|  |  |  |
| --- | --- | --- |
| **KSKSKSKS**  **KSKSKSK**  **KSKSKS**  **KSKSK**  **KSKS**  **KSK**  **KS** | | KS X ITUT X1341 |
|  | **전자우편 전달 및 전자 우체국 배달증명 프로토콜**  KS X ITUT X1341:2015 | |
| **방 송 통 신 표 준 심 의 회**  **2017년 12월 27일 제정** | | |

**심 의 : 정보보호 기술심의회(X)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 성명 |  | 근 무 처 |  | 직위 |  |
| (회 장) |  | 염흥열 |  | 순천향대학교 |  | 교수 |  |
| (위 원) |  | 권대성 |  | 국가보안기술연구소 |  | 책임연구원 |  |
|  |  | 김재성 |  | 한국인터넷진흥원 |  | 수석연구원 |  |
|  |  | 나재훈 |  | 한국전자통신연구원 |  | 책임연구원 |  |
|  |  | 이창훈 |  | 서울과학기술대학교 |  | 교수 |  |
|  |  | 전명근 |  | 충북대학교 |  | 교수 |  |
|  |  | 진승헌 |  | 한국전자통신연구원 |  | 책임연구원 |  |
| (간 사) |  | 권병욱 |  | 과학기술정보통신부 국립전파연구원 |  | 과장 |  |

**원안작성협력 : 한국전자통신연구원**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 성명 |  | 근 무 처 |  | 직위 |  |
| (연구책임자) |  | 나재훈 |  | 한국전자통신연구원 |  | 책임연구원 |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

표준열람 : 국립전파연구원(<http://www.rra.go.kr>)

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

제 정 자：방송통신표준심의회 위원장 담당부처：과학기술정보통신부 국립전파연구원

제 정：2017년 12월 27일

심 의：방송통신표준심의회 정보보호 기술심의회(X)

원안작성협력：한국전자통신연구원

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

이 표준에 대한 의견 또는 질문은 국립전파연구원 웹사이트를 이용하여 주십시오.

이 표준은 방송통신표준화지침 제18조의 규정에 따라 매 5년마다 방송통신표준심의회에서 심의되어 확인, 개정 또는 폐지됩니다.

목 차

[머 리 말 iii](#_Toc499716835)

[개 요 iv](#_Toc499716836)

[1 적용범위 1](#_Toc499716837)

[2 인용표준 1](#_Toc499716838)

[3 용어와 정의 및 약어 2](#_Toc499716839)

[3.1 용어와 정의 2](#_Toc499716840)

[3.2 약어 3](#_Toc499716841)

[4 배달증명 전자 메일 기본 개념 4](#_Toc499716842)

[5 배달증명 전자 메일 명령어 타입 4](#_Toc499716843)

[5.1 CMTP 명령어 타입 4](#_Toc499716844)

[5.2 CPOP 명령어 타입 5](#_Toc499716845)

[6 CMTP의 상세 규격 6](#_Toc499716846)

[6.1 CELO : 배달 타입 목록 요청 6](#_Toc499716847)

[6.2 배달 타입 목록 6](#_Toc499716848)

[6.3 선택된 배달 타입 7](#_Toc499716849)

[6.4 배달 타입 확인 7](#_Toc499716850)

[6.5 송신자 전자 메일 주소 7](#_Toc499716851)

[6.6 송신자 전자 메일 주소 확인 7](#_Toc499716852)

[6.7 수신자에게 전자 메일 송신 요청 7](#_Toc499716853)

[6.8 원격 Cmail 서버에 의한 수신자 전자 메일 주소 체크 7](#_Toc499716854)

[6.9 수신자의 전자 메일 주소 확인 8](#_Toc499716855)

[6.10 수신자의 전자 메일 확인 8](#_Toc499716856)

[6.11 봉투 전달 요청 8](#_Toc499716857)

[6.12 봉투 수신 준비 8](#_Toc499716858)

[6.13 봉투 9](#_Toc499716859)

[6.14 서버의 서명된 발신 통지 9](#_Toc499716860)

[6.15 발신자와 서버의 서명된 발신 통지 9](#_Toc499716861)

[6.16 Cmail 서버간의 봉투 10](#_Toc499716862)

[6.17 Cmail 서버간의 서명된 전송 통지 10](#_Toc499716863)

[6.18 서명된 전송 통지 10](#_Toc499716864)

[7 배달증명 우체국 프로토콜 11](#_Toc499716865)

[7.1 메시지 펜딩 요청 11](#_Toc499716866)

[7.2 수신자 챌린지와 서버의 서명된 수신 통지 11](#_Toc499716867)

[7.3 챌린지 응답 및 수신자와 서버의 서명된 수신 통지 12](#_Toc499716868)

[7.4 봉투 13](#_Toc499716869)

[7.5 Cmail 서버간의 수신자와 서버의 서명된 수신 통지(옵션) 13](#_Toc499716870)

[7.6 수신자와 서버의 서명된 수신 통지 13](#_Toc499716871)

[부속서 A (규정) XML 스키마 정의(XSD) 내의 통지 14](#_Toc499716872)

[A.1 XSD 개요 14](#_Toc499716873)

[A.2 XSD로 작성된 통지의 공식 규격 17](#_Toc499716874)

[부속서 B (규정) ASN.1의 통지 21](#_Toc499716875)

[부속서 C (규정) 공개키 인프라구조 콤포넌트들에 대한 요구사항 25](#_Toc499716876)

[C.1 개요 25](#_Toc499716877)

[C.2 Cmail 서버 최종(end)-개체 공개키 인증서 25](#_Toc499716878)

[C.3 Cmail 고객 최종(end)-개체 공개키 인증서 25](#_Toc499716879)

[C.4 정보 검증 요구사항 26](#_Toc499716880)

[부속서 D (규정) 전송 계층 보안(TLS)의 요구사항 27](#_Toc499716881)

[부속서 E (규정) 대상 식별자 28](#_Toc499716882)

[부속서 F (참조) 봉투와 통지의 포맷 29](#_Toc499716883)

[F.1 발신 통지 29](#_Toc499716884)

[F.2 수신 통지 29](#_Toc499716885)

[F.3 전송 통지 30](#_Toc499716886)

[F.4 봉투 30](#_Toc499716887)

[참고문헌 32](#_Toc499716888)

[KS X ITUT X1341:2015 해 설 33](#_Toc499716889)

머 리 말

이 표준은 방송통신발전기본법 관련 규정에 따라 방송통신표준심의회의 심의를 거쳐 제정한 방송통신표준이다.

이 표준은 저작권법에서 보호 대상이 되는 저작물이다.

이 표준의 일부가 기술적 성질을 가진 특허권, 출원공개 이후의 특허출원, 실용신안권 또는 출원공개 후의 실용신안등록출원에 저촉될 가능성이 있다는 것에 주의를 환기한다. 관계 중앙행정기관의 장과 방송통신표준심의회는 이러한 기술적 성질을 가진 특허권, 출원공개 이후의 특허출원, 실용신안권 또는 출원공개 후의 실용신안등록출원에 관계되는 확인에 대하여 책임을 지지 않는다.

개 요

이 표준은 2015년에 발행된 ITU-T X.1341 Certified mail transport and certified post office protocols를 기초로 기술적인 내용 및 대응국제표준의 구성을 변경하지 않고 작성한 방송통신표준이다.

**방송통신표준**

**KS X ITUT X1341:2015**

|  |
| --- |
| **전자우편 전달 및 전자 우체국 배달증명 프로토콜** |

|  |
| --- |
| Certified mail transport and certified post office protocols |

# 적용범위

이 표준은 식별 및 기밀성 관점에서 신뢰하는 전자 우편을 만들 수 있는지에 대하여 기술한다.

배달증명 전자 우편 전달 프로토콜/배달증명 전자 우체국 프로토콜(CMTP/CPOP)는 다음 사항을 가능하게 한다.

**—** 전자서명을 이용하여 부인 이슈에 대한 솔루션

**—** 암호화를 이용하여 기밀성 이슈에 대한 솔루션

**—** 신뢰적인 발신, 전송 및 수신 통지의 생성

**—** 처리단계에서 전자우편의 손실을 피하기 위해서 전자우편을 추적하는 배달증명 전자우편(Cmail) 서버의 이용

**—** 보다 강한 식별을 제공하여 전송 계층 보안(TLS) 접속을 이용. 이 강한 수준의 식별은 배달증명(Cmail) 서버에 의하여 요구된다.

이 표준과의 적합성은 해당 국가의 지역적 법의 준수에 대한 주장을 위한 증거 입증으로서 채택되지 않는다. 본 표준에서 기술된 기술적, 조직적 그리고 절차적 수단은 특정 국가나 지역의 법과 규제와 정책에 의한 서신교환에 이용하는 정보보호 수준의 규약을 보장하지 않는다.

# 인용표준

다음의 인용표준은 이 표준의 적용을 위해 필수적이다. 발행 연도가 표기된 인용표준은 인용된 판만을 적용한다. 발행 연도가 표기되지 않은 인용표준은 최신판(모든 추록을 포함)을 적용한다.

ITU-T X.520 (2012) | ISO/IEC 9594-6:2014, Information technology — Open Systems Interconnection — The Directory: Selected attribute types

ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation

ITU-T X.690 (2008) | ISO/IEC 8825-1: 2008, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

ITU-T X.693 (2008) | ISO/IEC 8825-4: 2008, Information technology — ASN.1 encoding rules: XML Encoding Rules (XER)

ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions — Part 1: Country codes

IETF RFC 822 (1982), Standard for the format of ARPA Internet text messages

IETF RFC 1939 (1996), Post office protocol — Version 3

IETF RFC 2045 (1996), Multipurpose internet mail extensions (MIME) — Part One: Format of internet message bodies

IETF RFC 5246 (2008), The transport layer security (TLS) Protocol – Version 1.2

IETF RFC 5321 (2008), Simple mail transfer protocol

XML1.0 (2000), Extensible markup language (XML) 1.0 (fifth edition)

XML Schema (2001), XML schema Part 1: Structures

# 용어와 정의 및 약어

이 표준의 목적을 위하여 다음의 용어와 정의 및 약어를 적용한다.

