공인인증서 관리 프로토콜 규격

Accredited Certificate Management Protocol Specification

v1.22

2015년 12월

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

공인인증서 관리 프로토콜 규격

Accredited Certificate Management Protocol Specification

1. 개 요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계 공인인증서비스에서 사용되는 유·무선 공인인증서 관리 프로토콜을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [RFC2510], [RFC6712] 등 국제 표준을 준용하여, 국내 공인전자서명인증체계 내에서 사용되는 유·무선 공인인증서 관리를 위한 기본적인 데이터 구조와 인증서 관리를 위한 운영 관련 데이터 구조를 정의한다.

첫 번째로, 제6장에서는 유선 공인인증서비스에서의 공인인증서 관리 프로토콜을 정의한다.

두 번째로, 제7장에서는 무선 공인인증서비스에서의 공인인증서 관리 프로토콜을 정의한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[RFC2119]	IETF RFC 2119 (1997), *Key Words for use in RFCs to Indicate Requirement Levels*
[RFC2511]	IETF RFC 2511 (1999), *Internet X.509 Certificate Request Message Format*
[RFC2510]	IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocol*
[RFC6712]	IETF RFC 6712 (2012), *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*
[PKCS10]	RSA Laboratories PKCS#10 v1.7 (2000), *Certification Request Syntax Standard*

3.2 국내 표준 및 규격

[KCAC.TS.RS] KISA, KCAC.TS.RS, v1.11, *공인인증서 발급을 위한 참조번호/인가코드 기술규격*, 2009

[KCAC.TS.CRMF] KISA, KCAC.TS.CRMF, v1.21, *공인인증서 요청형식 프로토콜 규격*, 2009

[KCAC.TS.DSIG] KISA, KCAC.TS.DSIG, v1.30, *전자서명 알고리즘 규격*, 2009

3.3 기타

해당사항 없음

4. 정의

본 규격에서 사용하는 용어의 정의는 제4장에서 정한 것을 제외하고는 관련 법령 등이 정하는 바에 의한다.

4.1 전자서명법 용어 정의

본 규격에서 사용된 다음의 용어들은 전자서명법 및 동법 시행령, 공인인증기관의 시설 및 장비 등에 관한 규정(미래창조과학부 고시)에 정의되어 있다.

가) 공인인증서
나) 공인인증기관
다) 가입자

4.2 용어의 정의

가) 유선 공인인증서비스 : 인터넷 기반의 전자거래를 위해 공인인증서를 이용하는 서비스
나) 무선 공인인증서비스 : 무선 단말기 기반의 전자거래를 위해 공인인증서를 이용하는 서비스
다) 키 갱신 : 키 및 인증서 갱신

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 전자서명인증체계 공인인증서 요청형식 프로토콜의 구현 정도를 의미하는 것으로 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

가) 해야한다, 필수이다, 강제한다 (기호 : M)
반드시 준수해야 한다.
나) 권고한다 (기호 : R)
보안성 및 상호연동을 고려하여 준수할 것을 권장한다.
다) 할 수 있다, 쓸 수 있다 (기호 : O)
주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.
라) 권고하지 않는다 (기호 : NR)
보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.
마) 금지한다, 허용하지 않는다 (기호 : X)
반드시 사용하지 않아야 한다.
바) 언급하지 않는다, 정의하지 않는다 (기호 : -)
준수 여부에 대해 기술하지 않는다.

5. 약어 및 기호

해당사항 없음

6. 유선 공인인증서비스에서의 공인인증서 관리 프로토콜

본 장에서는 유선 공인인증서 관련 가입자 등록 및 인증서 발급, 폐지 등 전자서명인증체계 공인인증서 관리 프로토콜에 필요한 기본적인 데이터 구조를 정의한다.

