通信情報保護學會誌
第9卷 第1號, 1999. 3

안전한 KT-EDI시스템 구현에 관한 연구
The Study of Implementing Secure KT-EDI System

염 용 섭*, 김 현 호*

요 약

정보화 사회로 다가갈수록 정보보호의 중요성이 커지고 있으며 이에따른 정보보호 위협요소 역시 비례하여 증가되고 있다. 이러한 위협요소의 증가는 정보통신 서비스, 특히 EDI와 같은 전자상거래 활용을 저해하는 주요 문제점으로 대두되고 있다. 이에 따라, 본 연구실에서는 EDI 시스템을 이용하여 안전하고 신뢰성을 갖춘 전자문서를 교환시킬 수 있게 하기위하여 기 구축되어있던 KT-EDI시스템에 암호화, 무결성, 인증, 감사추적 등의 필수적인 정보보호 기능을 첨부한 KT-EDI정보보호시스템을 개발 하였고, 본 논문에서는 이에 대한 구현기술을 기술한다.

1. 서 론

EDI란 종이 없는 상역거래를 실현하기위해서 전자문서를 컴퓨터통신망을 이용해 상호교환하는 제반행위를 말한다. EDI시스템은 컴퓨터통신망을 통해서 고부가 가치의 상역거래 전자문서를 유통시키므로써 중요 거래정보들이 통신망상에서 불법적으로 노출될 위험을 가지고 있다.

오늘날 상역거래에 보편화되어있는 EDI 서비스를 이용하는 모든 분야에 있어서 반드시 해결해야될 공통 과제는 정보보호(Security) 문제라 할 수 있다. EDI 서비스를 이용하여 주고 받는 모든 상역문서에 대한 진위 여부의 확인이나 송수신 과정에서의 정보의 변조, 누락 및 노출이 없없는지 확인할 수 있는, 그리고 송수신자의 메시지 송수신 사실을 부인하지 못하게 하는 제반 정보보호책이 강구되지 않는다면 상역거래의 특성상 EDI 의 광범위한 이용은 불가능하게 될것이다.

최근 정보통신 기술의 발달이 급속도로 진행되고, 컴퓨터의 보급이 빠르게 확대됨에 따라 컴퓨터 통신망을 이용한 정보의 교환량이 날로 증가하고 있다. 하지만 공개된 통신망을 통해 정보가 오고가기 때문에 전송과정에서 비인가된 자에 의해 정보가 불법적으로 유출 또는 손실될 위험 부담 또한 그 만큼 크다. 이에 따라, 증가하고 있는 많은 정보보호 위협요소로부터 정보를 보호하는 문제가 통신망을 통한 정보 교환에 있어 무엇보다도 중요한 문제로 제기되고 있다.

본 논문에서는 한국통신에서 개발한 KT-EDI 정보보호시스템의 구현기법을 제시함으로써 통신망을 통한 정보교환에서의 정보보호

* 한국통신 멀티미디어 연구소

문제해결을 위한 하나의 솔루션을 제시하고자 한다.

2. 정보보호 위협요소와 정보보호

EDI 시스템이란 기업간 거래 문서를 컴퓨터에서 인식할 수 있는 약속된 표준 전자문서 형태로 변환하여 통신망을 통해 거래 당사자간 교환하는 전자교환시스템이다. 이를 위해 KT-EDI시스템은 교환대상이 되는 전자문서의 표준은 현재 국제표준전자문서 규격으로 되어 있는 UN/EDIFACT 표준을 따르며, 그러한 전자문서를 유통시킬 통신표준은 EDI 국제통신 표준인 ITU-T X.435표준을 따르고 있다.

EDI 시스템은 통신망을 통하여 정보를 상호 교환하므로, 보다 안전하고 신뢰성 있는 정보 유통을 보장하기 위해서는 교환되는 정보에 대한 보호 서비스 기능이 요구된다. 이를위해 KT-EDI시스템은 국제 통신표준화 되어가고 있는 ITU-T X.509/X.500 표준을 따라 정보보호 시스템을 구현하였다.

본 장에서는 EDI 환경 하에서 존재하는 정보보호를 위협하는 여러 요소들에 대응할 수 있는 KT-EDI 정보보호 시스템의 정보보호 서비스에 관해서 다루고자 한다.

가. KT-EDI 정보보호 서비스

EDI 환경 하에서의 정보 위협요소에는 대표적으로 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. 이과 같은 정보보호 위협요소로부터 안전하게 정보교환을 송수신자에게 보장하기 위해서는 여러 가지 정보보호 서비스 기능이 요구된다. 전술한 정보보호 위협들에 효율적으로 대응하고 안전한 정보교환을 이루기 위해 EDI 국제통신표준인 ITU-T X.435에서는 EDI시스템의 정보보호를 위해 28종의 정보보호 서비스가 정의되어 있다. 정의된 서비스들은 다양한 시스템 환경 및 정보보호 정책을 반영한 결과로 광범위하게 정의되어 있다. KT-EDI 정보보호 시스템에서는 권고된 28종 서비스를 모두 구현하지는 않고, EDI 시스템의 용도 및 특성에 맞게 선택 기준을 설정하여 이에따라 선정된 서비스를 대상을 시스템을 설계, 구현하였다. KT-EDI 시스템에서는 구현할 정보보호 서비스 요소의 선택기준을 아래와 같이 다섯가지로 결정하였다.