## 용어와 정의

### 인증 기관(certification authority, CA) [b-ITU-T X.509]

공개키 인증서를 생성하고 발행하는 하나 이상의 사용자가 신뢰하는 기관. 선택적으로 인증기관은 사용자들의 키를 생성할 수도 있다.

### 인증서 검증(certificate validation) [b-ITU-T X.509]

인증 경로의 구축과 처리를 포함하여 특정 시점에서의 인증서의 유효 여부를 확인하고 그 경로상의 모든 인증서 유효 여부(즉 만료 또는 폐지 여부)를 확인하는 과정

### 해시 함수(hash function) [b-ITU-T X.509]

대규모 영역(가능한 매우 큰 영역) 상의 값들을 소규모 영역으로 매핑시키는 (수학적) 함수. “좋은” 해쉬 함수는 이 함수를 적용한 결과들이 전 영역에 걸쳐 고르게(무작위적으로) 분포하는 것이다.

### 개인키(private key) [b-ITU-T X.509]

(공개키 암호시스템에서) 사용자 키 쌍 중에서 그 사용자만 알고 있는 키

### 공개키(public key) [b-ITU-T X.509]

(공개키 암호시스템에서) 사용자 키 쌍 중에서 공개적으로 알려진 키

### 공개키 인증서(public-key certificate, PKC) [b-ITU-T X.509]

인증서를 발급한 인증기관의 개인키를 사용하여 사용자의 공개키와 기타 몇몇 정보를 위조할 수 없게 만든 데이터 구조

### 공개키기반 구조(public-key infrastructure, PKI) [b-ITU-T X.509]

이 기반구조는 공개키 관리를 지원하며 인증, 암호화, 무결성, 부인방지 서비스를 지원한다

### 배달증명 메일(certified mail)

배달증명 전달 프로토콜(CMTP)과 배달증명 전자 우체국 프로토콜을 이용하여 교환 되어지는 전자 메일

### 배달증명 메일 전달 프로토콜(certified mail transfer protocol, CMTP)

배달증명 메일을 전송 하기 위하여 사용되는 전자 우편 전송 프로토콜 기반의 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 접속 상의 응용 계층 프로토콜

### 배달증명 우체국 프로토콜(certified post office protocol, CPOP)

배달증명 메일을 수신 하기 위하여 사용되는 우체국 프로토콜 버전 3(POP3) 기반의 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 접속 상의 응용 계층 프로토콜

### 배달증명 메일 서버(Cmail server)

배달증명 메일 트랜잭션에 포함된 신뢰 실체

### 발신 통지(notice of deposit)

메일의 발신 증명을 가능하게 하는 정보를 포함하는 발신자와 배달증명 메일 서버가 서명한 전자 문서

### 수신 통지(notice of reception)

수신자에 의하여 메일의 수신 증명을 가능하게 하는 정보를 포함하는 수신자와 배달증명 메일 서버가 서명한 전자 문서

### 전송 통지(notice of transit)

메일 서버에 메일 전송 증명을 가능하게 하는 정보를 포함하는 배달증명 메일 트랜잭션에 포함되어 있는 서버가 서명한 전자 문서

### 전자 우체국 프로토콜 버전 3(post office protocol version 3, POP3)

메일을 수신 하기 위하여 사용되는 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 접속 위의 응용 계층 프로토콜

### 전자 우편 전송 프로토콜(simple mail transfer protocol, SMTP)

메일을 전송 하기 위하여 사용되는 전송 제어 프로토콜/ 인터넷 프로토콜 (TCP/IP) 접속 위의 응용 계층 프로토콜

## 약어

AES Advanced Encryption Standard

ASN.1 Abstract Syntax Notation One

CA Certification Authority

CBC Cipher Block Chaining

Cmail Certified Mail

CMTP Certified Mail Transfer Protocol

CPOP Certified Post Office Protocol

DER Distinguished Encoding Rules

DNS Domain Name System

id identity

MIME Multipurpose Internet Mail Extensions

PKI Public-Key Infrastructure

POP3 Post Office Protocol version 3

RSA Rivest, Shamir and Adleman algorithm

RSCK Random Symmetric Cipher Key

S/MIME Secure/Multipurpose Internet Mail Extensions

SMTP Simple Mail Transfer Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TLS Transport Layer Security

UTF-8 Universal Character Set Transformation Format-8

XER XML Encoding Rules

XML eXtensible Markup Language

XSD XML Schema Definition

# 배달증명 전자 메일 기본 개념

전자 우편 전송 프로토콜(SMTP)과 전자 우체국 프로토콜 버전 3(POP3)를 이용하는 전통적인 전자 메일 통신은 전자 메일 수신자가 전자 메일 수신을 거부할 수 있다. 이것은 다목적의 인터넷 전자우편 보안(S/MIME)이 프로토콜 모음에 추가된 것이다. S/MIME 은 송신자의 인증과 메시지 암호를 제공하고 메세지의 배달을 증명하지는 않는다.

이 표준은 배달증명 전자우편 전달 프로토콜과 배달증명 전자 우체국 프로토콜을 포함하는 배달증명 메일이라 불리는 프로토콜 모음을 기술한다.

전자 우편 전송 프로토콜(SMTP)/전자 우체국 프로토콜 3(POP3)의 통신에 있어서, 메일 서버는 통신에 있어서 주요 부분이 아니고, 단지 수신자가 메일 서버에게 접속 할 때에 수신된 메시지를 전달하는 것이다. 이것은 다목적의 인터넷 전자우편 보안(S/MIME)이 채택된 경우에도 동일하다.

배달증명 전자 우편에 있어서, 메일 서버는 배달증명 메일(Cmail) 서버가 수신자가 메일 수신을 동의하였는가를 증명 하도록 허용하는 방식으로 송신자와 수신자 간의 통신에 있어서 능동적으로 관여를 한다. 메일은 암호화하여 전송되며, 배달증명 메일(Cmail) 서버가 전자메일의 내용을 읽을 수 없도록 허용하지 않는다. 구체적인 규격은 8절에서 다루어지지만, 다음절에서 절차의 개요가 기술된다.

송신자와 배달증명 메일(Cmail) 서버와의 상호작용은 6 절에서 기술된다.

수신자와 배달증명 메일(Cmail) 서버와의 상호작용은 7 절에서 기술된다.

# 배달증명 전자 메일 명령어 타입

배달증명 전자 메일은 SMTP와 POP3 명령어들과 개선된 SMTP와 POP3 명령어와 배달증명 전자 메일에 특화된 명령어들을 조합하여 이용한다. **표 1**과 **표 2**에서는 SMTP/POP3와 상응하는 것이 없는 명령어는 “추가“라고 표시하였으며, 개선된 SMPT/POP3 명령어인 경우에는 “수정“ 이라고 표시하였으며, 변경되지 않은 SMTP/POP3 명령어는 “동일“이라고 표시하였다.

명령어 타입은 메세지 타입을 위한 추가적인 기술과 함께 메시지 타입을 식별할 수 있게 대문자를 이용하여 키워드로 정의하였다.

## CMTP 명령어 타입

표 1 — CMTP 명령어

|  |  |
| --- | --- |
| **명령어** | **명령어 기능** |
| **CELO**  추가 | 서버에게 CMTP 명령어의 처리를 확인 할 수 있도록 활성화 |
| **DELV**  추가 | 배달 모두 확인: certifiedMail |

표 1 — CMTP 명령어(계속)

|  |  |
| --- | --- |
| **명령어** | **명령어 기능** |
| **MAIL FROM**  수정 | 메시지 송신자 확인. “MAIL FROM”과 같이 사용. 서버에 그에 해당하는 계정이 있다면, 알려진 송신자의 공개키 인증서의 base64를 회신함 |
| **RCPT TO**  수정 | 메시지 수신자를 확인. “RCPT TO” 양식을 따름. 만약 서버에 그에 해당하는 계정이 존재하면, 알려진 송신자의 공개키 인증서의 base64를 회신함. 만약 키 교환이 이루어진 다른 CMTP 서버에 해당 계정이 존재한다면, 그 서버는 CHCK RCPT 명령어와 함께 알려진 수신자에게 속한 공개키 인증서의 base64를 보내며 두 번째 서버에게 송신자의 공개키 인증서의 base64를 요청 |
| **CHCK RCPT**  추가 | 수신자가 송신자의 배달증명 메일 서버가 아닌 다른 배달증명 메일 서버에 첨부된 경우에 보내짐 |
| **DATA**  수정 | 메시지 내용 전달을 개시하는 클라이언트에 의하여 보내짐. 서버에 의하여 서명되고 송신자에 의하여 서명 받게 되는 발신통지를 서버는 회신을 보냄 |
| **DEPO**  추가 | 서버에 의하여 서명 받고 송신자에 의하여 부서명 한 발신통지의 전달 개시를 클라이언트가 보냄 |
| **SEND EVLP**  추가 | 하나의 배달증명 메일 서버에서 다른 서버로 봉투를 전달 |
| **HELP**  동일 | CMTP 서버로부터 지원받은 명령어 리스트를 회신 |
| **QUIT**  동일 | 세션 종료 |

## CPOP 명령어 타입

표 2 — CPOP 명령어

|  |  |
| --- | --- |
| **명령어** | **명령어 기능** |
| **USER**  동일 | 로그인 하는 이용자의 이름을 기술하기 위하여 사용 |
| **PASS**  동일 | 로그인 하는 이용자의 패스워드 |
| **LIST**  수정 | 메시지 목록과 크기를 표시하기 위하여 사용. 예로, 파라미터 없이 LIST 명령어를 호출하면, 2+OK 메시지(320 옥텟)과 메시지 목록. ID(identity), 길이 그리고 CertifiedMail과 같은 배달 모드(가능한 경우)를 회신 |
| **RETR**  수정 | *N*이 1과 LIST 명령어에 이하여 회신된 마지막 번호 사이의 번호인 경우에, 이 명령어는 삭제로 표시된 메시지를 검색하는 것에는 사용하지 않는다. 만약 배달 타입이 없는 경우, 서버는 MIME 코딩 전자 메일을 송신. 그러나 배달 타입이 있는 경우에는 서버는 특별히 메시지를 처리. CertifiedMail 경우의 예로, 서버는 RCPT 명령어를 사용하여 봉투를 송신하기 이전에 수신자를 증명요구 한다. |
| **CHLG RESP**  추가 | 메시지의 수신통지 전달과 비밀 질의데 대한 응답 전달을 위하여 클라이언트가 송신. 만약 응답이 올바르다면, 서버는 MIME 봉투를 회신 |
| **SEND NORP**  추가 | 서명된 수신 통지를 송신 |
| **HELP**  동일 | CPOP 서버로부터 지원받은 명령어 리스트를 회신 |
| **QUIT**  동일 | 세션 종료 |