6.1. PKI 메시지

공인인증서 관리 프로토콜에 이용되는 모든 메시지는 다음의 구조를 따른다.

```
PKIMessage ::= SEQUENCE {
        header          PKIHeader,
```

```
    body            PKIBody,
    protection   [0] PKIProtection OPTIONAL,
    extraCerts   [1] SEQUENCE SIZE (1..MAX) OF Certificate OPTIONAL}
```

6.1.1 PKI Message Header

모든 PKI 메시지들은 트랜잭션 ID와 주소정보 등을 포함한 헤더를 가지며, 만약 PKI 메시지가 서명 및 MAC을 이용해 보호된다면 헤더 정보도 역시 보호되어야 한다. 메시지 헤더의 구조는 다음과 같다.

```
PKIHeader ::= SEQUENCE {
    pvno            INTEGER { ietf-version2 (1) },
    sender          GeneralName,
    recipient       GeneralName,
    messageTime     [0] GeneralizedTime    OPTIONAL,
    protectionAlg   [1] AlgorithmsIdentifier OPTIONAL,
    senderKID       [2] KeyIdentifier      OPTIONAL,
    recipKID        [3] KeyIdentifier      OPTIONAL,
    transactionID   [4] OCTET STRING       OPTIONAL,
    senderNonce     [5] OCTET STRING       OPTIONAL,
    recipNonce      [6] OCTET STRING       OPTIONAL,
    freeText        [7] PKIFreeText        OPTIONAL,
    generalInfo     [8] SEQUENCE SIZE (1..MAX) OF InfoTypeAndValue
                        OPTIONAL}
PKIFreeText ::= SEQUENCE SIZE (1..MAX) OF UTF8String
```

pvno 필드는 이 프로토콜의 버전[1]을 나타낸다.

sender 및 recipient 필드는 메시지의 송·수신자 이름을 포함하며, 메시지에 protection 필드가 설정되어 있는 경우, 즉, 해당 PKI 메시지가 보호되는 경우, 이 필드들은 해당 메시지에 대한 protection을 검증하는데 사용되어야 한다.

protectionAlg 필드는 메시지를 보호하기 위해 사용되는 알고리즘을 명시하며,

1) 프로토콜 버전은 [RFC2510] 이전은 0, [RFC2510]은 1로 정의되고 있으므로 본 규격은 이를 준용하도록 함

protection 필드가 설정된 경우에만 사용된다.

senderKID 및 recipKID는 메시지 보호를 위해 사용된 키를 식별하기 위해 사용된다. 특히, sender 필드가 NULL인 경우, senderKID는 반드시 존재해야 한다.

transactionID 필드는 요청메시지와 이에 대한 응답메시지를 식별하기 위해 사용되는 필드로 요청 및 응답메시지에 동일한 값이 포함된다.

senderNonce, recipNonce 필드는 메시지의 재사용 공격을 막기 위해 사용되는 필드로 senderNonce는 메시지 생성자에 의해 설정되고, 요청 및 응답 메시지에 동일한 값이 포함된다.

messageTime 필드는 송신자가 메시지를 생성하는 시간을 포함한다.

6.1.2 PKI Message Body

PKIBody는 가입자 초기화 및 인증서 발급, 폐지, 키 갱신 등에 대한 응답 및 요청 메시지를 포함해서 PKI 개체 간에 송·수신되는 일반적인 요청 및 응답 메시지들의 실제 내용이 포함된다.

```
PKIBody ::= CHOICE {
        ir          CertReqMessage,
        ip          CertRepMessage,
        cr          CertReqMessage,
        cp          CertReqMessage,
        p10cr       CertificateionRequest,
        popdecc     POPODecKeyChallContent,
        popdecr     POPODecKeyRespContent,
        kur         CertReqMessage,
        kup         CertRepMessage,
        krr         CertReqMessage,
        krp         KeyRecRepContent,
        rr          CertReqMessage,
        rp          CertRepMessage,
        ccr         CertReqMessage,
        ccp         CertReqMessage,
        ckuann      CAKeyUpdAnnContent,
```

```
        cann        CertAnnContent,
        rann        RevAnnContent,
        crlann      CRLAnnContent,
        conf        PKIConfirmContent,
        nested      NestedMessageContent,
        genm        GenMsgContent,
        genp        GenRepContent,
        error       ErrorMsgContent }
```

6.1.3 protection

protection은 메시지의 무결성을 위해 사용될 수 있으며, 다음의 구조를 가진다.

```
PKIProtection ::= BIT STRING
```

PKIProtection은 해당 메시지의 header와 body를 포함한 ProtectedPart에 대해 DER 인코딩한 값을 MAC하거나 혹은 서명한 값이다. ProtectedPart는 다음의 구조를 가진다.

```
ProtectedPart ::= SEQUENCE {
        header PKIHeader,
        body   PKIBody }
```

6.1.4 extraCerts

extraCerts 필드는 메시지 수신자가 유용하게 이용할 수 있는 인증서를 포함할 수 있다. 예를 들면, 이것은 CA나 RA가 자신의 새로운 인증서를 증명하기 위해 사용자에게 기존 인증서를 전송하는데 사용될 수 있다.