첫째, 현실성 기준. 여기서 현실성이라함은 EDI시스템 특성상 현실적으로 구현 가능한 서비스 인가 라는 것이다.

둘째, 실용성 기준. 실용성이라함은 사용환경 측면에서의 서비스 요구도가 있어야 한다는 것이다.

세째, 효율성 기준. 효율성이라함은 서비스 제공으로 인한 추가적인 시스템 복잡도가 없어야 한다는 것이다.

네째, 실질성 기준. 실질성이라함은 정보보호 서비스의 실질적인 수혜자가 사용자이어야 한다는 것다.

다섯째, 이익성 기준. 이익성이라함은 서비스 제공댓가로 수익(사용료)창출의 대상이 되어야 한다는 기준이다.

ITU-T X.435에서 규정하고 정보보호 요소들에 대해 상기 다섯가지 서비스 선택기준에 따라 선택된 KT-EDI의 정보보호 서비스는 〈표1〉과 같다. 표의 구현필요성 난에 "M"은 필수적으로 구현해야하는 서비스 요소임을 나타내며,

"O"는 우선순위가 "M"보다 떨어지지만 선택적으로 구현할 서비스 요소,"X"는 KT-EDI정보보호시스템에서 구현할 필요가 없는 서비스임을 나타낸다.

표1 KT-EDI 시스템의 정보보호 서비스의 구현 우선순위

서 비 스 요 소		구현필요성
Origin Authentication	Message Origin Authentication	M
	Probe Origin Authentication	X
	Report Origin Authentication	X
	Proof of Submission	O
	Proof of Delivery	O
Secure Access Management	Peer Entity Authentication	O (MTA/MTA)
	Security Context	X
Data Confidentiality	Connection Confidentiality	X
	Content Confidentiality	M
	Message Flow Confidentiality	X
Data Integrity Service	Connection Integrity	X
	Content Integrity	M
	Message Sequence Integrity	X
Non-repudiation	Non Repudiation of Origin	M
	Non-Rep. of Submission	O
	Non-Repudiation of Delivery	O
Message Security Labeling Security Management	Message Security Labeling	X
	Change Credentials	X
Service	Register	X
	MS-Register	X
EDIM Responsibility Authentication	Proof of Transfer	X
	Proof of Retrieval	O
	Proof of Transfer	X
	Proof of EDI Content	M
Non-repudiation of EDIM Responsibility	Non-Repudiation of EDI Notification	M
	Non-Repudiation of EDI Retrieval	X
	Non-Repudiation of Transfer	X
	Non-Repudiation of EDI Content	M

3. KT-EDI 시스템 구성

KT-EDI시스템은 EDI의 국제표준 통신규약인 X.435와 국제 EDI문서표준인 UN/EDIFACT에 준거하여 개발된 국제표준 공중서비스용 EDI시스템이며, 표준 메시지의 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 메시지들에 대한 정보보호를 실행하기 위해서 ITU-T X.500/509 프로토콜에 따라 구현한 정보보호시스템이 부가되어 있다.

KT-EDI 시스템은 크게 사용자측 시스템과 중계 역할을 수행하는 서버시스템, 정보보호 기능을 수행하는 정보보호시스템으로 대별된다.

가. 가입자시스템

가입자시스템은 사용자가 EDI 메시지를 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.

문서변환시스템은 응용시스템(Application)이 생성하는 데이터화일을 플랫화일로 매핑시켜주는 송신매퍼(SAM:Standard Application Mapper), 플랫화일을 EDI 표준화일(IC:InterChange file)로 변환하는 송신변환시스템(Encoder), 반대로 EDI 표준화일을 플랫화일로 변환하는 수신변환시스템(Decoder), 플랫화일을 응용시스템이 이용할 수 있는 데이터화일로 매핑시켜주는 수신매퍼(PAM:Private Application Mapper)로 구성 되어있다.

문서변환시스템은 UN/EDIFACT에서 정의되었거나 ISO9735 구문규칙에 준하여 작성된 문서포멧과 KEDIFACT에서 정의되었거나 KSC5863에 준하여 작성된 문서포멧을 작업의 기본으로 하여 거래 상대방에 따라 달라질 수 있는 다양한 EDI표준메시지 버젼의 지원을 위해 다중버젼 지원기능을 수반한다.

또한 문서변환시스템은 사설문서포멧을 표준전자문서로 변환하면서 UN/EDIFACT 메시지 레벨에서 전자문서 인증(Authorization)과 전자문서 암호화를 수행하거나 수신된 표준전자문서를 사설문서포멧으로 역변환하면서 암호화된 전자문서의 복호화 또는 인증검사를 수행한다.

