교육부

KERIS
한국교육학술정보원

교육부 행정전자서명인증센터
상호연동기술표준

2019. 12.

교육부
행정전자서명인증센터
Education Public Key Infrastructure Center

1. 개요

1.1. 목적

본 기술표준에서는 교육부 행정전자서명인증센터 인증서의 상호 연동을 위한 기술적인 기본 사항들을 정하고자 한다.

1.2. 적용범위

본 표준은 교육업무 서비스에 사용되는 인증서를 생성, 폐지, 관리 및 검증하기 위해 인증기관 및 인증서를 활용하는 각 기관에 본 표준을 적용한다.

1.3. 주요내용

본 표준에서는 다음과 같은 사항에 대해 정의한다.

- 인증서 및 인증서폐지목록 프로파일
- 알고리즘
- 인증서 관리
- 인증서 유효성 검증
- OID 및 DN
- 인증서 체계
- 보안토큰 기술규격

1.4. 전제 조건

본 표준은 다음과 같은 전제조건을 고려하여 기술한다.

- X.509 인증서 버전 3와 인증서 폐지목록 버전 2를 사용한다.
- 모든 인증서 사용자들이 최상위 인증기관(루트 즉 Self-signed CA)을 가장 신뢰하는 하향식(Top-down) 신뢰 구조를 가정한다.
- 송수신 메시지 중에 out-of-band로 교환되는 것은 별도로 정의하지 않는다.
- 저장소에 대한 사용자 인증(authentication) 프로토콜을 포함하지 않는다.
- 저장소는 X.500 디렉토리 또는 URI(Uniform Resource Indicator)를 이용하는 다른 형태일 수 있으나, LDAPv3를 반드시 지원하여야 한다.
- 본 규격에 기술되지 않은 사항은 일차적으로 행정전자서명인증관리센터에서 권고하는 기술규격을 따르며, 이외의 사항에 대해서는 국내외 기술규격 및 표준을 준용한다.

1.5. 용어 정의

- ASN.1(Abstract Syntax Notation One) : 복잡한 데이터 구조들을 추상적으로 표현하기 구문 표기법
- ARIA(Academy Reasearch Institute Agency) : KS X 1213, 128비트 블록 암호 알고리즘
- CMP(Certificate Management Protocols) : 인증기관, 등록기관, 사용자 간 인증서 발급, 갱신, 폐지 등 각종 인증업무를 처리하는 데에 사용되는 인증서 관리 프로토콜
- DER(Distinguished Encoding Rules) : 동일한 데이터 구조에 대해서는 유일한 인코딩/디코딩 값을 생성해 내는 ASN.1 인코딩 규칙
- DN(Distinguished Name) : 사용자 객체를 명확히 구별할 수 있도록 부여하는 고유한 이름
- KCDSA : 이산대수 문제에 기반을 둔 TTAS.KO-12.0001/R4에 따르는 한국표준 전자서명 알고리즘
- LDAP(Lightweight Directory Access Protocol) : 디렉토리 서버와 클라이언트 간의 통신에 사용되는 디렉토리시스템 접근 프로토콜로서, DAP보다 간결하고 실용적으로 만들어진 프로토콜
- OCSP(Online Certificate Status Protocol) : 인증서 폐지목록을 획득하지 않고도 실시간으로 인증서의 상태를 검증할 수 있도록 하는 인증서상태 실시간검증프로토콜
- SCVP(Server-base Certificate Validation Protocol) : 클라이언트를 대신하여 서버가 인증경로의 설정과 인증경로를 검증할 수 있도록 하는 프로토콜
- OID(Object IDentifier) : 객체를 식별하기 위하여 객체에게 부여하는 고유한 식별자
- PKCS(Public Key Cryptography Standards) : RSA사에서 RSA알고리즘의 구현방법론과 여러 가지 구문표현에 대해 정의한 문서
- SEED : TTA.IS-10118을 따르는 한국표준 암호 알고리즘
- SHA-1 : 미국전자서명 표준인 DSS(Digial Signature Standard)와 함께 사용될 목적으로 설계된 알고리즘으로 160bit를 출력함
- SHA256 : SHA-1의 안전성이 문제가 되면서 출력길이를 확장한 알고리즘으로 FIP

180-2에 정의되어 있음

- 개인키(private key) : 공개키 암호 시스템에서 전자서명을 하거나 복호화를 하는데 사용하기 위해 개인만이 보유하는 키
- 공개키(public key) : 공개키 암호 시스템에서 사용자의 전자서명을 검증하거나 암호화를 하는데 쓰이는 키
- 디렉토리 시스템(DS: Directory System) : 정보를 저장, 관리할 수 있는 분산된 데이터베이스 시스템
- 인증 경로(Certification Path) : 서명 검증자가 신뢰하는 인증서부터 검증하고자 하는 인증서까지의 일련의 인증서의 집합
- 인증기관(CA : Certification Authority) : 사용자 및 다른 인증기관들에게 공개키 인증서를 발급하는 신뢰 기관으로 인증서 폐지 목록을 주기적으로 발행하며, 디렉토리에 인증서와 인증서 폐지 목록을 게시함
- 인증서 신뢰목록(CTL : Certificate Trust List) : 최상위인증기관이 他 인증기관과의 상호연동을 하기 위한 방식으로서 他 최상위인증기관에서 발급한 인증서를 인증하기 他 최상위인증기관의 인증서 목록임
- 인증서(certificate) : 공개키와 사용자의 관계를 연결해주는 전자 정보로 인증기관에서 발급함
- 인증서 정책 : 보안이 요구되는 응용의 등급 또는 특정 환경에서 인증서의 용도 등을 지정하는 규칙들의 집합
- 인증서 폐지목록(CRL : Certificate Revocation List) : 여러 가지 폐지 사유로 인하여 더 이상 사용할 수 없는 인증서들의 목록
- 해쉬 함수: 가변 길이의 비트를 일정 길이의 비트로 대응시켜주는 함수
- 보안토큰 : 전자서명 생성키 등 주요자료를 안전하게 저장・보관할 수 있게 하며, 키생성・전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기
- 보안토큰 API(PKCS#11) : 보안토큰에 대한 응용프로그램 인터페이스

1.6. 준용 표준목록

알고리즘 표준규격	암호화	• 공공기관 암호화용 알고리즘 • SEED : TTAS.KO-12.0004 : 128비트 블록암호알고리즘(SEED) • AES : FIPS 197 ADVANCED ENCRYPTION STANDARD (AES) • 3DES : FIPS PUB 46-3 DATA ENCRYPTION STANDARD • ARIA : KS X 1213, 128비트 블록 암호 알고리즘 ARIA • KCAC.TS.ENC, 암호 알고리즘 규격 (v1.21)
	전자 서명	• KCDSA : TTAS.KO-12.0001R1, 부가형 전자서명방식표준(KCDSA) • RSA : PKCS #1 v2.0 RSA Encryption Standard • KCAC.TS.DSIG, 전자서명 알고리즘 규격(v1.30)
	해쉬함수	• HAS-160 : TTAS.KO-12.0011/R2 해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160) • SHA-1 : FIPS 180-1 Secure Hash Standard • SHA256 : FIPS 180-2 Secure Hash Standard • KCAC.TS.HASH, 해쉬 알고리즘 규격 (v1.20)
	난수 생성	• ANSI X9.62 RNG • FIPS 186-2 General Purpose RNG
	HMAC	• RFC2104 HMAC : Keyed-hashing for Message Authentication
데이터 형식 및 프로토콜 표준규격	객체 인증	• ISO/IEC IS 9798-3 Entity authentication - Part 3: Mechanisms using digital signature techniques
	ASN & DER Encoding	• ITU-T X.680 Information Technology Abstract Syntax Notation One (ASN.1) : Specification of basic notation • ITU-T X.690 Information Technology ASN.1 Encoding Rules Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules(DER)
	인증서/인증서폐지목록 형식	• RFC3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile • ITU-T X.509 Information Technology Open Systems Interconnection The Directory : Authentication Framework (ISO/IEC 9594-8) • KCAC.TS.CERTPROF, 전자서명인증서 프로파일 규격 (v1.70) • KCAC.TS.CRLPROF, 전자서명인증서 효력정지 및 폐지목록 프로파일 규격 (v.1.50)