6.2 운영 관련 데이터 구조

6.2.1 초기화 요청 메시지

ir은 초기화 요청 메시지로 [KCAC.TS.CRMF]의 CertReqMessage의 구조를 가지며, 발급 요청하는 인증서에 포함될 정보가 포함된다. 일반적으로 CertTemplate에 SubjectPublicKeyInfo, KeyID 및 Validity이 포함될 수 있으며, 메시지에 대한 protection을 위해서는 MAC을 사용해야 한다.

6.2.2 초기화 응답 메시지

ip는 가입자 초기화 요청에 대한 응답 메시지로, 인증서 요청에 대한 상태정보, 가입자 인증서 등을 포함한다. 초기화 응답의 데이터 구조는 다음과 같다.

```
CertRepMessage ::= SEQUENCE {
        caPubs [1]      SEQUENCE SIZE (1..MAX) OF Certificate OPTIONAL,
        response        SEQUENCE OF CertResponse }

CertResponse ::= SEQUENCE {
        certReqId       INTEGER,
        status          PKIStatusInfo,
        certifiedKeyPair CertifiedKeyPair     OPTIONAL,
        rspInfo         OCTET STRING          OPTIONAL }

CertifiedKeyPair ::= SEQUENCE {
        certOrEncCert           CertOrEncCert,
        privateKey      [0]     EncryptedValue        OPTIONAL,
        publicationInfo [1]     PKIPublicationInfo    OPTIONAL }

CertOrEncCert ::= SEQUENCE {
        certificate     [0]     Certificate,
        encryptedCert   [1]     EncryptedValue }
```

certReqID는 요청메시지의 certReqID와 동일해야 하며, 요청메시지에 certReqID가 명시되어 있지 않은 경우, -1의 값을 가져야 한다.

PKIStatusInfo는 인증 요청 메시지에 대한 처리 상태를 나타내며, 다음의 구조를 가진다.

```
PKIStatusInfo ::= {
        status          PKIStatus,
        statusString    PKIFreeText    OPTIONAL,
        failInfo        PKIFailureInfo OPTIONAL }
```

응답메시지는 다음에서 정의된 상태정보의 일부를 포함할 수 있다.

```
PKIStatus ::= INTEGER {
```

```
        granted                 (0),
        grantedWithMods         (1),
        rejection               (2),
        waiting                 (3),
        revocationWaring        (4),
        revocationNotification  (5),
        keyUpdateWarning        (6) }
```

인증 요청이 실패한 경우, 응답메시지의 송신자는 실패 사유에 대한 정보를 제공하기 위해 다음의 데이터 구조를 사용한다.

```
PKIFailureInfo ::= BIT STRING {
        badAlg              (0),
        badMessageCheck     (1),
        badRequest          (2),
        badTime             (3),
        badCertID           (4),
        badDataFormat       (5),
        wrongAuthority      (6),
        incorrectData       (7),
        missingTimeStamp    (8),
        badPOP              (9) }
```

6.2.3 등록 및 인증서 요청 메시지

cr은 등록 및 인증서 요청 메시지로 [KCAC.TS.CRMF]의 CertReqMessage 구조의 데이터를 가진다.

6.2.4 등록 및 인증서 요청 응답 메시지

cp는 등록 및 인증서 요청에 대한 응답 메시지로 6.2.2에 정의된 CertRepMessage 구조의 데이터를 가진다.

6.2.5 키 갱신 요청 메시지

kur은 키 갱신 요청으로 [KCAC.TS.CRMF]의 CertReqMessage의 구조를 가지며,

일반적으로 갱신될 키에 대한 SubjectPublicKeyInfo, KeyID 및 Validity이 CertTemplate에 포함될 수 있다.