문서변환시스템에의해 이루어지는 전자문서 인증과 암호화는 송수자가 메시지 교환전에 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.

위의 인증을 위해 KT-EDI문서변환시스템에서는 DSA(Decimal Shift and Add)알고리즘과 자체에서 개발한 MATRIX인증 알고리즘을 이용한다.

나. 중계시스템

KT-EDI시스템의 서버 역할을 수행하는 중계시스템은 크게 메시지전송시스템(MTA: Message Transfer Agent)과 메시지저장기 (MS: Message Store)로 구성된다.

메시지저장기는 ITU-T X.413으로 정의되어 있는 기능을 수행하기 위해 가입자시스템과 메시지전송시스템 사이에 위치하여 원격지(Remote) 가입자시스템으로부터 제출된 EDI 메시지나 수신된 EDI 메시지를 보관하는 가입자 메일박스 기능을 수행한다.

메시지전송시스템은 ITU-T X.411로 정의되어 있으며 메시지저장기를 통해 제출된 가입자시스템으로 부터의 EDI메시지를 동일 시스템내의 수신자 메시지저장기로 배달하거나 타시스템의 메시지전송시스템으로 배달해주는 기능을 한다. 이때 메시지저장기와 메시지전송시스템간에는 P3 프로토콜(메시지 제출 및 배달규약)을, 메시지전송시스템간에는 P1프로토콜(메시지 전송규약)을 사용하는데 이들 프로토콜에 대해서는 ITU-T X.419로 정의되어 있다.

메시지전송시스템은 크게 메시지저장기와 접속을 위한 클라이언트/서버형의 P3인터페이

스와 P1 인터페이스, 그리고 메시지전송시스템 내부 프로세싱을 수행하는 시스템을 포함한 세부분으로 나뉘어진다. P3인터페이스는 원격지에서 메시지저장기를 통해 메시지를 송수신하는 가입자와 메시지전송시스템과 직접 접속하는 UA(User Agent)을 위해 제출/배달 및 관리하는 부차적 기능으로 나뉜다. 또한 메시지전송시스템간의 접속을 위한 P1 인터페이스는 메시지 전송기능을 수행한다. 마지막으로 내부 프로세싱 시스템은 메세지전송처리기의 Kernel로서 메시지 splitting, routing, redirection 등의 내부 기능을 수행한다.

KT-EDI시스템에서는 중계시스템을 이용하는 EDI-UA나 사설 메일시스템들이 KT-EDI 중계시스템의 서비스를 쉽게 이용할 수 있도록 하기 위해 메세지저장기 API(이하 MS-API)와 응용 API(이하 AAPI)를 별도 제공하므로써 중계시스템의 사용자 유형은 메시지 저장기능을 필요로 하는 P7 사용자, 메시지 저장기능을 필요로 하지 않는 P3 사용자, 기타 사설 메일시스템 사용자로 구별 지울 수 있다.

중계시스템 사용자 유형별 프로세스 흐름을 약술하면 다음과 같다. 우선 P7 사용자가 작성한 메세지는 P7 UA와 MS-API를 통하여 중계시스템의 MS에 전달되고, 이는 다시 메세지 큐를 통해 MTA에게 최종 제출된다. 제출된 메세지는 MTA에서 라우팅과 같은 일련의 과정을 거쳐 해당 목적지 MTA로 전달되며, 목적지 MS, MS-API를 거쳐 최종적으로 수신 UA에게 전달된다[3][4]. 다른 사설 메일시스템이 KT-EDI MTA를 통하여 메세지를 송수신 할 수 있도록 하기 위하여 관문 API(Gateway API:이하 GAPI)가 제공된다. 이외에 MTA는 디렉토리 서비스 및 84 MHS와의 연동서비스 기능을 제공한다[6]. 정보보호 기능이 결합되어 있지않은 상기 기술한 기능을 수행하는 KT-EDI 시스템의 구성도는 (그림 1)과 같다.

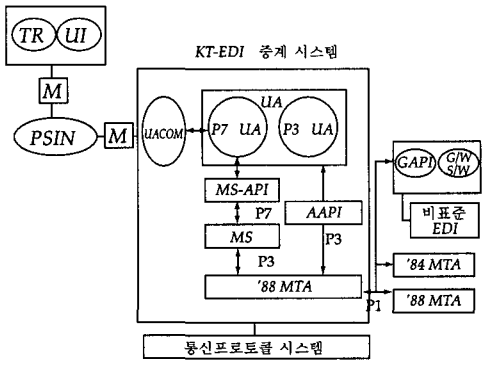


그림 1 기존 KT-EDI 시스템 구성도

4. KT-EDI 정보보호시스템

가. KT-EDI 정보보호 서비스 레벨

그림 1에서와 같이 순수 KT-EDI시스템(가입자시스팀과 중계시스템)과 정보보호기능을 수행하는 정보보호시스템인 CA(Certificate Authority), DS(Directory Server), 감사추적(Audit)시스템이 결합된 전체시스템을 본고에서는 KT-EDI 정보보호시스템이라 한다.

