# PKI을 기반으로한 하이브리드 메시징 시스템 설계 및 구현

이 준 석[†] · 윤 기 송[†] · 정 연 정[†] · 옥 재 호[†] · 김 명 준[††]


## 요 약

본 논문은 PKI(Public Key Infrastructure)를 기반으로 기존의 일반 우편과 전자 메일을 통합한 하이브리드 메시징 시스템 설계 및 구현에 관한 것이다. 사용자는 웹 브라우져 상에서 메일을 작성하여 웹서버로 전송하고, CGI(Common Gateway Interface) 프로그램은 웹 서버를 통해 받은 메일을 우체국 전자 메일 서버로 SMTP(Simple Mail Transfer Protocol)를 이용하여 전송한다. 관내 우체국에 설치된 하이브리드 메시징 시스템의 후처리 프로그램은 자신의 관내 우체국에서 처리해야할 메일을 POP3(Post Office Protocol 3) 프로토콜로 가지고 오고 인쇄한 후 배달한다. 또한 사용자는 인증 기관으로부터 받은 서명 비밀키를 이용하여 전송할 메일을 서명할 수 있으며 우체국 웹서버의 공개키를 이용하여 전송한 메일을 암호화한다.


# Design and Implementation of the Hybrid Messaging System Based on PKI

Jun-Seok Lee[†] · Ki-Song Yoon[†] · Yeon-Jeong Jeong[†] · Jae-Ho Ock[†] · Myung-Joon Kim[††]


## ABSTRACT

The paper is a design and implementation of the Hybrid Messaging System as integrating electronic mail system and common mail system based on PKI(Public Key Infrastructure). A user writes mail through Web Browser and sends the mail to Web Server. CGI(Common Gateway Interface) program sends the mail that was received through the Web Sever to Post Office Electronic Mail Server using SMTP(Simple Mail Transfer Protocol). The End Process program of the Hybrid Messaging System in a Post Office fetches the mail from the Post Office Electronic Mail Server using POP3 (Post Office Protocol 3), prints it and deliver it to recipients. Also, the Hybrid Messaging System is able to sign the mail with a sign private key that the Certificate Authority publics for users and encrypts the mail with a public key of the Post Office Web Server.


## 1. 서 론

인터넷 사용자의 급증과 컴퓨터의 대중화에 따라 전자우편의 사용이 활성화되고 통상 우편의 약 85%가 컴퓨터를 이용하여 작성되고 있는 실정이다. 컴퓨터를 사용하여 전자우편을 사용하는 이용자와 기존 통상우편을 이용하는 이용자간의 통신 연결의 필요성이 증대되고 있다. 이에 따라 우체국에서도 전자우편 서비스를 시범적으로 시작하고 있으며 다양한 서비스 및 기존 통상우편과의 연동 방안이 연구되고 있는 것이 전세계적 추세이다.

하이브리드 메일 시스템은 9개 국가에서 운영하고 있는 IDP(International Data Post)에서 솔루션을 개발하고 있다. 1992년이래 총 18개국이 IDP 커뮤니티를 구성하여 IDP 솔루션을 운영하고 있으며, 이들 18개

† 정 회 원 : 한국통신연구원 컴퓨터 · 소프트웨어연구소 연구원
†† 정 회 원 : 한국통신연구원 컴퓨터 · 소프트웨어연구소 연구원
논문접수 : 2000년 2월 8일, 심사완료 : 2000년 9월 14일

국가의 우편량은 전세계 우편량의 75% 이상을 차지하는 것으로 보고된다.

현재 국가별 하이브리드 메일이 차지하는 비중에 대해서는 정확히 알려진 바는 없으나 하이브리드 메시징 시스템을 가장 먼저 도입한 나라가 덴마크, 핀란드, 노르웨이, 스웨덴 등 북유럽에 해당하는 국가들이 가장 높은 비중의 하이브리드 메일을 사용하고 있을 것으로 추정된다.

IDP 커뮤니티를 이루는 18개 국가에서 하이브리드 메일의 볼륨은 매년 증가하고 있으며, 1997년도에는 20억통에 달한다. 또한 IDC(International Data Corporation)가 발표하고 있는 자료에 의하면 하이브리드 메일은 매년 20% 이상 증가하여, 98년도 하이브리드 메일의 분량은 92년와 비교할 때 40배가량 증가한 것으로 보고되고 있다[1].

캐나다의 경우 인터넷 전자우편시스템과 과금시스템을 범국가적으로 구축 중에 있으며, 캐나다 포스트에서는 PC에서 전자 우편을 보낼 수 있는 "OmniPost Service"와 발신처 및 수신처에 내용증명을 할 수 있는 "Lettermail Plus" 서비스를 할 예정이다. 또한 캐나다 포스트는 전자소인을 이용하여 도착증명과 메시지의 무결성을 증명해 주는 서비스를 제공할 예정에 있다[2].

하이브리드 메시징 시스템은 우편정보 자동처리기술 개발의 한 분야로서 일반 인터넷 사용자가 다양한 응용 소프트웨어를 이용하여 작성한 다양한 형태의 전자문서를 웹 또는 그 외 다른 전자적 방식으로 인터넷을 통하여 우체국의 인터넷 전자우편 서버에 전송한다. 다시 서버는 수신자의 우편정보를 활용하여 수신자에게 가장 근접한 우체국을 선별하여 전자적으로 선정하여 송신하고 수신 우체국에서는 전자적으로 수신된 메시지를 문서화 과정을 거쳐 최종 수신자에게 통상우편과 같은 방식으로 전달할 수 있는 시스템을 말한다.

본 논문에서 개발한 하이브리드 메시징 시스템은 PKI를 이용하여 메시지 송신자의 확인 및 메시지 위변조를 방지하는 신뢰성을 보장하고 또한 전송되는 메일을 암호화하여 메일의 노출을 방지할 수 있도록 구현하였다.