	실시간 인증서 상태확인	• RFC6960 Internet X.509 Internet Public Key InfrastructureOnlineCertificateStatusProtocol-OCSP • KCAC.TS.OCSP (실시간 인증서 상태확인 기술규격 v1.21)
	서버기반 인증서 검증	• RFC5055 Server-Based Certificate Validation Protocol-SCVP
	인증서 관리	• RFC6712Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP)
	인증서 발급 신청 형식	• RFC4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) • KCAC.TS.CRMF, 공인인증서 요청형식 프로토콜 규격 (v1.21)
	CMS (Cryptographic Message Syntax)	• PKCS #7 v1.5 Cryptographic Message Syntax Standard
	Base64 Encoding	• RFC2045 Multipurpose Internet Mail Extensions(MIME) Part One : Format of Internet Message Bodies
	키 저장	• Private Key Information Syntax : PKCS #8 v1.2 Private-key Information Syntax Standard • Password-based Encryption : PKCS #5 v2.0 Password-based Encryption Standard • PKCS#11 v2.2 Cryptographic Token Interface Standard
	Directory System	• LDAP v3 Lightweight Directory Access Protocol (v3): Technical Specification • KCAC.TS.LDAP, 전자서명인증체계 디렉토리 프로토콜 규격 [v1.11]
	본인 확인	• KCAC.SIVID (식별번호를 이용한 본인확인 기술 규격 v1.21)
보안토큰 인증규격	저장 및 이용 규격	• KCAC.TS.HSMU : 보안토큰 기반 공인인증서 이용기술 규격[v2.4] • KCAC.TS.HSMS : 보안토큰 기반 공인인증서 저장형식 기술규격 [v1.13]

2. 프로파일 규격

본 장에서는 인증서 및 인증서폐지목록의 데이터 구조와 프로파일을 정의한다.
인증서 프로파일 및 인증서 폐지목록 프로파일 등은 인증기관 간 상호연동 보장을 위해서 다음의 표준을 준수하여야 한다.

- TTAS.KO-12.0012/R1, "전자서명 인증서 프로파일 표준"
- TTAS.KO-12.0013/R1, "전자서명 인증서 효력정지 및 폐지목록 프로파일 표준"

단, 위에 나열한 표준과 본 표준에서 상충하는 부분이 있으면, 본 표준을 우선 준용한다.

2.1. 인증서 프로파일

본 표준에서는 X.509 V3 인증서를 사용한다. X.509 V3 인증서의 구조는 다음과 같다.

```
Certificate ::= SEQUENCE {
        tbsCertificate              TBSCertificate,
        signatureAlgorithm          AlgorithmIdentifier,
        signatureValue              BIT STRING }

TBSCertificate ::= SEQUENCE {
        version [0]                 EXPLICIT Version DEFAULT v1,
        serialNumber                CertificateSerialNumber,
        signature                   AlgorithmIdentifier,
        issuer                      Name,
        validity                    Validity,
        subject                     Name,
        subjectPublicKeyInfo        SubjectPublicKeyInfo,
        issuerUniqueID [1]          IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- If present, version MUST be v2 or v3
        subjectUniqueID [2]         IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- If present, version MUST be v2 or v3
        extensions [3]              EXPLICIT Extensions OPTIONAL
                                    -- If present, version MUST be v3 }


    Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
    CertificateSerialNumber  ::=  INTEGER

    Validity ::= SEQUENCE {
          notBefore                 Time,
          notAfter                  Time }

    Time ::= CHOICE {
          utcTime                   UTCTime,
          generalTime               GeneralizedTime }

    UniqueIdentifier  ::=  BIT STRING
```

```
SubjectPublicKeyInfo  ::=  SEQUENCE  {
        algorithm                AlgorithmIdentifier,
        subjectPublicKey         BIT  STRING   }

Extensions   ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension    ::=  SEQUENCE  {
        extnID                   OBJECT  IDENTIFIER,
        critical                 BOOLEAN  DEFAULT  FALSE,
        extnValue                OCTET  STRING   }
```

인증서는 교육부 인증기관의 개인키로 서명된다. 인증서는 선택적인 확장필드로 확장될 수 있으며, 표준화된 확장필드들은 다음을 포함한다.

- 키 및 보안정책 정보 (Key and Policy Information)
- 인증서 주체와 발급자 속성 (Subject and Issuer Attributes)
- 인증서 폐지목록 식별 (CRL Identification)

2.1.1. 기본 필드

인증서 기본필드는 인증서의 버전, 발급자, 유효기간 등 인증서의 기본 정보를 나타내며, 아래 정의된 기본필드는 인증서에 모두 포함되어야 한다. 또한, 인증서를 처리하는 모든 소프트웨어는 아래에 명시된 기본 필드를 모두 처리할 수 있어야 한다.

필드명	설정 정보		비고
	인증기관	가입기관	
Version	V3 (2)	V3 (2)	정수값
Serial Number	정수값	정수값	최대 20바이트 난수
Signature	RSA	RSA	OID 참조 관련표준 준수 ASN.1 DER 인코딩
Issuer	최상위인증기관 DN	인증기관 DN	X.500 DN 형식 한글은 [KCAC.TS.DN] 준수
Validity	발급일/만료일	발급일/만료일	GTM(Zulu) 형식 UTCTime 또는 GeneralizedTime
Subject	인증기관 DN	가입기관 DN	X.500 DN 형식 한글은 [KCAC.TS.DN] 준수
Subject Public Key Info	RSA	KCDSA(서명용) RSA(암호용)	알고리즘 OID, 공개키, 알고리즘은 관련 표준 준수

※ 교육부 행정전자서명인증센터에서 발급하는 가입자 인증서는 개인용/전자관인용(기관용)/특수목적용(업무용)/서버용(컴퓨터용)/SSL용으로 구분되며 각 경우에 따라 DN 구성 방식이 다르며 이는 별도의 교육부 행정전자서명인증센터 가입자 DN 정책에 따른다.

2.1.2. 인증서 확장 필드

확장 필드는 OID와 ASN.1의 구조를 준수해야 하며, 다음 사항이 필수적으로 지원되어야 한다.

- 발급자 공개키 식별자 (Authority Key Identifier)
- 소유자 공개키 식별자 (Subject Key Identifier)
- 키 사용목적 (Key Usage)
- 인증서 정책 (Certificate Policy)
- 소유자 대체이름 (Subject Alternative Name)
- 발급자 대체이름 (Issuer Alternative Name)
- CRL 배포지점 (CRL Distribution Point)
- 기관정보 접근지점 (Authority Information Access)

본 표준에서 권고하는 인증서 확장영역은 다음과 같은 표로 요약할 수 있다.

확장필드	설정 정보	인증기관		가입기관	
		사용여부	중요도	사용여부	중요도
Authority Key Identifier	발급자 공개키의 DER 값을 SHA-1로 해쉬	Y	F	Y	F
Subject Key Identifier	소유자 공개키의 DER 값을 SHA-1로 해쉬	Y	F	Y	F
Key Usage	키 용도 설정[1)]	Y	T	Y	T
Extended Key Usage	OCSP서버 인증서에서 사용	O	T	O	F
certificate Policies	인증서 정책 및 OID 정책에 따라 설정[2)]	Y	-	M	
Subject Alternative Names	가입자 한글실명과 VID(SHA-256으로 해쉬)[3)]	O	-	M	F
Issuer Alternative Names	-	O	-	O	F
Authoricy Information Access	OCSP서버 위치	O	-	Y	F
Basic Constraints	인증기관여부(cA:Ture), 경로길이 제한	Y	T	-	-
Name Constraints	-	O	T	-	-
Policy Constraints	-	O	T	-	-
CRL Distribution Points	LDAP 서버 위치	Y	-	Y	F
OCSP NoCheck	OCSP서버 인증서에서 사용	O	F	O	F

사용여부	C(Criticality)
Y : 사용함 , - : 사용안함, O : Optional	T : True, F, False

1) 교육부 행정전자서명인증센터에서 발급하는 인증서는 전자서명용과 암호용이 있으며, 인증서 용도는 구분되어 설정된다.

- 전자서명용 : digitalSignature, nonRepudiation 만 설정한다.

• 암호용 : keyEncipherment, dataEncipherment, KeyAgreement 만 설정한다.

2) 인증서 정책 및 OID는 인증업무준칙 및 OID 규격을 참고한다.

3) 소유자의 실명 및 식별번호를 주입하는 방법은 'KCAC.SIVID, 식별번호를 이용한 본인확인 기술규격 v.1.21' 을 준용한다.

