PKI기반 KT-EDI 정보보호시스템 구현

염용섭,강경희,황미화
한국통신 멀티미디어연구소

The implementation of Secure KT-EDI System based on PKI

Yong-Seop Yeom, Kyung-Hee Kang, Mi-Hwa Hwang
Multimedia Technology Research Laboratory Korea Telecom R&D Group

요 약

정보화 사회로 다가갈수록 정보보호 위협요소가 증가되고 있고, 이러한 위협요소의 증가는 정보통신 서비스의 활용을 저해하는 주요 문제점으로 대두되고 있다. 이에 따라, 본 연구실에서는 안전하고 신뢰성을 갖춘 EDI 시스템을 구축하기 위하여, '95년 개발 완료된 KT-EDI시스템을 토대로 암호화, 무결성, 인증, 감사추적 등의 필수적인 정보보호 서비스를 제공할 수 있는 시스템을 개발하였고, 본 논문에서는 이에 대한 구축사례를 기술한다.

1. 개 요

EDI 란 종이 없는 문서 거래를 실현하기 위한 전자문서교환으로, EDI 시스템을 사용하여 문서 교환이 이루어지는 경우, 기업의 주요 정보들이 사설, 혹은 공공 통신망을 통해 전송된다 이러한 과정에서 정보가 노출되거나, 변조된 다면 문서 거래 당사자들은 상호 전달받는 정보에 대해 신뢰성을 가질 수 없게 된다 특히, 전자상거래와 같은 경제 분야나 공공기관에서의 EDI 방식 도입이 증가하는 현 시점에는 안전성과 신뢰성을 갖춘 EDI 시스템의 구현은 주요한 이슈로 제기되고 있다 따라서 본 논문에서는 한국통신에서 개발한 정보보호 서비스 기능을 갖춘 KT-EDI 정보보호 시스템의 구현 사례를 소개하여 정보교환에서의 안전성확보에 대한 해결방향을 제시하고자 한다

본 논문은 5장으로 구성된다. 2장에서 EDI 환경 하에서의 정보보호 서비스 요소를 기술하고, 이를 토대로 KT-EDI 정보보호 시스템의 설계 시, 선정된 정보보호 서비스 종류를 열거한다 3장에서 기존 KT-EDI 시스템의 구성도를 소개하고, 4장에서 보안 서비스 제공에 따른 KT-EDI 시스템의 재 구성도와 각 서브 시스템의 기능을 기술한다. 제 5장에서는 KT-EDI 정보보호 시스템 구현과 관련된 향후의 연구방향을 제시하고자 한다.

2. EDI 시스템의 정보보호 서비스

가. EDI 시스템에서의 정보보호 위협 요소 분석

EDI 환경에서의 정보 위협요소로는 위장(Masquerade), 메시지 순번 변조(Modification of Message Sequence), 정보의 변조(Modification of Information), 정보누출(Leakage of Information) 등이 있다. 이러한 정보보호 위협 요소로부터 정보 교환의 안전성을 확보하기 위해서는 다수의 정보보호 서비스가 필요하다 <표1>은 앞서 언급된 각 위협요소와 관련 표준안에 정의된 정보보호 서비스간의 대응 관계를 나타내고 있다

위협 요소		대응 서비스
대 분류	소 분류	
위장 (Masquerade)	- MTS의 위장 - 거짓 수신 확인 - 메시지 발신의 거짓 주장 - MTS사용자에 대한 MTA위장	- Message Origin Authentication - Secure Access Management - Peer Entity Authentication - Proof of Delivery - Message Origin Authentication - Proof of Submission - Report Origin Authentication - Secure Access Management
메시지 순번 변조	- 메시지 replay/ reordering	- Message Sequence Integrity
정보 변조	- 메시지 변조 - 메시지 파괴	- Content Integrity - Message Sequence Integrity
부인 (Repudiation)	- 발신 부인 - 제출 부인 - 배달 부인 - 전달 부인 - 검색 부인 - EDI 접수통지 부인 - 내용 부인	- Non-repudiation of Origin - Non-repudiation of Submission - Non-repudiation of Delivery - Non-repudiation/proof of Transfer - Non-repudiation/proof of EDI Retrival - Non-repudiation/proof of EDI Notification - Non-repudiation/proof of Content
정보 노출	- 기밀성 손실 - 익명성 손실 - 트래픽 분석	- Content Confidentiality - Disclosure of other recipients - Message Flow Confidentiality

