합되어 있다.

따라서 KT-EDI 정보보호시스템이란, (그림 1)에 나타난바와 같이 순수 EDI 기능을 수행하는 가입자시스템과 중계시스템 그리

고 정보보호기능을 수행하는 정보보호시스템인 CA (Certificate Authority), 디렉토리서버(DS:Directory Server), 감사추적(Audit)시스템이 결합된 시스템을 지칭한다.

가입자시스템은 사용자가 EDI 메세지를 만들어 전송하거나 수신할 수 있도록 하는 기능과 , 사설문서 포멧을 표준 전자문서(UN/EDIFACT) 포멧으로 변환하거나 표준 전자문서 포멧을 사설문서 포멧으로 변환시켜주는 문서변환(Translator) 기능, 정보보호 모듈과 인터페이싱을 이루어 송신 또는 수신할 문서들에 대한 정보보호 기능을 수행한다.

KT-EDI시스템의 서버 역할을 수행하는 중계시스템은 크게 메세지전송시스템(MTA: Message Transfer Agent)과 메세지저장기 (MS: Message Store)로 구성된다[4][5].



(그림 1) KT-EDI시스템

메세지저장기는 ITU-T X.413으로 정의되어 있는 기능을 수행하기 위해 가입자시스템과 메세지전송시스템 사이에 위치하여 원격지(Remote) 가입자시스템으로부터 제출된 EDI메세지나 수신된 EDI 메세지를 보관하는 가입자 메일박스 기능을 수행한다.

메세지전송시스템은 ITU-T X.411로 정의되어 있으며 메세지저장기를 통해 제출된 가입자시스템으로부터의 EDI메세지를 동일 시스템내의 수신자 메세지저장기로 배달하거나 타 시스템의 메세지전송시스템으로 배달해주는 기능을 한다. 이때 메세지저장기와 메세지전송시스템간에는 P3 프로토콜(메세지 제출 및 배달규약)을, 메세지전송시스템간에는 P1프로토콜을 사용한다.

KT-EDI 정보보호시스템에서는 유통 메세지에 대한 정보보호를 두단계 레벨로 나누어서 구현하였다.

첫번째 레벨은 UN/EDIFACT 전자문서 레벨에서 이루어지는 정보보호이며, 두번째 레벨은 ITU-T X.435 메세지 레벨에서 이루어지는 정보보호 기능이다.

UN/EDIFACT 전자문서 레벨에서의 정보보호란, EDI 표준 전자문서(Interchange)를 생성(Generation)하는 단계와 수신한 EDI 표준 전자문서를 응용시스템에 전달하기 위하여 역변환(Interpretation)하는 단계에서 가입자시스템내의 문서변환시스템에의해 시행되는 정보보호 행위를 말한다.

ITU-T X.435 메세지 레벨에서의 정보보호는 UN/EDIFACT 전자문서 레벨에서의 정보보호가 시행되었든지에 관계없이 ITU-T X.435 프로토콜에 따라 유통시킬 메세지를 대상으로하여 이루어지는 메세지 인증 및 무결성, 암호화 등의 정보보호를 말한다.

KT-EDI시스템에서 이와같이 두가지 레벨에서의 정보보호를 시행했던 이유는, 전자문서가 송신자에 의해 생성되는 순간부터 정보보호가 시행되어 정당한 수신자에 의해 수신변환처리 되는 순간 까지 엔드-투-엔드 정보보호 서비스를 제공하기 위함이 첫번째 목적이었고, 두번째 목적은 사설문서 포맷이 문서변환시스템을 거쳐 국제 표준전자문서 포맷으로 바뀐이후에는 어떤 유통수단 즉, KT-EDI에서와 같은 ITU-T X.435 또는 X.420 통신처리시스템이나 Internet 메일, 기타 통신처리 장치를 이용하여 유통된다 하더라도 KT-EDI문서변환시스템을 사용하는 사용자들에게 최소한의 정보보호 기능인 인증과 무결성을 이루기 위함이다.

ITU-T X.435 메세지 레벨에서의 정보보호는 실제적으로 EDI 중계시스템과는 무관하게 정보보호 기능을 시행하게 하였다. 다시말하여 EDI 중계시스템은 자신이 중계해야되는 메세지가 정보보호가 이루어져 있는 메세지인지 아닌지 전혀 알 필요가 없다. 이는 ITU-T X.435메세지 레벨에서의 정보보호는 실제적으로 EDI 중계시스템과 떨어져 원격지에 위치한 가입자시스템에서 이루어지기 때문이다. 따라서 일단 가입자시스템에서 송신할 메세지를 대상으로하여 시행된 모든 정보보호 서비스들은 메세지 수신자의 가입자시스템에 의해 정상적으로 수신되어 정보보호 시스템과 문서변환시스템에 의해 정보보호 검증이 수행되지 않으

면 유통된 메세지는 사용될 수 없다.

이와같이 완전한 엔드-투-엔드 정보보호를 이루게 함으로써 정보보호로 인한 오버헤드로부터 중계시스템을 자유롭게 하였으며, 중계시스템의 개입을 완전히 배제시킴으로써 보다 강화된 메세지 무결성을 이룰 수 있게 하였다.

