The Journal of Korean
Institute of CALS/EC
Vol. 5, No. 2, Dec. 2000

웹 환경의 E-Mail 기반 인터넷 EDI 시스템*

EIEW : An E-Mail based Internet EDI System on Web Environment

권혁인**, 이진용***

Hyeog In Kwon, Jin Yong Lee

Abstract

Lately, electronic commerce through the Internet has been rising in attention. An important element in such commerce is EDI. EDI is mainly used with VAN but its use is not common due to the high cost of EDI transfer. Thus, only large corporations with frequent use of EDI are able to benefit from it. To smaller companies that have small usage, EDI is becoming a burden. Considering this fact as well as current changes within the enterprise environment, it is apparent that a new generation of EDI is required. To resolve the problems of VAN EDI, the proposed Internet EDI was implemented. Internet EDI deals with the use of the widely spread Internet instead of VAN. By using Internet EDI, it is possible to reduce the high cost that came when using VAN. There would be no extra transfer cost since transmission will be done through the Internet. Also, electronic commerce that is mostly used today between an individual and a company may grow to become a true electronic commerce between companies.

Keyword : EDI, VAN EDI, Internet EDI, Public Key Encryption

---

* 본 연구는 중앙대학교 연구용기자재지원사업의 지원에 의해서 수행되었음.

** 중앙대학교 경영학과

*** (주)넥센

1. 서론

오늘날 세계는 인터넷을 이용한 비즈니스 거래가 확대되면서 인터넷을 기반으로 한 디지털 경제의 중요성과 발전 가능성이 강조되고 있다. 범세계적 정보 통신망인 인터넷의 급속한 확산과 정보 기술 발전은 일상생활과 비즈니스 관행을 근본적으로 변화시키고 있으며, 인터넷을 이용한 전자상거래는 가장 각광받고 있는 분야 중 하나로 자리 잡고 있다.

현재 인터넷을 통한 전자상거래 머천트 서버의 개발이 활발하게 이루어지고 있고 머천트 서버를 이용한 인터넷 쇼핑몰의 수는 기하급수적으로 늘어나고 있다. 이러한 전자상거래의 핵심 요소로 인식되는 것이 EDI(Electronic Data Interchange)이다. EDI는 국제간 또는 국내 기업간에 상거래와 관련된 각종 문서 및 데이터를 표준화된 형태로 컴퓨터로 주고받는 정보기술이다. 그동안 VAN을 통해서 이루어져 왔던 EDI는 전송량에 따른 비용의 부담으로 인해 대기업을 제외하고는 그 효과를 보지 못하고 있다. 또한 기업환경의 변화에 따라 이에 맞는 차세대 EDI가 요구되고 있다[2, 4, 5, 6, 7].

인터넷 EDI는 VAN EDI의 문제점을 해결하기 위해 제시되었다. 인터넷 EDI는 EDI 문서를 전송함에 있어 하부통신 프로토콜로 TCP/IP, 즉 인터넷의 사용을 의미한다[6, 7, 22]. 인터넷 EDI는 VAN EDI의 가장 큰 문제점으로 지적되고 있는 비용의 문제를 해결할 수 있다. 그리고 기존의 업무환경을 크게 변화시키지 않고서도 경비 등의 문제로 EDI를 사용하지 못했던 기업에게 EDI 시스템에 참여할 수 있는 기회를 제공함으로써 시장 확대를 가져 올 수 있다[2, 4, 5, 6, 7, 8, 9, 25, 26].

본 논문에서는 웹 환경의 E-Mail 기반 인터넷 EDI 시스템 EIEW(E-Mail based Internet EDI System on Web Environment)의 설계와 구현에 대해서 논한다. EIEW에서는 개방적인 인터넷의 특성에 따라 발생하게 되는 EDI 문서의 변경(Modification), 판독(Reading), 송수신 부인(Repudiation), 가장(Masquerade)의 문제를 공개키 기반의 암호화를 통해 해결했다. 웹 환경의 E-Mail 기반 인터넷 EDI로서, 인터넷 EDI의 전송방식 중 EDI의 요구조건에 가장 부합하는 E-Mail 이용하여, 웹 환경에서 구현되어 웹에서 이루어지고 있는 전자상거래와 통합적인 운영이 가능하다.

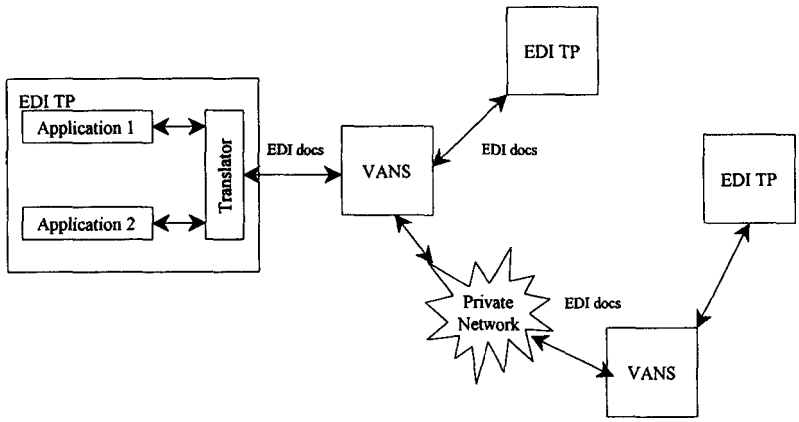
본 논문의 구성은 2장에서 기반 기술연구로서 VAN 기반 EDI의 문제점과 인터넷 EDI, 보안에 관해서 알아본다. 3장에서는 인터넷 EDI 동향 분석과 본 논문에서 구현하는 EIEW의 설계에 대해서 설명하고, 4장에서는 EIEW의 구현에 대해 논한다. 5장에서는 EIEW의 성능 평가와 마지막으로 6장에서 결론과 향후 연구 방향에 대해서 서술한다.

2. 기반 기술

2.1 VAN EDI

초창기에 EDI를 전송하는데 있어 거래 기업간에 직접 연결된 통신 경로를 이용하기도 했으나, 이 방법은 거래하는 기업의 수가 늘어나면 다루기가 어렵다는 단점을 가지고 있다. 현재 많이 사용하고 있는 방법이 VAN(Value Added Network)을 이용하는 방법이다[그림 1].