4) 특수목적용으로 발급되는 인증서에는 소유자 대체명칭을 포함하지 않는다.

2.2. 인증서폐지목록

인증서 소유자가 단체를 떠나거나 개인키의 신뢰가 손상이 되었을 때 인증서를 폐지할 필요가 있다. 본 표준에서는 X.509 버전2 형식의 인증서폐지목록을 사용한다. 본 표준에 따라 교육부 행정전자서명인증센터는 CRL을 생성하여 지정된 디렉토리에 등록하여 게시한다. 디렉토리 내 게시되는 위치는 인증서 내의 인증서폐지목록 분배점(CRL Distribution Point) 확장필드에 지정한다.

2.2.1. 기본 필드

인증서폐지목록 기본필드는 인증서의 버전, 일련번호, 발급자, 유효기간, 폐지목록 등 인증서폐지목록의 기본 정보를 나타내며, 아래 정의된 기본필드는 인증서폐지목록에 모두 포함되어야 한다. 또한, 인증서를 처리하는 모든 소프트웨어는 아래에 명시된 기본 필드를 모두 처리할 수 있어야 한다.

필드명	설정 정보	비고
Version	V2 (1)	정수값
Signature	SHA256WithRSAEncryption	서명알고리즘 OID 및 파라미터
Issuer		교육부 행정전자서명인증센터 인증서의 소유자 DN
ThisUpdate	CRL 발급일	UTCTime 또는 GeneralizedTime (GMT)
NextUpdate	CRL 다음 발급일	UTCTime 또는 GeneralizedTime (GMT)
RevokedCertificate	폐지된 인증서 목록	폐지된 인증서 일련번호, 폐지시각 포함

2.2.2. 인증서폐지목록 확장 필드

인증서폐지목록 확장 필드는 OID와 ASN.1의 구조를 준수해야 하며, 다음 사항이 필수적으로 지원되어야 한다.

- 발급자 공개키 식별자 (Authority Key Identifier)
- 발급자 대체이름 (Issuer Alternative Name)
- CRL 번호 (CRL Number)
- 발급 CRL 분배점 (Issuing Distribution Point)

본 표준에서 권고하는 인증서폐지목록 확장영역은 다음과 같은 표로 요약할 수 있다.

확장필드	설정 정보	사용여부	중요도 (Criticality)
Authority Key Identifier	발급자 공개키의 DER 값을 SHA1로 해쉬	필수	False
Issuer Alternative Names	발급기관 대체명	선택	False
CRL Number	CRL 번호	필수	False
Issuing Distribution Point	발급된 CRL을 획득할 수 있는 LDAP 정보	선택	True

2.2.3. 인증서폐지목록 엔트리 확장 필드

인증서폐지목록 내에 포함되는 각각의 폐지된 인증서 엔트리에 대한 확장 필드는 OID와 ASN.1의 구조를 준수해야 하며, 다음 사항이 필수적으로 지원되어야 한다.

- 폐지사유 (CRL Reason)

본 표준에서 권고하는 인증서폐지목록 엔트리 확장영역은 다음과 같은 표로 요약할 수 있다.

확장필드	설정 정보	사용여부	중요도 (Criticality)
CRL Reason	인증서 폐지사유 지정	필수	False

3. 알고리즘 규격

본 표준에서 사용되는 암호 알고리즘에 대해 기술한다. 일방향 해쉬알고리즘과 인증서와 인증서 폐지목록을 서명하기 위해 사용될 전자서명 알고리즘, 인증서에 포함될 공개키 암호 알고리즘, 메시지 인증을 위한 알고리즘, 그리고 데이터 암호화를 위한 비밀키 암호 알고리즘의 표준규격을 제시한다.

3.1. 해쉬 알고리즘

본 표준에서는 SHA-256의 사용을 권장한다. 해쉬알고리즘은 다음에 나열한 표준을 준수하여야 한다.

- SHA-256 : FIPS 180-2 Secure Hash Standard

3.2. 전자서명 알고리즘

인증서 또는 인증서폐지목록을 서명하는 데 사용되는 전자서명 알고리즘은 알고리즘 식별자(Algorithm Identifier)를 통해 표시된다. 알고리즘 식별자는 객체식별자(OID: Object Identifier)와 이에 대응되는 파라미터 인자로 구성된다.

본 규격에서는 전자서명 알고리즘으로 KCDSA를 권고한다. 사용되는 전자서명 알고리즘은 다음의 표준을 준수하여야 한다.

- RSA : PKCS #1 v2.2 RSA Encryption Standard
- KCDSA : TTAS.KO-12.0001/R4, 부가형 전자서명방식표준(KCDSA)

3.3. 가입자 공개키 알고리즘(Subject Public Key Algorithm)

인증서에 포함되는 가입자의 공개키 알고리즘은 알고리즘 식별자(Algorithm Identifier)를 통해 표시된다. 알고리즘 식별자는 객체식별자(OID: Object Identifier)와 이에 대응되는 파라미터 인자로 구성된다.

본 규격에서 사용되는 공개키 알고리즘은 다음의 표준을 준수하여야 한다.

- RSA : PKCS #1 v2.2 RSA Encryption Standard
- KCDSA : TTAS.KO-12.0001/R4, 부가형 전자서명방식표준(KCDSA)

3.4. 비밀키 암호 알고리즘

대칭키 암호 알고리즘 또는 관용키 암호 알고리즘이라고도 하며, 데이터의 암호화를 위하여 사용된다. 본 표준을 따르는 경우, 128비트 이상의 키길이를 가지면서 안전성이 널리 인정된 암호 알고리즘을 사용하여야 한다. 또한, 국가·공공기관 표준 블록암호인 ARIA에 대하여 지원할 수 있어야 한다.

- ARIA : KS X 1213-1, 128비트 블록 암호 알고리즘

4. 인증서 관리 규격

사용자와 인증기관(CA : Certification Authority)간에 온라인 상호동작을 지원하기 위해 관리 프로토콜이 필요하다. 관리 프로토콜은 인증기관과 키 쌍과 연관된 사용자 시스템 간에 사용될 수 있고, 또한 상호 인증하려는 두 인증기관 간에 사용될 수 있다. 관리 프로토콜은 사용자 시스템의 등록 정보를 전달하거나 인증서 폐지 요청을 전달하기 위해 사용될 수 있다.

4.1. 인증서 관리 프로토콜(CMP)

인증서 관리 프로토콜인 CMP(Certificate Management Protocols)는 인증서 발급/갱신/폐지 요청 및 응답 처리에 사용된다. 인증서 관리 프로토콜은 PKI 구성요소 간의 온라인 상호연동 뿐만 아니라, 상호인증 하려는 두 인증기관 사이에서도 사용될 수 있다. 본 표준에서는 유선구간에서는 RFC6712 을 준용하여 인증서 관리를 수행하며, 인증서를 신청하기 위해서 인증기관에게 보낼 메시지는 RFC4211에 명시된 메시지 형태를 활용한다.

CMP는 다음에 나열한 표준을 준수하여야 한다.

- RFC6712 : Internet X.509 Public Key Infrastructure
- RFC4211 : Certificate Request Message Format

4.2. 인증서 요청형식 프로토콜

인증서 요청은 온라인으로 CMP를 통하여 인증서버에 요청이 가능하다.

온라인 요청형식은 인증서 요청정보와 개인키 소유여부 검증정보 및 추가 등록 정보로 구성되며, 온라인 요청형식의 구성은 RFC6712을 준수하여야 한다.

- RFC6712 : Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol(CMP)

4.3. 보안 메시지 규격

인증서를 이용하여 생성되는 보안 메시지의 형식 및 메시지 구문은 다음에 나열한 표준을 준수하여야 한다.

- PKCS#7 V1.5 : Cryptographic Message Syntax Standard

인증서 기반의 전자서명 데이터는 SignedData 구조를 사용하며, 인증서를 이용한 암호화 데이터는 EnvelopedData의 형식을 사용한다.