# CMTP의 상세 규격

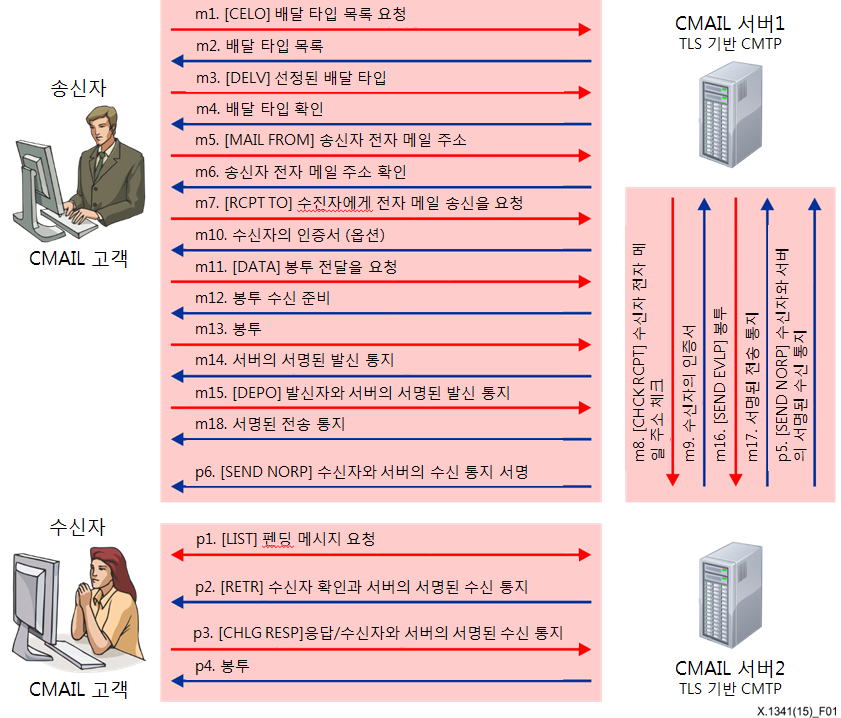


그림 1 — 프로토콜 교환 개요

m으로 표기되어 있는 명령어들은 CMTP 프로토콜에서 사용되고 있고, p로 표기되어 있는 명령어들은 CPOP 프로토콜에서 사용된다. 6.1 항부터 6.18 항은 **그림 1**에서 명령어 m1에서 명령어 m18까지의 교환에 대한 상세 규격을 기술하고, 7 절은 명령어 p1에서 명령어 p6까지의 교환에 대한 상세 규격을 기술한다.

## CELO : 배달 타입 목록 요청

이 명령어 타입은, 마치 HELP 명령어와 유사하게, 전체 도메인 이름을 붙인 SMTP 메시지로서 전송된다, 목적은 배달 타입의 목록을 검색하기 위한 것이다.

## 배달 타입 목록

배달 타입 목록은 CELO 명령어의 응답으로 주어진다. 다음과 같은 내용을 (인센티브 경우) 포함하는SMTP 형식이다.

250-<Fully qualified domain name of the Cmail server>

250-8BITMIME

250-Delivery-Types CertifiedMail <other delivery types>

250 OK

이 표준은 CertifiedMail을 위한 규격을 단순히 기술한다. 향후 발행판에서는 다른 배달 타입을 기술 할 수 있다.

## 선택된 배달 타입

이 메시지는 배달 타입 목록에서 나열되어 있는 배달 타입을 확인한다. 다음의 포맷을 갖는다.

DELV <delivery type>

## 배달 타입 확인

만약 선정된 배달 타입이 수락되면, 이 메시지는 다음의 SMTP 포맷을 (인센티브 경우) 갖는다.

250 Delivery-Type <delivery type>OK

향후 응답이 선정된 배달 메시지의 오류구문의 경우이면

501 Syntax: DELV <delivery type>

향후 응답이 선정된 배달 메시지가 무순서로 발행된 경우이면

501 Syntax: use CELO command first

향후 응답이 선정된 배달 메시지가 알려지지 않은 경우이면

501 Unknown Delivery-Type: <delivery type>

## 송신자 전자 메일 주소

이 메시지는 배달증명 전자 메일의 발송 요청과 선택적으로 Cmail 서버로부터 송신자의 공개키 인증서를 요청하려고 할 때에 Cmail 서버에게 보내진다.

MAIL FROM <sender's email address> [CertificateRequested]

## 송신자 전자 메일 주소 확인

이 메시지는 송신자의 전자 메일 주소가 Cmail 서버 데이터베이스에 존재하는 것을 확인하기 위하여 보내진다. 만약 송신자가 자신의 공개키 인증서를 요청하였다면, 송신자의 공개키 인증서도 포함된다:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

## 수신자에게 전자 메일 송신 요청

이 메시지는 배달증명 전자 메일을 수신자에게 발송을 요청하기 위하여 그리고 선택적으로 수신자의 공개키 인증서를 요청하는 경우에 Cmail 서버에게 보내진다.

RCPT TO <recipient's email address> [CertificateRequested]

이 명령어는 만약 수신자가 여러 명인 경우에 각 수신자를 추가하기 위하여 필요할 때마다 사용될 수 있다. 수신자가 “To” 또는 "CC” 인지를 나타내는 정보는 봉투의 헤더에 포함된다[IETF RFC 5321]. “BCC” 수신자는 허락되지 않는다.

## 원격 Cmail 서버에 의한 수신자 전자 메일 주소 체크

이 메시지는 수신자가 송신자의 서버가 아닌 다른 서버에 속한경우에 전송된다. 전자 메일 주소의 유효성을 확인하기 위하여 또 선택적으로 수신자의 공개키 인증서를 요청하기 위하여 송신자 Cmail 서버에서 수신자 Cmail 서버로 전송된다.

CHCK RCPT <recipient's email address> [CertificateRequested]

## 수신자의 전자 메일 주소 확인

이 메시지는 “원격 Cmail 서버에 의한 수신자 전자 메일 주소 체크”에 대한 응답으로 전송된다. 다음은 전자 메일 주소의 확인과 요청된 경우에 수신자의 공개키 인증서를 포함한다:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

만약 전자 메일 주소가 확인이 될 수 없는 경우, 다음 오류 메시지들이 전송 될 수 있다.

503 Sender already specified

중복된 요청에 대한 응답인 경우 전송

501 Syntax: CHCK RCPT <address>

수신자의 전자 메일 주소에 구문오류가 있는 경우 전송

501 Syntax: CHCK RCPT <address> Error in parameters <parameter>

전자 메일 주소 이후에 파라미터가 인식되지 않는 경우 전송

553 <email address> Invalid email address

전자 메일 주소가 원격 Cmail 서버에 존재하지 않는 경우 전송

## 수신자의 전자 메일 확인

이 메시지는 수신자의 전자 메일 주소가 존재하는지를 확인하기 위하여 전송된다. 송신자가 수신자의 공개키 인증서를 요청한 경우, 수신자의 공개키 인증서가 포함된다.

다음은 전자 메일 주소를 확인과 요청된 경우에 수신자의 공개키 인증서를 포함한다:

[250 User-Certificate: <public-key certificate encoded in Base64>]

250 OK

만약 전자 메일 주소가 확인이 될 수 없는 경우, 다음 오류 메시지들이 전송 될 수 있다.

503 Error: need MAIL FROM command

메시지가 무순서로 전송된 경우 전송

452 Error: too many recipients

너무 많은 수신자가 나열된 경우 전송

501-6.1.1 Syntax: RCPT TO <address>

수신자의 전자 메일 주소에 구문오류가 있는 경우 전송

501-6.1.2 Syntax: RCPT TO <address> Error in parameters: <parameters>

전자 메일 주소 이후에 파라미터가 인식되지 않는 경우 전송

550-5.1.1 <email address> Invalid email address.

전자 메일 주소가 존재하지 않는 경우 전송

## 봉투 전달 요청

송신자에 의하여 데이터 전송을 위하여 Cmail 서버의 허락을 문의하는 경우에 사용되는 포맷

DATA

## 봉투 수신 준비

Cmail 서버가 데이터 수신 준비가 된 경우 다음 메시지가 전송된다.

354 Start mail input; end with <CRLF>.<CRLF>

MAIL FROM 명령어가 전송되지 않은 경우에 다음 메시지가 전송된다.

503 Error: need MAIL FROM command

RCPT TO 명령어가 전송되지 않은 경우에 다음 메시지가 전송된다.

503 Error: need RCPT TO command

DELV 명령어가 전송되지 않은 경우에 다음 메시지가 전송된다.

503 Error: need DELV command

## 봉투

클라이언트는 다음을 한다.

1. 랜덤 대칭 사이퍼 키 (RSCK)를 생성, 예, AES 256

2. 메시지의 본문과 부속이 있다면 위의 키를 이용하여 암호화

3. 암호한 메시지를 포함하는 ENVELOPE 이름의 부분을 포함하는 MIME 메시지 작성 (IETF RFC 2045 참조)

4. 메시지를 <CR><LF>.<CR><LF>로 마침. 그리고

5. MIME 메시지 전송

## 서버의 서명된 발신 통지

250 Notice-of-deposit:

<notice of deposit signed by the Cmail server encoded in base64>

250 Ok

서버는 봉투에 대한 정보를 포함하는 발신 통지를(봉투 ID, 배달 타입 그리고 MIME 해시) 작성하고 비밀키로 서명한다.

## 발신자와 서버의 서명된 발신 통지

송신자는 다음을 한다.