## 2. 관련 연구

### 2.1 전자 메일

현재 인터넷 환경에서 쓰이고 있는 보안기능이 포함된 전자우편 시스템으로는 인터넷 전자우편의 최초 보안 표준인 PEM(Privacy Enhanced Mail), 멀티미디어를 지원하는 MIME(Multi-Purpose Internet Mail Extension)에 보안기능이 추가된 MOSS(MIME Object Security Service)와 비 표준인 PGP(Pretty Good Privacy) 및 S/MIME(Secure MIME) 등이 있다. PEM과 MOSS는 현재 인터넷의 표준으로 이미 발표되었고 상품화까지 되어 있으나 각각의 문제점으로 인하여 널리 보급되지 않고 있다. 또한 PGP는 송수신자의 인증방식의 한계에 따라 일부 작은 집단에서만 사용되고 있다. 또한 X.509 Certificate를 기반으로한 S/MIME은 RSA사에서 제안한 전자우편 보안 프로토콜로서 마이크로소프트의 Exchange, Eudora, Netscape 등에서 구현되었고, 인터넷의 대표적인 보안 프로토콜로 자리 잡아가고 있다. 한편 OSI/MHS의 X.400 전자우편 시스템은 인터넷의 전자우편과는 달리 배달증명(Proof of Delivery), 제출 증명(Proof of Submission)등과 같이 인터넷 전자우편 보다 많은 기능을 지원하고 역사가 오래되어 주로 유럽지역을 중심으로 널리 사용되고 있다.

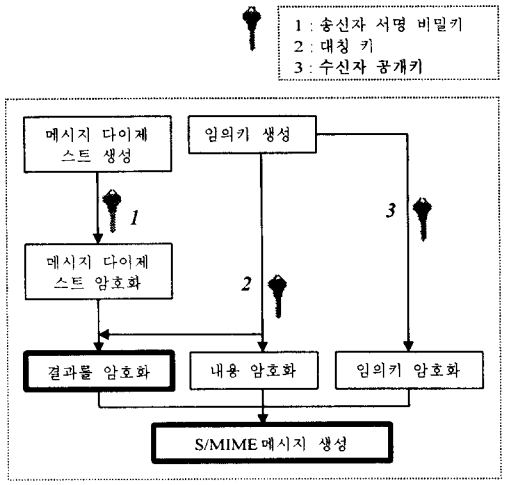
현재 가장 널리 보급되고 있는 S/MIME은 인터넷의 멀티미디어 전자우편 프로토콜인 MIME기능에 보안기능을 추가하는 프로토콜로서 아래의 세 가지 형태의 보안 기능을 지원한다[3].

- 전자서명 (Signed)
- 데이터암호화 (Enveloped)
- 전자서명과 데이터암호화 (SignedAndEnveloped)

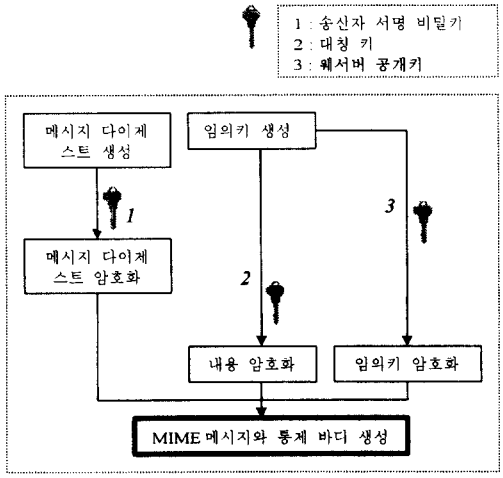
S/MIME의 입력 데이터는 MIME 메시지로서 MIME 메시지 전체에 대하여 전자서명 및 암호화 처리를 한다. 따라서 인터넷으로부터 수신된 S/MIME 메시지처리 결과는 MIME 메시지가 된다.

(그림 1)과 (그림 2)는 S/MIME과 본 시스템의 암호화 과정의 흐름도를 나타내고 있으며 이것을 기반으로 차이점을 설명한다. 첫째, 본 시스템에서는 메시지 다이제스트를 단지 송신자의 서명 비밀키로만 암호화한다. 둘째, 임의키 즉 대칭키는 수신자의 공개키로 암호화하지 않고 우체국의 웹서버의 공개키로 암호화 한다. 셋째, S/MIME은 전자 서명의 결과, 송신자의 비밀키등을 어떻게 전송해야 하는지를 명시하고 있다. 그러나 본 시스템은 이와 같은 데이터들 즉, 서명 결과, 대칭키 뿐만 아니라 송신자, 수신자의 실제 주소( 예

서울 강남구 역삼동 120번지 ), 메일 서비스 형태등을 포함한 새로운 MIME 바디 생성하여 전달된다. 이것을 통제바디(Control Body)라고 부른다.



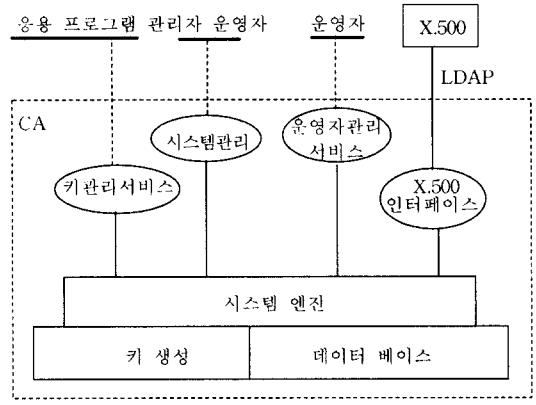

(그림 1) 전자서명과 데이터암호화 흐름도




(그림 2) 하이브리드 메시징 시스템 암호화 흐름도

2.2 PKI의 기본 구성도

X.500을 기반으로 한 PKI의 표준화가 IETF를 중심으로 이루어지고 있으며, 많은 RFC가 있다[4-7]. PKI와 관련된 제품을 Entrust, VeriSign, GTE Cybertrust, Certco, USPS/Cylink, BBN, 그리고 XCert 등에서 만들었고[7] 국내에서는 한국전자통신연구원, 이니텍등에서 만들었다. PKI의 기본 구성요소는 <그림 3>와 같으며 그 기능을 설명하면 다음과 같다.