초기의 VAN에서는 각기 다른 VAN들간에



<그림 1> VAN EDI 구조도

상호 연결이 되지 않았기 때문에 같은 VAN을 사용하고 있는 기업들간에만 거래가 가능하였다. 현재는 VAN들 사이에 통신이 가능하여 거래에 참여하는 기업이나 은행 등이 반드시 동일한 네트워크를 사용하지 않아도 된다. 이는 기업이 거래의 폭을 넓히는데 유리하다. [1, 2, 3].

그러나 VAN EDI는 초기설치비용, 유지비용, 전송비용, 등 기본적으로 필요한 비용이 과다하며 VAN-to-VAN 연결 또한 추가비용을 필요로 한다. 축적전송 및 일괄처리 방식은 실시간 업무에 적용을 제한하고 있다.

2.2 인터넷 EDI

전통적인 EDI의 문제점을 해결하기 위해 개방형 EDI(Open-edi), 대화형 EDI(Interactive EDI), 인터넷 EDI가 제시되고 있다. 특히 인터넷의 확산에 따라 인터넷 EDI가 가장 큰 관심을 받고 있다. 인터넷 EDI(Internet EDI)란 EDI 문서를 전송함에 있어 하부통신 프로토콜로서 TCP/IP, 즉 인터넷을 사용하는 것을 의미한다.

인터넷을 이용하는 경우는 VAN을 이용할 때보다 네트워크 경비를 비롯한 각종 경비가 적게 들고 사용자에게 친숙한 인터페이스를 제공함으로써 좀 더 쉽게 EDI를 사용할 수 있다. 따라서 인터넷을 이용하는 경우 기존의 EDI와 크게 다른 환경으로 변화하지 않으면서도, 경비 등의 문제로 인하여 EDI를 활용하지 못했던 소규모 기업들이 EDI 시스템에 참여하게 되어 시장 확대를 가져 올 수 있다.[2, 4, 8, 9]

인터넷 EDI와 VAN EDI의 특성을 비교하면 <표 1>과 같다[2, 5, 6 10].

인터넷 EDI는 인터넷을 이용하므로 지역이나 업종, 시스템에 관계없이 사용자들이 정보를 교환할 수 있다. 또한 자체 네트워크를 갖지 못한 사용자들도 손쉽게 EDI 문서를 전송할 수 있으며, 단기간 내에 거래관계를 체결할 수 있다[22]. 인터넷 EDI가 가져다 줄 수 있는 이점을 요약하면 다음과 같다.

· VAN을 이용하는 경우보다 인터넷을 이용하는 것이 비용이 저렴하다. 또한 많은 VAN 들이 비표준적인 인터페이스를 사용하는

<표 1> VAN EDI와 인터넷 EDI의 비교

	VAN EDI	인터넷 EDI
개방성	· 폐쇄적	· 개방적
사용자 인터페이스	· 복잡하고 통합 관리가 필요	· GUI를 이용한 쉬운 사용자 인터페이스
경비	· 고가의 네트워크 사용료	· 저렴한 네트워크 사용료
사용자범위	· 사용자의 범위가 넓지 않다	· 전세계적인 사용자
메시지표준 계층	· EDI 문서 표준 (EDIFACT, ANSI X.12)	· EDI 문서 표준(EDIFACT, ANSI X.12) · 특정(Proprietary) 파일 형태 · HTML
봉합계층	· X.400 표준 · 특정 봉합 표준	· SMTP/MIME, FTP, HTTP · 특정 프로토콜
전송계층	· X.25 패킷 스위칭 네트워크 · 특정 프로토콜	· TCP/IP
물리계층	· 직접연결 · 다이얼업 회선 (Dial up lines) · 사설 네트워크	· 인터넷 · 다이얼업 회선

점을 감안하면 대기업의 경우 통신 환경을 인터넷의 TCP/IP 환경으로 통일함으로써 통신 회선 임대, 시스템, 인력에 대한 비용 등을 절감할 수 있다.

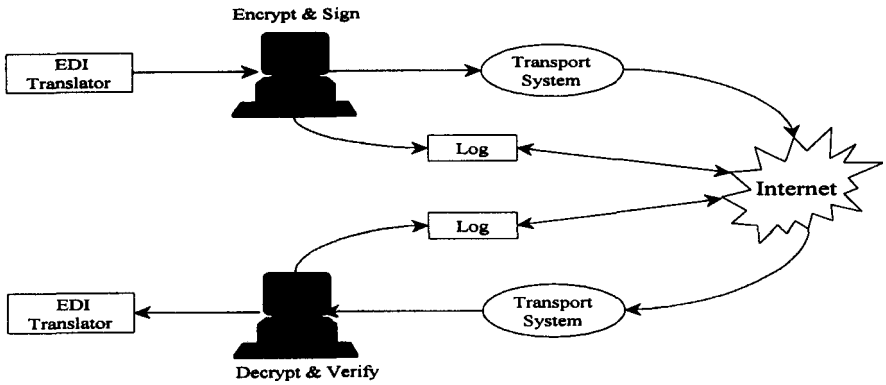
· VAN업체가 제공하는 네트워크는 폐쇄적이며 비표준적인 인터페이스를 가지고 있어서 거래 기업의 확대가 용이하지 않은 반면, 인터넷을 이용할 경우 인터넷의 개방성과 공중성으로 인해 글로벌하게 많은 기업들과 EDI를 실행할 수 있다.

· 자료 전송 속도 측면에서 인터넷을 이용하는 것이 VAN을 이용하는 것보다 빠르다.

· 경쟁력 확보 측면에서 JIT, QR, ECR 등과 같은 EDI를 기반으로 하는 새로운 기업 모형의 구현이 VAN을 이용하는 방식보다 용이하다.[7, 8].