1. 수신된 발신 통지를 푼다.

2. 각 수신자에 대하여 챌린지를 작성한다.

3. 서버가 서명한 발신 통지를 자신의 비밀키로 서명한다.

4. 베이스64로 결과를 인코딩한다. 그리고

5. 다음 명령어를 이용하여 Cmail 서버로 전송한다.

DEPO <notice of deposit base64 encoded>

챌린지(challenge)는 **그림 A.6**에 정의되어 있다.

챌린지는 **SecretQuestion, CipherEnvelopeKey**와 수신자의 공개키 인증서를 포함하고 있다.

**SecretQuestion**은 **Request**와 **Response**로 구성된다.

Request는 **RandomNumber**를 포함 할 수 있다. Response는 ENVELOPE를 수신하기 위하여 송신자의 의하여 재계산되는 **AlgorithmIdentifier**를 포함한다. **AlgorithmIdentifier**은 해시를 계산하기 위한 알고리즘을 식별한다. 챌린지(challenge)은 첫번째 수신자의 공개키로 암호화된 사이퍼 키 RSCK를 복구파트와 **RandomNumber**와 RSCK를 연결해서 응답을 만들기 위하여 해시를 계산한 파트를 포함한다.

XML로 기술된 챌린지(challenge)의 예는 다음과 같다.

**<Entity EmailAddress="john.doe@example.org" Type="to">**

**<SecretQuestion>**

**<Request RandomNumber="30987497498789739837"/>**

**<Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>**

**</SecretQuestion>**

**<CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER" KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>**

**<Certificate Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…**

**/gy7</Certificate>**

**</Entity>**

**비고 1** 이 챌린지는 다른 인코딩 규칙인 ASN.1을 사용할 수 있다.

**비고 2** 서버는 암호 키를 알 지 못하기 때문에 해시를 재계산할 수 없다.

**비고 3** 수신자와의 챌린지 과정에서, 서버는 단지 비밀 질문을 보낼 수 있고 수신자의 응답을 기다린다.

## Cmail 서버간의 봉투

송시자와 수신자가 서로 다른 Cmail 서버에 속한 경우에 6.13 항의 정의된 메시지가 다른 Cmail 서버에게로 전달된다(**그림 1** m16 참조).

SEND EVLP <MIME message>

## Cmail 서버간의 서명된 전송 통지

다음 포맷이 사용된다.

250 Notice-of-transit:

<notice of transit base64 encoded>

다음 메시지는 Cmail 서버가 전송 통지를 수신한 경우에 전송된다.

250 Ok

다음 메시지는 전송 통지가 부정확한 경우에 전송된다.

503 Error: incorrect Notice-of-transit

전송 통지는 ENVELOPE를 수신한 Cmail 서버에 의하여 작성된다.

이 Cmail 서버는 봉투에 대한 정보를(봉투ID, 배달 타입, MIME 해시) 포함하는 발송 통지를 작성하고, 자신의 개인키로 서명한다. 이 통지는 발송통지와 동일하다.

## 서명된 전송 통지

Cmail 서버는 다음을 한다.

1. 수신된 전송통지를 푼다.

2 자신의 개인키를 이용하여 서버가 서명한 전송통지를 서명한다.

3. 베이스64로 결과를 암호화한다. 그리고

4. 다음을 이용하여 Cmail 서버에게 전달한다.

250 Signed-notice-of-transit:

<signed notice of transit base64 encoded>

250 Signed-notice-of-deposit:

<signed notice of deposit base64 encoded>

250 Ok

# 배달증명 우체국 프로토콜

7.1 항부터 7.6 항까지는 **그림 1**의 명령어 p1에서 명령어 p6까지를 설명한다.

## 메시지 펜딩 요청

펜딩 메시지에 대한 정보는 추가적인 파라미터와 함께 [IETF RFC 1939]의 LIST 명령어의 5 절에 기술되어 있는 절차를 이용하여 처리된다. 펜딩 메시지의 각 라인별 상세한 것에 대하여는 표준 전자 메일이 아닌 경우에 있어서 배달 타입을 가리키는 파라미터가 추가 되었다(**그림 1** 명령어 p1 참조). 예로서:

C: LIST

S: +OK 2 messages (320 octets)

S: 1 120

S: 2 200 CertifiedMail

S: .

이러한 절차는 또한 Cmail 서버상의 배달 타입으로 태그 된 메시지를 담당하는 모든 표준 전자 메일의 검색을 포함한다.

## 수신자 챌린지와 서버의 서명된 수신 통지

배달 타입으로 태그된 메시지에 대하여, RETR 명령어는 그 메시지를 검색하지 않고 챌린지(challenge)와 서버가 서명한 베이스64 인코드의 수신 통지를 검색한다. 수신 통지에 포함되어 있는 고객 디지털 서명과 송신자의 인증서 클라이언트를 검증한다.

예시:

C: RETR 2

The following message is sent if the Cmail server sends the notice of reception:

S: +OK 200 octets

S: <the Cmail server sends the notice of reception including the challenge>

S: .

다음 메시지는 서버가 수신 통지를 송신할 수 없는 경우에 송신된다.

503 Error: impossible to send Notice-of-reception

Cmail 서버는 발신 통지 안에서 수신자에게 관련 있는 노드 개체를 발견한다. 그리고 Cmail 서버는 이 노드를 수신자 통지에 카피하고 그 개체 노드에 포함되어 있는 Response node의 내용을 삭제한다.

예시: 발신 통지 안에 있는 노드

**<Entity EmailAddress="john.doe@example.org" Type="to">**

**<SecretQuestion>**

**<Request RandomNumber="30987497498789739837"/>**

**<Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64">5mYZWhtl0yxBa/wl7VLiiQ=</response>**

**</SecretQuestion>**

**<CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER" KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>**

**<Certificate Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…**

**/gy7</Certificate>**

**</Entity>**

**비고 1**  이 챌린지는 ASN.1 DER 인코딩을 사용 할 수 있다.

그리고 동일 노드가 수신 통지 안에 카피된다:

**<Entity EmailAddress="john.doe@example.org" Type="to">**

**<SecretQuestion>**

**<Request RandomNumber="30987497498789739837"/>**

**<Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64" />**

**</SecretQuestion>**

**<CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER" KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>**

**<Certificate Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…**

**/gy7</Certificate>**

**</Entity>**

**비고 2**  이 챌린지는 ASN.1 DER 인코딩을 사용 할 수 있다.

## 챌린지 응답 및 수신자와 서버의 서명된 수신 통지

수신자는 다음을 한다.

1. 수신된 수신 통지를 푼다.

2. RSCK를 검색한다.

3. 챌린지(challenge)을 계산한다.

4. 자신의 개인키를 이용하여 서버가 서명한 수신 통지를 서명한다.

5. 베이스64로 결과를 인코딩 한다. 그리고

6. 다음을 이용하여 Cmail 서버로 전달한다.

CHLG RESP <challenge response and recipient and server signed notice of reception>

수신자는 다음과 같이 암호를 푼다:

**<Entity EmailAddress="john.doe@example.org" Type="to">**

**<SecretQuestion>**

**<Request RandomNumber="30987497498789739837"/>**

**<Response AlgorithmIdentifier="2.16.840.1.101.3.4.2.1" Encoding="base64"></response>**

**</SecretQuestion>**

**<CipherEnvelopeKey Algorithm="AES" CipheredKey="RSA" Encoding="base64-DER" KeySize="256">UjBg…b1PHDOOM4IFnTpzHn9TQ==</cipherEnvelopeKey>**

**<Certificate Encoding="base64">MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM…sdjn7VDBlb+WS10j2rJcAHHsUyr…**

**/gy7</Certificate>**

**</Entity>**

**비고**  이 챌린지는 ASN.1 DER 인코딩을 사용 할 수 있다.

수신자는 자신의 개인키를 이용하여 그 노드 **CipherEnvelopeKey**의 내용의 암호를 풀어 RSCK를 복구한다. 그리고 수신자는 **RandomNumber**와 RSCK를 연결하고 정의된 **AlgorithmIdentifier**를 이용하여 그것을 해시 하고, **SecretQuestion**의 결과를 얻는다.

수신자는 서명된 수신 통지에 결과를 카피하고, 그것을 서명하고 Cmail 서버에게 전송한다.

## 봉투

챌린지(challenge)가 정상인 경우에, Cmail 서버는 RETR 명령어의 결과와 같은 방식으로 ENVELOPE를 전송한다. 수신자는 비로서 메시지와 그것을 여는 키를 갖게 된다.

다음 메시지는 서버가 ENVELOP를 전송할 수 없는 경우에 전송된다:

503 Error: impossible to send ENVELOPE

## Cmail 서버간의 수신자와 서버의 서명된 수신 통지(옵션)

이 메시지는 송신자와 수신자가 다른 Cmail 서버에 속한 경우에만 전송된다.

SEND NORP <base64 encoded Recipient and server signed notice of reception>

## 수신자와 서버의 서명된 수신 통지

이 메시지는 송신자와 수신자가 다른 Cmail 서버에 속한 경우에만 전송된다.

SEND NORP <base64 encoded Recipient and server signed notice of reception>

1. (규정)  
     
   XML 스키마 정의(XSD) 내의 통지

이 부속서는 [XSD]에서 정의된 것과 같이 XML 스키마 정의(XSD)를 이용한 통지를 기술한다. 통신의 예는 [XML]에 기술된 것과 같이 XML로 인코딩 되었고 이 부속서에 주어진 것과 같이 XSD 규격과 일치하여야 한다.