<표 1> EDI 위협요소 및 대응서비스

나. KT-EDI 시스템의 정보보호 서비스

X.400계열 표준안에서는 다양한 시스템 환경 및 보안 정책을 고려하여, 광

범위한 정보보호 서비스를 정의하고 있다. 따라서 정의된 서비스들이 모두 제공될 필요는 없으며, 시스템의 용도 및 특성에 맞게 선택 기준을 설정하여 이에 따라 선정된 서비스를 대상으로 하여 시스템을 설계, 구현해야 한다. KT-EDI 시스템의 특성을 고려하여 선정된 정보보호 서비스는 <표2>와 같다.

서비스 요소	우선 순위
Message Origin Authentication	M (Mandatory)
Proof of Submission	O (Opuonal)
Proof of Delivery	O
Peer Entity Authentication	O
Content Confidentiality	M
Content Integrity	M
Non Repudiation of Origin	M
Non-Rep of Submission	O
Non-Repudiation of Delivery	O
Proof of Retrieval	O
Proof of EDI Content	M
Non-Repudiation of EDI Notification	M
Non-Repudiation of EDI Content	M

<표 2> KT-EDI시스템을 고려한 정보 보호 서비스의 우선 순위

3 기존 KT-EDI 시스템 구성

KT-EDI 시스템은 크게 세가지 하부 시스템들로 구성된다. 즉 ① EDI 메시지를 만들어 KT-EDI 중계시스템에 전송하는 기능과 메시지를 수신할 수 있는 기능 및 사설문서와 표준 문서간의 상호변환 등의 기능을 수행하는 문서변환 가입자(TR/UI) 시스템, ② 사용자가 제출한 메시지를 해당 사용자에게 배달 및 전송, 저장기능을 수행하는 중계시스템, 및 ③ 이 기종간의 메시지 전송을 위해 개발된 OSI 7계층으로 개발된 통신 프로토콜 시스템이 그것이다.

KT-EDI 문서변환가입자 시스템은 UN/EDIFACT에 의거하여 개발된 시스템이다. 문서변환 가입자시스템은 트랜스레이터(Translator)와 응용 매핑 시스템 및 표준 테이터 데이블 관리 모듈로 구성된다.

KT-EDI 중계시스템은 ITU-T X.435/F.435와 X.400/F.400 표준안을 채택한 개방형 EDI시스템이다. 중계시스템은 메시지 저장 시스템(Message Store' 이하 MS), 메시지 전송 처리기(Message Transfer Agent 이하 MTA) 및 가입자 처리기(User Agent 이하 UA)로 중계시스템의 주요 기능은 TR/UI로 부터 제출된 메시지를 수신자에게 전달하는 것이다. 이때 중계시스템을 이용하는 EDI-UA나 사설 메일 시스템이 중계시스템의 서비스를 쉽게 이용할 수 있도록 하기' 위해, 메시지 저장기 API(이하 MS-API)와 응용 API(이하 AAPI)를 제공한다. 중계시스템의 사용자 유형은 아래와 같다