KT-EDI정보보호시스템에서는 유통 메시지에 대한 정보보호를 두단계 레벨로 나누어서 구현하였다.

첫번째 레벨은 UN/EDIFACT 전자문서 레벨에서 이루어지는 정보보호이며, 두번째 레벨은 ITU-T X.435메시지 레벨에서 이루어지는 정보보호 기능이다. UN/EDIFACT 전자문서 레벨에의 정보보호란, EDI 표준 전자문서(Interchange)를 생성(Generation)하는 단계와 수신한 EDI 표준 전자문서를 응용시스템에 전달하기 위하여 역변환(Interpretation)하는 단계에서 문서변환시스템에의해 시행되는 정보보호 행위를 말한다.

ITU-T X.435메시지 레벨에서의 정보보호는

UN/EDIFACT 전자문서 레벨에의 정보보호가 시행되었든지에 관계없이 ITU-T X.435 프로토콜에 따라 유통시킬 메시지를 대상으로하여 인증 및 무결성,암호화 등의 정보보호를 말한다.

KT-EDI시스템에서 위와같이 두 레벨에서의 정보보호를 시행했던 이유는, 전자문서가 송신자에 의해 생성되는 순간부터 정보보호가 시행되어 정당한 수신자에의해 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, X.420 통신처리시스템이나 Internet 메일, 키타 통신처리 장치를 이용하여 유통된다 하더라도 최소한의 정보보호 기능인 인증과 무결성을 이루기 위함이다.

UN/EDIFACT 전자문서 레벨에서 이루어지는 정보보호의 종류는 송신시 전자문서 인증(Authorization)과 전자문서 암호화(Encryption)가 있으며, 수신시 전자문서에 시행된 인증검증과 복호화(Decryption) 기능이 있다. 전자문서 인증과 암호화/복호화를 위해 송수자가 메시지 교환전에 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.

전자문서 인증을 위해 문서변환시스템에서는 DSA(Decimal Shift and Add)알고리즘과 자체에서 개발한 MATRIX인증 알고리즘을 이용한다.

ITU-T X.435메시지 레벨에서의 정보보호는 실제적으로 EDI 중계시스템과는 무관하게 정보보호 기능을 시행하게 하였다. 다시말하여 EDI 중계시스템은 자신이 중계해야되는 메시지가 정보보호가 이루어져 있는 메시지인지 아닌지 전혀 알필요가 없다.이는 ITU-T X.435 메시지 레벨에서의 정보보호는 실제적으로 EDI 중계시스템과 떨어져 원격지에 위치한 가입자시스템에서 이루어지기 때문이다. 따라서 일단 가입자시스템에서 송신할 메시지를 대상으로하여 시행된 모든 정보보호 서비스들은 메시지 수신자의 가입자시스템에의해 정상적으로 수신되어 정보보호 시스템과 문서변환 시스템에의해 정보보호 검증이 수행되지 않으면 유통된 메시지는 사용될 수 없다.

이와같이 완전한 엔드-투-엔드 정보보호를 이루게 하므로써 정보보호로 인한 오버헤드로부터 중계시스템을 자유롭게 하였으며, 중계시스템의 개입을 완전히 베제시키므로써 보다 강화된 메시지 무결성을 이룰 수 있게하였다.

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

특히 메시지내용 자체의 암호화에는 속도를 고려해 대칭키방식 암호화 알고리즘인 DES 와 순수 국산화개발된 불럭암호화 알고리즘인 BASE96를 사용한다.

따라서 ITU-T X.435메시지 레벨에서의 정보보호를 시행키 위해 전자 보증서를 생성, 유지관리할 수 있는 CA(Certificate Authority)와 생성된 보증서를 인터넷상에 공개관리할 수 있는 DS(Directory Server) 기능의 구현이 요구되었다. 이를위해 CA에서는 ITU-T X.509 공개키 보증서 버전 V3와 취소목록 버전 V2를 채택적용하였으며, LDAP 프로토콜 지원 DS 서버를 구현하였다.

KT-EDI정보보호시스템의 구성은 그림 2에 나타난 바와같이 크게 가입자시스템과 중계시스템 그리고 정보보호를 위한 정보보호시스템으로 구성하였다. 가입자시스템과 중계시스템 또는 정보보호시스템과의 연동은 TCP/IP 프로토콜을 이용하여 실현하였다.