* 1. XSD 개요

**그림 A.1**에서 **그림 A.10**까지 참조

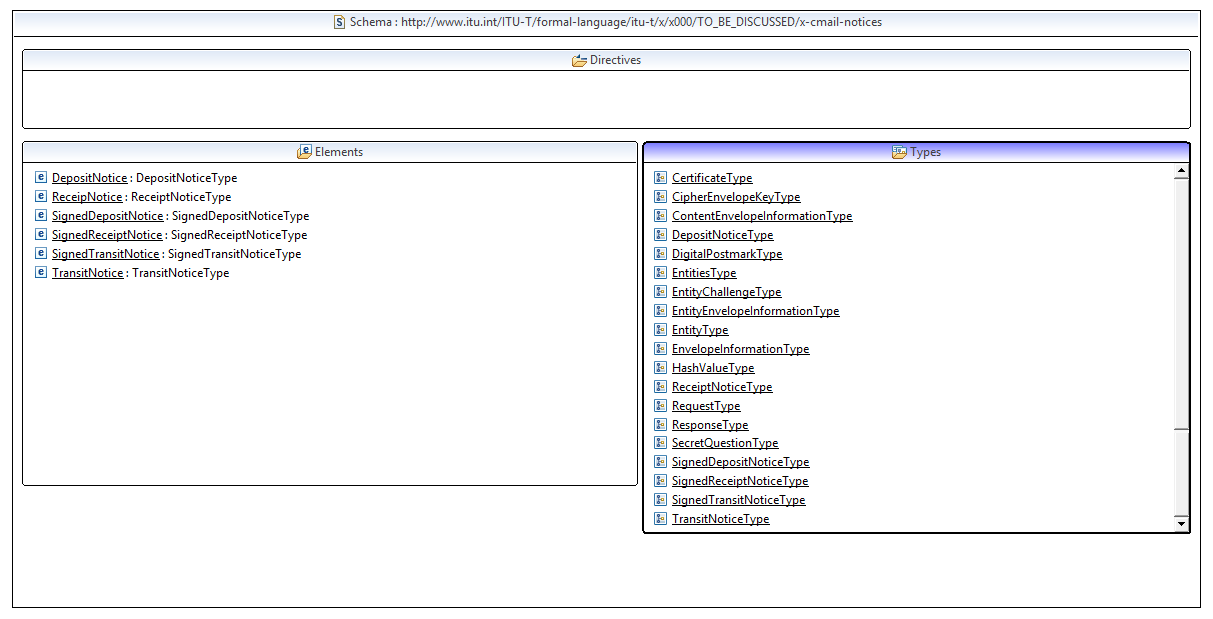


그림 A.1 — 요소와 타입 목록

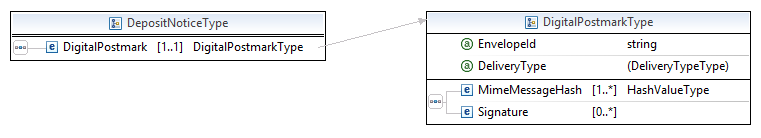


그림 A.2 — 발신 통지

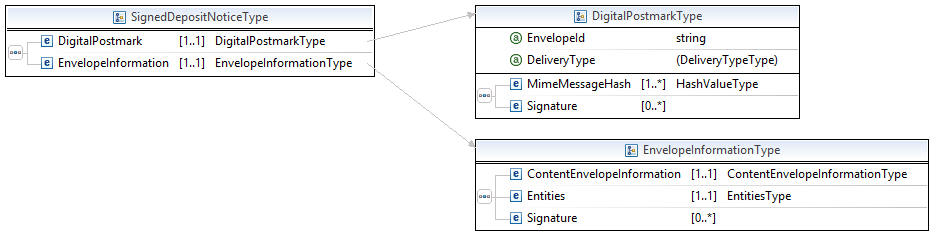


그림 A.3 — 서명된 발신 통지

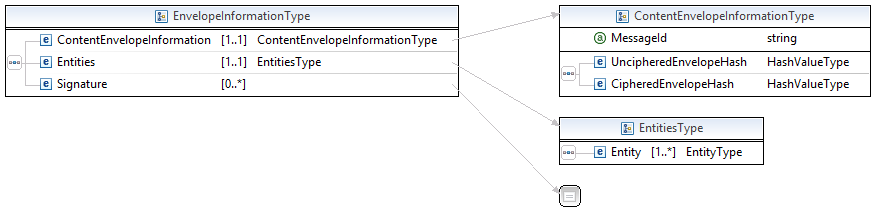


그림 A.4 — 봉투 정보 타입

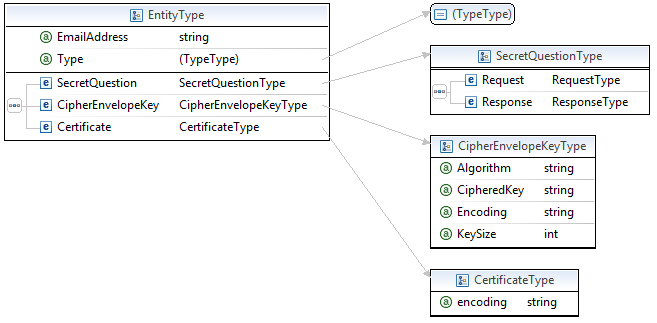


그림 A.5 — 개체 타입

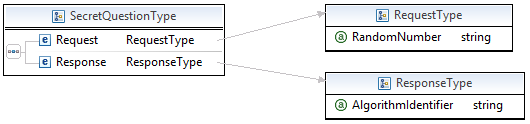


그림 A.6 — 챌린지(Challenge)

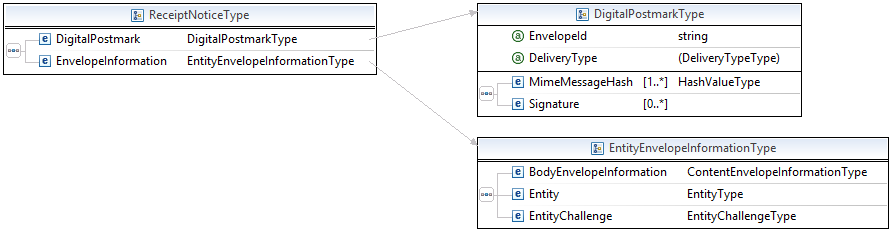


그림 A.7 — 수신 통지

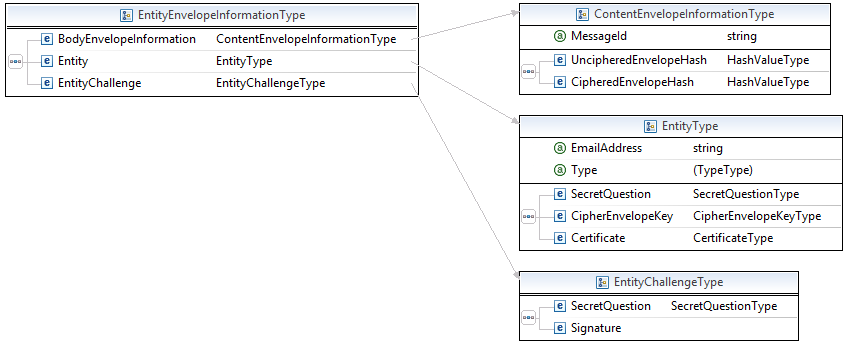


그림 A.8 — 챌린지에 대한 수신자의 응답

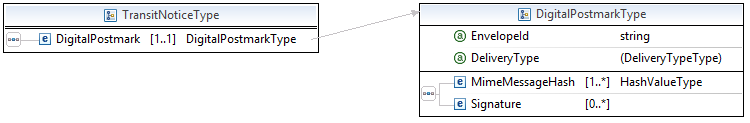


그림 A.9 — 전송 통지

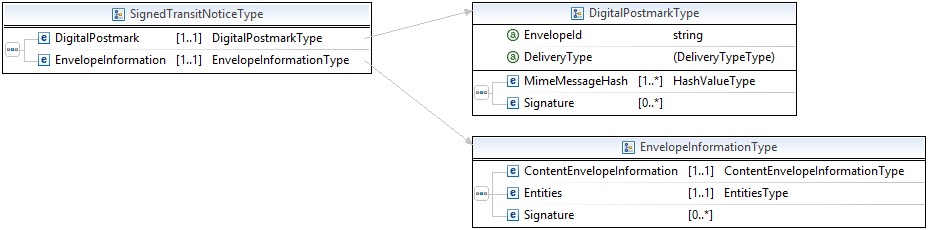


그림 A.10 — 서명된 전송 통지

* 1. XSD로 작성된 통지의 공식 규격

**<?xml version="1.0" encoding="UTF-8"?>**

**<schema targetNamespace="**[**http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices**](http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices)**"**

**elementFormDefault="qualified" xmlns="http://www.w3.org/2001/XMLSchema" xmlns:tns="**[**http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices**](http://www.itu.int/xml-namespace/itu-t/x.1341/x-cmail-notices)**" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">**

**<import namespace="http://www.w3.org/2009/xmldsig11#"**

**schemaLocation="http://www.w3.org/TR/xmldsig-core1/xmldsig11-schema.xsd" />**

**<import namespace="http://www.w3.org/2009/xmldsig-properties"**

**schemaLocation="http://www.w3.org/TR/xmldsig-properties/xmldsig-properties.xsd" />**

**<import namespace=http://www.w3.org/2000/09/xmldsig#**

**schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd" />**

**<element name="DepositNotice" type="tns:DepositNoticeType"></element>**

**<element name="SignedDepositNotice" type="tns:SignedDepositNoticeType"></element>**

**<element name="TransitNotice" type="tns:TransitNoticeType"></element>**

**<element name="SignedTransitNotice" type="tns:SignedTransitNoticeType"></element>**

**<element name="ReceipNotice" type="tns:ReceiptNoticeType"></element>**

**<element name="SignedReceiptNotice" type="tns:SignedReceiptNoticeType"></element>**

**<complexType name="DigitalPostmarkType">**

**<sequence>**

**<element name="MimeMessageHash" type="tns:HashValueType"**

**maxOccurs="unbounded" minOccurs="1">**

**</element>**

**<element name="Signature" type="ds:SignatureType"**

**maxOccurs="unbounded" minOccurs="0">**

**</element>**

**</sequence>**

**<attribute name="EnvelopeId" type="string" use="required"></attribute>**

**<attribute name="DeliveryType" use="required">**

**<simpleType>**

**<restriction base="string">**

**<enumeration value="CertifiedMail"></enumeration>**

**</restriction>**

**</simpleType>**

**</attribute>**

**</complexType>**

**<complexType name="EnvelopeInformationType">**

**<sequence>**

**<element name="ContentEnvelopeInformation"**

**type="tns:ContentEnvelopeInformationType" maxOccurs="1" minOccurs="1">**

**</element>**

**<element name="Entities" type="tns:EntitiesType"**

**maxOccurs="1" minOccurs="1">**

**</element>**

**<element name="Signature" type="ds:SignatureType"**

**maxOccurs="unbounded" minOccurs="0">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="ContentEnvelopeInformationType">**