• SignedData

필 드		내 용
version		버전정보
digestAlgorithms		데이터 해쉬에 사용된 알고리즘 ID
contentInfo	contentType	서명대상 원본 데이터 유형
	content	서명대상 원본 데이터 내용
certificates (optional)		서명에 사용한 인증서
crls (optional)		(사용하지 않음)
signerInfo	version	버전정보
	IssuerAndSerialNumber	서명에 사용된 인증서의 발급자 DN 서명에 사용된 인증서의 일련번호
	digestAlgorithm	데이터 해쉬에 사용된 알고리즘 ID
	authenticatedAttributes (optional) [1]	시간정보 등 포함
	digestEncryptionAlgorithm	데이터 서명에 사용된 알고리즘 ID
	encryptedDigest	전자서명된 결과값
	unauthenticatedAttributes (optional)	(사용하지 않음)

1) authenticatedAttributes 필드에 포함되어야 하는 attribute 들은 다음과 같다.
- Content Type : contentInfo 내 contentType 값
- Message Digest : contentInfo 내 content를 해쉬한 값
- Signing Time : 전자서명 수행 시각

• EnvelopedData

필 드		내 용
version		버전정보
recipientInfos	version	버전정보
	IssuerAndSerialNumber	수신자 인증서의 발급자 정보 수신자 인증서의 일련번호
	keyEncryptionAlgorithmID	대칭키 암호화를 위한 공개키 암호알고리즘 ID
	encryptedKey	공개키로 암호화된 대칭키
encrypted Contentinfo	contentType	암호화되는 content 유형
	contentEncrpytionAlgorithm	content 암호화에 사용한 대칭키 암호알고리즘 ID
	encryptedContent	content의 암호화 결과

4.4. 개인키 저장 방식

가입자의 인증서에 대응되는 개인키를 안전하게 저장하기 위해서는 다음의 기술규격을 준용한다.

- 개인키 암호화 방식 : PKCS#5 v2.1 Password-Based Encryption Standard
- 개인키 암호화 메시지 구조 : PKCS#8 v1.2 Private-Key Information Syntax Standard

구 분		적용 알고리즘 및 표준
키 쌍 생성	전자서명용	KCDSA (2048bit)
	암호화용	RSA (2048bit)
개인키 저장	암호화	ARIA
	암호화 방식	PKCS#5
	저장형식	PKCS#8

5. 인증서 유효성 검증 프로토콜 규격

5.1. 인증서 경로검증 기술 규격

인증서 경로검증은 인증서 유효성을 확인하는 기본 절차이며, 이에 대하여 다음의 기술규격을 기반으로 한다.

- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

인증서 경로검증 절차 구현 시, 기술되는 알고리즘을 구현해야 하는 것은 아니지만, 주어진 인증서에 대하여 같은 결과가 나오도록 기능상 동일해야 한다.

5.2. LDAP 프로토콜

사용자 및 인증서를 검증하는 서버가, 특정 인증서의 유효성을 검증하기 위하여 디렉토리 시스템을 이용하는 경우, LDAP 프로토콜을 준용한다.

교육부 행정전자서명인증센터에서는 인증서 및 인증서폐지목록을 디렉토리 시스템에 저장한다.

본 표준에서는 인증서와 인증서폐지목록 배포 방식으로 LDAP 버전3을 준용하며 관련 표준으로는 다음과 같다.

- RFC2251 Lightweight Directory Access Protocol (v3)

5.3. 실시간 인증서 유효성 상태 검증(OCSP)

OCSP는 인증서의 유효성을 실시간으로 판단하기 위해 인증서의 폐지 여부를 요청 및 확인할 수 있게 하여 인증서 폐지 정보 및 부가적인 상태 정보를 획득할 수 있도록 하는 서비스이며, 다음의 표준을 준용하여야 한다.

- KCAC.TS.OCSP, "실시간 인증서 상태확인 기술규격 (v1.21)"
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

OCSP 서버는 적법한 클라이언트가 원하는 인증서의 상태를 조회할 수 있도록 하며, 다음의 조건을 만족해야 한다.

- 인증서 상태 조회를 위한 요청 메시지와 응답메시지 전송을 위한 프로토콜은 HTTP(POST,GET)를 사용해야 한다.

- 클라이언트가 OCSP 서버 인증서를 획득하기 위하여 응답 메시지에 OCSP 서버의 인증서를 포함하여 보내야 한다.
- OCSP 요청 및 응답은 재연 공격에 대처할 수 있도록 requestExtensions 및 responseExtensions에 Nonce를 반드시 사용해야 한다.
- 사용자가 요청한 인증서의 상태 조회 결과가 폐기인 경우 이용자가 인증서의 폐지 사유를 명확히 알 수 있도록 응답 메시지의 revocationReason 필드를 반드시 사용해야 한다.

5.3.1. 인증서 유효성 상태 검증 프로세스

■ 인증서 상태 검증 요청

OCSP 사용자는 상태 검증을 하고자 하는 인증서에 대한 상태 정보 요청문(request)를 생성하여 OCSP 서버에게 보내고 응답문(response)이 올 때까지 주어진 인증서에 대한 수용 여부를 미루어둔다. 요청 메시지에는 상태 검증을 요청할 인증서의 일련번호, 인증서 발급자 DN, 인증서 발급자 공개키에 대한 해쉬값 등을 포함한다.

- protocol version
- service request
- target certificate identifier
- optional extensions

■ 인증서 상태 검증 응답

인증서 상태 검증 요청을 받은 OCSP 서버는 요청 메시지를 보낸 사용자가 요청을 하도록 허가 받은 사용자인지를 확인한다. 만약 허가 받지 않은 사용자가 요청을 했다면 에러 메시지를 보낸다.

요청자의 허가 여부는 사용자의 요청 메시지의 버전이 올바른지, 난수 값이 명시되어있는지를 확인한 후, 서명이 되어 있는지 판단하고, 서명 검증을 실시한다.

다음으로 검증 요청을 받은 인증서가 폐지된 것인지 판단한 후, 다음과 같은 응답 메시지를 구성하여 사용자에게 보낸다.

- version of the response syntax
- name of the responder
- responses for each of the certificates in a request

- optional extensions
- signature algorithm OID
- signature computed across hash of the response

인증서 상태 유형	내용
good(1)	상태 검증 요청된 인증서가 유효함
revoked(2)	상태 검증 요청된 인증서가 폐지 또는 유효기간이 초과되었음
unknown(3)	상태 검증 요청된 인증서에 대한 어떠한 정보도 알 수 없음

■ 인증서 상태 검증 응답 검증

사용자는 OCSP 서버로부터 받은 응답 메시지를 확인한다. 이는 응답에 서명한 서버가 허가 받은 상태인지를 확인한다.

응답자의 허가 여부는 받은 응답이 사용자가 요청했던 서버로부터의 응답인지를 버전과 난수로 확인을 하고, 응답에 포함된 서명이 올바른지를 확인한다. 다음으로 응답서버의 인증서가 폐지 된 것인지 판단함으로써 이루어진다. 단 응답서버의 인증서 내에 id-pkix-ocsp-nocheck가 정의된 경우 응답 서버의 폐지 여부는 체크하지 않아야 한다.

5.3.2. 인증서 유효성 상태 검증 데이터 구조

5.3.2.1. 요청 메시지

RequestList에는 상태 검증을 요청할 인증서에 대한 정보가 포함되며, 복수 개의 인증서의 상태 검증 요청이 가능하다. 요청 메시지에 서명을 할 경우에는 requestor Name에 요청자의 DN값을 명시해야 한다.

optionalSignature의 certs에는 요청자의 인증서 외에 요청자의 서명 검증에 필요한 인증서들이 포함되어야 한다. service locator는 요청 메시지를 받을 OCSP 서버에 대한 정보이다.

<table>
<tr><th colspan="5">필 드</th><th>내 용</th></tr>
<tr><td rowspan="7">tbsRequest</td><td colspan="4">Version</td><td>V1 (0)</td></tr>
<tr><td colspan="4">requestorName(optional)</td><td>요청자의 DN</td></tr>
<tr><td rowspan="4">requestList</td><td rowspan="4">reqCert</td><td rowspan="4">certID</td><td>hash Algorithm</td><td>해쉬 알고리즘 ID, 대상 인증서 발급자 DN과 공개키 해쉬에 대한 알고리즘 정의 (현재 SHA256 방식을 사용)</td></tr>
<tr><td>issuerNameHash</td><td>발급자 DN의 해쉬값</td></tr>
<tr><td>issuerKeyHash</td><td>발급자 공개키의 tag와 length를 제외한 해쉬값</td></tr>
<tr><td>serialNumber</td><td>검증 대상 인증서의 일련번호</td></tr>
<tr><td colspan="4">singleRequestExtensions</td><td>Service locator (검증대상 인증서의 AIA값)</td></tr>
<tr><td colspan="4">request Extensions (optional)</td><td>난수, 수용 가능한 응답 형식 (현재 수용 가능한 응답 oid : id_pkix_ocsp_basic)</td></tr>
<tr><td rowspan="3">optionalSig</td><td colspan="4">signataure Algorithm</td><td>서명 알고리즘 ID</td></tr>
<tr><td colspan="4">Signature</td><td>tbsRequest의 DER 인코딩한 값에 대한 서명값</td></tr>
<tr><td colspan="4">Certs</td><td>요청자의 인증서</td></tr>
</table>

5.3.2.2. 응답 데이터 구조

responseStatus 값이 successful(0)이라면 responseBytes 값을 포함한다. 그렇지 않다면 responseBytes을 포함하지 않는 다음과 같은 에러 응답을 보낸다.