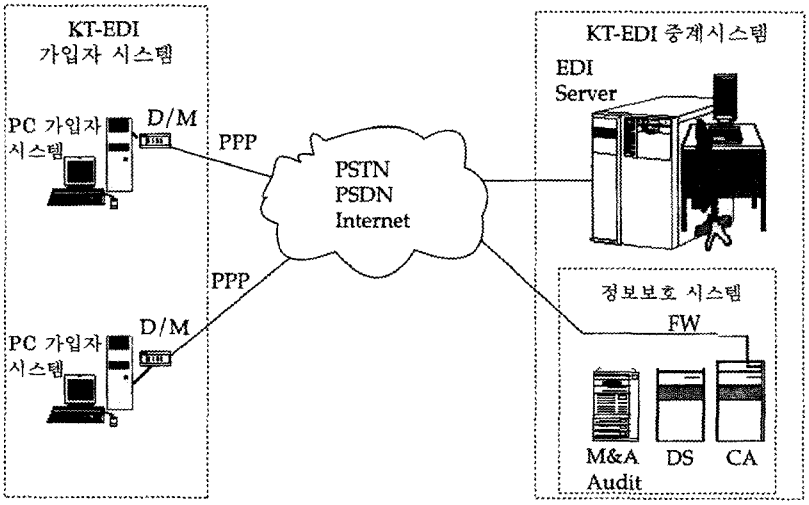


그림 2 KT-EDI정보보호시스템 네트워크

나. 정보보호 시스템 구성

KT-EDI시스템에서 정보보호 기능을 수행하는 정보보호시스템은 그림 3에 나타난바와 같이 정보보호 시스템은 기능 측면에서 크게 4가지로 구성된다. 응용시스템과 정보보호시스템 사이에서 인터페이스 기능을 수행하는 가입자시스템과, 정보보호 처리에 사용할 키 관리 및 보증서 발급, 보증서 취소 등의 기능을 담당하는 KMS(Key Management System) 모듈, 디렉토리 서버, 정보보호 서비스를 실제 처리하는 SES(Secure EDI System) 모듈 및 송수신 부인봉쇄(Non-Repudiation)을 위해 필요 증거들을 유지, 관리하여 감사추적(Audit) 기능을 수행하는 SAS(Secure Audit System) 모듈로 이루어져 있다. 이들간의 논리적인 시스템 구성도는 그림 3과 같다.

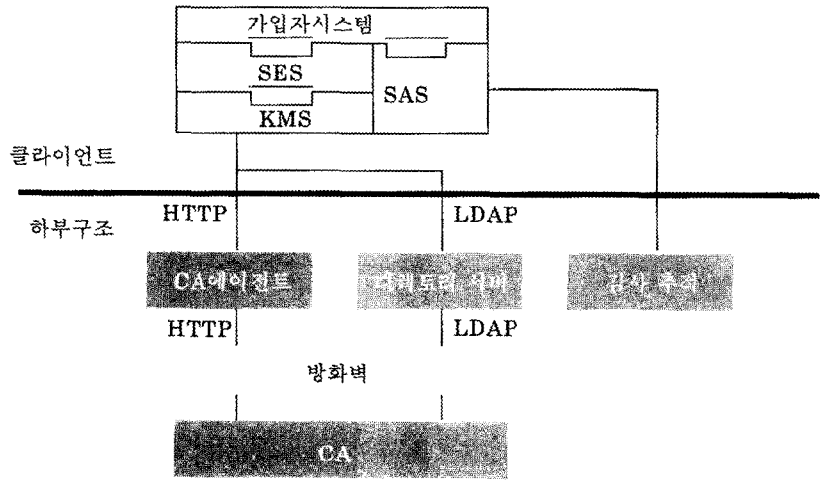


그림 3 정보보호 시스템 구성

1) KMS 모듈

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[7]. KMS(Key Management System) 시스템은 이러한 요구사항에 의해 개발된 KT-EDI시스템용 PKI시스템이다. SSLeay를 사용하여 개발된 KMS시스템의 주요 구성요소는 PKI클라이언트와 CA이다. PKI클라이언트는 키 관리 서비스를 제공하기 위해 keyman API 인터페이스 모듈, DER지원 모듈, 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[8]. 그림 4는 KT-EDI가입자시스템과 KMS와의 인터페이싱을 나타낸다.

2) SES 모듈

SES(Secure EDI System)은 KT-EDI 정보보호시스템에서 정보보호 서비스를 처리하는 핵심 기능 을 담당한다. SES는 가입자시스템으로부터 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[9].