2.2.1 E-Mail 기반 인터넷 EDI

SMTP/MIME(Simple Mail Transport Protocol/Multi-Purpose Internet Mail Extensions), 기반의 전자메일 즉, E-Mail을 EDI 문서 전송수단으로 사용한다. SMTP는 현재 인터넷상의 전자메일 전달방식으로 ITU에서 제정한 메시지 전달 서비스에 의한 표준인 X.400과 더불어 범용적으로 사용되는 전자메일 표준이다. MIME은 SMTP의 텍스트 메시지 포맷을 확장하여 멀티미디어 데이터를 수용할 수 있도록 확장된 표준이다. 축적전송 방식의 E-mail은 EDI의 요구조건에 부합하고 있다. 또한 SMTP/MIME을 이용하여 멀티파트를 지원할 수 있고 다수의 수신자를 지원할 수 있다. 또한 보안에서는 PEM, SMIME과 같은 방법을 이용하여 문서의 암호화를 할 수 있다. E-Mail 기반 인터넷 EDI의 기본적인 구조는 다음 <그림 2>와 같다.



<그림 2> E-Mail 기반 인터넷 EDI

2.2.2 FTP 기반 인터넷 EDI

FTP는 한 호스트에서 다른 호스트로 파일 전송할 때 사용하는 프로그램으로서 SMTP와 같이 TCP/IP 네트워크에서 사용하는 상위 응용 프로그램이다. 그러나 SMTP/MIME과 같은 메시지 기반의 시스템이 아니라 파일 전송 시스템이라는 측면을 고려하면 네트워크 상에서 EDI 자료를 교환하는 방식으로 보다 적합할 수도 있다. FTP로 자료를 교환하기 위해서는 두 호스트간에 세션을 설정하여 자료의 교환이 이루어지게 된다.

FTP는 동기화(Synchronous) 응용 프로토콜로서 클라이언트/서버 모델이다. FTP를 SMTP/MIME에 비교하면 다음과 같은 장·단점을 가지고 있다. 첫째 FTP는 세션을 설정하기 위해서 ID와 패스워드가 암호화 되지 않고 전송되므로 보안에 관련되어 추가적인 비용이 발생한다. 또한 SMTP/MIME 방식의 EDI는 기본적으로 전자우편시스템을 이용하여 EDI 파일을 전송하므로 FTP 방식보다 약 1/3정도 파일 용량이 증가하게 된다.[9] 따라서 FTP 방식은 전송 속도가 빠르며, 대용량의 자료 전송에 적합하다. 셋째, FTP 방식은 거래 상대방의 내부 시스템에 대한 직접 접속에 대한 위험 부담과 이에 대한 관리가 용이하지 않다.

인터넷 이용하여 EDI 자료를 교환하려할 때 FTP를 이용하는 방식은 VAN을 매개로 할 경우 SMTP/MIME을 이용하는 방식보다 용이하게 인터넷의 장점을 활용할 수 있다는 측면에서 단기적으로 현실적인 방안일 수 있다. 그러나 인터넷상의 보안 문제를 해결을 위한 기술적인 발전과 관리상의 문제점 등을 고려하면 장기적으로는 SMTP/MIME을 이용하는 방식을 이용해야 한다.

2.2.3 HTTP기반의 웹-EDI

웹-EDI는 HTTP를 이용한다. 웹 환경에서 사용자는 인터넷 접속과 브라우저만을 가지고 전자자료 교환을 할 수 있는 방식으로 응용 프로그램, 변환 기능 등 EDI 실행에 필요한 서비스를 웹 서버가 제공해주는 형태이다. 따라서 기업 입장에서는 EDI 실행을 위한 기술, 시스템, 인력에 대한 투자부담에서 벗어나 적은 비용으로 전자적인 자료 교환을 할 수 있다.

<표 2> EDI 기준에 따른 인터넷 전송방식 비교

기준	FTP	HTTP	E-Mail	EDI 요구조건
Mode	Synchronous	Synchronous	Asynchronous	Asynchronous
Model	Client/Server	Client/Server	Store and Forward	Store and Forward
Security	No	SHTTP	PEM, SMIME	High security
EDIFACT 지원	Yes	Yes	Possible with MIME	Yes
Multipart Body	No	Yes	Possible with MIME	Yes
Multidestination	No	No	Yes	Yes
Forwarding	No	No	Yes	Yes

HTTP는 EDI에서 요구하고 있는 비동기화(Asynchronous) 방식이 아니기 때문에 EDI에 적합하지 않다. 그러나 HTTP는 정보를 전달하는 관점에서 서로 다른 형태의 멀티파트를 포함할 수 있고 S-HTTP와 같은 보안 기능을 가지고 있어 긍정적인 면도 포함하고 있다.

2.2.4 인터넷 EDI 기반기술 비교

인터넷 EDI의 구현방법인 인터넷 메일, FTP, 웹을 EDI의 요구조건과 비교하면 <표 2>와 같다[24, 25, 26].

<표 2>에서 볼 수 있듯이 EDI 요구조건에 가장 부합하는 인터넷 응용 프로토콜은 E-Mail이다. EDI에서 요구하고 있는 비동기화 전송 방식, 축적 전송, SMIME과 PEM을 이용한 보안, MIME을 이용한 EDIFACT의 지원, 다수 수신자, 또한 포워딩(Forwarding)을 지원하고 있다.

웹-EDI는 사용자가 시큐어 웹 서버(Secure Web Server)에 접속하여 EDI를 전송하게 된다. 웹-EDI 사업자는 HTML과 같은 형태의 폼을 사용자에게 제공하여 사용자가 입력을 하여 이용된다. 웹-EDI 사업자가 제공하는 EDI 변환소프트웨어에 의해 EDI 포맷으로 변환된다. 웹-EDI는 E-Mail 기반 인터넷 EDI와 달리 거래상대자의 백엔드 시스템에 직접 연결되지 않는다. 이와 같은 방식의 장점은 사용자가 EDI 인프라스트럭처(Infrastructure)를 갖지 않아도 되기 때문에 자주 사용하지 않는 작은 규모의 기업에게 적합하며, 단점으로 전송비용과, 재입력을 통한 기입오류와 시간이 소요된다.

E-Mail 기반 인터넷 EDI와 웹-EDI의 특징과 장단점을 비교하면 다음 <표 3>과 같다.