6.2.6 키 갱신 응답 메시지

kup는 키 갱신 요청에 대한 응답으로 CertRepMessage의 구조를 가지며, 포함되는 내용은 인증서 신규발급 요청에 대한 응답 메시지에 포함된 정보와 동일하다.

6.2.7 인증서 폐지 요청 메시지

rr은 인증서 폐지 요청으로 다음의 데이터 구조를 가진다.

```
RevReqContent ::= SEQUENCE OF RevDetails
RevDetails ::= SEQUENCE {
        certDetails         CertTemplate,
        revocationReason    ReasonFlags       OPTIONAL,
        badSinceDate        GeneralizedTime   OPTIONAL,
        crlEntryDetails     Extensions        OPTIONAL }
```

인증서 폐지 요청자의 이름은 PKIHeader에 포함된다.

certDetails은 요청자가 폐지 요청한 인증서에 대한 상세 정보를 가지고, revocationReason은 폐지 요청 사유를 포함한다.

6.2.8 인증서 폐지 응답 메시지

rp는 인증서 폐지 요청에 대한 응답으로 다음의 데이터 구조를 가진다.

```
RevRepContent ::= SEQUENCE {
        status          SEQUENCE SIZE (1..MAX) OF PKIStatusInfo,
        revCerts [0]    SEQUENCE SIZE (1..MAX) OF CertID OPTIONAL,
        crls     [1]    SEQUENCE SIZE (1..MAX) OF CertificateList
                        OPTIONAL }

CertId ::= SEQUENCE {
        issuer          GeneralName,
        serialNumber    INTEGER }
```

6.2.9 확인 메시지

conf는 3-way 프로토콜에서 final 메시지로 사용되는 확인 메시지이다. 이 필드의 값은 NULL로 모든 경우에 동일하며, 요청된 모든 정보가 PKIHeader에 포함되기 때문에 실제로 포함되는 정보는 없다

```
PKIConfirmContent ::= NULL
```

6.2.10 일반 요청 메시지

genm은 PKI 개체 간 일반적인 요청 메시지로 다음의 데이터 구조가 사용될 수 있다.

```
GenMsgContent ::= SEQUENCE OF InfoTypeAndValue

InfoTypeAndValue ::= SEQUENCE {
        infoType        OBJECT IDENTIFIER,
        infoValue       ANY DEFINED BY infoType OPTIONAL }
```

InfoTypeAndValue은 다음의 예와 같은 내용을 포함할 수 있으며, 필요에 의해 새로운 요청 및 응답메시지를 정의하여 사용할 수 있다.

```
{ CAProtEncCert      = {id-it 1}, Certificates                    }
{ SignKeyPairTypes   = {id-it 2}, SEQUENCE OF AlgorithmIdentifier }
{ EncKeyPairTypes    = {id-it 3}, SEQUENCE OF AlgorithmIdentifier }
{ PreferredSymmAlg   = {id-it 4}, AlgorithmIdentifier             }
{ CAKeyUpdateInfo    = {id-it 5}, CAKeyUpdAnnContent              }
{ CurrentCRL         = {id-it 6}, CertificateList                 }
```

※ 여기서, { id-it } = { 1 3 6 1 5 5 7 4}

6.2.11 일반 응답 메시지

genp는 일반적인 요청 메시지에 대한 응답으로 다음의 데이터 구조를 가진다.

```
GenRepContent :: SEQUENCE OF InfoTypeAndValue
```

6.2.12 에러 메시지

error는 다음의 구조를 가진다.

```
ErrorMsgContent ::= SEQUENCE {
        pKIStatusInfo           PKIStatusInfo,
        errorCode               INTEGER         OPTIONAL,
        errorDetails            PKIFreeText     OPTIONAL }
```

부록 1. 웹 표준 기반 구현 기술의 예

1.1 소개

웹 표준 기술만으로 HTTP를 통해 전자서명키 쌍과 인증서 요청양식의 생성, 응답을 처리하여 저장하는 기능 등을 구현하는 방법을 제시한다.