SES에서의 정보보호 서비스 처리과정을 살

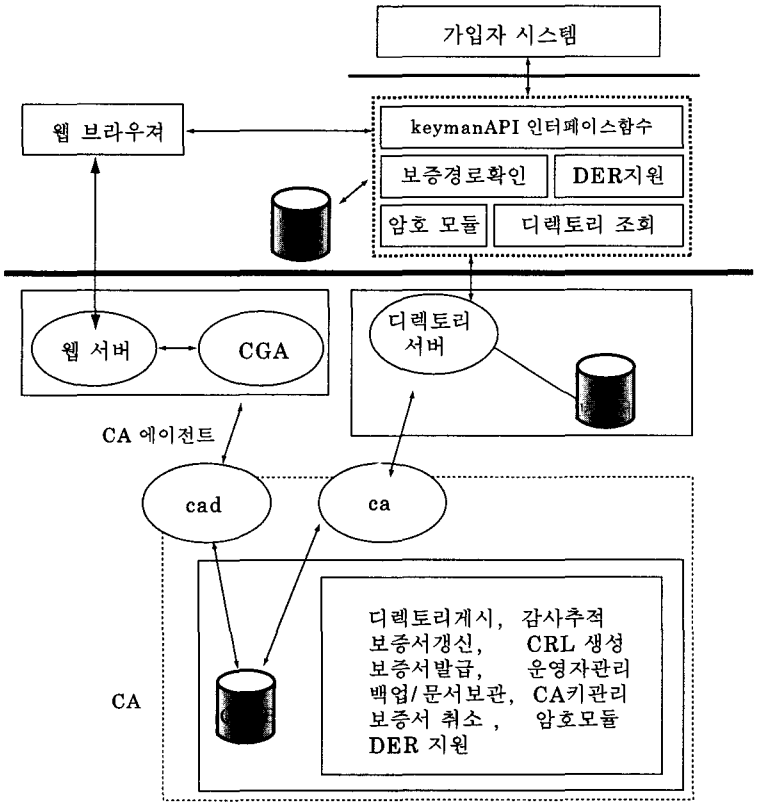


그림 4 KMS 구성

펴보면, 먼저 SES 인터페이스를 통해 요청 서비스의 종류와 서비스 처리에 필요한 데이터들을 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 KMS 인터페이스와 SAS인터페이스 등을 사용하게 된다. KMS, SAS 인터페이스가 필요한 이유는 다음과 같다. 첫째, 정보보호 서비스의 제공을 위해서 자신의 비밀키, 공개키 또는 상대방의 공개키가 필요하다. 이들 데이터를 획득하기 위해서는 EDI 각 컴포넌트에 첨가되는 KMS 인터페이스를 이용하여야 한다. 둘째, SES에서 발생한 정보보호 서비스 관련 행위는 기록되고 관리되어야 한다. 이를 위하여 SAS 인터페이스를 이용한다. 그림 5는 SES의 구성요소 및 가입자 시스템 및 중계시스템과의 상호 동작에 대해 나타내고 있다.

3) SAS 모듈

SAS(Secure Audit System)은 KT-EDI시스템을 이용하여 교환된 문서에 대해 분쟁이 발생하는 경우를 대비해 준비된 시스템이다. SAS 시스템은 정보보호 서비스 처리 시 이후에 논란의 여지가 발생할 수 있는 정보를 획득, 저장해 두었다가 분쟁 발생시 저장된 정보를 분쟁 조정에 이용할 수 있도록 한다. 일반적으로 정보보호시스템에서의 감사추적은 정보보호