<표 3> E-Mail 기반 인터넷 EDI와 웹-EDI 비교

	E-Mail 기반 인터넷 EDI	웹-EDI
특징	· E-Mail 기반 · EDI SW 사용	· HTTP · 폼 기입
장점	· 전송에 따른 추가적인 비용 없음 · 실시간 업무 지원 · 다양한 데이터의 전송	· VAN과 연계 용이 · EDI SW 비용 없음 · 단시간의 업무에 적합 · 웹 환경 전자상거래와 통합 용이
단점	· EDI SW 비용 · 웹환경의 전자상거래와 통합의 어려움	· 전송에 따른 비용 · 키입력 오류 발생 · 실시간 업무에 부적합

제3장 EIEW 설계와 구현

3.1 EIEW 설계

인터넷 EDI의 주요 방식인 E-Mail 기반의 인터넷 EDI와 웹은 전자상거래를 지원하는 인터넷 EDI 방식으로는 그 방법이나 활용에 있어서 약간의 문제점을 가지고 있다. E-Mail 기반의 인터넷 EDI을 이용한 방법은 웹에서가 아니라 EDI 변환 프로그램을 통하여 작성된 EDI 문서를 메일을 이용하여 전송하기 때문에 사용자는 웹에서의 통합적인 사용을 하지 못하게 된다. 웹을 이용한 인터넷 EDI는 웹에서의 통합적인 사용은 가능하지만, 웹 EDI를 제공하는 특정회사를 이용해야 하기 때문에 인터넷 EDI의 장점인 비용 절감을 이루지 못하게된다.

본 논문에서는 이러한 문제점을 극복하기 위해서 웹 환경의 E-Mail 기반 인터넷 EDI(E-Mail based Internet EDI System on Web Environment : EIEW)를 설계하고 구현한다. EIEW의 설계원칙은 다음과 같다.

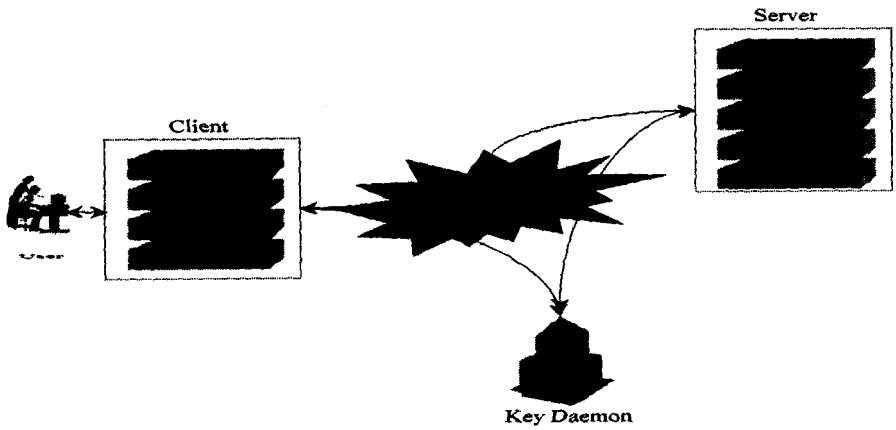
- 통합적인 운영 - 기업간의 거래를 지원하는 EIEW는 웹 환경에서의 통합적인 운영을 지원한다.
- 인터넷 메일 기반의 인터넷 EDI - 웹 EDI가 갖고 있는 비용의 문제를 해결하기 위해서 인터넷 메일을 사용하는 인터넷 EDI를 원칙으로 한다.
- 보안 - 인터넷 가장 큰 특징이자 단점인 개방적인 환경에서 운영되므로 이를 해결하기 위해 보안을 강화한다.
- 멀티미디어 - 멀티미디어 데이터의 전송의 요구를 충족하기 위하여 EIEW는 멀티미디어 데이터의 전송이 가능해야 한다.
- 문서관리 - 작성된 문서의 검색, 읽기, 수정 등의 관리 기능을 제공하여 사용자의 편리성을 높인다.
- 로그 - 기존 VAN에서와 같은 송수신과 관련된 로그를 기록할 수 있는 방법을 제공해야 한다.
- 송·수신 부인 방지 - EDI 문서의 송·수신

부인 방지 기능을 제공해야 한다.

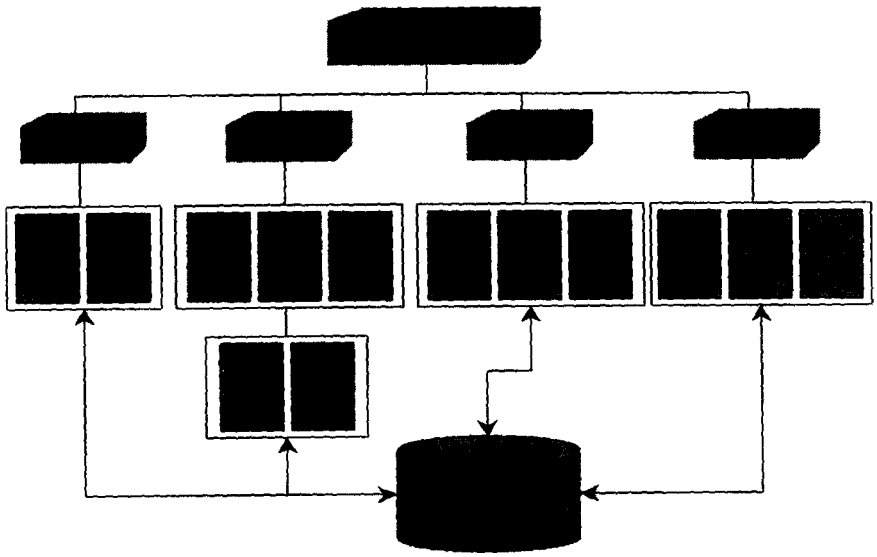
<그림 3>은 EIEW 구성도이다. EIEW는 클라이언트/서버 구조로 이루어져 있다. 각각은 RMI(Remote Method Invocation)를 이용하여 동작한다.

3.1.1 EIEW의 서버

<그림 4>는 EIEW의 서버 구조이다. 서버는 클라이언트의 요청을 받아 각각의 명령을 수행한다. EDI 문서의 저장과 검색, 메일을 이용한 송신, 사용자의 등록을 담당하고 있다.