KT-EDI시스템에서는 ITU-T X.435 메세지 레벨에서의 정보보호를 시행하기 위해서 SHA-1 다이제스팅 알고리즘과 X.509/X.500에 준거한 공개키 기반 암호화 알고리즘인 RSA 암호화 알고리즘을 사용하였다[9].

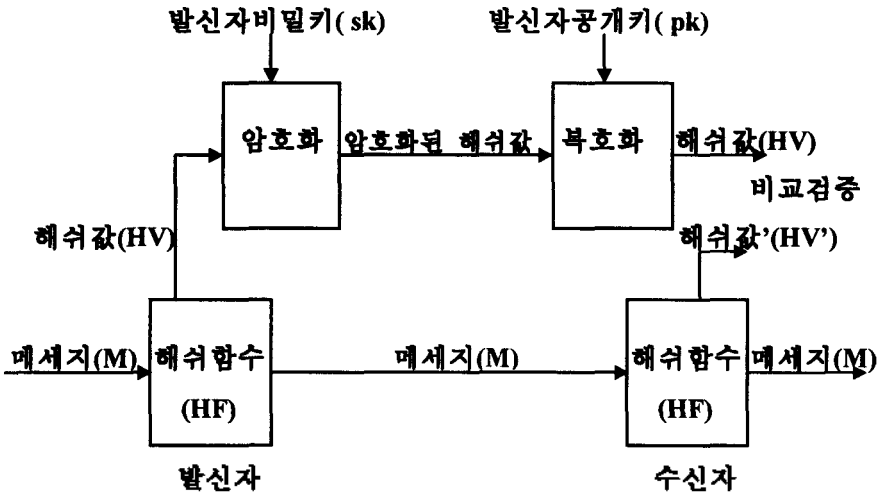
특히 메세지내용 자체의 암호화에는 속도를 고려해 대칭키방식 암호화 알고리즘인 DES 와 순수 국산화개발된 블럭암호화 알고리즘인 BASE96을 사용한다. 따라서 ITU-T X.435 메세지 레벨에서의 정보보호를 시행키 위해 전자 보증서를 생성, 유지관리할 수 있는 CA(Certificate Authority)와 생성된 보증서를 인터넷상에 공개, 관리할 수 있는 DS(Directory Server) 기능의 구현이 요구되었다. 이를위해 KT-EDI 정보보호시스템에서는 CA를 위해 ITU-T X.509 공개키 보증서 버전 V3와 취소목록 버전 V2를 채택적용하였으며, LDAP 프로토콜 지원 DS(Directory Server)를 구현하였다.

다음 장에서는 KT-EDI 정보보호시스템에서 제공하는 정보보호서비스 중 메세지 출처인증과 내용 기밀성 서비스를 UN / EDIFACT 레벨에서의 구현방법을 기술한다.

3. 메세지출처 인증

일반적으로 메세지출처 인증 정보보호 서비스는 수신된 메세지가 메세지의 발신자 필드(Originator field) 에 적혀있는 발신자명(OR name) 을 갖는 발신자로 부터 온 원본 메세지임을 수신자에게 보장해 주는 서비스다[6].

메세지출처인증을 구현하기 위해서 일반적으로 많이 사용하는 기법으로는 전자서명(Digital signature) 방법이 있으며 (그림 2)에서와 같이 발신자는 전송할 메세지를 대상으로 하여 일정한 해쉬함수(Hash function)를 적용하여 얻은 해쉬결과 값을 자신의 비밀키(Secret Key)로 암호화한 전자서명(Digital signature) 을 메세지와 함께 수신자에게 전송한다. 수신자는 먼저 발신자의 공개키(Public Key) 를 이용하여 암호화 되어 있는 발신자의 전자서명을 복호화 하여 얻은 결과와, 수신한 메세지를 대상으로 하여 발신자와 동일한 해쉬함수를 적용하여 얻은 결과값을 비교하여 일치여부를 확인 함으로써 메세지출처인증을 실현한다. 만약 비교결과 두 값이 일치한다면 수신자는 일단 자신이 수신한 메세지는 전송도중에 내용변조가 없었으며 자신이 적용한 공개키의 소유자인 발신자가 전송한 메세지란 사실을 확인할 수 있다. 따라서 비교결과 두 값이 일치하였다면 메세지출처인증 서비스와 데이타 무결성(Data integrity) 서비스가 동시에 제공되었다고 할 수 있다.



(그림 2) 메세지출처인증

그러나 비교결과 값이 서로 다르다면 다음과 같은 2 가지의 사실을 추론할 수 있다. 즉, 메세지가 전송 도중에 변조되었거나, 적용한 공개키를 소유한 발신자가 전송한 메세지가 아님을 알 수 있다.

KT-EDI 시스템에서는 메세지출처인증(MOA:Message Origin Authentication) 서비스를 두가지 레벨(UN/EDIFACT 전자문서 레벨과 X.435 메세지 레벨)에서 구현하고 있다.

UN/EDIFACT 전자문서 레벨에서는 전자문서의 부당한 변조 및 위조를 방지하기 위해서 다음과 같이 두가지 전자문서 인증방법을 선택적으로 시행할 수 있다.

첫번째 방법은 전자문서 인증용 세그먼트인 AUT(Authentication) 세그먼트를 전자문서의 구성 요소로 포함하고 있는 경우에 일반적으로 시행하는 방법으로서 기본적으로 적용하고 있는 방법이기도 하다.