(그림 3) PKI의 기본 시스템 구성도

2.2.1 시스템 관리

CA(Certification Authority)의 전체 시스템을 관리하기 위해 필요한 기능 즉 관리자의 인터페이스, 시스템 설치, 운영자 정보 관리, 데이터베이스 무결성 확인, 데이터 베이스 백업 스케쥴 결정, 예외적인 일의 발생시 회복 등과 같은 기능을 수행한다. 관리자는 시스템에서 모든 일을 수행할 수 있기 때문에 관리자 패스워드는 가장 중요한 데이터이다. 패스워드와 사용자 이름을 해쉬 함수(hashing function)에 적용하여 하나의 토큰을 생성하고 이 토큰을 데이터 베이스에 저장한다. 관리자가 로그인 할 때, 패스워드와 이름을 입력하고 앞에서 실행한 똑같은 해쉬 함수를 이용하여 토큰을 생성하고 데이터베이스에 저장된 토큰과 비교하여 정확한 패스워드인가를 확인한다.

2.2.2 운영자 관리 서비스

운영자는 사용자 등록, 삭제, 변경 등을 담당하는 사람으로써, 운영자 관리 서비스 모듈은 이와 같은 기능을 수행한다. 이 모듈은 CA가 설치된 시스템과 독립된 시스템에 설치할 수 있으며, CA와 운영자 관리 서비스 프로그램 사이에 통신 보안이 보장된다. 일반적으로 이것을 지역등록기관이라고 한다.

2.2.3 키관리 서비스

응용프로그램(예 하이브리드 메시징 시스템), 또는 다른 CA로부터의 인증서 요구, 암호화 키 생성 요청

등을 받고 수행하며 그 결과를 요청자에게 전송한다.

2.2.4 키 생성

CA 비밀키와 공개키, 사용자 암호화 키 등을 생성하는 역할을 담당한다. 이 부분은 하드웨어로 구성하는 것이 좋다.

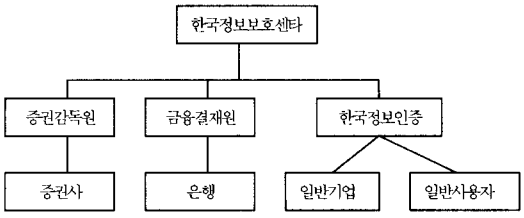
2.2.5 데이터베이스

운영자와 관련된 정보, 관리자와 운영자가 수행할 수 있는 시스템 모듈과 영역을 정의한 privilege set, 키 history 등을 저장한다. CA의 서명키는 CA 관리자 비밀키에 의해 암호화되며, 다른 중요한 데이터는 운영자 비밀키에 의해 암호화된다. CA 관리자 비밀키와 운영자 비밀키는 각각의 패스워드를 기반으로 시스템이 자동 생성한다.

2.2.6 시스템 엔진

시스템 관리, 운영자 관리 서비스, 키관리 서비스, 그리고 X.400 인터페이스 모듈은 시스템 엔진 위에서 시행되고, 시스템 엔진이 데이터베이스와 키 생성 모듈을 관리한다.

현재 국내 인증 기관의 구성도를 살펴보면 <그림 4>와 같다.




(그림 4) 국내 인증 기관 구성도

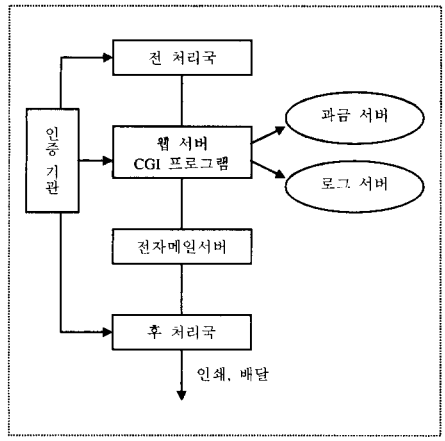
한국정보보호센타를 루트 인증기관으로 하고 증권감독원, 금융결재원, 그리고 한국정보인증(주)가 공인된 인증기관 역할을 수행할 계획이다. 또한 행자부에서는 자체의 인증기관을 구축 중에 있다. 본 시스템은 일반 사용자를 대상으로 하기 때문에 한국정보인증(주)의 인증기관을 이용할 계획이다.

이와 같은 PKI의 응용 기술로 SSL, IPsec[8], Signed Applet, S/MIME등을 들 수 있다.

## 3. 시스템 설계

3.1 시스템 구성

전처리국(Front Agent), CGI 프로그램을 포함한 웹 서버, 메일 서버, 과금 서버, 로그 서버, 그리고 후처리국(End Agent)으로 (그림 5)와 같이 구성되어 있다. 사용자가 본 시스템을 웹 브라우저를 통해 이용하는 곳을 전처리국이라 명하고, 관내우체국에 설치된 본 시스템을 후처리국이라 명한다. 전처리국에서 후처리국까지 메일의 기본 전달 방법으로 MIME 메시지의 형태를 따른다.




(그림 5) 하이브리드 메시징 시스템 구성도

본 시스템의 흐름도를 각 구성 요소를 기반으로 설명하면 다음과 같다.

3.1.1 전 처리국

본 시스템을 통하여 사용자는 전자메일 수신자나 통상 우편 수신자에게 메일을 전송할 수 있으며, 통상 우편 수신자에게는 보통우편, 등기우편, 그리고 내용증명서비스를 제공한다. 사용자가 작성한 우편은 수신자에서 가장 가까운 관내 우체국에 전송되고 보통 우편과 등기 우편의 차이는 메일의 전달 유무를 송신자에게 통보해 주는지의 차이이다. 내용 증명 서비스란 인증기관에서 발부되는 인증서와 서명 비밀키를 이용하여 송신자를 인증하고 내용 위변조를 확인한다.