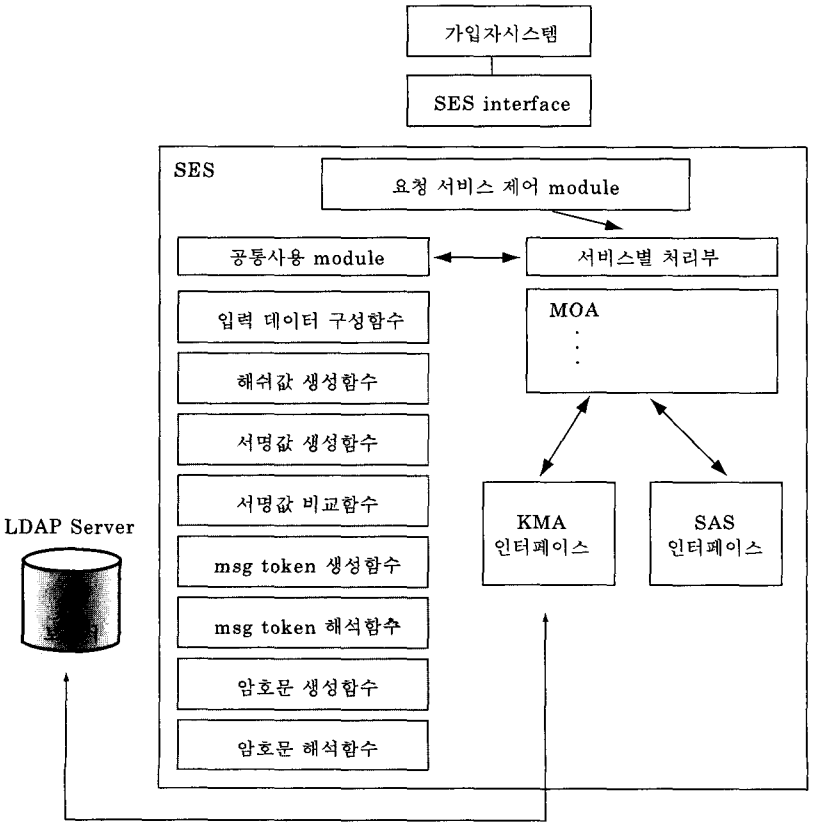


그림 5 SES 구성

서비스와 관련된 모든 행위의 기록을 요구한다. 하지만 네트워크 환경에서 발생하는 수많은 정보를 전부 관리할 수는 없다. 따라서 KT-EDI 시스템에서의 감사추적은 부인봉쇄 서비스와 연관되어 정의되어야 한다. 여기서 한가지 고려할 사항은 부인봉쇄의 대상이 되는 데이터를 중앙에서 관리해야 하느냐, 아니면 사용자가 중요하다고 판단되는 데이터를 자체 보관하다가 문제 발생시 이를 제출하도록 하여 부인봉쇄 서비스를 제공하느냐 하는 것이다. SAS 시스템은 중앙에서 집중 관리하도록 설계되었다.

SAS 모듈은 크게 다섯개의 모듈로 구성된다. 시스템의 보안을 위하여 시스템에 로그하는 모든 사용자의 이름과 패스워드를 관리하는 로그인 처리모듈, 생성된 메세지를 관리하는 큐(Queue) 관리 모듈, 큐에서 메세지를 가져오는 SAS 인터페이스 모듈, TCP/IP를 통해 SAS 인터페이스 모듈에서 받은 메시지를 감사정보로 분류/저장하는 사건분류 저장모듈 및 사건분류 저장 모듈에 의해 분류된 데이타를 저장하는 화일과 사용자 요구에 의해 화일에 저장된 감사 정보를 제공해 주는 감사제공 처리모듈이 그것이다. 이들간의 관계를 그림 6으로 나타낸 것이다.

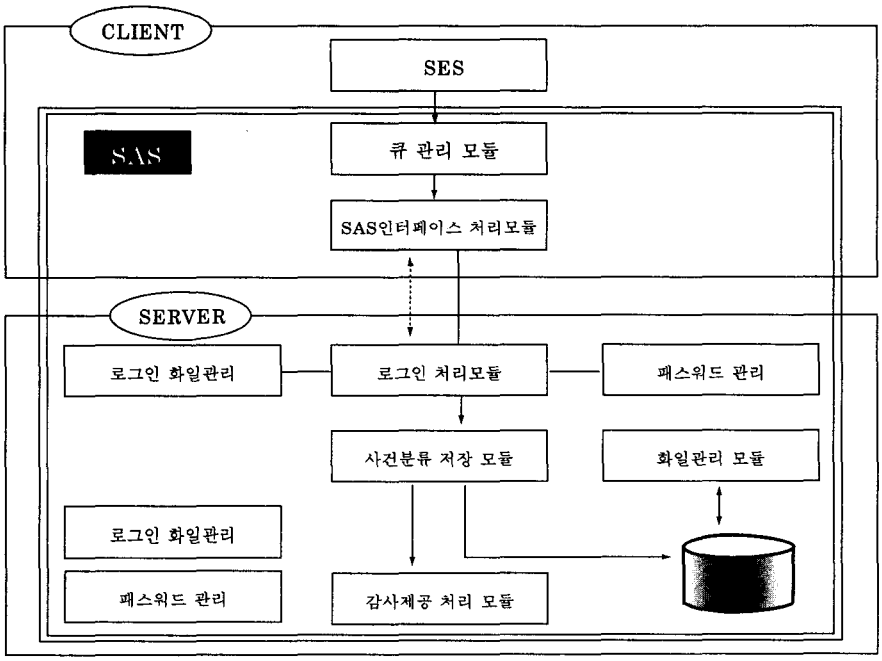


그림 6 SAS 구성

5. KT-EDI시스템 정보보호 처리

KT-EDI 가입자시스템은 크게 4개의 계층으로 구성되어 있다. 최상위 계층인 사용자 인터페이스 모듈은 다양한 응용시스템들과 인터페이싱 하기 위한 도구들과 시스템 관리를 위한 사용자인터페이스를 제공한다. 두번째 계층인 문서변환 계층은 응용 시스템으로부터 받은 사설 데이터를 EDI 표준 데이터 포맷으로 변환 시키거나, 반대로 수신한 EDI 표준 데이터 포맷을 사설 데이터 포맷으로 변환하는 기능

을 수행한다. 세번째 계층은 정보보호 모듈로서 실제적으로 정보보호 모듈과 인터페이싱을 이루어 사용자 정보보호 요구사항을 처리하는 기능을 수행한다. 최하위 계층인 통신계층은 중계시스템과의 EDI메세지를 교환 및 정보보호 관련 서버, 즉 CA, 디렉토리 서버, SAS서버와 정보보호 관련 정보를 교환할 수 있도록 하기 위한 TCP/IP 통신 기능을 제공한다.

정보보호 모듈을 이용하여 실제적으로 정보보호가 이루어지는 단계를 메시지의 송신과 수신단계로 나누어 설명하면 다음과 같다.