**<sequence>**

**<element name="UncipheredEnvelopeHash" type="tns:HashValueType"></element>**

**<element name="CipheredEnvelopeHash" type="tns:HashValueType"></element>**

**</sequence>**

**<attribute name="MessageId" type="string"></attribute>**

**</complexType>**

**<complexType name="SecretQuestionType">**

**<sequence>**

**<element name="Request" type="tns:RequestType"></element>**

**<element name="Response" type="tns:ResponseType"></element>**

**</sequence>**

**</complexType>**

**<complexType name="EntityType">**

**<sequence>**

**<element name="SecretQuestion" type="tns:SecretQuestionType"></element>**

**<element name="CipherEnvelopeKey"**

**type="tns:CipherEnvelopeKeyType">**

**</element>**

**<element name="Certificate" type="tns:CertificateType"></element>**

**</sequence>**

**<attribute name="EmailAddress" type="string" use="required">**

**<annotation>**

**<documentation>Email address has to be in RFC 822format</documentation>**

**</annotation></attribute>**

**<attribute name="Type" use="required">**

**<simpleType>**

**<restriction base="string">**

**<enumeration value="from"></enumeration>**

**<enumeration value="to"></enumeration>**

**<enumeration value="cc"></enumeration>**

**<enumeration value="transit"></enumeration>**

**</restriction>**

**</simpleType>**

**</attribute>**

**</complexType>**

**<complexType name="CipherEnvelopeKeyType">**

**<attribute name="Algorithm" type="string"></attribute>**

**<attribute name="CipheredKey" type="string"></attribute>**

**<attribute name="Encoding" type="string"></attribute>**

**<attribute name="KeySize" type="int"></attribute>**

**</complexType>**

**<complexType name="CertificateType">**

**<attribute name="encoding" type="string"></attribute>**

**</complexType>**

**<complexType name="EntitiesType">**

**<sequence>**

**<element name="Entity" type="tns:EntityType"**

**maxOccurs="unbounded" minOccurs="1">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="SignedDepositNoticeType">**

**<sequence>**

**<element name="DigitalPostmark" type="tns:DigitalPostmarkType"**

**maxOccurs="1" minOccurs="1">**

**</element>**

**<element name="EnvelopeInformation"**

**type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="DepositNoticeType">**

**<sequence>**

**<element name="DigitalPostmark" type="tns:DigitalPostmarkType"**

**maxOccurs="1" minOccurs="1">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="TransitNoticeType">**

**<sequence>**

**<element name="DigitalPostmark" type="tns:DigitalPostmarkType"**

**maxOccurs="1" minOccurs="1">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="SignedTransitNoticeType">**

**<sequence>**

**<element name="DigitalPostmark" type="tns:DigitalPostmarkType"**

**maxOccurs="1" minOccurs="1">**

**</element>**

**<element name="EnvelopeInformation"**

**type="tns:EnvelopeInformationType" maxOccurs="1" minOccurs="1">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="ReceiptNoticeType">**

**<sequence>**

**<element name="DigitalPostmark"**

**type="tns:DigitalPostmarkType">**

**</element>**

**<element name="EnvelopeInformation"**

**type="tns:EntityEnvelopeInformationType">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="SignedReceiptNoticeType">**

**<sequence>**

**<element name="DigitalPostmark"**

**type="tns:DigitalPostmarkType">**

**</element>**

**<element name="EnvelopeInformation"**

**type="tns:EntityEnvelopeInformationType">**

**</element>**

**</sequence>**

**</complexType>**

**<complexType name="HashValueType">**

**<attribute name="AlgorithmOID">**

**<simpleType>**

**<restriction base="string">**

**<enumeration value="1.3.14.3.2.26"></enumeration>**

**<enumeration value="2.16.840.1.101.3.4.2.1"></enumeration>**

**</restriction>**

**</simpleType>**

**</attribute>**

**</complexType>**

**<complexType name="EntityEnvelopeInformationType">**

**<sequence>**

**<element name="BodyEnvelopeInformation" type="tns:ContentEnvelopeInformationType">**

**</element>**

**<element name="Entity" type="tns:EntityType"></element>**

**<element name="EntityChallenge" type="tns:EntityChallengeType"></element>**

**</sequence>**

**</complexType>**

**<complexType name="EntityChallengeType">**

**<sequence>**

**<element name="SecretQuestion" type="tns:SecretQuestionType"></element>**

**<element name="Signature" type="ds:SignatureType"></element>**

**</sequence>**

**</complexType>**

**<complexType name="RequestType">**

**<attribute name="RandomNumber" type="string"></attribute>**

**</complexType>**

**<complexType name="ResponseType">**

**<attribute name="AlgorithmIdentifier" type="string"></attribute>**

**</complexType>**

**</schema>**

1. (규정)  
     
   ASN.1의 통지

이 부속서는 ITU-T X.680에서 기술된 것과 같이 ASN.1 (abstract syntax notation one)에서의 통지규격을 제공한다. 통지는 ITU-T X.690에서 기술된 것과 같이 ASN.1 DER (distinguished encoding rules)을 이용하거나 ITU-T X.693에서 기술된 것과 같이 확장XML 인코딩 규칙(EXTENDED-XER)을 이용하여 인코딩 할 수 있다. 마지막의 경우는, 이러한 인코딩의 결과로 XML이 **부속서 A**에서 기술된 XDS를 따라 생성된 XML과 일치하고 있다.