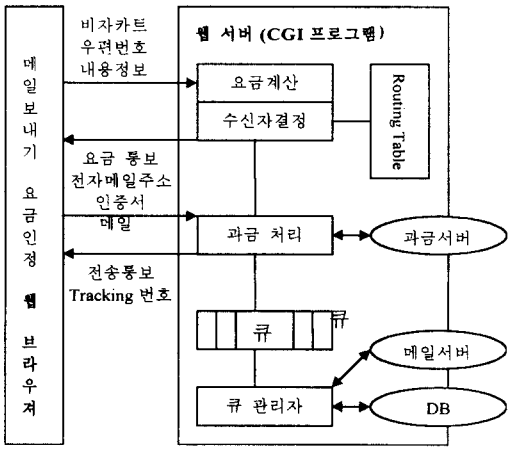
송신자로부터 송신자 정보, 수신자 정보, 메일 내용, 및 메일 종류 등을 입력받고, 만약 송신자가 메일 종류를 내용증명서비스로 선택하는 경우이면 우편 내용

에 대하여 전자 서명을 하기 위해 송신자로부터 인증서와 서명키를 입력받는다. 그리고 나서, 전처리국은 우선 수신자의 우편번호를 웹 서버에 전송한다. 웹서버는 수신자의 우편번호에 대응하는 관내 우체국의 전자메일 주소를 찾아 다시 전처리국에 전송하면, 전처리국은 전자메일 주소를 기반으로 MIME 메시지를 생성하여 웹 서버로 전달한다.

전자메일 수신자인 경우에는 MIME 메시지를 생성하고 이것을 웹서버를 통해 메일서버로 전달한다.

3.1.2 웹 서버

웹서버에서 수행되는 CGI 프로그램의 역할을 (그림 6)을 기반으로 설명한다. 사용자가 메일을 작성하고 보내기 버튼을 누르면 비자카드의 정보, 수신자 우편번호, 작성한 내용의 정보가 웹서버에 전송한다. CGI프로그램은 작성한 내용의 정보를 가지고 요금을 계산하고, 우편 번호를 기반으로 한 라우팅 정보를 이용하여 전자 메일 주소를 생성한다. 즉 라우팅 정보란, 모든 관내 우체국에 할당한 한 개의 전자메일 주소와 각 관내 우체국에서 처리해야할 우편번호를 저장하고 있다.




(그림 6) 웹서버의 기능

웹서버는 요금과 각 수신자에 해당하는 전자메일 주소 그리고 웹서버 인증서를 웹 브라우져에 전송한다.

사용자는 요금을 받아들일 수 있으면 OK 버턴를 누르면 전처리국에서 암호화된 메일을 생성하고 이것이 웹서버로 전달한다.

CGI 프로그램은 과금 서버와 연결하여 과금 승인을 얻고 MIME 메시지를 큐에 넣은 후 전송 완료 메시지를 웹 브라우져에 전달한다. 큐 관리자는 큐에 있는 메일의 헤더 부분을 분석하여 수신자 전자 메일 주소를 얻고 SMTP 프로토콜을 이용하여 메일 서버에 전송한다. 또한 로그 정보를 데이터 베이스에 전송한다.

3.1.3 메일 서버

메일 서버는 전처리국으로부터 웹을 통하여 전체 메일을 받아 관할 우체국의 후처리국으로 전달하기 위하여 메일 저장 및 전달 기능을 수행한다.

3.1.4 후처리국

관내 우체국에 설치된 후처리국은 POP3 프로토콜을 이용하여 메일 서버에 도착한 메일 중에서 자신 관내 우체국으로 보낸 메일을 가지고 온다. 후처리국은 수신한 메일의 내용을 분석하고 인쇄한다. 또한 상태 정보를 데이터 베이스에 전달한다.

만약 내용 증명 서비스인 경우에는 송신자의 인증서를 확인하고 인증서에 포함한 서명 공개키로 메일 내용을 확인한다.

3.2 시스템 설계

본 시스템을 설계함에 있어 중요 결정 상황은 다음과 같다.

3.2.1 하이브리드 시스템

첫째는 내용증명 서비스의 영역이다.

기존의 우편 시스템과 일부 전자 메일에서는 내용증명 서비스를 제공하고 있다. 그러나 이 두 시스템의 차이점은 법적인 효력과 메일 수신 가능이다. 현재 보안 메일의 표준인 S/MIME이 있지만 이것은 법적인 효력을 가지고 있지 않으며 또한 수신자 메일을 읽는 환경(예 : Outlook Express, ELM)에 따라 S/MIME 메시지의 수신 문제가 결정되며 또한 어디서 발부된 인증서를 사용하느냐에 따라서도 수신 가능 여부가 결정된다. 그러므로 현재 환경으로써는 전자 메일을 통하여 법적이 효력을 갖는 내용증명 서비스를 할 수 없기 때문에 본 시스템에서는 전자메일 수신자에게는 내용증명 서비스를 제공하지 않고 단지 하이브리드 메일인 경우에만 내용 증명 서비스를 제공한다.

둘째는 우편을 전송하기 위해 MIME 타입의 선택이다. 시스템은 전자 메일 수신자와 기존 우편 수신자에게

메일을 동시에 전송 할 수 있다. 전자메일 수신자에게 다양한 양식의 데이터를 전송하기 위해서 MIME 메시지 양식을 준하였다. 그러나 기존 우편 수신자에게 메일을 전송하기 위해서는 MIME 표준에 있지 않는 정보 즉, 실질적 주소, 우편 번호, 우편 종류, 인증서, 그리고 서명 결과를 포함 시켜야 했다. 이것을 효율적으로 처리하기 위해 MIME 메시지 안에 이와 같은 정보를 포함하는 바디(본 논문에서 통제 바디라고 명함)를 생성하고 이것의 포맷을 정의했다. 즉 전자 메일 수신자에게는 이 바디만 제거하고 전송하고 일반 우편 수신자에게는 이 바디 부분을 추가하여 전송한다.