- malformedRequest (1) : 요청 메시지 형식이 맞지 않는 경우
- internalError(2) : OCSP서버 내부 에러가 발생한 경우
- tryLater(3) : OCSP 서버가 작동은 하고 있으나, 잠시 서비스를 할 수 없는 경우
- sigRequired(5) : 요청 메시지에 요청자의 서명이 포함되어야 하는 경우
- unauthorized(6) : 허가받지 않은 사용자에게서 요청이 온 경우

responses에는 검증 요청을 받은 인증서에 대한 상태 정보가 포함되며, 복수 개의 인증서에 대한 상태 검증 응답이 가능하다.

optional Signature의 certs에는 응답자 인증서 외에 응답자 서명 검증에 필요한 인증서들이 포함되어야 한다.

<table>
<tr><th colspan="5">필 드</th><th>내 용</th></tr>
<tr><td colspan="5">responseStatus</td><td>0: ResponseBytes 포함 (good,revoked)
1-6: ResponseBytes 없음</td></tr>
<tr><td rowspan="13">responseBytes(optional)</td><td rowspan="11">basicOCSPResponse</td><td colspan="3">responseType(optional)</td><td>수용 가능한 응답 형식 (현재 수용 가능한 응답 : value : id_pkix_ocsp_basic)</td></tr>
<tr><td rowspan="10">tbsResponseData</td><td colspan="2">Version</td><td>V1</td></tr>
<tr><td colspan="2">responderID</td><td>응답자 공개키의 해쉬값</td></tr>
<tr><td colspan="2">productAt</td><td>응답에 서명한 시간</td></tr>
<tr><td rowspan="6">response</td><td rowspan="4">certID</td><td>hash Algorithm</td><td>해쉬 알고리즘 ID (요청문과 동일. SHA1)발급자</td></tr>
<tr><td>issuerNameHash</td><td>발급자 DN의 해쉬값</td></tr>
<tr><td>issuerKeyHash</td><td>발급자 공개키의 해쉬값</td></tr>
<tr><td>serialNumber</td><td>검증 대상 인증서의 일련번호</td></tr>
<tr><td colspan="2">certStatus</td><td>good/revoked/unknown</td></tr>
<tr><td colspan="2">thisUpdate</td><td>서버의 현재 시간(사용하지 않음)</td></tr>
<tr><td colspan="2">nextUpdate(optional)</td><td>사용하지 않음</td></tr>
<tr><td colspan="2">singleExtensions(optional)</td><td>사용하지 않음</td></tr>
<tr><td colspan="3">responseExtensions(optional)</td><td>난수(요청자가 보낸 값을 그대로 전송)</td></tr>
<tr><td rowspan="3">optionalSignature(optional)</td><td colspan="3">signature Algorithm</td><td>서명 알고리즘 ID</td></tr>
<tr><td colspan="3">signature</td><td>tbsResponseData의 DER인코딩한 값에 대한 서명값</td></tr>
<tr><td colspan="3">Certs</td><td>응답자의 인증서</td></tr>
</table>

5.4. HTTP 프로토콜(HTTP's CRL)

사용자 및 인증서를 검증하는 서버가, 특정 인증서의 유효성을 검증하기 위하여 웹브라우저를 이용하는 경우, HTTP 프로토콜을 통해 준용한다.

교육부 행정전자서명인증센터에서는 디렉토리 시스템에 저장된 인증서폐지목록을 웹브라우저를 통해 제공한다.

본 표준에서는 인증서폐지목록 배포 방식의 관련표준은 다음과 같다.

- RFC1945 : Hypertext Transfer Protocol - HTTP/1.0
- RFC2616 : Hypertext Transfer Protocol - HTTP/1.1

5.5. 서버기반 인증서 검증 프로토콜(SCVP)

SCVP는 클라이언트를 대신하여 서버가 인증 경로의 설정과 인증 경로를 검증하는 서비스이며, 다음의 표준을 준용하여야 한다.

- RFC 5055 Server-Based Certificate Validation Protocol - SCVP

SCVP 서버는 적법한 클라이언트가 원하는 인증서의 경로 설정 및 경로 검증을 할 수 있도록 하며, 다음의 조건을 만족해야 한다.

- 인증서 검증을 위한 요청 메시지와 응답메시지 전송을 위한 프로토콜은 HTTP를 사용해야 한다.
- SCVP 요청 및 응답은 PKCS#7의 SignedData 포맷에 따라 생성 처리되어야 한다.
- SCVP 요청 및 응답은 재연 공격에 대처할 수 있도록 requestNonce를 지원해야 한다.
- SCVP 서버는 요청에 대한 상태 코드 응답을 보내야 한다.

5.5.1. 서버기반 인증서 검증 프로세스

■ 인증서 검증 요청

SCVP 사용자는 검증을 하고자 하는 인증서에 대한 정보 요청문(CVRequest)를 생성하여 SCVP 서버에게 보내고 응답문(CVResponse)이 올 때까지 주어진 인증서에 대한 수용 여부를 미루어둔다. 요청 메시지에는 아래의 값 등을 포함한다.

- cvRequest version
- SCVP query
- requestorRef
- requestNonce
- requestorName
- responderName
- requestExtensions
- signatureAlg
- hashAlg
- requestorText

■ 인증서 검증 응답

인증서 검증 요청을 받은 SCVP 서버는 요청 메시지를 보낸 사용자가 요청을 하도록 허가 받은 사용자인지를 확인한다. 만약 허가 받지 않은 사용자가 요청을 했다면 에러 메시지를 보낸다.

요청자의 허가 여부는 서명이 되어 있는지 판단하고, 서명 검증을 실시한다.

다음으로 정의된 검증 정책 또는 사용자로 부터 요청된 검증 정책을 사용하여 인증서 검증을 수행 후, 다음과 같은 응답 메시지를 구성하여 사용자에게 보낸다.

- cvResponseVersion
- serverConfigurationID
- producedAt
- responseStatus
- respValidationPolicy
- requestRef
- requestorRef
- requestorName
- replyObjects
- respNonce
- serverContextInfo
- cvResponseExtensions
- requestorText

응답 상태 유형		내용
Success	okay(0)	The request was fully processed.
	skipUnrecognizedItems(1)	The request included some unrecognized non-critical extensions; however, processing was able to continue ignoring them.
Error	tooBusy(10)	Too busy; try again later.
	invalidRequest(11)	The server was able to decode the request, but there was some other problem with the request.
	internalError(12)	An internal server error occurred.
	badStructure(20)	The structure of the request was wrong.
	unsupportedVersion(21)	The version of request is not supported by this server
	abortUnrecognizedItems(22)	The request included unrecognized items, and the server was not able to continue processing.
	unrecognizedSigKey(23)	The server could not validate the key used to protect the request.
	badSignatureOrMAC(24)	The signature or message authentication code did not match the body of the request.
	unableToDecode(25)	The encoding was not understood.
	notAuthorized(26)	The request was not authorized.
	unsupportedChecks(27)	The request included unsupported checks items, and the server was not able to continue processing.
	unsupportedWantBacks(28)	The request included unsupported wantBack items, and the server was not able to continue processing.
	unsupportedSignatureOrMAC(29)	The server does not support the signature or message authentication code algorithm used by the client to protect the request.
	invalidSignatureOrMAC(30)	The server could not validate the client's signature or message authentication code on the request.
	protectedResponseUnsupported(31)	The sever could not generate a protected response as requested by the client.
	unrecognizedResponderName(32)	The server does not have a certificate matching the requested responder name.
	relayingLoop(40)	The request was previously relayed by the same server.
	unrecognizedValPol(50)	The request contained an unrecognized validation policy reference.
	unrecognizedValAlg(51)	The request contained an unrecognized validation algorithm OID.
	fullRequestInResponseUnsupported(52)	The server does not support returning the full request in the response.
	fullPolResponseUnsupported(53)	The server does not support returning the full validation policy by value in the response.
	inhibitPolicyMappingUnsupported(54)	The server does not support the requested value for inhibit policy mapping.
	requireExplicitPolicyUnsupported(55)	The server does not support the requested value for require explicit policy.