두번째 방법은 공개키 기반 전자서명 기법을 이용하여 시행하는 방법으로서 전자문서가 구조적으로 AUT 세그먼트를 포함하고 있지 않은 경우에도 시행할 수 있는 방법이다.

3.1 전자문서 인증방법 1

KT-EDI 시스템에서는 UN/EDIFACT 전자문서 레벨에서의 출처인증 및 데이타 무결성 실현을 위해 문서변환시스템이 사설문서를 EDI 표준 전자문서인 인터체인지 화일(Interchange file) 로 변환하는 과정에서 인증값을 생성한다. 생성된 인증값은 (그림 3)에 나타난 바와 같이 전자문서 내에 AUT 세그먼트[11] 항목에 포함되어 수신자에게 전달된다.

문서변환시스템은 전자문서 인증값을 생성하기 위해 수발신자가 인터체인지 협약(Interchange Agreement)를 맺을 때 서로 알려준 거래 상대방의 비밀키 10자리 십진수와 자신의 10자리 십진 비밀키를 조합한 20자리의 십진 비밀키를 이용해 알고리즘을 전개한다. 문서변환시스템은 AUT 세그먼트의 항목으로 포함시킬 인증값을 생성하기 위해서 이 비밀키와 전자문서의 시작 세그먼트인 UNH 세그먼트 항목부터 전자문서의 끝 세그먼트인 UNT 세그먼트 항목까지(AUT 세그먼트는 제외)의 전자문서 내용(Content)을 대상으로 하여 DSA (Decimal Shift and Add Algorithm) 또는 Matrix 전자문서 인증 알고리즘을 적용하여 생성된 10자리 인증값을 AUT 세그먼트 항목에 포함시켜 전송한다. 여기서 10자리 인증값을 사용하는 이유는 역계산을 통한 암호해독 시도를 방지하기 위함이다.

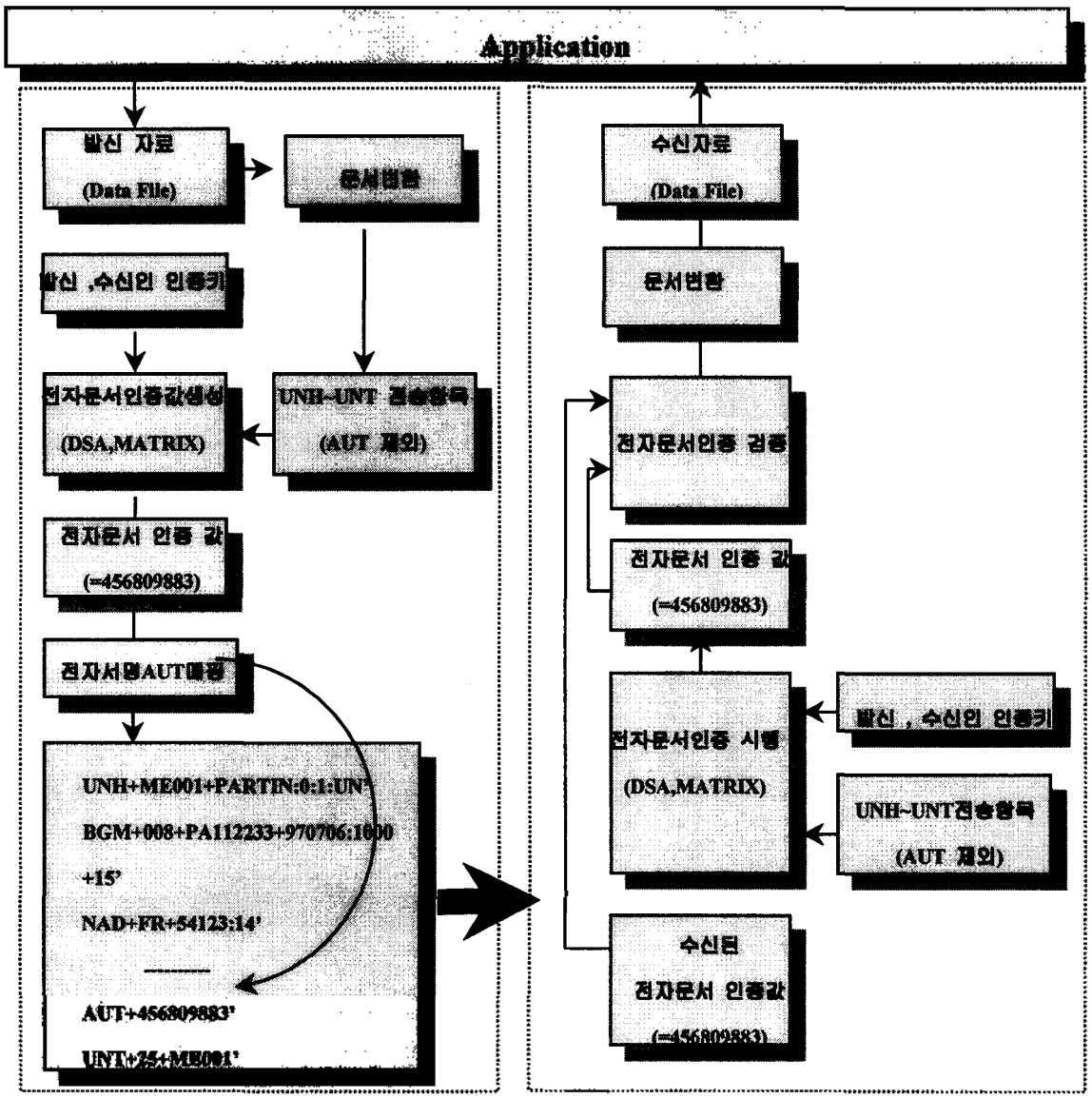
수신자는 수신한 전자문서를 대상으로 하여 발신자가 서명 값을 생성하기 위해서 적용하였던 동일한 20 자리 십진수 비밀키와 인증 알고리즘(DSA,Matrix)을 적용시켜 생성한 결과 값과 수신한 전자문서의 AUT 세그먼트 항목에 포함된 서명 값을 비교하여 수신문서의 변조 여부 및 올바른 발신자 여부를 확인할 수 있다.