셋째는 일반 우편 보안문제이다.

기존의 우편 시스템은 봉투에 넣어 발송함으로써 우편 내용의 암호화 기능을 수행한다. 본 시스템 또한 인터넷 상에서 메일의 보안을 지원하기 위해 웹 서버의 공개키를 이용하여 메일의 내용을 암호화한다.

넷째는 내용증명서비스를 지원하기 위해 어떤 인증기관에서 발부된 인증서와 비밀키를 이용 것인지 이다.

모든 인증기관에서 발부되는 인증서를 이용하여 내용 서비스를 제공하는 것이 궁극적인 목적이다. 그러나 각 인증 기관에서 제공하는 서비스가 아래와 같은 호환성 문제 때문에 본 시스템에서는 국가 공인을 받은 인증기관에서 민간인을 대상으로 발부한 인증서 만을 지원한다.

㉠ 크라이언트에서 인증서와 비밀키를 저장하는 곳과 저장 양식이 다르다. 예를 들어 윈도 환경에서 어떤 인증기관은 레지스트리에 저장하고 어떤 인증기관은 파일로 저장한다. 또한 그 양식도 다르다.

㉡ 각 인증 기관 마다 인증서 정책이 다르기 때문에 각 인증기관이 본 시스템에 각 인증서를 적용할 수 있도록 정책을 수립해야 한다.

㉢ 본 시스템은 인증기관에서 제공하는 라이브러리를 이용하여 전자 서명이나 암호화를 수행해야 한다. 그러나 각 인증 기관이 제공하는 라이브러이 인터페이스에 호완성이 없다.

다섯째는 암호화와 서명 알고리즘이다.

인증기관에서는 다양한 암호화와 서명 알고리즘을 제공하고 있다. 본 시스템 사용자는 암호화 알고리즘에 관련된 지식이 없다고 판단하여 사용자가 서명 알고리즘이나 암호화 알고리즘을 선택하여 서명 또는 암호화 알 수 없고 본 시스템이 정해 놓은 알고리즘을 이용한다. 현재 가장 많이 사용되고 있는 RSA 1024와 SHA-1을 본 시스템에서 이용한다.

3.2.2 전처리국

가장 많은 CPU 타임을 소요하는 MIME 작성의 작업을 사용자 시스템에서 할 것인지 아니면 웹서버에서 수행할 것인지이다. 본 시스템에서는 전처리국에서 수행한다. 그 첫번째 이유는 웹 서버의 부하를 줄이기 위해서 이고, 두 번째 이유는 우편의 보안과 내용 증명 서비스를 제공하기 위해서이다. 만약 웹서버에서 MIME을 작성한다면 사용자의 서명 비밀키를 SSL로 웹서버에게 전달해야하는데 이것은 근본적인 비밀키 노출이라는 문제점이 발생한다.

3.2.3 웹서버

웹 서버에서 수행되는 중요한 기능은 큐 관리자이다. 큐 관리자의 역할은 CGI 프로그램으로부터 입력된 메일을 데이터베이스와 메일 서버에 전달하는 역할을 수행한다. 이것은 사용자에게 빠른 응답 시간을 제공해 준다. 만약 CGI 프로그램이 이와 같은 기능을 수행한다면 CGI 프로그램은 메일 서버와 데이터베이스에 우편을 전송한 이후에 사용자에게 전송 완료 응답을 제공해야 한다.

3.2.4 후처리국

후처리국에서는 모든 작업이 운영자의 없이 수행될 수 있도록 자동으로 모든 작업을 이행한다. 메일 서버에서 메일 가져오기, MIME 분석, 복호화, 우편물 작성, 내용 증명 서비스인 경우 서명 확인, CRL 검토등을 수행한다. 또한 인쇄하여 자동 봉함까지 이행된다. 이와 같은 기능을 제공하는 것은 운영자라 하더라도 우편물 내용을 볼 수 없도록하기 위해서이다.

## 4. 구 현

본 시스템의 개발 환경과 사용된 언어는 <표 1>과 같다.

사용자 인터페이스는 자바 스크립트을 사용하였으며 기존에 C 언어로 작성되어 있는 암호화 프로그램을 이용하기 위하여 JNI(Java Native Language)을 이용하였다. 그리고 전처리국 프로그램은 서명 비밀키, 인증

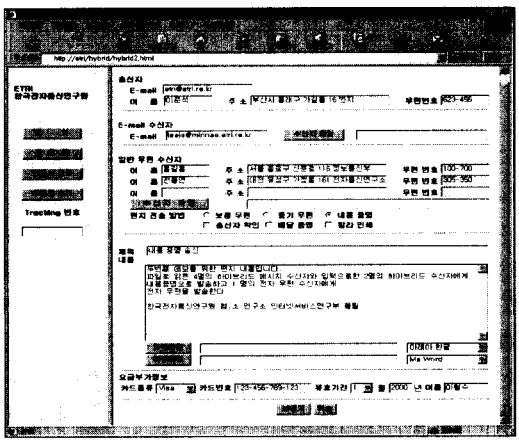
서, 및 첨부 파일을 사용자 시스템의 하드 디스크로부터 읽어야하기 때문에 전처리프로그램을 코드 서명을 하였다. 그리고 본 시스템은 한글과 Ms Word파일만 지원한다.