응답 상태 유형		내용
Error	inhibitAnyPolicyUnsupported(56)	The server does not support the requested value for inhibit anyPolicy.
	validationTimeUnsupported(57)	The server only validates requests using current time.
	unrecognizedCritQueryExt(63)	The query item in the request contains a critical extension whose OID is not recognized.
	unrecognizedCritRequestExt(64)	The request contains a critical request extension whose OID is not recognized.

5.5.2. 인증서 검증 데이터 구조

5.5.2.1. 요청 메시지

서버에 대한 SCVP 클라이언트 요청은 단일 CVRequest 항목이어야 한다.

서버는 모든 요구가 보호되도록 요구할 수 있으며, 서버는 모든 보호되지 않은 요청을 폐기할 수 있습니다. 보호된 요청은 SignedData로 캡슐화 된 CVRequest로 구성됩니다.

필 드			내 용
CVRequest	cvRequestVersion		SCVP CVRequest 버전
	query	queriedCerts	검증 요청 인증서
		checks	사용자 검증 지정
		wantBack	응답 오브젝트 지정
		validationPolicy	유효성 검증 정책
		responseFlags	응답에 대한 선택적 기능 요청
		serverContextInfo	이전 서버 응답에 대한 추가 정보 필요
		validationTime	검증 시간
		intermediateCerts	사용자 요청에 대한 컨텍스트
		revInfos	사용자 요청에 대한 컨텍스트
		producedAt	캐시된 SCVP 응답 사용 허용 여부
		queryExtensions	요청 확장
	requestorRef		SCVP 서버 식별 이름
	requestNonce		사용자에 의해 생성 된 요청 식별자
	requestorName		
	responderName		
	requestExtensions		
	signatureAlg		서명 알고리즘
	hashAlg		해쉬 알고리즘
	requestorText		

5.5.2.2. 응답 데이터 구조

클라이언트에 대한 SCVP 서버 응답은 단일 CVResponse 항목이어야 한다.

응답 데이터는 SignedData로 캡슐화 된 CVResponse 구성이며, SCVP 서버는 자체 인증서를 SignedData 내 인증서 필드에 포함하여야 하며(MUST) 다른 인증서도 포함될 수 있다(MAY).

필 드				내 용
CVResponse	cvResponseVersion			SCVP CVResponse 버전
	serverConfigurationID			SCVP 서버 구성 버전
	producedAt			SCVP 응답 생성 시간
	responseStatus			요청에 대한 상태 정보
	respValidationPolicy			유효성 검증 정책에 대한 참조 또는 전체 정책
	requestRef	requestHash		CVRequest 해시
		fullRequest		CVRequest
	requestorRef			SCVP 중계가 사용되는 경우 원래 요청자를 식별하는데 사용
	requestorName			응답에서 사용자와 관련된 하나 이상의 ID를 반환하는데 사용
	replyObjects	CertReference		사용자가 정보를 요청한 인증서 또는 인증서에 대한 참조
		replyStatus		인증서 요청에 대한 상태 정보
		replyValTime		검사 수행 시간
		replyChecks	OID	객체 식별자
			INTEGER	검사 성공 여부
		replyWantBacks		wantBack 항목에 대한 응답
		validationErrors		실패 응답시 실패 이유(OID)
		nextUpdate		서버의 인증서 유효성에 대한 정보 업데이트 예상 시간
		certReplyExtensions		queryExtensions 항목에 대한 응답
	respNonce			요청 구분 식별자
	serverContextInfo			
	cvResponseExtensions			응답 확장
	requestorText			

5.6. 본인확인 프로세스

본인확인은 식별번호 인증서를 이용한 본인확인 기능과 본인확인 클라이언트 데몬을 이용하여 본인확인 서버를 이용하는 방법이 있다.

본 표준에서는 식별번호 인증서를 이용한 본인확인 방법을 준용하며, 다음 표준문서를 준수하여야 한다.

- KCAC.TS.SIVID 식별번호를 이용한 본인확인 기술 규격 v1.21

6. OID 및 DN 체계

6.1. OID 체계

교육부 행정전자서명인증센터에서 사용하는 OID(Object Identifier)는 행정전자서명인증관리센터에서 정의한 OID 체계를 준용한다.

행정전자서명인증관리센터 OID Table에서 명시하지 않은 OID는 다음 표준을 준용한다.

- KCAC.TG.OID, “전자서명인증체계 OID 가이드라인”
- RFC 5794, “A Description of the ARIA Encryption Algorithm"

6.1.1. OID의 체계

- 한국(Korea) : {1(iso) 2(member-body) 410(Korea)}로 정의
  - arc 410은 ISO에서 국내 Member body에 할당
  - 410 이하의 arc는 국내에서 할당
- 행정전자서명인증관리센터 (GCMA) : {1.2.410.100001(GCMA)}로 정의
  - arc 100001은 국내에서 할당
  - 100001 이하의 arc는 행정전자서명인증관리센터에서 할당
- 알고리즘 OID (Gpki-alg) : {1.2.410.100001.1(Gpki-alg)}로 정의
  - arc 1 이하는 행정전자서명인증관리센터 알고리즘 OID로 할당
- 인증서 정책 OID (Gpki-cp) : {1.2.410.100001.2(Gpki-cp)}로 정의
  - arc 2 이하는 행정전자서명인증관리센터 인증서 정책 OID로 할당
- 키용도 OID (Gpki-kp) : {1.2.410.100001.3(Gpki-kp)}로 정의
  - arc 3 이하는 행정전자서명인증관리센터 키용도 OID로 할당
- 인증서 속성 OID (Gpki-at) : {1.2.410.100001.4(Gpki-at)}로 정의
  - arc 4 이하는 행정전자서명인증관리센터 인증서 속성 OID로 할당
- 행정전자서명 인증기관 OID (Gpki-lca) : {1.2.410.100001.5(Gpki-lca)}로 정의
  - arc 5 이하는 행정전자서명인증관리센터 정부인증기관 OID로 할당
- 교육부 인증기관 OID (CA-MOE) : {1.2.410.100001.5.3(CA-MOE)}로 정의
  - arc 3 이하는 교육부 인증기관 OID로 할당
  - 3 이하의 arc는 행정전자서명인증관리센터와 협의하여 교육부가 할당

6.1.2. 행정전자서명인증관리센터 OID TABLE

OID								명칭	설명
1								ISO	
1	2							member-body	
1	2	410						korea	대한민국
1	2	410	100001					gcma	행정전자서명인증관리센터
1	2	410	100001	1				gpki-alg	인증관리센터 알고리즘
1	2	410	100001	1	1			neat	국가용 암호 알고리즘
1	2	410	100001	1	2			neatECB	neat 알고리즘 - ECB모드
1	2	410	100001	1	3			neatCBC	neat 알고리즘 - CBC모드
1	2	410	100001	1	4			neatOFB	neat 알고리즘 - OFB모드
1	2	410	100001	1	5			neatCFB	neat 알고리즘 - CFB모드
1	2	410	100001	1	6			neatMAC	neat 알고리즘 - MAC
1	2	410	100001	1	7			pbeWithSHA1AndNEAT_CBC	패스워드기반 neat - CBC모드
1	2	410	100001	1	8			pbeWithHAS160AndNEAT_CBC	패스워드기반 neat - CBC모드
1	2	410	100001	1	9			Reserved	
1	2	410	100001	1	10			Reserved	
1	2	410	100001	1	11			Reserved	
1	2	410	100001	1	12			Reserved	
1	2	410	100001	1	13			Reserved	
1	2	410	100001	1	14			Reserved	
1	2	410	100001	1	15			Reserved	
1	2	410	100001	1	16			Reserved	
1	2	410	100001	1	17			Reserved	
1	2	410	100001	1	18			ARIA	ARIA128
1	2	410	100001	1	19			ARIA_ECB	ARIA128 - ECB모드
1	2	410	100001	1	20			ARIA_CBC	ARIA128 - CBC모드
1	2	410	100001	1	21			ARIA_OFB	ARIA128 - OFB모드
1	2	410	100001	1	22			ARIA_CFB	ARIA128 - CFB모드
1	2	410	100001	1	23			ARIA_MAC	ARIA128 - MAC
1	2	410	100001	1	24			pbewithSHA1andARIA_CBC	패스워드기반 ARIA128 - CBC모드
1	2	410	100001	1	25			pbewithSHA256andARIA_CBC	패스워드기반 ARIA128 - CBC모드
1	2	410	100001	1	26			pbewithHAS160andARIA_CBC	패스워드기반 ARIA128 - CBC모드
1	2	410	100001	2				gpki-cp	GPKI 인증정책
1	2	410	100001	2	1			Class 1	기관용
1	2	410	100001	2	1	1		department	전자관인(기관용)
1	2	410	100001	2	1	2		computer	서버용(컴퓨터용)
1	2	410	100001	2	1	3		special	특수목적용(업무용)
1	2	410	100001	2	1	4		public_department	공공/민간 전자관인
1	2	410	100001	2	1	5		public_computer	공공/민간 컴퓨터용
1	2	410	100001	2	1	6		public_special	공공/민간 특수목적용