AUT 세그먼트 항목의 길이는 UN/EDIFACT 에서는 35 자리로 구성되어 있는데 현재 국내에서는 이 중 10 자리를 이용하고 있다.

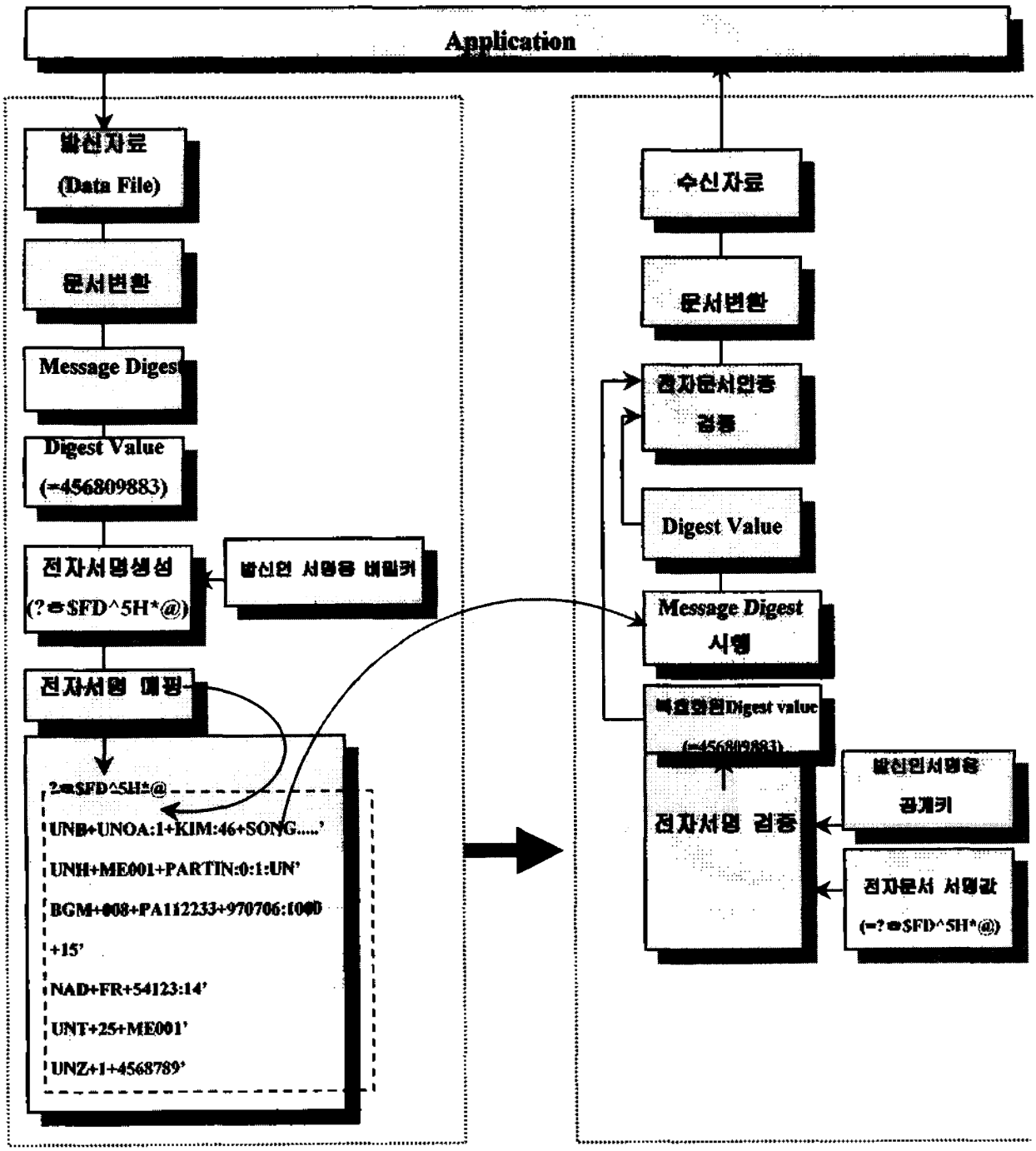
전자문서 인증 알고리즘인 DSA 는 전자문서의 인증 목적으로 교수 시이비에 의해 1980 년에 만들어졌으며 "이동 및 가산(SHIFT and ADD)" 을 기본 연산방법으로 사용한다[9]. KT-EDI 문서변환 시스템에서 전자문서의 인증 목적으로 사용하고 있는 또 하나의 알고리즘은 자체에서 개발한 Matrix 알고리즘이다. 이 알고리즘은 DSA 알고리즘과 같이 발신인과 수신인이 갖고 있는 알고리즘 작동 제어키를 구성하는 2 개의 비밀 10 자리 십진수에 의존하여 작동되며, 전자문서의 세그먼트를 기본 입력 단위로 하여 계산이 이루어 진다. 전자문서를 행과 열을 갖는 논리구조로 치환하여 행과 열에 공통 알고리즘을 적용하여 인증값을 산출한다.