1.2 구현

1.2.1 서버 측면

공인인증서의 발급과 관리는 발급시스템과 클라이언트 간의 요청과 응답을 위한 메시지를 통해 이루어지며, 이때 메시지는 특정 프로토콜이 아닌 HTTP (또는 HTTPS)를 통해 전송되어야 한다.

1.2.1.1 HTTP Transfer for the CMP

기존 공인인증서 발급시스템을 활용하고 웹 표준을 적용할 수 있는 방법은 'HTTP Transfer for the Certificate Management Protocol'를 준용하는 것이다 [RFC6712]. 공인인증서 발급·관리와 관련한 모든 요청과 응답은 HTTP를 통해 PKI 메시지로 처리 가능하며 기존 발급시스템의 활용 또한 가능하다.

[RFC6712]를 준용하기 위해서, CMP(Certificate Management Protocol) 메시지는 반드시 HTTP를 사용하여야 하며 HTTP/1.0 (필수), HTTP/1.1 (권고)을 지원해야 한다. 또한 GET이 아닌 POST방식만을 사용하여 메시지를 전송하여야 한다. PKIMessage를 전송하는 동안 HTTP 헤더의 콘텐츠 타입으로 application/pkixcmp으로 설정하여야 한다. CMP 요청을 위한 PKIMessage는 Base64 디코딩하여 처리한다. CMP 응답 또한 Base64 인코딩하여 메시지를 전송한다.

DER 인코딩[ITU.X690.1994]된 PKIMessage[RFC4210] 혹은 PKIMessage가 포함된 TCPMessage를 HTTP POST 요청의 본문에 담아 보내며 HTTP 요청이 성공하면 서버는 HTTP 응답에 CMP 응답메시지를 담아 보낸다. 이 경우 HTTP 응답코드는 200이어야 하며 요청 성공과 관련한 다른 응답코드(2XX)는 이 경우 사용

해선 안된다. 이와 관련한 더 상세한 표준내용은 [RFC6712], [RFC4210] 등의 표준문서를 참고한다.

1.2.1.2 CSR 등 발급방법

CMP를 HTTP를 통해 전송하는 방법 이외에도 SSL 인증서 발급 시 이용되는 CSR(Certificate Signing Request), HTML5 keygen 태그를 활용한 방법 등이 있다[PKCS10][Keygen].

1.2.2 클라이언트 측면

웹브라우저에서 공인인증서 발급 기능을 구현하기 위해서는 전자서명 키쌍 생성, 전자서명 생성·검증, 개인키 암호화, 전자서명 대상 원문의 축약 등을 위해 암호화 알고리즘 구현과 인증서 요청 및 응답 메시지 처리 등을 위한 기능 구현이 필요하다.

1.2.2.1 자바스크립트 암호 알고리즘 구현

웹 표준 구현기술만으로 공인인증서 발급 및 이용이 가능하기 위해서는 자바스크립트를 사용하여 암호 라이브러리를 개발하거나 W3C에서 표준화하고 있는 웹 암호 API(Web Cryptography API)를 사용하여 개발하는 방법이 있다.

1.2.2.2 CMP 요청 및 응답 메시지 처리

공인인증서 발급을 위해서는 암호라이브러리 외에도 기존 TCP 방식으로 구현되어 있는 CMP를 HTTP 방식으로 전송하도록 구현해야 한다. CMP 요청을 위한 PKIMessage는 Base64 인코딩되어 POST 데이터로 서버에 전송된다. CMP 응답 또한 Base64 디코딩하여 메시지를 처리한다.

1.2.2.3 웹 암호 API 활용

웹 암호 API를 사용하여 전자서명 키쌍을 생성 및 전자서명을 수행할 수 있다. 웹 암호 API에 관한 상세한 내용은 W3C 페이지[WebCrypto]를 참고할 수 있다.

부록 2. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2004년 12월	・“공인인증서 관리 프로토콜 규격”으로 제정
v1.10	2007년 4월	・“무선인증서 관리프로토콜 v1.32” 흡수통합
v1.20	2008년 10월	・관련 국내 표준 및 규격 갱신 내용 반영 ・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.21	2009년 9월	・관련 국내 표준 참조 오류 정정
v1.22	2015년 12월	・웹 표준 기반 구현 기술 반영