- 메시지 저장기능을 필요로 하는 P7 사용자
- 메시지 저장기능을 필요로 하지 않는 P3 사용자
- 기타 사설 메일 시스템 사용자

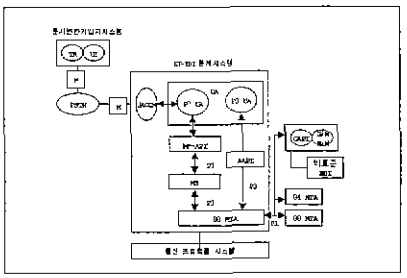
시스템 사용자 유형별 프로세스 흐름을 약술하면 다음과 같다. 우선 P7사용자가 작성한 메시지는 P7UA와 MS-API를 통하여 중계시스템의 MS에 전달되고, 이는 다시 메시지 큐를 통해 MTA에게 최종 제출된다. 전달된 메시지는 MTA에서 라우팅과 같은 일련의 과정을 거쳐 해당 MTA로 전달되며, MS, MS-API를 거쳐 최종적으로 목적하는 수신 UA에게 전달된다. P3사용자의 경우에는, P3-UA와 AAPI를 이용하여 MTA에게 전달되고, 전달된 메시지는 동일한 방법으로 최종 목적 수신 UA에게 전달된다. 다른 사설 메일 시스템의 KT-EDI MTA를 통하여 메시지를 송수신 할 수 있도록 하기 위하여 관문 API(Gateway API 이하 GAPI)가 제공된다. 이외에 MTA는 디렉토리 서비스 및 '84 MHS와의 연동서비스 기능도 제공한다.

국제 표준기술에 따라 개발된 KT-EDI 시스템의 기본 구성도는 (그림 1)과 같다.

4. KT-EDI 보안 시스템

가. KT-EDI 보안 시스템의 정보보호 서비스 적용 범위

EDI 시스템에서 정보보호 서비스를 제공하기 위해 근간으로 사용하고 있는 X.400관련 표준에서는 그 적용 범위를 송신 UA의 사용자와 수신 UA의 사용자로 가정하고 있다. 그러나 실제로 KT-EDI 시스템의 사용자 환경을 분류해 보면, 일반 PC 사용자들이 PSTN이나 PSDN망을 통해 UA가 제공하는 인디페이스를 사용하여 메시지를 송수신하는 경우가 대부분이다. 따라서 위와 같은 사용자들에게는 현재 X.400관련 표준에 정의되어 있는 방법을 따라 정보보호 서비스를 제공하면 실질적인 정보보호 서비스를 제공할 수 없게 된다. KT-EDI 보안 시스템 구현 시, 이러한 문제점을 해결하기 위해 일차적으로 고려된 방안은 다음과 같다.



(그림 1) 기존 KT-EDI 시스템 구성도

- PC용 UA의 사용
- EDIFACT를 이용한 정보보호 서비스의 처리

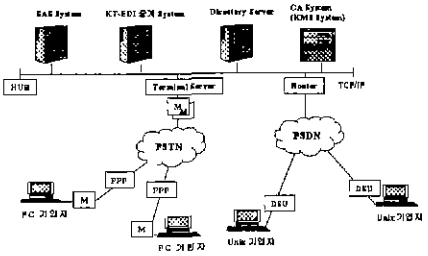
위의 두 가지 방법 중에서 사용자들에게 PC용 UA를 설치하게 하는 것은 다음과 같은 이유로 인해 현실성이 떨어진다. 첫째, 현재의 일반적인 추세가 PC에서는 UN/EDIFACT 문서의 변환 부분만을 제공하는 것이고, 둘째, PC용 UA를 개발한다면 단말 PC사용자에게 너무 무거운 시스템을 설치하도록 요구하게 되기 때문이다. 더불어 인터넷환경을 기반으로 한 시스템개발 추세로 볼 때 사용자들에게 시스템을 설치하라고 요구할 타당한 근거가 미약하다고 판단된다. UN/EDIFACT를 이용한 정보보호 서비스 처리방법도 현계점을 내포한다. 일반적으로 PC사용자들의 환경은 PSTN망을 사용하는 것이다. 따라서 UN/EDIFACT를 이용한 정보보호 서비스를 제공하는 사용자 단말에서부터 UA 간에는, EDI 표준문서에서 정의한 EDI시스템의 정보보호 서비스, 즉 메시지 발신처 인증, 제출증명, 배달증명과 같은 것들을 제공할 수 없게 된다.