**CMAIL {itu-t(0) recommendation(0) x(24) cmail(1341) asn1Module(1) cmail(1)}**

**DEFINITIONS AUTOMATIC TAGS ::=**

**BEGIN**

**IMPORTS String**

**FROM XSDv2 {joint-iso-itu-t asn1(1) specification(0) modules(0)**

**xsd-module(2) version2(2)};**

**DepositNotice ::= DepositNoticeType**

**SignedDepositNotice ::= SignedDepositNoticeType**

**TransitNotice ::= TransitNoticeType**

**SignedTransitNotice ::= SignedTransitNoticeType**

**ReceiptNotice ::= ReceiptNoticeType**

**SignedReceiptNotice ::= SignedReceiptNoticeType**

**DigitalPostmarkType ::= SEQUENCE {**

**mimeMessageHash SEQUENCE (SIZE(1..MAX)) OF**

**mimeMessageHash HashValueType,**

**signature SEQUENCE (SIZE(0..MAX)) OF**

**signature SignatureType,**

**envelopeId String,**

**deliveryType ENUMERATED {**

**certifiedMail,**

**...**

**}**

**}**

**EnvelopeInformationType ::= SEQUENCE {**

**contentEnvelopeInformation ContentEnvelopeInformationType,**

**entities EntitiesType,**

**signature SEQUENCE (SIZE(0..MAX)) OF**

**signature SignatureType**

**}**

**ContentEnvelopeInformationType ::= SEQUENCE {**

**uncipheredEnvelopeHash HashValueType,**

**cipheredEnvelopeHash HashValueType,**

**messageId String**

**}**

**SecretQuestionType ::= SEQUENCE {**

**request RequestType,**

**response ResponseType**

**}**

**EntityType ::= SEQUENCE {**

**secretQuestion SecretQuestionType,**

**cipheredEnvelopeKey CipheredEnvelopeKeyType,**

**certificate CertificateType,**

**emailAddress String**

**(CONSTRAINED BY**

**{-- "Email address has to be in IETF RFC 822 format --}),**

**type ENUMERATED {**

**from,**

**to,**

**cc,**

**transit**

**}**

**}**

**CipheredEnvelopeKeyType ::= SEQUENCE {**

**algorithm String,**

**cipherededKey String,**

**encoding String,**

**keySize String**

**}**

**CertificateType ::= SEQUENCE {**

**encoding String**

**}**

**EntitiesType ::= SEQUENCE {**

**entity SEQUENCE(SIZE(1..MAX)) OF entity EntityType**

**}**

**SignedDepositNoticeType ::= SEQUENCE {**

**digitalPostmark DigitalPostmarkType,**

**envelopeInformation EnvelopeInformationType**

**}**

**DepositNoticeType ::= SEQUENCE {**

**digitalPostmark DigitalPostmarkType**

**}**

**TransitNoticeType ::= SEQUENCE {**

**digitalPostmark DigitalPostmarkType**

**}**

**SignedTransitNoticeType ::= SEQUENCE {**

**digitalPostmark DigitalPostmarkType,**

**envelopeInformation EnvelopeInformationType**

**}**

**ReceiptNoticeType ::= SEQUENCE {**

**operatorPostmark DigitalPostmarkType**

**}**

**SignedReceiptNoticeType ::= SEQUENCE {**

**operatorPostmark DigitalPostmarkType,**

**envelopeInformation EntityEnvelopeInformationType**

**}**

**HashValueType ::= SEQUENCE {**

**algorithmOID ENUMERATED {**

**sha-1,**

**sha-256**

**}**

**}**

**EntityEnvelopeInformationType ::= SEQUENCE {**

**bodyEnvelopeInformation ContentEnvelopeInformationType,**

**entity EntityType,**

**entityChallenge EntityChallengeType**

**}**

**EntityChallengeType ::= SEQUENCE {**

**secretQuestion \_SecretQuestionType,**

**signature SignatureType**

**}**

**RequestType ::= SEQUENCE {**

**randomNumer String**

**}**

**ResponseType ::= SEQUENCE {**

**algorithmIdentifier String**

**}**

**SignatureType ::= String**

**ENCODING-CONTROL XER**

**GLOBAL-DEFAULTS MODIFIED-ENCODINGS**

**[NAME AS CAPITALIZED] DigitalPostmarkType.mimeMessageHash**

**[UNTAGGED] DigitalPostmarkType.mimeMessageHash**

**[NAME AS CAPITALIZED] DigitalPostmarkType.signature.\***

**[UNTAGGED] DigitalPostmarkType.signature**

**[NAME AS CAPITALIZED] DigitalPostmarkType.envelopeId**

**[ATTRIBUTE] DigitalPostmarkType.envelopeId**

**[NAME AS CAPITALIZED] DigitalPostmarkType.deliveryType**

**[ATTRIBUTE] DigitalPostmarkType.deliveryType**

**[TEXT AS CAPITALIZED] DigitalPostmarkType.delivetyType:certifiedMail**

**[NAME AS CAPITALIZED] EnvelopeInformationType.contentEnvelopeInformation**

**[NAME AS CAPITALIZED] EnvelopeInformationType.entities**

**[NAME AS CAPITALIZED] EnvelopeInformationType.signature**

**[UNTAGGED] EnvelopeInformationType.signature**

**[NAME AS CAPITALIZED]**

**ContentEnvelopeInformationType.uncipheredEnvelopeHash**

**[NAME AS CAPITALIZED]**

**ContentEnvelopeInformationType.cipheredEnvelopeHash**

**[NAME AS CAPITALIZED] ContentEnvelopeInformationType.messageId**

**[ATTRIBUTE] ContentEnvelopeInformationType.messageId**

**[NAME AS CAPITALIZED] SecretQuestionType.request**

**[NAME AS CAPITALIZED] SecretQuestionType.response**

**[NAME AS CAPITALIZED] EntityType.secretQuestion**

**[NAME AS CAPITALIZED] EntityType.cipheredEnvelopeKey**

**[NAME AS CAPITALIZED] EntityType.certificate**

**[NAME AS CAPITALIZED] EntityType.emailAddress**

**[ATTRIBUTE] EntityType.emailAddress**

**[NAME AS CAPITALIZED] EntityType.type**

**[ATTRIBUTE] EntityType.type**

**[NAME AS CAPITALIZED] CipheredEnvelopeKeyType.algorithm**

**[ATTRIBUTE] CipheredEnvelopeKeyType.algorithm**

**[NAME AS CAPITALIZED] CipheredEnvelopeKeyType.cipheredKey**

**[ATTRIBUTE] CipheredEnvelopeKeyType.cipheredKey**

**[NAME AS CAPITALIZED] CipheredEnvelopeKeyType.encoding**

**[ATTRIBUTE] CipheredEnvelopeKeyType.encoding**

**[NAME AS CAPITALIZED] CipheredEnvelopeKeyType.keysize**

**[ATTRIBUTE] CipheredEnvelopeKeyType.keysize**

**[NAME AS CAPITALIZED] CertificateType.encoding**

**[ATTRIBUTE] CertificateType.encoding**

**[UNTAGGED] EntitiesType.entity**

**[NAME AS CAPITALIZED] EntitiesType.entity.\***

**[NAME AS CAPITALIZED] SignedDepositNoticeType.digitalPostmark**

**[NAME AS CAPITALIZED] SignedDepositNoticeType.envelopeInformation**

**[NAME AS CAPITALIZED] DepositNoticeType.digitalPostmark**

**[NAME AS CAPITALIZED] TransitNoticeType.digitalPostmark**

**[NAME AS CAPITALIZED] SignedTransitNoticeType.digitalPostmark**

**[NAME AS CAPITALIZED] SignedTransitNoticeType.envelopeInformation**

**[NAME AS CAPITALIZED] ReceiptNoticeType.digitalPostmark**

**[NAME AS CAPITALIZED] SignedReceiptNoticeType.digitalPostmark**

**[NAME AS CAPITALIZED] SignedReceiptNoticeType.envelopeInformation**

**[NAME AS CAPITALIZED] HashValueType.algorithmOID**

**[ATTRIBUTE] HashValueType.algorithmOID**

**[TEXT AS "1.3.14.3.2.26"] HashValueType.algorithmOID:sha-1**

**[TEXT AS "2.16.840.1.101.3.4.2.1"] HashValueType.algorithmOID:sha-256**

**[NAME AS CAPITALIZED]**

**EntityEnvelopeInformationType.BodyEnvelopeInformation**

**[NAME AS CAPITALIZED]**

**EntityEnvelopeInformationType.entityChallenge**

**[NAME AS CAPITALIZED] EntityChallengeType.secretQuestion**

**[NAME AS CAPITALIZED] EntityChallengeType.signature**

**[NAME AS CAPITALIZED] RequestType.randomNumber**

**[ATTRIBUTE] RequestType.randomNumber**

**[NAME AS CAPITALIZED] ResponseType.algorithmIdentifier**

**[ATTRIBUTE] ResponseType.algorithmIdentifier**

**END**

1. (규정)  
     
   공개키 인프라구조 콤포넌트들에 대한 요구사항
   1. 개요

이 부속서는 Cmail 서버와 고객에게 제안되는 공개키 인프라구조 콤포넌트들에 대한 요구사항을 제공한다.

* 1. Cmail 서버 최종(end)-개체 공개키 인증서

Cmail 서버에게 발급되는 최종(end)-개체 공개키 인증서는 다음의 내용을 갖고 있어야 한다:

a) 버전 3이 명기 되어야 한다.

b) CA는 비순차적 일련의 번호를 생성해야 한다.

c) 주체(Subject) 항목은 ITU-T X.520에 정의된 **dnsName** 속성 타입을 이용하여 단일 콤포넌트로 디렉토리 식별 이름을 담아야 한다. 값은 도메인 이름 시스템(DNS)의 등록된 이름이어야 한다.

d) 주체 대안 이름 확장으로는 두 개의 요소로 제시되어야 한다:

**— rfc822Name** 대안은 요소중에서 하나이어야 하고 또는 Cmail 서버의 관리자의 전자 메일 주소이어야 한다.

**— directoryName** 대안은 다른 요소이어야 하고 또는 다음 콤포넌트와 차별 이름 이어야 한다:

**— countryName**은 있어야 하고, [ISO 3166-1]의 3 개의 코드(alpha-3)를 담아야 한다.

**— organizationName**은 있어야 하고, Cmail 서버를 관리하는 조직의 신뢰하는 이름을 담아야 한다.

**— streetAddress**은 있어야 하고, 거리 이름과 집 번호를 담아야 한다.

**— localityName**은 있어야 하고, 지방 이름을 담아야 한다.

**— stateOrProvinceName**은 유일한 식별에 필수적이라면 있어야 한다. 그렇지 않으면 삭제되어야 한다.

**— postalCode**은 있어야 하고, 위치를 위한 우편번호 담아야 한다.

e) **certificatePolicies** 확장은 있어야 하고, 적어도 공개키 인증서가 이 표준에 따라 발급되었다는 것을 나타내기 위하여 대상(Object) 식별자를 **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(1)}** 담아야 한다.

* 1. Cmail 고객 최종(end)-개체 공개키 인증서

Cmail 고객에게 발급되는 최종(end)-개체 공개키 인증서는 다음의 내용을 갖고 있어야 한다:

a) 버전 3이 명기 되어야 한다.

b) CA는 비순차적 일련의 번호를 생성해야 한다.

c) 주체(Subject) 항목은 아래와 같은 콤포넌트를 갖는 디렉토리 이름을 갖어야 한다:

– **surname**은 고객이 개인인 경우에 있어야 하고, 고객이 기관이면 삭제하여야 한다.

– **givenName**은 surname이 있는 경우에 있어야 하고, 그렇지 않은 경우에는 삭제한다.

– **initials**은 surname이 있는 경우에 있을 수 있고, 그렇지 않은 경우에는 삭제한다.

– **generationQualifier**은 surname이 있는 경우에 있을 수 있고, 그렇지 않은 경우에는 삭제한다.

– **organizationName**은 고객이 주거인이 아니면 있어야 하고, 그렇지 않으면 삭제되어야 한다. 만약 표시를 하려면, 고객이 소속하고 있는 기관의 신뢰할 수 있는 이름을 담아야 한다.

– **streetAddress**은 있어야 하고, 거리 이름과 집 번호를 담아야 한다.

– **localityName**은 있어야 하고, 지방 이름을 담아야 한다.

– **stateOrProvinceName**은 유일한 식별에 필수적이라면 있어야 한다. 그렇지 않으면 삭제되어야 한다.

– **postalCode**은 있어야 하고, 위치를 위한 우편번호 담아야 한다.

– **countryCode3c**은 있어야 하고, [ISO 3166-1]의 3 개의 코드(alpha-3)를 담아야 한다.

d) **subjectAltName** 확장은 있어야 하고, 다음과 같이 표시된 한 개의 요소를 포함하여야 한다:

**— rfc822Name** Cmail 서버의 관리자의 전자 메일 주소이어야 한다.

e) **certificatePolicies** 확장은 있어야 하고, 적어도 공개키 인증서가 이 표준에 따라 발급되었다는 것을 나타내기 위하여 대상(Object) 식별자를 **{itu-t(0) recommendation(0) x(24) cmail(1341) certificatePolicy(2) cmailServer(2)}** 담아야 한다.

* 1. 정보 검증 요구사항

공개키 인증서를 발급하기 이전에, 발행자는 다음을 검증해야 한다:

a) 주체(지원자)는 공개키 인증서에 포함되어야 할 도메인 이름의 등록자이다.

b) 주체는 실질적으로 존재한다.

c) 주체는 운영적으로 존재한다(비즈니스 활동).

d) 주체는 신뢰적으로 인식되는 개체이다.

e) 이름과 주소 정보는 공개키 인증서에 저장되어 있다.

f) 공개키 인증서에 등재되는 **organizationName**은 주체를 식별하는 인정되는 이름이다.

1. (규정)  
     
   전송 계층 보안(TLS)의 요구사항

IETF RFC 5246 또는 이후 버전이 지원되어야 한다.

협상에 있어서, Cmail 서버나 또는 그 고객이 TLS 1.2 보다 앞선 TLS 버전을 협상하는 시도가 있는 경우에는 접속을 받아들이지 않는다.

구현은 다음 사이퍼 슈트를 지원하여야 한다:

TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA256

1. (규정)  
     
   대상 식별자

IETF RFC 5246 또는 이후 버전이 지원되어야 한다.

협상에 있어서, Cmail 서버나 또는 그 고객이 TLS 1.2 보다 앞선 TLS 버전을 협상하는 시도가 있는 경우에는 접속을 받아들이지 않는다.