3.2 전자문서 인증방법 2

(그림 4)에 기술한 전자문서 인증방법 2 에서는 전술한 방법 1 에서와는 달리 인증처리를 공개키 기반 전자서명 기법을 이용한다. 전자문서변환 결과로 생성된 인터체인지를 대상으로하여 SHA-1 메세지 다이제스팅 알고리즘을 이용해 다이제스트 값을 생성하고, 그 값을 대상으로 송신자의 서명용 비밀키를 이용하여 전자서명을 시행한다. 생성된 서명값을 전자문서의 UNB 세그먼트 전에 포함시켜서 전송하면, 수신자는 해당 전자문서를 수신하여 먼저 송신자의 공개키를 이용하여 전자문서에 포함되어 있는 전자서명의 진위를 먼저 확인한다. 전자서명 검증 결과로 얻게 되는 복호화된 메세지 다이제스트 값을 이용하여 전술한 전자문서 인증방법 1 에서와 같은 과정을 거쳐 전송과정에서의 메세지 내용변경 여부를 확인하게 된다.



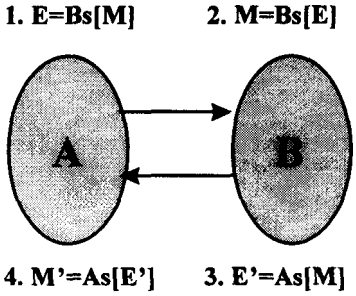
(그림 3) 전자문서 인증 절차 1



(그림 4) 전자문서 인증 절차 2

4. 내용기밀성

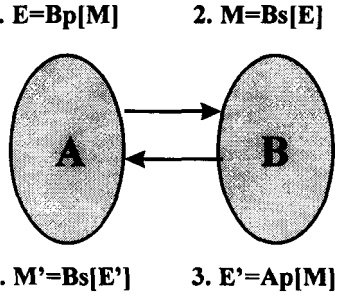
내용기밀성(Content Confidentiality) 은 발송한 메세지를 정당한 수신자 외에는 메세지의 내용을 읽을 수 없게하는 정보보호 서비스로서, 메세지 내용의 부당한 노출을 방지하기 위해서 일반적으로 암호화 기법이 사용된다.



(그림 5) 대칭비밀키 암호화

일반적으로 암호화를 이루기 위해 적용되는 방법으로는 대칭 비밀키 암호 방법과 비대칭 공개키 암호 방법이 있다. 대칭 비밀키 암호 방법은 (그림 5) 와 같이 암호를 만들 때 사용하였던 키와 암호를 해독할 때 사용하는 키를 동일한 하나의 키로하여 사용하는 방법으로서, 발신자와 수신자가 동일한 비밀키를 공유함으로써 암호화가 빠르고 쉽게 이루어 질 수 있는 반면, 수신자별로 달라질 수 있는 많은 비밀키를 관리해야하는 어려움과 비밀키가 외부에 노출되면 쉽게 공격 당할 수 있는 문제점들을 갖고 있다. 이 방법을 사용하는 대표적인 암호화 방법으로는 잘알려진 DES(Data Encryption Standard) 가 있다.

(그림 6)은 비대칭 공개키 암호화 방법으로서 암호화할 때 사용하는 키(공개키)와 복호화할 때 사용하는 사용하는 키(비밀키)가 서로 다르게 하는 방법으로서 공개키는 공개하고 비밀키만 각각이 관리한다. A 는 B의 공개키를 이용하여 송신할 내용을 암호화하여 B에게 전송하면, B는 수신한 메세지를 자신의 비밀키를 이용하여 복호화



(그림 6) 비대칭공개키 암호화

한다. 비대칭 공개키 방법에서는 대칭 비밀키 방법과는 달리 키의 안전한 분배가 필요없으며 관리할 키의 갯수가 상대적으로 적으며, 전자서명으로 이용 가능하다는 특징을 가지고 있다[8].

그러나 B는 자신에게 전송되는 메세지를 암호화 할 수 있도록 불특정 다수에게 키를 공개(공개키) 하였으므로 어느 누구라도 특정한 사람 A를 가장하여 위조된 메세지를 B에게 보낼 수 있다. 따라서 공개키 암호 시스템에서는 발신자의 신원을 확인할 수 있도록 전자서명 기법을 병행 사용할 수 있다. 비대칭 공개키 방법을 사용하는 대표적인 암호화 방법으로는 RSA (Rivest,Shamir,Adleman) 가 있다.