따라서 현재 KT-EDI 보안 시스템에서의 정보보호 서비스 적용범위를 기존 KT-EDI 시스템의 실용환경으로 보고, Pomt-to-Pomt Protocol(이하 PPP)기반의 가입자시스템을 개발하여, 일반 PC사용자와 UNIX사용자에게 X.400에 정의된 방식의 정보보호 서비스를 제공하도록 하였다.

나 KT-EDI 시스템 보안 시스템 구현

1) KT-EDI 보안 시스템 구성도

KT-EDI 보안 시스템은 기능 측면에서 크게 6가지로 구성된다. ① PC가입자들에게 EDI 보안 서비스 제공하는 MICS 시스템, ② 사용자가 제출한 메시지를 해당 사용자에게 배달, 전송 및 저장기능을 수행하는 KT-EDI중계시스템, ③ 키 관리 및 보증서 발급, 보증서 취소 등의 기능을 담당하는 KMS시스템, ④ 디렉토리 서버, ⑤ 정보보호 서비스를 실제 처리하는 SES 시스템 및 ⑥ EDI 보안서비스 처리시 논란의 여지가 발생할 수 있는 정보들을 획득, 저장하는 SAS시스템이다. 이들간의 논리적인 시스템 구성도는 (그림 2)와 같다.



(그림 1) KT-EDI 보안 시스템 전체 구성도

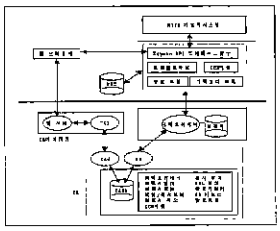
2) KMS와의 인터페이스

EDI 시스템에서 공개키 방식의 보안 서비스를 제공하기 위해서는, 안전하게 키를 생성, 배포, 보증서(Certificate) 생성/등록 및 취소관리 할 수 있는 공개키 기반구조(Public Key Infrastructure 이하 PKI)가 존재하여야 한다.

KMS(Key Management System) 시스템은 이러한 요구사항에 의해 개발된 EDI용 PKI시스템이다. SSLeay등 사용하여 개발된 KMS시스템의 주요 구성요소는 PKI클라이언트와 CA이다

PKI클라이언트는 키 관리 서비스를 제공하기 위해 keyman API 인터페이스 모듈, DER지원모듈, 암호 모듈, 디렉토리 조회 모듈 및 보증경로 확인 모듈로 구성되어 있다

CA를 구성하는 주요 모듈로는 CA 키 관리 모듈, 보증서 발급 모듈, 보증서 취소 모듈, 보증서 갱신 모듈, CRL 생성 모듈, 디렉토리 게시 모듈, DER 지원 모듈, 암호 모듈이다 (그림 3)은 MICS 시스템과 KMS 시스템간의 관계를 나타낸다



(그림 3) KMS로의 인터페이스

3) SES 단위 시스템

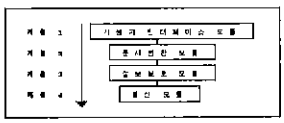
SES(Secure EDI System)은 EDI시스템의 UI 또는 UA시스템에 통합되는 단위 시스템으로, KT-EDI 보안시스템에서 정보보호 서비스를 처리하는 핵심 기능을 담당한다. SES는 4개의 하부 모듈로 구성된다. 즉 ① UI, UA로부터 정보보호 서비스 요청을 받아들이는 SES 인터페이스 모듈과 ② SES 인터페이스를 통해 요청 받은 정보보호 서비스 요구들간의 상호관계를 조사하여 처리 순서를 결정하고 해당 처리 함수를 호출하는 요청서비스 제어처리 부, ③ 정보보호 서비스에 공통적으로 사용되는 함수들을 모아놓은 공통 사용 함수처리 부, ④ 요청된 각각의 서비스를 처리하는 함수들로 구성된 서비스별 함수처리 부기 그것이다.