OID								명칭	설명
1	2	410	100001	2	2			Class 2	개인용
1	2	410	100001	2	2	1		personal	공무원 전자서명
1	2	410	100001	2	2	2		public_personal	공공/민간 개인용 전자서명
1	2	410	100001	3				gpki-kp	키용도
1	2	410	100001	3	1			signature	서명용
1	2	410	100001	3	2			encryption	암호용
1	2	410	100001	4				gpki-at	인증서속성
1	2	410	100001	4	1			gpki-identifyData	인증서 소유자의 부가 대체명칭
1	2	410	100001	4	1	1		vid	virtual ID
1	2	410	100001	4	1	2		encryptedVID	encrypted virtual ID
1	2	410	100001	4	1	3		randomNum	random number
1	2	410	100001	5				gpki-gov-ca	행정전자서명인증관리센터
1	2	410	100001	5	1			CA-CWD	CA-대통령비서실 * 사용중지
1	2	410	100001	5	1	1		CA-CWD-CP	CA-대통령비서실 인증서정책 * 사용중지
1	2	410	100001	5	2			CA-NIS	CA-국가정보원 * 사용중지
1	2	410	100001	5	2	1		CA-NIS-CP	CA-국가정보원 인증서정책 * 사용중지
1	2	410	100001	5	3			CA-MOE	CA-교육부
1	2	410	100001	5	3	1		CA-MOE-CP	CA-교육부 인증서정책
1	2	410	100001	5	3	1	1	MOE-department	전자관인
1	2	410	100001	5	3	1	3	MOE-personal	개인용
1	2	410	100001	5	3	1	5	MOE-special	특수목적용
1	2	410	100001	5	3	1	7	MOE-computer	컴퓨터용
1	2	410	100001	5	3	1	9	MOE-SSL	SSL용
1	2	410	100001	5	4			CA-MND	CA-국방부 * 사용중지
1	2	410	100001	5	4	1		CA-MND-CP	CA-국방부 인증서정책 * 사용중지
1	2	410	100001	5	5			CA-SPPO	CA-대검찰청
1	2	410	100001	5	5	1		CA-SPPO-CP	CA-대검찰청 인증서정책
1	2	410	100001	5	6			CA-MMA	CA-병무청
1	2	410	100001	5	6	1		CA-MMA-CP	CA-병무청 인증서정책
1	2	410	100001	5	7			CA-MOGAHA	CA-행정안전부
1	2	410	100001	5	7	1		CA-MOGAHA-CP	CA-행정안전부 인증서정책
1	2	410	100001	5	8			CA-SCOURT	CA-법원
1	2	410	100001	5	8	1		CA-SCOURT-CP	CA-법원 인증서정책
1	2	410	100001	6				Gpki-Int	상호연동 * 사용중지 (NPKI 대체)
1	2	410	100001	6	1			CTL	인증서신뢰목록방식 * 사용중지 (NPKI 대체)
1	2	410	100001	6	1	1		Npki-ctl	민간공인인증기관간상호연동 * 사용중지 (NPKI 대체)

6.2. DN 체계

사용자가 유일한 인증서를 소유하는 것을 식별하기 위해 표준화된 DN(Distinguished Name) 체계를 정의하여 사용한다. 인증기관, 등록기관, 가입기관의 DN 체계를 ITU-T X.500에서 정의하는 표준을 따르며 관련 표준은 다음과 같다.

- ITU-T Recommendation X.520 & ISO/IEC 9594-6 - Information Technology Open Systems Interconnection The directory: Selected attribute types
- IETF RFC2256 - A Summary of the X.500 User Schema for use with LDAPv3
- IETF RFC2253 Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
- PKCS#9 : Selected Attribute Types

6.2.1. 인증서 DN 규격

인증서 DN을 위한 규격은 행정전자서명인증관리체계에서 정의하고 있는 내용을 기반으로 한다.

6.2.2. 인증정책별 DN 구조

교육부 행정전자서명인증센터에서 자체적으로 발급하는 인증서에 대해서는 다음의 규칙을 따른다.

구 분		인증서 식별명칭(DN) 규칙
개인용	개인사용자	cn=기관구분자[1](3)+이름[2]+일련번호[3](3),ou=people,ou=최상위기관명,o=Government of Korea,c=KR 예)cn=850홍길동001,ou=people,ou=교육부,o=Government of Korea,c=KR 예)cn=851홍길동001,ou=people,ou=서울특별시교육청,o=Government of Korea,c=KR 예)cn=867홍길동001,ou=people,ou=대학,o=Government of Korea,c=KR
기관용	전자관인 (기관용)	ou=최하위기관명,ou=상위기관명,ou=최상위기관명,o=Government of Korea,c=KR 예)ou=지식정보기반과,ou=정보화정책관,ou=평생직업교육국,ou=교육부,o=Government of Korea,c=KR 예)ou=덕소고등학교,ou=경기도교육청,o=Government of Korea,c=KR 예)ou=서울대학교,ou=대학,o=Government of Korea,c=KR
	서버용 (컴퓨터용)	cn=SVR+기관코드[4](7)+일련번호[5](3),ou=교육부,ou=Group of Server,o=Government of Korea,c=KR 예)cn=SVR1341000001,ou=교육부,ou=Group of Server, o=Government of Korea,c=KR
	SSL용	cn=웹서버 도메인명, ou=발급요청기관부서명,o=발급요청기관명,l=지역정보,s=구역정보,c=KR 예)cn=www.epki.go.kr, ou=Personal Information Policy Section,o=KERIS,l=Dong-gu,s=Daegu,c=KR
	특수목적용 (업무용)	cn=업무정책ID,ou=최상위기관명,o=Government of Korea,c=KR 예)cn=1341049(행정업무),ou=교육부,o=Government of Korea,c=KR 예)cn=9010275(대학입학),ou=경상남도교육청,o=Government of Korea,c=KR 예)cn=7006431(대학입학),ou=대학,o=Government of Korea,c=KR
RA/ LRA	RA	cn=RA+기관코드(7)+기관명+일련번호(3),ou=교육부, o=Government of Korea,c=KR 예)cn=RA7010000서울특별시교육청,ou=교육부,o=government of Korea,c=KR
	LRA	cn=LRA+기관코드(7)+기관명+일련번호(3),ou=상위기관명,ou=교육부,o=Government of Korea,c=KR 예)cn=LRA7060000서울특별시중부교육청,ou=서울특별시교육청,ou=교육부,o=government of Korea,c=KR

1) 기관구분자 : 교육부 행정전자서명인증센터에서 기관식별을 위하여 부여한 3자리 구분정보

2) 이름 : 개인용 인증서를 발급받는 개인의 실명

3) 일련번호 : 동일한 식별명칭의 생성을 방지하기 위하여 부여되는 3자리 양의 정수

4) 기관코드 : 행정안전부에서 부여한 행정표준기관코드로 각 기관의 고유한 7자리 코드

5) 기관명 : 인증서를 요청하는 기관명으로, 행정안전부에서 부여한 행정표준기관코드에 대응되는 명칭

6.2.3. 개인용 인증서의 기관구분자(CN)

개인사용자에게 발급되는 개인용 인증서의 CN은 기관구분자(3자리) + 이름 + 일련번호(3자리)로 구성한다.