〈표 1〉 시스템 하드웨어와 소프트웨어

| | 프랫폼 | 사용 언어 | 비고 |
|---|---|---|---|
| 전처리국 | WIndow 98<br>WIndow NT | Java Script<br>Java Applet<br>JNI<br>C, C++ | Internet Explore 5.0 |
| 웹 서버 | Solaris | | 아파치 |
| 전자메일 | Solaris | | SendMail |
| Log 서버 | Solaris | | 바다 |
| 후처리국 | WIndow 98<br>WIndow NT | Visual C++ | |

### 4.1 전처리국

사용자가 전처리국 프로그램을 수행하기 위해서는 먼저 (그림 7)에서 설치 버튼을 통해 프로그램을 설치해야 한다. 설치 버튼을 누르면 전처리국을 수행하기 필요한 DLL을 자동으로 설치하며 이 DLL은 MIME 생성, 암호화등과 관련된 프로그램이다.



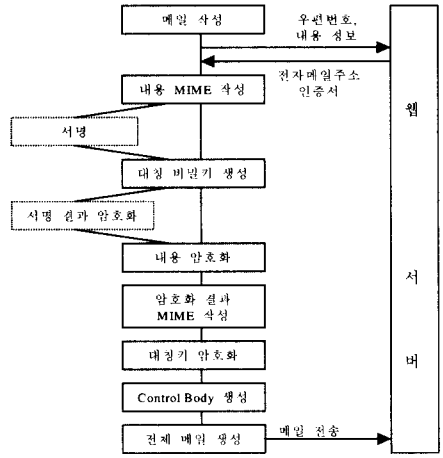
(그림 7) 초기 화면

내용 증명 서비스를 받기 위해서는 RA에 방문하여 인증서를 신청하고 그리고 인증서 신청 버튼을 누르면 인증 기관 웹 서버와 연결되고 이것을 통하여 인증서를 download 받아 사용자 시스템에 저장한다.

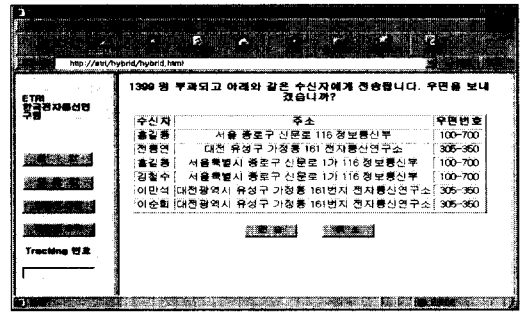
사용자는 (그림 7)에 보여 주는 웹 화면에 송신자 정보, 수신자 정보, 서비스 형태, 내용, 그리고 비자 정보를 입력하고 보내기 버튼을 누른다. 만약 사용자가 내용증명 서비스를 선택하면 인증서와 서명키의 위치를 물어보는 윈도가 생성되고 사용자는 인증서와 서명키의 위치를 지정한다. 웹 브라우져에 설치된 DLL 프로그램은 요금을 산정하기 위해 필요함 정보 즉 수신자 수, 편지 전송 방법, 에디트 박스에 작성한 내용의 페이지 수, 첨부 파일의 페이지 수를 계산하다. 그리고 이 정보, 비자 정보, 그리고 수신자 우편번호들을 웹 서버에 전달한다.

(그림 8)과 같이 웹서버는 요금 계산을 하고 각 하이브리드 수신자 우편 번호를 기반으로 도착해야할 전자 메일 주소를 얻어 웹 브라우져에 전달한다 또한 웹 서버 인증서도 보낸다.

웹 브라우저는 요금과 하이브리드 수신자의 목록을 (그림 9)과 같이 사용자에게 보여준다.




(그림 8) 전처리국 기능 흐름도




(그림 9) 요금 부과 화면

사용자는 부과된 요금과 수신자 리스트를 확인 후에 확인 버튼을 누른다. 이때 DLL 프로그램은 (그림 8)과

같이 사용자가 작성한 메일의 내용과 첨부 파일에 대하여 base64로 canonicalization 작업을 하고 MIME 메시지를 생성한다. 그 결과의 예는 (그림 10)과 같다.

```
------ =_NextPart_000_01BEEE14.DAB71220
Content-Type text/plain; charset="ISO-2022-KR"
Content-Transfer-Encoding base64

^[$)Ctttttttttttttt
^N@L@L@L@L@L@L^O

------ =_NextPart_000_01BEEE14.DAB71220
Content-Type application/octet-stream;name="=?EUC-
KR?B?xde9mh3cA==?="
Content-Transfer-Encoding:base64

B0AHQAdAB0AHQAdAB0AHQAdAB0AHQAdAB0A0AAB0AHQAd
AHQADQAKAKG3obeht6G3obeht6G3obeht6G3obeht6bchtw0AAIAE
AHE8AAA==

------ =_NextPart_000_01BEEE14.DAB71220
```

(그림 10) MIME 메시지의 예

사용자가 내용 증명서비스를 선택하면 위의 MIME 메시지의 시작 경계선에서 마지막 경계선까지에 대하여 메시지 다이제스트를 생성하고 인증 기관으로부터 받은 서명 비밀키를 가지고 메시지 다이제스트를 암호화한다. 이때 사용되는 알고리즘은 SHA-1과 RSA 1024이다.