<그림 3> EIEW 구성도



<그림 4> EIEW의 서버 구조

서버는 총 4개의 구성 요소를 가지고 있다.

- File - 문서의 작성과 읽기, 저장
- Search - 작성된 문서와 수신된 문서의 검색
- Mail - 문서의 수신과 송신, 폴링(Polling)
- Key - 사용자의 키 생성과 키 데몬(Key Daemon)의 연결

3.1.2 EIEW의 클라이언트

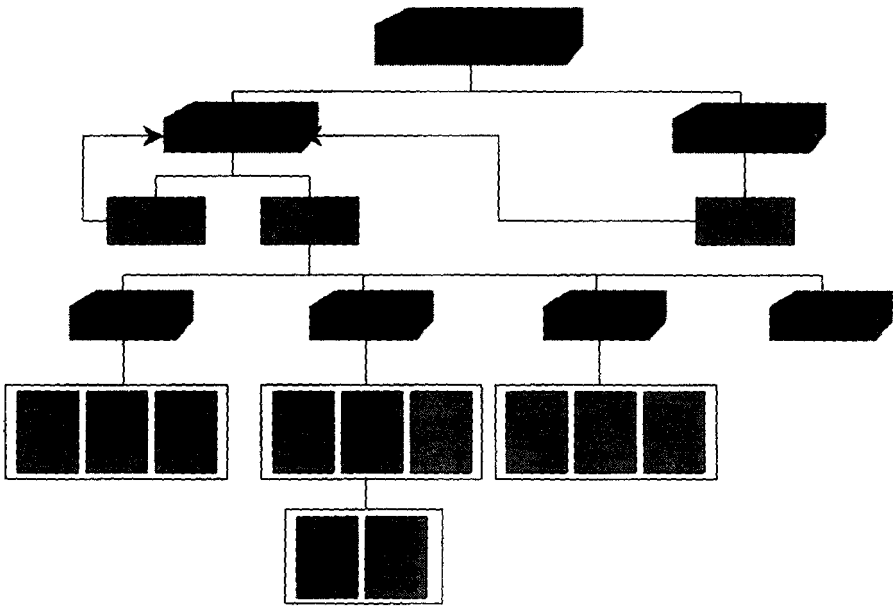
<그림 5>는 EIEW의 클라이언트 구조이다. 클라이언트는 총 6개의 구성요소로 이루어져 있고, 인터넷 EDI 시스템에서 인터페이스 역할을 담당하면서 서버와 연결이 되어 있다. 서버와는 RMI을 이용하여 연결이 되어 있다.

- User Register - 새로운 사용장의 등록
- User Connection - 사용자의 ID와 Password을 이용하여 인터넷 EDI 시스템과 연결
- File - EDI 문서의 생성과 읽기, 저장
- Search - 송수신된 문서의 검색
- Mail - EDI 문서의 송수신과 폴링
- Help - 도움말

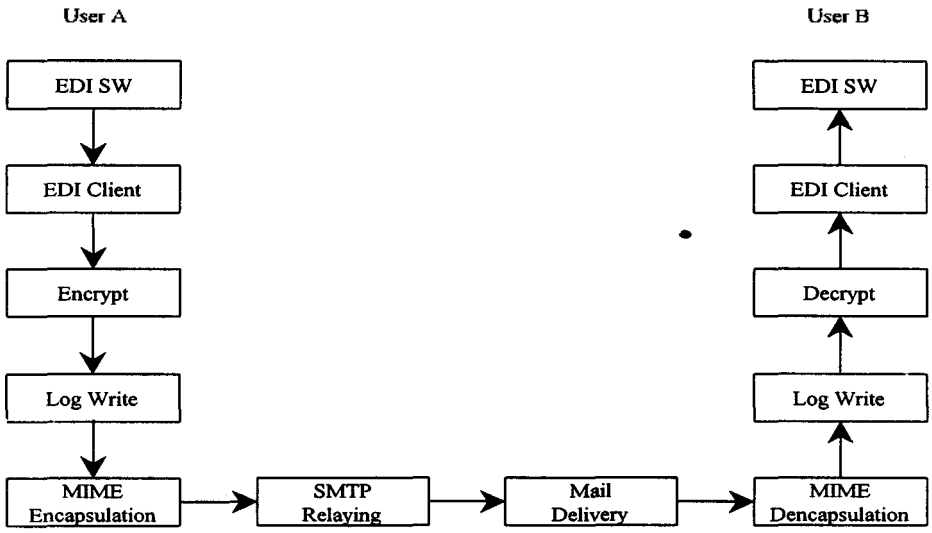
3.1.3 EDI 문서의 송수신

인터넷의 가장 큰 장점인 개방적인 환경에서 발생하는 다음과 같은 문제점들을 고려하여 설계하였다.

- 분실(Loss) - 네트워크나 시스템을 통해 전송되는 자료가 분실되는 것
- 변경(Modification) - 수신인이 자료를 수신하기 전에 제 3자로 인하여 자료가 변경되는 경우, 데이터 무결성의 손실
- 판독(Reading) - 중요한 자료가 제 3자에 의해서 읽혀지는 것
- 송수신 부인(Repudiation) - 수신인이 메시지의 수신을 부인하고 송신자는 메시지의



<그림 5> EIEW의 클라이언트



<그림 6> EIEW의 문서 송수신 과정

송신을 부인하는 것

· 가장(Masquerade) - 제 3자가 잘못된 수신인의 정보를 전송하기 위해서 확실한 거래 상대방으로 가장하여 행동하는 것

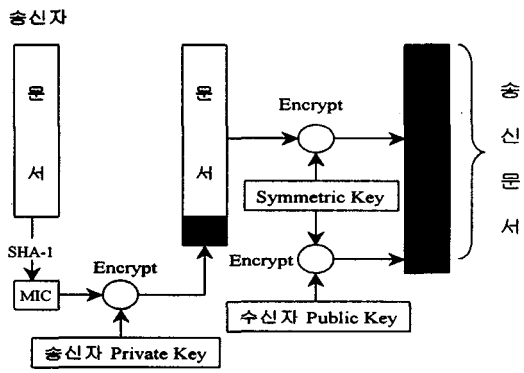
EIEW의 문서 송수신 과정은 다음 <그림 6>과 같다.