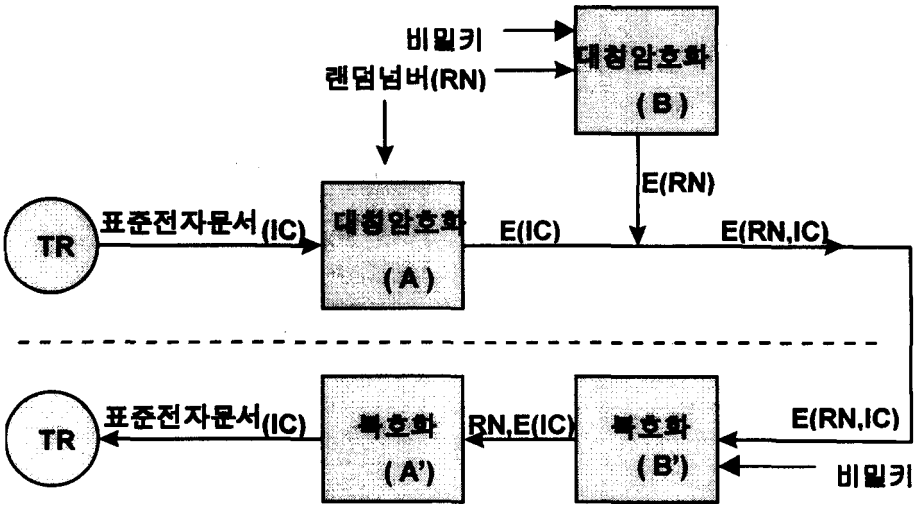
KT-EDI 시스템에서는 메세지내용기밀성(Message Content Confidentiality) 서비스를 메세지출처인증 서비스와 마찬가지로 두가지 레벨(UN/EDIFACT 전자문서 레벨과 X.435 메세지 레벨)에서 구현하였지만 본고에서는 UN/EDIFACT 전자문서 레벨에서의 메세지내용기밀성 서비스 구현에 관하여 다룬다.

KT-EDI 문서변환시스템은 EDI 표준전자문서(Interchange)를 무인가자의 부당한 읽기(Reading), 복사(copying) 또는 폭로(Disclosure)로부터 보호하기 위하여 세그먼트 단위로 암호화를 수행하여 EDI 표준전자문서를 작성한다. 이는 형태상 대칭 비밀키 암호화 방법을 사용한다. 암호화를 실행하기 위해 문서변환시스템은 먼저 암호화에 사용될 랜덤넘버(Random number)를 생성하여 이 키를 근간으로 하여 세그먼트 단위로 대칭키 암호 알고리즘(A)를 수행하면서 EDI 표준전자문서를 생성한다. EDI 표준전자문서가 다 만들어지면 암호화에 사용되었던 랜덤넘버를 수신자에게 전달하기 위한 방법에는 두가지 방법이 적용될 수 있다.

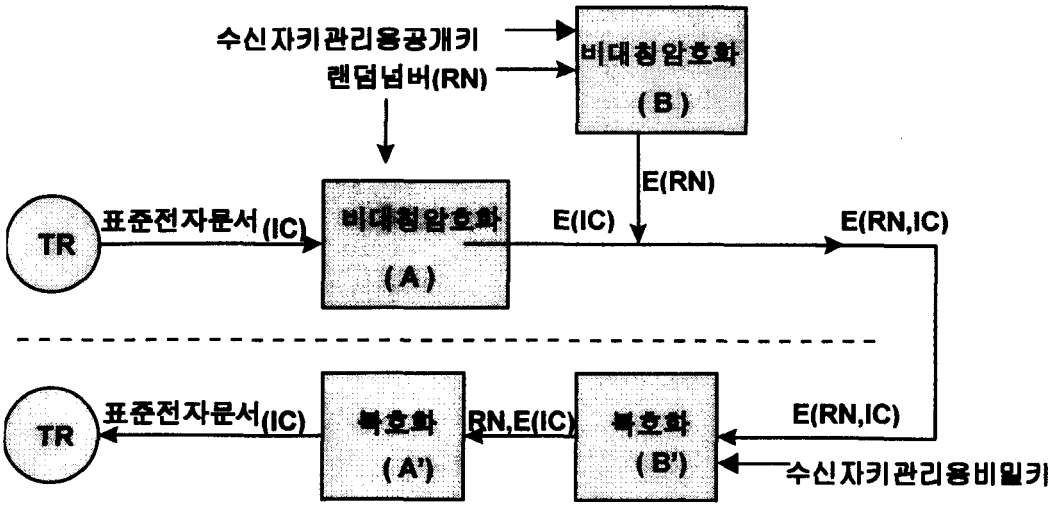
첫째 방법은, 수신자와 사전에 EDI 거래약정(IA:Interchange Agreement) 체결시에 교환한 십진수 20 자리 (발신자키 10 자리, 수신자키 10 자리) 키를 이용하여 전자문서 내용을 암호화했던 알고리즘과는 다른 대칭키 암호화 알고리즘(B)를 이용해 암호화를 시행하여 EDI 표준전자문서의 첫 머리에 부가시켜서 수신자에게 전송한다. 수신자는 암호화된 EDI 표준전자문서를 복호화하기 위해서 먼저 발신자와 사전에 EDI 거래약정 체결시에 교환한 십진수 20 자리 키를 이용하여 복호 알고리즘(B')을 사용하여 발신자가 전자문서 내용을 암호화하기 위해 사용했던 랜덤넘버를 얻어 낸다. 복호된 랜덤넘버를 키로하여 복호 알고리즘(A')을 수행하여 수신한 암호된 EDI 표준전자문서를 평문으로 복호 시킨다. 이의 과정을 그림으로 나타내면 (그림 7) 과 같다.