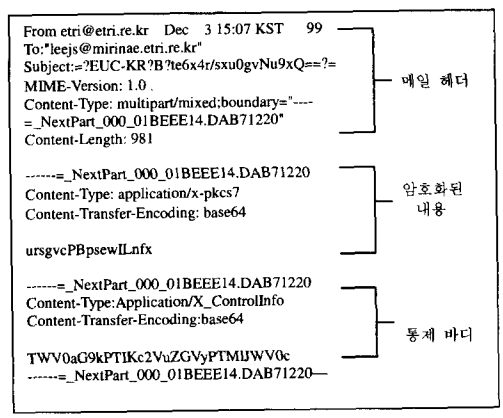
내용의 암호화는 대칭 비밀키를 생성하고 이것을 이용하여 (그림 10)의 MIME 메시지의 시작 경계선에서 마지막 경계선까지 암호화하고 그 결과에 대하여 다시 MIME 메시지를 생성한다. 그리고 대칭 비밀키를 웹서버의 공개 비밀키로 암호화한다.

```
// 서비스 형태 (보통,등기,내용증명)
Method=1
// 송신자 정보
sender=1%%leejs@etri.re.kr%%
sender=2%%우편번호%%이름%%주소%
sender=3%%leejs@etri.re.kr%%우편번호%%이름%%주소%%
// 수신자 정보
receiver=700-200@post.go.kr%%3%%우편번호%%이름%%주
소%%tracking 번호%%;우편번호%%이름%%주소%%tracking
번호%%;우편번호%%이름%%주소%%tracking 번호;
receiver=701-200@post.go.kr%%2%%우편번호%%이름%%주
소%%tracking 번호%%;우편번호%%이름%%주소%%tracking
번호;
//  대칭 비밀키
start PrivateKey  ====

End PrivateKey  ====

  // 송신자 인증서
  start certificate  =====

  end certificate  =====
  // 서명 결과
  start signature =====

  end signature =====
```

(그림 11) 통제 바디

메일 서비스 형태, 송신자 정보, 수신자 정보, 및 대칭 비밀키를 포함한 통제 바디를 (그림 11)과 같이 생성하고 만약 사용자가 내용증명서비스를 선택할 경우에는 송신자 인증서와 서명 결과를 (그림 11)과 같이 추가한다.

메일 헤더, 암호화된 내용, 통제 바디를 포함하여 전체메일(메일헤더+내용바디+통제 바디)를 (그림 12)와 같이 생성하여 HTTP 프로토콜로 웹 서버로 보낸다.




(그림 12) 메일의 형태

### 4.2 웹 서버

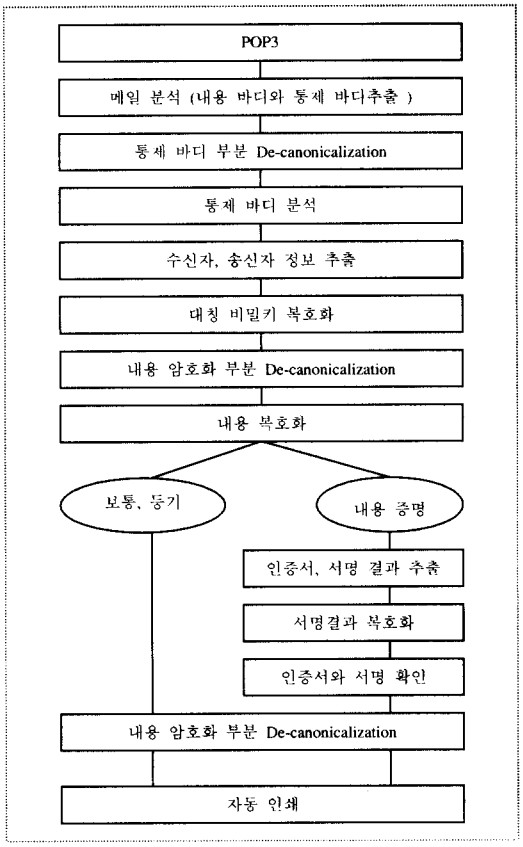
CGI 프로그램는 웹 브라우져에서 MIME 메시지가 오면 먼저 과금 서버와 연결하여 요금 승인을 얻는다. 이와 관련된 프로그램은 과금을 담당하는 업체가 제공하는 API을 이용하여 개발된다.

요금 승인을 얻으면 MIME 메시지에 고유번호를 부여하고 큐에 그대로 넣는다. 큐 관리자는 일정 시간을 주기로 큐에 데이터가 있는지를 확인하고 있으면 MIME 메시지에서 수신자 정보만을 추출하여 SMTP을 작성하고 메일 서버에 전송한다. 메일 서버로부터 OK 메시지를 받으면 데이터베이스에 Log 정보를 남긴다.

### 4.3 후처리국

후처리국의 기능을 (그림 13)를 기반으로 설명한다. 관내 우체국에 설치된 후처리국은 POP3 프로토콜을 이용하여 메일 서버에 도착한 메일 중에서 자신 관내 우체국으로 보낸 메일을 가지고 온다. 후처리국은 수신한 메일의 내용을 분석하여 내용 바디와 통제바디를 추출하고, 통제 바디를 디코딩한다. 그리고 통제 바디

내용을 보고 서비스의 형태를 결정하고 수신자 송신자 정보를 추출한다. 통제바디에 있는 대칭 비밀키를 웹 서버의 비밀키로 복호화하여 대칭 비밀키를 얻는다.




(그림 13) 후처리국의 기능

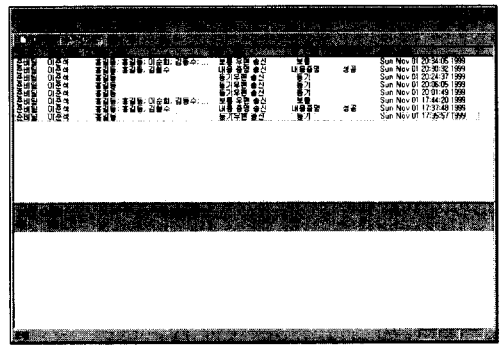
암호화된 내용 바디를 디코딩하고 대칭 비밀키로 복호화한다.

보통, 등기 우편인 경우에는, 복호화된 내용 바디 결과를 디코딩하면 내용 부분을 얻을 수 있다.

만약 내용 증명인 경우에는, 통제바디에 포함된 인증서와 서명결과를 얻는다. 인증서를 인증기관의 서명 공개키로 유효기간 등을 확인한 후에 인증서에 포함된 사용자 서명 공개키를 이용하여 메시지 다이제스트를 복호화하고 SHA-1 해싱 알고리즘을 이용하여 내용의 위변조를 확인한다.