구현은 다은 사이퍼 슈트를 지원하여야 한다:

TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA256

이 표준은 다음의 대상(object) 식별자를 정의한다:

a) ASN.1 모듈에 연합된 대상 식별자

**{itu-t recommendation(0) x(24) cmail(1341) asn1module(0) cmail(1)}**

b) Cmail 서버의 certificatePolicies 확장에 의하여 사용되는 대상 식별자

**{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailServer(1)}**

c) Cmail 고객의 certificatePolicies 확장에 의하여 사용되는 대상 식별자

**{itu-t recommendation(0) x(24) cmail(1341) certificateProfile(2) cmailClient(2)}**

1. (참조)  
     
   봉투와 통지의 포맷

본 부속서는 통지 인코딩의 예를제공한다.

* 1. 발신 통지

발신 통지는 송신자와 봉투에 대한 정보, 그리고 Cmail 서버와 송신자의 함께 수행한 서명을 포함하고 있다.

이것은 소송의 경우에 송신자가 사용할 수 있는 발신 근거이다.

발신 통지의 공식 규격은 **부속서 A**에서 찾아볼 수 있다.

예: file ''1373360283931.deposit.notice"

|  |
| --- |
| Received: from localhost ([127.0.0.1])  by begmeil  with SMTP (SubEthaSMTP null) id HIWV8HF9  for laura.prin@legalbox.com;  Tue, 09 Jul 2013 10:58:14 +0200 (CEST)  Content-Type: application/octet-stream  Content-Transfer-Encoding: base64  Content-Disposition: attachment; filename=depositNotice.xml  PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs  ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk  bG9wZWQtc2lnbmF0dXJlIi8+CiAgICAgICAgICA8L1RyYW5zZm9ybXM+CiAgICAgICAgICA8RGln  ...  ICAgPFJTQUtleVZhbHVlPgogICAgICAgICAgICA8TW9kdWx1cz5tMkFSUURXUGJBMmgvMzJEQWs4  ICAgICAgICAgIDxFeHBvbmVudD5BUUFCPC9FeHBvbmVudD4KICAgICAgICAgIDwvUlNBS2V5VmFs  dWU+CiAgICAgICAgPC9LZXlWYWx1ZT4KICAgICAgPC9LZXlJbmZvPgogICAgPC9TaWduYXR1cmU+  CiAgPC9lbnZlbG9wSW5mb3JtYXRpb24+CjwvbGV0dGVyRGVwb3NpdFBvc3RtYXJrPgo= |

* 1. 수신 통지

수신 통지는 송신자와 봉투, 봉투를 여는 챌린지(challenge)에 대한 정보와, 그리고 Cmail 서버와 수신자가 함께 수행한 서명을 포함하고 있다.

이것은 소송의 경우에 송신자가 사용할 수 있는 수신 근거이다.

발신 통지의 공식 규격은 **부속서 A**에서 찾아볼 수 있다.

예: file ''[1373360283931.laura.prin@legalbox.com.receipt.notice](mailto:1373360283931.laura.prin@legalbox.com.receipt.notice)"

|  |
| --- |
| Received: from begmeil get hostname ([127.0.0.1])  by localhost  with SMTP (LegalBox POP Server v1.0) id HIWX27L5  for laura.prin@legalbox.com;  Tue, 09 Jul 2013 11:49:01 +0200 (CEST)  Content-Type: application/octet-stream  Content-Transfer-Encoding: base64  Content-Disposition: attachment; filename=receiptNotice.xml  PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs  ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk  PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0  dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk  ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz  ...  MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo  dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs  WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6  WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY  NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l  bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv  S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy  RGVwb3NpdFBvc3RtYXJrPgo= |

* 1. 전송 통지

전송 통지는 송신자와 봉투, 봉투를 여는 챌린지(challenge) 대한 정보와, 그리고 Cmail 서버들이 공히 수행한 서명을 포함하고 있다.

이것은 소송의 경우에 송신자가 사용할 수 있는 전송 근거이다.

발신 통지의 공식 규격은 **부속서 A**에서 찾아볼 수 있다.

예: file ''[1373360283931.laura.prin@legalbox.com.receipt.notice](mailto:1373360283931.laura.prin@legalbox.com.receipt.notice)''

|  |
| --- |
| Received: from begmeil get hostname ([127.0.0.1])  by localhost  with SMTP (LegalBox POP Server v1.0) id HIWX27L5  for laura.prin@legalbox.com;  Tue, 09 Jul 2013 11:49:01 +0200 (CEST)  Content-Type: application/octet-stream  Content-Transfer-Encoding: base64  Content-Disposition: attachment; filename=receiptNotice.xml  PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Im5vIj8+Cjxs  ZXR0ZXJEZXBvc2l0UG9zdG1hcms+CiAgPG9wZXJhdG9yUG9zdG1hcms+CiAgICA8ZW52ZWxvcElk  PjEzNzMzNjAyODM5MzE8L2VudmVsb3BJZD4KICAgIDxkZWxpdmVyeU1vZGU+Y2VydGlmaWVkTGV0  dGVyPC9kZWxpdmVyeU1vZGU+CiAgICA8bWltZU1lc3NhZ2VIYXNoPgogICAgICA8c2hhMT5hNTVk  ZDhmYWU0Mzg2M2VmYWRmMWY3ZjM3MmEwYmU1MmEwMGRhYTFkPC9zaGExPgogICAgPC9taW1lTWVz  ...  MDkwSDl0NFVkTTdWVU92bjY3WlU2aTJvVSt3b3lGR2tYMDJ3YkVMM2pDYmpJCm5VR1BwUGpoT3Zo  dzNPTy9mYmhKVk13dkM2NXB1MTl1cnA2M05kS0tHNlBuNjZtQkVnUldxZ2cvTVBITmZmWkhrOXFs  WExSSXhETi8Kb0ZnS285RmI0NExlSzBnZ3Vyb1Y2azNicm1TeGM1UnpYVWNxTzdwbldUN0FoNFl6  WXJJUHdYL1hjS1VqbXYxZi9JZjQ5VHVnWGtLcgpodklyOG9qUkdQcEdPdlB4cWR5QWNQR1BOUVRY  NFJrc29kSEVwdz09PC9Nb2R1bHVzPgogICAgICAgICAgICA8RXhwb25lbnQ+QVFBQjwvRXhwb25l  bnQ+CiAgICAgICAgICA8L1JTQUtleVZhbHVlPgogICAgICAgIDwvS2V5VmFsdWU+CiAgICAgIDwv  S2V5SW5mbz4KICAgIDwvU2lnbmF0dXJlPgogIDwvcmVjaXBpZW50Q2hhbGVuZ2U+CjwvbGV0dGVy  RGVwb3NpdFBvc3RtYXJrPgo= |

* 1. 봉투

봉투는 AES 암호화에 의하여 암호된 전자 메일 내용을 포함하는 MIME 메시지이다.

예: file ''1373360283931.certifiedLetter.msg"

|  |
| --- |
| Received: from localhost ([127.0.0.1])  by begmeil  with SMTP (SubEthaSMTP null) id HIWV8HF9  for laura.prin@legalbox.com;  Tue, 09 Jul 2013 10:58:03 +0200 (CEST)  Date: Tue, 9 Jul 2013 10:57:51 +0200 (CEST)  From: david.keller@legalbox.com  To: laura.prin@legalbox.com  Message-ID: proto\_cmtp\_1373360269856  Subject: =?UTF-8?Q?Bienvenue\_=C3=A0\_CMTP!?=  MIME-Version: 1.0  Content-Type: multipart/mixed;  boundary="----=\_Part\_1\_1013939722.1373360271613"  ------=\_Part\_1\_1013939722.1373360271613  Content-Type: multipart/mixed;  boundary="----=\_Part\_0\_2062834323.1373360271584"  ------=\_Part\_0\_2062834323.1373360271584  Content-Type: application/octet-stream  Content-Transfer-Encoding: base64  Content-Disposition: attachment; filename=envelop  RG44gUlyr1A/L+ps0R+yKMUpgPcJACmcRQdLZSMoLnm07gtRataSAWkG5qnc/f5Q  ------=\_Part\_0\_2062834323.1373360271584--  ------=\_Part\_1\_1013939722.1373360271613-- |

참고문헌

[1] [b-ITU-T X.509] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

KS X ITUT X1341:2015  
해 설

이 해설은 본체 및 부속서(규정)에 규정한 사항, 부속서(참고)에 기재한 사항 및 이들과 관련된 사항을 설명하는 것으로 표준의 일부는 아니다.

# 제정의 취지

이 표준은 e-메일서비스 제공에 있어서 기밀성, 상호확인, 무결성 및 부인봉쇄 서비스를 제공하여 안전하게 e-메일 전달 증명을 위하여 배달증명 메일 전달 프로토콜(certified mail transfer protocol, CMTP)과 배달증명 우체국 프로토콜(certified post office protocol, CPOP)을 위해 제정하였다.

# 주요 내용

이 표준은 인증, 정보보호 및 부인봉쇄를 위하여 전자 우편 전송 프로토콜(simple mail transfer protocol, SMTP)과 전자 우체국 프로토콜 버전 3 (post office protocol version 3, POP3)을 확장한다.

위의 서비스를 위하여 두 개의 프로토콜을 구비하여 기밀성, 상호확인, 무결성 및 부인봉쇄 서비스를제공한다.

**—** 배달증명 메일 전달 프로토콜(CMTP) : 전자 우편 전송 프로토콜(SMTP)의 확장으로 e-메일 송신자와 메일 서버와의 통신 지원

**—** 배달증명 우체국 프로토콜(CPOP) : 전자 우체국 프로토콜 버전 3(POP3)의 확장으로 e-메일 수신자와 메일 서버간의 통신 지원

**KS X ITUT X1341**:**2015**

|  |
| --- |
| **KSKSKS**  **KSKSK**  **KSKS**  **KSK**  **KS**  **KSK**  **KSKS**  **KSKSK**  **KSKSKS** |

|  |
| --- |
| **Certified mail transport and certified** |
| **post office protocols** |
| **ICS 35.040** |