둘째 방법은, 공개키 기반 암호화 방법으로서 전자문서 내용의 암호화에는 랜덤넘버를 이용하여 대칭키 암호화 방법으로 암호화하고, 사용한 랜덤넘버를 수신자의 공개키를 이용하여 비대칭 암호화 알고리즘을 이용하여 암호화를 시행하여 EDI 표준전자문서의 첫 머리에 부가시켜서 수신자에게 전송한다(그림 8).

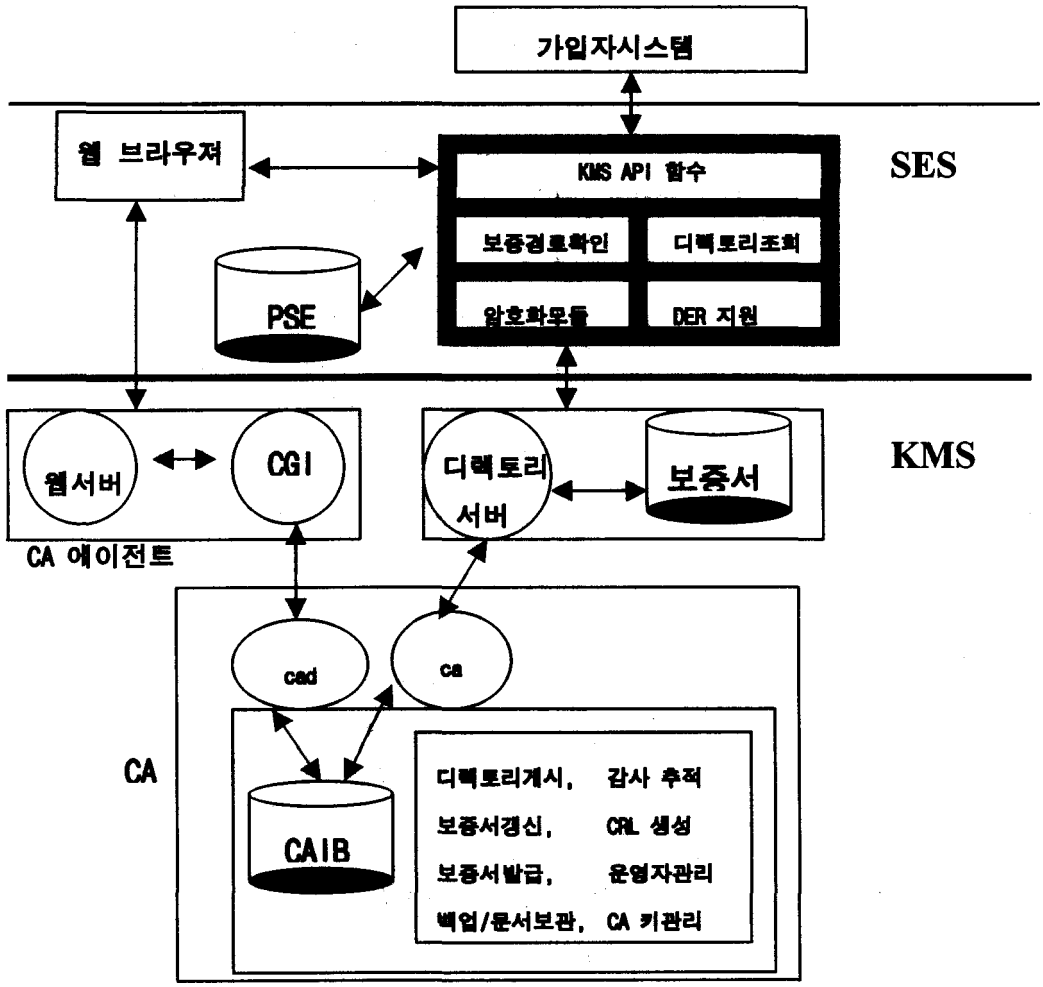
수신자는 암호화된 EDI 표준전자문서를 복호화하기 위해서 먼저 자신의 비밀키를 이용하여 전자문서의 머리에 있는 랜덤넘버를 복호화한다. 복호된 랜덤넘버를 키로하여 대칭키 암호화 알고리즘을 이용해 수신한 암호된 EDI 표준전자문서를 평문으로 복호 시킨다. 이의 과정을 그림으로 나타내면 (그림 8) 과 같다.



(그림 7) 비밀키기반 전자문서 암호화



(그림 8) 공개키기반 전자문서 암호화



(그림 9) 공개키기반 보안구조

가입자시스템의 문서변환시스템에 의해 이루어지는 제반 정보보호에 이용되는 공개키 기반 보안구조는 크게 4 가지 기능모듈로 구성된다.