가. 송신 정보보호 처리

ITU-T X.435 레벨에서 EDI 메세지 송신의 경우, 정보보호 처리를 위한 첫 단계는 가입자 시스팀의 사용자 인터페이스모듈을 통해 사용자가 로그할 때, 사용자의 로그인 아이디와 패스워드를 매개변수로 사용하여 KMS 클라이언트 모듈을 호출함으로써 시작된다. KMS 클라이언트 모듈은 암호화된 상태로 저장된 사용자의 비밀키(private key)를 복호화하여 사용자 시스템의 메모리에 유지관리하므로 이후 정보보호 서비스 시행시 사용자의 비밀키가 필요할때 사용할 수 있도록 준비한다. 다음 단계는 변환모듈의 송신변환 시스템이 송신변환기능을 수행하여 인터체인지 화일을 생성하고, 인터체인지 화일의 정보보호 서비스 시행을 위한 정보보호 인터페이싱 화일을 작성하여 정보보호 모듈의 SES 클라이언트 모듈을 호출한다. 정보보호 계층의 SES 클라이언트는 통신모듈을 통해서 디렉토리서버에 접속하여 필요한 보증서(certificate)를 얻고 정보보호 인터페이싱 화일에 설정되어 있는 정보보호 서비스 요청내역을 참조하여 정보보호 서비스를 시행한다. 마지막 단계로 상기 과정으로 생성된 인터체인지 화일과 정보보호 인터페이싱 화일은 통신모듈의 TCP/IP 통신 에뮬레이터를 이용해 중계시스템에 제출된다.

나. 수신 정보보호 처리

ITU-T X.435 레벨에서 EDI 메세지 수신의 경우, 정보보호 처리를 위한 첫 단계는 송신시와 같이 가입자시스템의 사용자 인터페이스를 통해 사용자가 로그인 할 때, 사용자의 로그인 아이디와 패스워드를 매개변수로 사용하여 KMS 클라이언트 모듈을 호출함으로써 시작된다. 가입자시스템의 통신모듈을 통해 인터체인지 화일과 정보보호 인터페이싱 화일을 중계시스템으로부터 수신한 후, 수신변환을 수행하기 이전에 수신자가 정보보호 서비스를 요청한다. 이 과정에서 정보보호 모듈의 SES 모듈을 호출하게 되는데, 이는 수신된 인터체인지 화일과 정보보호 인터페이싱 화일을 대상으로 정보보호를 검증하고, 검증에 문제가 없을 경우에 걸려있는 정보보호를 해제하기 위함이다. 정보보호 모듈의 SES 클라이언트는 디렉토리 서버에 접속하여 메세지 송신자의 보증서(certificate)를 얻고 정보보호 인터페이싱 화일에 설정되어 있는 정보보호 서비스 요청내역을 참조하여 정보보호 검증 및 해제 서비스를 시행한다. 이러한 과정을 거친후에야 인터체인지 화일은 정상적으로 수신 변환시스템을 통해서역변환되어 응용시스템이 처리할 수 있는 사설 데이터 포맷으로 바뀌어 응용시스템에 전달시킴으로써 수신과정을 종료한다.

5. 결 론

금번 구현된 KT-EDI 정보보호 시스템은 OSI 기반에서 동작하는 KT-EDI시스템을 대상으로 하여 공개키 기반(PKI)에서 동작되도록 설계, 구현되었다. 기 구현된 정보보호 모듈을 활용하여 OSI기반이 아닌 인터넷기반에서 동작되는 메세징시스팀들에 활용될 수 있도록 인터페이싱 기능을 보편화 시키는 작업이 더 요구되며 더 나아가 인터넷 기반 전자상거래 분야의 적용을 위해서 더 많은 연구가 필요하다.

참 고 문 헌

[1] ITU-T X.400, Message Handling Services : Message Handling System & Service overview, 1993

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

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

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

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

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

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

[8] 이정현, 안전한 EDI 시스템의 데이타 구조, 제 2차 안전한 EDI 관련기술 심포지움, 1996

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

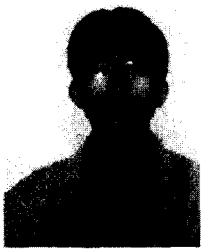
[10] Mitchell, Walker, Rush, "CCITT/ISO standards for Secure Message Handling", IEEE Journal on Selected areas in Communications, Vol.7, No.4, May 1989

□ 著者紹介

염 용 섭

1982년 숭전대학교 전산학과(학사)
1986년 충남대학교 전자계산과(석사)
~ 현재 한국통신 멀티미디어연구소 물류기술 연구실

※ 주관심분야: EDI 시스템, 공개키기반 정보보호 시스템,



김 현 호

1989년 2월 서울대학교 물리학과(학사)
1993년 2월 서울대학교 물리학과 (석사)
~ 현재 한국통신 멀티미디어연구소 물류기술 연구실

※ 주관심분야 :EDI 시스템, 공개키기반 정보보호 시스템,