EDI 변환 소프트웨어에 의해 생성된 EDI 문서는 클라이언트를 통해 암호화되고 송신과 관련된 로그를 기록하여 수신자에게 송신하게 된다. 수신자는 수신과 관련된 로그를 기록하고 EDI 문서를 복호화하여 EDI 변환소프트웨어에 의해 수신자에게 전달된다.

3.2 EIEW의 문서의 송수신과 송수신 부인 방지

3.2.1 문서의 송신

문서의 송신 과정을 단계별로 설명하면 다음과 같다<그림 7>.



<그림 7> EIEW의 문서 송신 과정

① 내용의 무결성을 위해 SHA-1 단방향 해쉬 함수를 이용하여 MIC 생성한다.

② MIC를 송신자의 비밀키로 암호화를 하여 인증을 위한 전자 사인과 송신 부인 방지를 한다.

③ 전자 사인된 MIC와 EDI 문서를 대칭키를 생성하여 암호화를 한다.

④ 키 데몬으로부터 수신자의 공개키를 획득한다.
⑤ 전자 사인된 MIC와 EDI 문서를 암호화하는데 대칭키를 획득한 수신자의 공개키로 암호화를 하여 송신 문서를 작성한다.
⑥ 송신문서를 MIME 방식으로 캡슐화하여 수신자에게 전송하고 수신 방지를 위한 응답문서를 대기하여 수신한다.

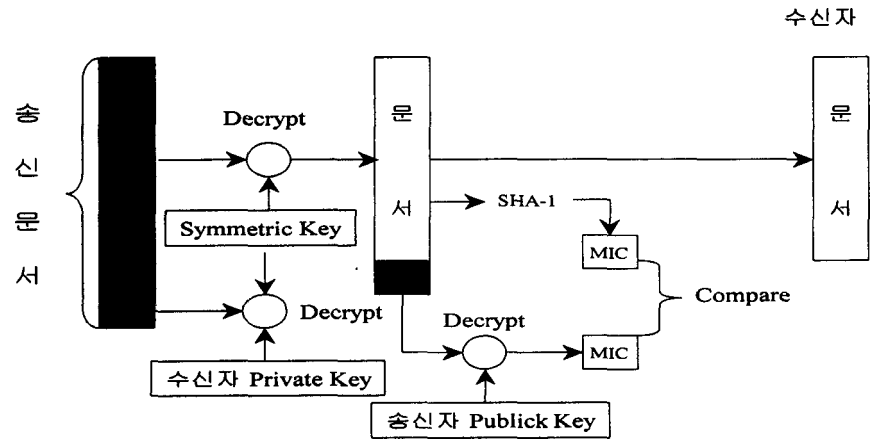
3.2.2 문서 수신 과정

문서의 수신 과정을 단계별로 설명하면 다음과 같다<그림 8>.

① 송신문서에서 문서 추출한다.
② 수신자의 비밀키를 사용하여 EDI 문서와 MIC에 암호화했던 대칭키를 추출한다.
③ 대칭키를 이용하여 EDI 문서와 MIC를 복호화 한다.
④ 키 데몬으로부터 송신자의 공개키를 획득한다.
⑤ 송신자의 공개키로 전자 사인된 MIC를 복호화 한다.
⑥ SHA-1 단 방향 해쉬 함수를 이용하여 EDI 문서에서 MIC 생성한다.
⑦ 생성된 MIC와 복호화된 MIC를 비교한다.
⑧ 수신자에게 EDI 문서를 전달하고 수신 부인 방지를 위하여 응답문서를 송신하는 방법과 같이 전송한다.

3.2.3 문서 송수신과 송수신 부인 방지

EIEW에서 사용되는 문서의 송수신은 비대칭키 암호화 방식을 이용하여 문서를 암호화하고 복호화 한다. 문서의 무결성 검사를 위해서 SHA-1 단 방향 해쉬 함수를 이용하여 MIC를 생성하여 문서와 송신하게 된다. MIC는 문서에 대해서 유일한 형태로 생성되기 때문에 MIC만을 검사하여 문서의 변조를 확인할 수 있다. 송신 부인 방지를 위해서 생선된 MIC에 대해서 송신자의 비밀키를 이용하여 암호화를 한다. 송신자의 비밀키는 송신자만이 알고 있고 이를 송신자를 공개키로만이 복호화 할 수 있다. 이를 통해서 수신자는 송신자를 알 수 있다. 수신 부인 방지를 위해서는



<그림 8> EIEW의 문서 수신 과정

EDI 문서를 수신한 경우 자동적으로 응답문서를 보낸다. 이때 EDI 문서를 송신하는 방법과 동일한 과정을 통하게 된다. 이때 수신자의 비밀키로 MIC를 암호화 함으로써 수신을 확인할 수 있다. 이를 통해서 수신 부인 방지가 이루어진다<그림 9>.

3.3 EIEW 구현

EIEW는 <표 4>와 같은 환경에서 구현되었다.

<표 4> EIEW 구현 환경

워크스테이션
CPU - Pentium III 500 MHz
OS - Solaris 2.5.1
메일서버 - 한글 Sendmail 8.8.5
POP3서버 - QPOP 2.2
PC
CPU - Pentium III 500 MHz
OS - Windows NT 4.0
데이터베이스 - MS SQL Server 6.5
구현 언어
JDK 1.1.6, Java Mail 1.1, JgMail 1.2.2, Java Swing 1.1.1 Beta 2, The Cryptonite Java Package.

3.3.1 사용자 등록

EIEW의 클라이언트는 사용자로부터 정보를 입력받아 서버로 전송하여 사용자 등록을 한다. 서버는 사용자의 정보와 사용자의 공개키와 비밀키를 생성하여, 공개키는 키 데몬에 전송하여 문서의 암호화와 복호화에 사용한다. 입력되는 사용자의 정보는 사용자 ID, 암호, 이름, 주소, E-Mail 주소, E-Mail 암호이다.

생성된 공개키는 키 데몬에게 전달되어 다른 사용자가 EDI 문서를 송신하는데 사용된다. 비밀키는 사용자가 사용하는 EIEW 서버에 저장된다.