응용시스템과 정보보호시스템 사이에서 인터페이스 기능을 수행하는 가입자시스템 모듈, 정보보호 처리에 사용할 키 관리 및 보증서 발급, 보증서 취소 등의 기능을 담당하는 KMS(Key Management System) 모듈, 디렉토리 서버, 정보보호 서비스 처리를 위해 가입자시스템과 인터페이스를 이루어 실제 정보보호 처리를 수행하는 SES(Secure EDI System) 모듈, 송수신 부인봉쇄(Non-Repudiation)을 위해 필요 증거들을 유지, 관리하여 감사추적(Audit) 기능을 수행하는 SAS(Secure Audit System) 모듈로

이루어져 있다. (그림 9)에는 위 4 모듈중 SAS를 제외한 3 모듈의 상호연관 구성도를 나타내고 있다.

KMS(Key Management System) 모듈은 공개키 방식의 정보보호 서비스를 제공하기 위해서 안전하게 키를 생성, 배포, 전자보증서(Certificate) 생성/등록 및 취소관리 할 수 있는 공개키 기반구조(Public Key Infrastructure:이하 PKI)가 존재하여야 한다[8]. KMS시스템은 이러한 요구사항에 의해 개발된 KT-EDI시스템용 PKI시스템이다. SSLeay를 사용하여 개발된 KMS시스템의 주요 구성요소는 PKI클라이언트와 CA이다. PKI클라이언트는 키 관리 서비스를 제공하기 위해 KMS API 인터페이스 모듈, DER지원모듈, 암호모듈, 디렉토리 조회모듈 및 보증경로 확인모듈로 구성되어 있다. CA를 구성하는 주요 모듈로는 CA 키 관리모듈, 보증서 발급모듈, 보증서 취소모듈, 보증서 갱신모듈, CRL 생성모듈, 디렉토리 게시모듈, DER 지원모듈, 암호모듈이다.

SES(Secure EDI System)은 KT-EDI 정보보호시스템에서 정보보호 서비스를 처리하는 핵심기능을 담당한다. SES는 가입자시스템으로 부터 정보보호 서비스 요청을 받아들이는 SES 인터페이스 모듈과 SES 인터페이스를 통해 요청받은 정보보호 서비스 요구들간의 상호관계를 조사하여 처리 순서를 결정하고 해당 처리 함수를 호출하는 요청서비스 제어처리부, 정보보호 서비스에 공통적으로 사용되는 함수들을 모아놓은 공통 사용 함수처리부, 요청된 각각의 서비스를 처리하는 함수들로 구성된 서비스별 함수처리부로 구성된다[12]. SES에서의 정보보호 서비스 처리과정을 살펴보면, 먼저 SES 인터페이스를 통해 요청 서비스의 종류와 서비스 처리에 필요한 데이타들을 받아들인다. SES 인터페이스는 입력받은 값들을 요청서비스 제어처리부로 넘기고, 요청서비스 제어처리부는 요구된 서비스들을 종류를 검사해서 서비스들의 처리순서, 요청 서비스간의 모순성 등을 검사한 다음, 요청 서비스의 종류와 처리 순서에 따라 서비스별 함수처리부를 이용해서 서비스를 제공한다. 서비스별 함수처리부는 처리 과정에서 공통 사용 함수처리부와 KMA 인터페이스와 SAS 인터페이스 등을 사용하게 된다.

5. 결론

본 고에서는 KT-EDI 시스템의 PC 사용자들이 원격지 중계시스템에 있는 UA(User Agent) 와의 상호작용을 통해 메세지를 송수신하는 실제 서비스 환경을 기반으로하여 KT-EDI 시스템이 제공하는 여러 보안서비스 중에서 기본 서비스라고할 수 있는 메세지출처인증 서비스와 내용 기밀성 서비스를 중심으로 그 구현 방법을 UN/EDIFACT 전자문서 레벨에서 해결하는 방안을 제시하였다.

본 고에서 제안된 보안구조를 이용한 인터넷기반 EDI 시스템에서 정보보호를 이루기 위해 현재 한국통신 EDI 연구실에서는 연구를 계속하고 있으며, 더 나아가 인터넷 기반 전자상거래에도 적용할 수 있는 연구가 더 필요하다고 사료된다.

참고문헌

[1] ITU-T F.400/X.400, Message Handling : System and Service overview, 1988

[2] EDI & X.400 using Pedi, Richard Hill ,1993

[3] ITU-T X.402, Message Handling Services : Overall Architecture, 1992

[4] ITU-T X.411, Message Handling Services : Message Transfer System : Abstract Service Definition and Procedures, 1988

[5] ITU-T X.413, Message Handling Services : Message Store : Abstract Service Definition, 1988

[6] ITU-T X.435, Message Handling Services : Electronic Data Interchange Messaging System, 1992

[7] ITU-T X.500, The Directory : Overview of Concepts, Models, and Services. 1988

[8] ITU-T X.509, The Directory : Authentication Framework. 1988

[9] EDI 시스템 시큐리티 선행기술 연구보고서,정진욱 ,1996

[10] EDI & SECURITY,KEB,1993

[11] EDIFACT-Application level syntax rules,Part5,1996

[12] 윤이중, 안전한 EDI 시스템의 구조설계, 제 2차 안전한 EDI 관련기술 심포지움, 1996

저자소개

염용섭

1988 년 : 충남대학교 대학원 졸업, 전산학 전공

현 재 : 한국통신 멀티미디어연구소 물류기술연구실 선임연구원

관심분야 : EDI, Security, 물류정보시스템