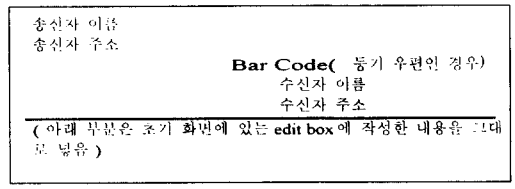
위와 같은 과정을 거쳐 (그림 14)와 같은 후처리국 프로그램에 보낸 사람, 받는 사람등을 나타낸다.

(그림 14) 도구 메뉴에는 자동 수행과 수동 수행을 선택할 수 있는데, 자동 수행은 전 과정을 자동으로 수행하고 수동 수행은 메일 가져오기, 수신자당 인쇄를 운영자가 선택하여 수행할 수 있다.



(그림 14) 후처리 프로그램 화면

인쇄되는 첫 페이지는 (그림 15)와 같은 양식에 준하고 그 다음 페이지는 첨부된 내용을 그대로 인쇄하여 배달된다.




(그림 15) 인쇄 양식

## 5. 결 론

본 시스템은 공인된 인증 기관를 이용하여 일반인을 대상으로 서비스하는 시스템으로써 전자 메일 시스템과 기존 우편 배달 시스템을 결합하고 인터넷에서 전달되는 메일의 보안과 인증을 제공하는 하이브리드 메시징 시스템을 구현하였다.

사용자에게 웹 브라우져 인테페이스를 사용함으로써 편리함을 제공해주고, 현재 표준화된 MIME의 프로토콜을 기반으로하여 메일을 전달함으로써 앞으로 도래할 전자메일의 보안 서비스에도 쉽게 접근할 수 있도록 설계하였다.

전자상거래, IPece, SSL 등과 같은 보안 응용 분야의 기본 하부 구조로 인증기관을 두고 있고, 전세계적으로 이와 같은 인증기관을 설치 중에 있으며 또한 많은 응용 분야가 도래하고 있다. 이와 같은 인증기관을

기반으로한 응용프로그램이 폭 넓게 사용하기 위해서는 사용자 인증서들의 검증을 효과적으로 수행하고 사용 영역을 확장하기 위하여 두 인증 기관 사이에 발행된 인증서들의 짧은 상호인증 경로로 상호 인증이 이루어져야 할 것이다.

## 참 고 문 헌


[1] http://www.idp.dk/

[2] http://dsp-psd.pwgsc.gc.ca/InfoSource/Info_1/CPC-PB-e.html

[3] J. Galvin, S. Murphy, S. Crocker, N. Freed, *Security Multiparts for MIME : Multipart/Signed and Multipart /Encrypted*, RFC1847, Oct. 1995.

[4] R. Housley, W. Ford, W. Polk., D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC2459, January 1999

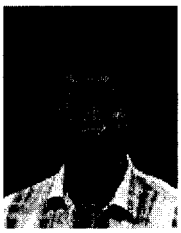
[5] R. Housley, W. Polk, *Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates*, RFC 2528, March 1999

[6] S. Boeyen, T. Howes, P. Richard, *Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2*, RFC 2559, April 1999

[7] C. Adams S. Farrell, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, RFC 2510, March 1999

[8] Ian Curry, "Entrust Architecture and Application Solutions," RSA Data Security Conference Proceedings, USA, San Francisco, Jan. 1998.

[9] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998


### 이 준 석

e-mail : leejs@etri.re.kr

1986년 아주대학교 전자계산학과 (학사)

1989년 동국대학교 대학원 전자계산학과(이학석사)

1991년~현재 한국전자통신연구원 컴퓨터·소프트웨어연구소 선임연구원

관심분야 : 암호화, 전자 메일, 전자 상거래 등



### 윤 기 송

e-mail : ksyoon@etri.re.kr

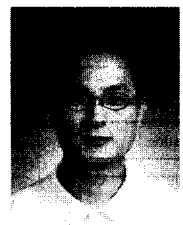
1984년 부산대학교 조선공학과 (학사)

1988년 City University of New York(전산학 석사)

1993년 City University of New York(전산학 박사)

1993년~현재 한국전자통신연구원 컴퓨터·소프트웨어연구소 책임연구원

관심분야 : 정보보호, 메시징, 분산처리


### 정 연 정

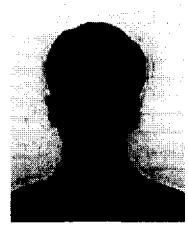
e-mail : yjjeong@etri.re.kr

1994년 부산대학교 전자계산학과 (이학사)

1996년 부산대학교 전자계산학과 (이학석사)

1996년~현재 한국전자통신연구원 컴퓨터·소프트웨어연구소 연구원

관심분야 : 정보보호, 분산처리, 실시간 처리


### 옥 재 호

e-mail : ojh62727@etri.re.kr

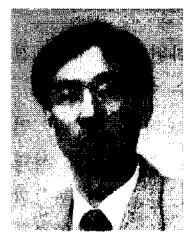
1997년 경남대학교 전자계산학과 (학사)

1999년 경남대학교 대학원 컴퓨터공학과(공학석사)

1999년~1999년 ㈜에듀뱅크

2000년~현재 전자통신 연구원 컴퓨터·소프트웨어연구소 위촉 연구원

관심분야 : 분산 네트워킹, 전자상거래, 자바 가상 머신


### 김 명 준

e-mail : joonkim@etri.re.kr

1978년 서울대학교 자연과학대학 계산통계학과(이학사)

1988년 한국과학기술원 전산학과 (이학석사)

1986년 프랑스 Nancy 제1대학교 응용수학 및 전산학과 (이학박사)

1980년~1981년 아주대학교 종합연구소 연구원

1981년~1986년 프랑스 Nancy 전산학 연구소(CRIN) 연구원

1993년 프랑스 Univ. of Nice Sophia-Antipolis 방문 교수('93)

관심분야 : 데이타베이스, 실시간 처리, 소프트웨어 공학