3.3.2 사용자 로그인(Login)

EIEW에 로그인을 하면 수신된 메일이 있으면 메일 폴링 결과가 나타난다. 그렇지 않은 경우에는 문서를 입력할 수 있는 화면이 생성된다.

3.3.3 문서 작성과 송신

문서입력화면에서 데이터를 입력하고 수신자의 E-Mail을 입력하여 인터넷 EDI 문서를 송신하도록 구현하였다. EDI 문서를 송신할 때 서버는 클라이언트로부터 데이터를 전달받아 EDI 문서에 대해 단 방향 해쉬 함수를 이용하여 MIC를 생성한다. 생성한 MIC를 송신자의 비밀키로 전자 사인을 한다. 서버는 EDI를 문서를 암호화 하기 위하여 대칭키를 생성한다.

생성된 대칭키를 이용하여 EDI 문서를 암호화하고 사용된 대칭키를 키 데몬으로부터 획득한 수신자의 공개키를 이용하여 암호화하여 송신자에게 전달한다. 송신자는 수신 부인 방지를 위하여 송신된 문서에 대한 수신자의 응답을 기다린다.

3.3.4 폴링과 문서의 수신

로그인시 폴링을 하여 수신된 문서가 있는지 검색한다. 수신된 문서가 있는 경우 선택하고 'Read' 버튼을 클릭하면 문서 작성화면에 송신된 문서가 표시된다. EDI 문서를 수신하기 위해서 수신측 EIEW 서버는 수신자의 비밀키를 이용하여 EDI 문서 암호화에 사용되었던 대칭키를 복호화한다. 복호화된 대칭키를

이용하여 암호화된 EDI 문서를 복호화한다. 송신자의 비밀키로 암호화된 MIC를 송신자의 공개키를 키 데몬으로부터 획득하여 MIC를 복호화 한다. 복호화된 EDI 문서를 단 방향 해쉬 함수를 이용하여 MIC를 생성하여 복호화된 MIC와 비교하여 문서의 무결성 검사와 송신자 확인을 한다. MIC가 서로 다르면 송신자에게 문서의 오류를 전달하다. 그렇지 않은 경우 EDI 수신에 대한 응답 문서를 EDI 문서의 송신과 같은 방법으로 송신하여 수신 부인 방지를 한다.

3.3.5 응답문서와 에러(Error) 문서

EDI 문서가 수신자에게 정확하게 전달된 경우에 수신자는 자동적으로 송신자에게 응답 문서를 보냄으로서 수신 부인방지를 하게 된다. 송신자에게 응답문서를 보내게 된다.

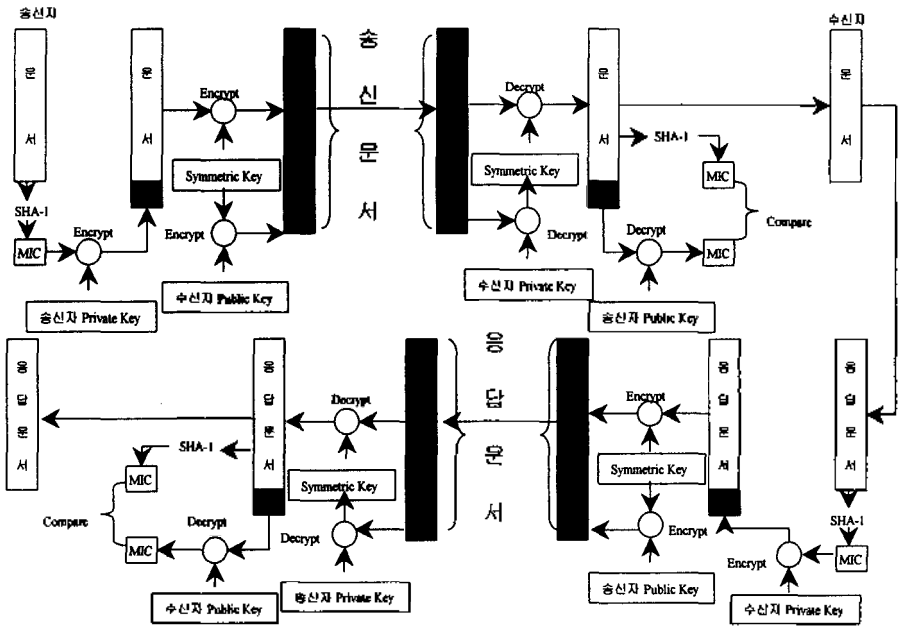
문서가 수신자에게 정확하게 수신되지 못하는 경우, 또는 송신 도중 제 3의 인물에 의해 문서가 변경되는 경우와 같이 비정상적으로 작동되는 경우 수신자는 송신자에게 문서의 오류를 알려줌으로써 송신자가 자동적으로 문서의 오류를 알 수 있다.

3.3.6 문서의 검색

EIEW는 검색 방법을 통해 사용자가 기존에 작성했던 문서와 수신했던 문서를 확인할 수 있고, 재사용할 수 있다<그림 9>.

3.3.7 파일을 송수신

EIEW는 웹-EDI와 같이 폼 기입형으로 사전에 정의된 문서를 송수신 할 수 있다. 이러



<그림 9> 문서의 보안과 송수신 부인 방지를 통한 문서의 송수신 과정

한 기능 외에도 EDI 변환 소프트웨어에 의해 변환된 EDI 문서와 각종 응용 프로그램 파일도 안전하게 송수신 할 수 있다.

4. 평가 및 결론

EIEW와 기존의 VAN 기반 EDI 시스템과의 성능 비교는 다음 <표 5>와 같다. 비교 기준은 EDIINT(EDI Internet Integration) 워킹 그룹(Working Group)과 기가 인포메이션 그룹(Giga Information Group)에서 참조하였다.

<표 5> VAN EDI와 EIEW의 비교

	VAN EDI	EIEW
사용자 범위	VAN에 가입한 사용자	전세계적인 사용자
EDIFACT 지원	가능	가능
전송 비용	전송량에 따른 비용	추가적인 전송비용 없음
실시간 업무 지원	지원하지 못함	지원
다양한 데이터 전송	지원하지 못함	지원
송수신 부인 방지	가능	가능
전자상거래 지원	이원적인 운영	웹 환경의 통합적인 운영
특정 포맷지원	지원하지 않음	지원

EIEW와 E-Mail 기반 인터넷 EDI, 웹-EDI와의 비교는 <표 5>와 같다. 비교 기준은 EDIINT(EDI Internet Integration) 워킹 그룹(Working Group)과 기가 인포메이션 그룹(Giga Information Group)에서 참조하였다.