4) SAS 단위 시스템

SAS(Secure Audit System)은 정보보호 서비스 처리 시 이후에 논란의 여지가 발생할 수 있는 정보를 획득/저장해 두었다가 분쟁 발생 시 저장된 정보를 이용, 분쟁 조정에 이용할 수 있도록 하는 시스템이다. SAS 시스템은 크게 다섯 개의 모듈로 구성된다 ① 시스템의 보안을 위하여 시스템에 로그인하는 모든 사용자의 이름과 패스워드를 관리하는 로그인 처리 모듈, ② 생성된 메시지를 관리하는 큐(Queue) 관리 모듈, ③ 큐에서 메시지를 가져오는 SAS 인터페이스 모듈, ④ TCP/IP를 통해 SAS 인터페이스 모듈에서 받은 메시지를 감사 정보로 분류/저장하는 사건분류 저장 모듈 및 ⑤ 사건분류 저장 모듈에 의해 분류된 데이터를 저장하는 파일과 사용자 요구에 의해 파일에 저장된 감시 정보를 제공해 주는 감사 제공 처리 모듈이 그것이다

5) MICS 구성

KT-EDI 가입자시스템인 MICS는 크게 4개의 모듈로 구성되어 있다(그림 6)



(그림 6) MICS의 계층 구성도

① 다양한 응용시스템들과 인터페이싱 하기 위한 도구들을 제공하며 시스템 관리를 위한 사용자 인터페이스 모듈, ② 응용 시스템으로부터 받은 사설 데이터를 EDI 표준 데이터 포맷으로 변환시키거나, 반대로 수신한 EDI 표준 데이터 포맷을 사설 데이터 포맷으로의 변환기능을 수행하는 변환 계층 모듈, ③ 정보보호 서비스를 제공하기 위해 KMS 시스템과 SES 시스템과의 인터페이싱을 담당하는 정보보호 모듈, ④ 중계시스템과의 EDI 메시지를 교환 및 보안관련 서버들(즉 CA, 디렉토리 서버, SAS 서버)과의 보안관련 정보를 교환할 수 있도록 하기 위해 TCP/IP 통신 기능을 제공하는 통신모듈이 그것이다.

5 향후 계획

인터넷 및 웹 관련 기술의 급속한 발전과 사용자층의 확대는 전자상거래의 활성화에 중요한 계기가 되었을 뿐만 아니라 전자상거래의 기반 기술인 EDI에도 상당한 영향을 주어 인터넷의 잠재적 EDI에 적용한 인터넷 EDI 개발에 관한 연구가 활발히 진행중이다. 그러한 추세에 부합하여, OSI기반으로 개발된 EDI 시스템을 인터넷 EDI 시스템으로 확장시키는 데 있어서 일차적으로 고려해야 할 요인이 보안 문제이다. 기존의 EDI 시스템은 사설 망을 통하여 문서교환이 이루어졌기 때문에 보안에 대한 신뢰성을 확보할 수 있었으나, 인터넷 EDI 시스템은 누구나 접속할 수 있는 공개된 망을 통하여 문서교환이 이루어지기 때문에, 시스템에서 보안문제를 확실하게 보장해야만 한다

이번 개발된 KT-EDI 보안 시스템은 MEDICOM으로 상용서비스 중인 KT-EDI 시스템에 공개키 기반구조에 입각한 정보보호 기비스 제공기능을 보강한 것이다 따라서 향후에는 기 구현된 하부구조를 토대로 인터넷 EDI 로의 전환연구에 중점을 두어 전자상거래와 같은 인터넷 기반의 응용환경에 기반구조(infrastructure)로 구축하고자 한다

참고문헌

[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 데이터 구조, 제 2차 안전한 EDI 관련기술 심포지움, 1996

[9] 윤미중, 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, Vol7, No.4, May 1989