<표 6>에서 보여지는 것처럼 EIEW는 E-Mail 기반 EDI와 웹-EDI의 장점을 통합하고 있다. 또한 인터넷 EDI의 가장 큰 이유인 추가적인 전송비용을 필요로 하지 않기 때문에 특히 EDI 사용율이 많은 대기업에서는 비용절감의 효과를 얻을 수 있다. 또한 각 기업에 맞는 특정 포맷을 사용할 수 있기 때문에 기업 업무에 직접적으로 연결 할 수 있다.

EDI는 전자상거래의 기본 요소로서 많은 관심이 집중되고 있다. EDI는 많은 관심과 효과에 비해 업무에 많이 사용되지 못하고 있다. 전송에 따른 비용의 부담으로 인해서 그 사용은 대기업에 한정되어 있었다. 또한 단 시간 내에 거래를 위해 EDI의 사용은 효과에 비해 비용의 부담이 너무 컸다. 또한 실시간 업무의 증가로 인해 실시간 업무를 지원하는 EDI의 요구가 커지고 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 제시되었던 인터넷 EDI를 설계하고 구현하였다. 또한 웹 환경에서 이루어지고 있는 전자상거래를 지원하기 위해

<표 6> EIEW, 웹-EDI, E-Mail 기반 EDI 비교

	E-Mail 기반 EDI	웹-EDI	EIEW
EDIFACT	지원	지원	지원
실시간 업무 지원	지원	지원하지 않음	지원
EDI SW 비용	소요	필요없음	소요
전송비용	추가적인 전송비용 없음	전송량에 따른 비용	추가적인 전송비용 없음
전자상거래 지원	이원적인 운영	웹환경의 통합적인 운영	웹환경의 통합적인 운영
다양한 데이터 전송	지원	지원하지 않음	지원

통합적인 운영이 가능한 인터넷 EDI를 구현하였다.

인터넷의 개방적인 환경으로 인해 발생할 수 있는 EDI 문서의 변경(Modification), 판독(Reading), 송수신 부인(Repudiation), 가장(Mas-querade)의 문제를 공개키 기반의 암호화방식을 통해서 해결하였다. EDI 문서의 송수신 절차는 EDIINT(EDI Internet Integration) 워킹 그룹(Working Group)에서 제시하는 기준에 따랐다.

EIEW 개인과 기업간의 거래로 한정되어있던 전자상거래를 기업과 기업간의 전자상거래로 확장할 수 있는 가장 중요한 요소로 활용될 수 있다. 앞으로 인증 서버와 연결을 통한 사용자 인증과 기업 업무 프로세스와의 연계에 대한 연구가 필요하며 EDI 문서의 암호화에 걸리는 시간을 단축하는 연구가 필요하다.

참고문헌

[1] 김태윤, 전자거래정보교환(EDI), 집문당, 1991.

[2] 심상렬, Internet 環境下에서의 EDI 向後展望, 1998.

[3] Giga Information Group, Approaches to Using the Internet for EDI

[4] 이종후, Internet EDI, 1998.

[5] Brent McConnel, Internet EDI, 1997.

[6] 이진용, 권혁인, 김영찬, 인터넷 EDI (Electronic Data Interchange) 설계 및 구현, 추계 학술발표, 1998

[7] 이진용, 김준범, 권혁인, 김영찬, 웹 환경에서의 메일기반 인터넷 EDI, 98년 CALS/EC 학술발표, 1998

[8] Arie Segev, Jaana Porra, Malu Roldan, Internet-Based EDI Strategy, 1997.

[9] B. Reilly, V. Wheatman, J. Graff, B. Enslow, EDI over Internet : Plotting a Safe Course, Strategic Analysis Report, Electronic Commerce Strategies, GartenerGroup, January 24, 1996.

[10] Horace Cheok Mak, Robert B. Johnston, A Survey Of Internet Strategies For EDI, 1997

[11] N. Borenstei, N Freed, MIME Part One : Mechanisms for Specifying and Describing the Format of Internet Mesages Bodies, RFC 1521, Network Working Group, 1993

[12] Klein S, Inderman M, New Architectures for Web-enabled EDI Application and their Impact on VANs, 1996.

[13] U. S. Department of Commerce - National Bureau of Standards, Data Encryption Standard, FIPS PUB 46, 1977.

[14] W. Diffie, M. Hellman, New Directions In Cryptography, IEEE Transactions on Information Theory, Vol. 6, 1976.
[15] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Crypto Systems, Communications of the ACM, Vol 21, No. 2, 1978.
[16] William Stallings, Data and Computer Communications, Prentis Hall International, 1994.
[17] R. Rivest, The MD4 Message Digest Algorithm, RFC 1186, 1990, RFC 1320, 1982.
[18] R. Rivest, The MD4 Message Digest Algorithm, RFC 1321, 1982.
[19] US. Department of Commerce - National Institute of Standards and Technology, A Proposed Federal Information Processing Standard for Digital Signature Standard, Federal Register, 1991.
[20] Premenos, http://www.premenos.com
[21] GEIS, http://www.getradeweb.com
[22] 안경림, 전자상거래와 EDI, 프로그램 세계, 1997.
[23] C. Shih, M. Jansson, R. Drummond, Requirements for Interoperable Internet EDI, IETF EDIINT Working Group, 1997.
[24] L. Ben Azzouz, H. Ben Ayed, F. Kamoun, Problematics of EDI Transport Mechanisms, 1998.

저자소개

권혁인
(프랑스)파리6대학 통신공학 박사
현재 중앙대학교 경영학과 교수
관심분야: E-business, 인터넷마케팅

이진용
중앙대학교 컴퓨터공학과 학사
중앙대학교 컴퓨터공학과 석사
현재 (주)넥센 근무
관심분야: 인터넷 EDI, 전자메일시스템