기관구분자는 행정전자서명인증관리센터에서 정의한 내용을 준용한다.

교육부에서 자체적으로 개인사용자에게 개인용 인증서를 발급하는 경우는, 행정안전부가 발급하는 경우와 구분하며, 기관구분자를 별도로 정의하여 사용한다.

교육부에서 개인용 인증서 발급 시 사용하는 기관구분자는 다음과 같다.

행정안전부[1]		교육부	
기관구분자	설명	기관구분자	설명
133	교육부	850	교육부(자체발급)
801	서울특별시교육청	851	서울특별시교육청(자체발급)
802	부산광역시교육청	852	부산광역시교육청(자체발급)
803	대구광역시교육청	853	대구광역시교육청(자체발급)
804	인천광역시교육청	854	인천광역시교육청(자체발급)
805	광주광역시교육청	855	광주광역시교육청(자체발급)
806	대전광역시교육청	856	대전광역시교육청(자체발급)
807	울산광역시교육청	857	울산광역시교육청(자체발급)
822	세종특별자치시교육청	872	세종특별자치시교육청(자체발급)
808	경기도교육청	858	경기도교육청(자체발급)
809	강원도교육청	859	강원도교육청(자체발급)
810	충청북도교육청	860	충청북도교육청(자체발급)
811	충청남도교육청	861	충청남도교육청(자체발급)
812	전라북도교육청	862	전라북도교육청(자체발급)
813	전라남도교육청	863	전라남도교육청(자체발급)
814	경상북도교육청	864	경상북도교육청(자체발급)
815	경상남도교육청	865	경상남도교육청(자체발급)
817	제주특별자치도교육청	866	제주특별자치도교육청(자체발급)
818	대학	867	대학(자체발급)
-	-	870	공공기관(자체발급)

1) 행정안전부 인증기관에서 교육부 기관명으로 개인용 인증서를 발급받을 경우 행정안전부 인증기관에서 정의한 기관구분자를 사용하므로 기관구분자로 인증기관을 구분할 수 있다.

7. 인증서 체계

7.1. 인증서 정책 구분

교육부 행정전자서명인증센터에서 발급하는 인증서들은 다음과 같은 인증서 정책 구분에 따라 발급되며 관리 된다.

정책 구분		내용	OID
개인용	개인사용자	일반 개인사용자에게 발급되는 인증서	1.2.410.100001.5.3.1.3
기관용	전자관인 (기관용)	기관 내 관인의 용도로 발급되는 인증서	1.2.410.100001.5.3.1.1
	서버용 (컴퓨터용)	기관 내 서버 등 장비에 발급되는 인증서	1.2.410.100001.5.3.1.7
	SSL용	기관 내 서버 등에 SSL 용도로 발급되는 인증서	1.2.410.100001.5.3.1.9
	특수목적용 (업무용)	기관 내 별도의 특수목적용으로 발급되는 인증서	1.2.410.100001.5.3.1.5

7.2. 인증서 기본정보 및 알고리즘

교육부 행정전자서명인증센터에서 사용하는 인증서는 인증서 정책에 따라 다음과 같은 정보를 포함하여 발급된다.

구 분		유효기간	전자서명 알고리즘	공개키 암호화 알고리즘	개인키 암호화 알고리즘
개인용	개인사용자	2년 3개월	KCDSA(2048bit)	RSA(2048bit)	ARIA
기관용	전자관인 (기관용)	2년 3개월	KCDSA(2048bit)	RSA(2048bit)	ARIA
	서버용 (컴퓨터용)	2년 3개월	KCDSA(2048bit)	RSA(2048bit)	ARIA
	SSL용	2년 3개월	-	RSA(2048bit)	-
	특수목적용 (업무용)	1년 3개월	KCDSA(2048bit)	RSA(2048bit)	ARIA
RA/LRA	RA	2년 3개월	KCDSA(2048bit)	RSA(2048bit)	ARIA
	LRA	2년 3개월	KCDSA(2048bit)	RSA(2048bit)	ARIA

7.3. 인증서 저장위치 및 저장형태

교육부 행정전자서명인증센터를 통하여 발급된 인증서와 개인키는 다음의 위치에 저장되어야 하며 저장되는 인증서와 개인키의 파일명은 정의된 기준을 준수해야 한다.

7.3.1. 개인용

구 분		전자서명용	암호화용
개인용	저장위치	[Windows]하드디스크레이블명\GPKI\Certificate\class2 [Linux]사용자계정/GPKI/Certificate/class2 [Linux](이동식디스크를 마운트한 디렉토리)/gpki/Certificate/class2/ [MacOS]사용자계정/Library/Preferences/GPKI/Certificate/class2 [MacOS]/Volumes/디스크명/GPKI/Certificate/class2	
	개인키 파일명	기관구분자(3)+이름+일련번호(3)_sig.key	기관구분자(3)+이름+일련번호(3)_env.key
	인증서 파일명	기관구분자(3)+이름+일련번호(3)_sig.cer	기관구분자(3)+이름+일련번호(3)_env.cer

7.3.2. 기관용

구 분		전자서명용	암호화용
전자관인 (기관용)	저장위치	[Windows] 하드디스크레이블명[1]/\GPKI\Certificate\class1 [Unix/Linux] 사용자계정[2]//gpki/Certificate/class1 [Unix/Linux] (이동식디스크를 마운트한 디렉토리)[3]//gpki/Certificate/class1/ [MacOS]사용자계정[2]/Library/Preferences/GPKI/Certificate/class1 [MacOS]/Volumes[4]/디스크명/Preferences/GPKI/Certificate/class1	
	개인키 파일명	850+ORG+기관명[5]_sig.key	850+ORG+기관명[5]_env.key
	인증서 파일명	850+ORG+기관명[5]_sig.cer	850+ORG+기관명[5]_env.cer
서버용 (컴퓨터용)	저장위치	[Windows] 하드디스크레이블명[1]/\GPKI\Certificate\class1 [Unix/Linux] 사용자계정[2]//gpki/Certificate/class1 [Unix/Linux] (이동식디스크를 마운트한 디렉토리)[3]//gpki/Certificate/class1/ [MacOS]사용자계정[2]/Library/Preferences/GPKI/Certificate/class1 [MacOS]/Volumes[4]/디스크명/Preferences/GPKI/Certificate/class1	
	개인키 파일명	SVR+기관코드(7)+일련번호(3)_sig.key	SVR+기관코드(7)+일련번호(3)_env.key
	인증서 파일명	SVR+기관코드(7)+일련번호(3)_sig.cer	SVR+기관코드(7)+일련번호(3)_env.cer
SSL용	저장위치	-	
	개인키 파일명	-	-
	인증서 파일명	-	-
특수목적용 (업무용)	저장위치	[Windows] 하드디스크레이블명[1]\GPKI\Certificate\class2 [Unix/Linux] 사용자계정[2]/gpki/Certificate/class2 [Unix/Linux] (이동식디스크를 마운트한 디렉토리)[3]/gpki/Certificate/class2/ [MacOS]사용자계정[2]/Library/Preferences/GPKI/Certificate/class2 [MacOS]/Volumes[3]/디스크명/Preferences/GPKI/Certificate/class2	
	개인키 파일명	업무정책[5]ID_sig.key	업무정책[5]ID_env.key
	인증서 파일명	업무정책[5]ID_sig.cer	업무정책[5]ID_env.cer

1) MS운영체제가 설치된 하드디스크
2) 사용자가 로그온한 계정
3) 이동식디스크
4) 기관명 : 전자관인 인증서 내 Subject DN 중 마지막 OU에 해당하는 값(최하위기관명)
5) 업무정책ID : 특수목적용 인증서 내 Subject DN 중 CN에 해당 하는 값

7.3.3. RA/LRA용

구 분		전자서명용	암호화용
RA	저장위치	[Windows] 하드디스크레이블명[1]/\GPKI\Certificate\class1 [Unix/Linux] 사용자계정[2]//gpki/Certificate/class1 [Unix/Linux] (이동식디스크를 마운트한 디렉토리)[3]//gpki/Certificate/class1/ [MacOS]사용자계정[2]/Library/Preferences/GPKI/Certificate/class1 [MacOS]/Volumes[4]/디스크명/Preferences/GPKI/Certificate/class1	
	개인키 파일명	RA+기관코드+기관명+일련번호(3)_sig.key	RA+기관코드+기관명+일련번호(3)_env.key
	인증서 파일명	RA+기관코드+기관명+일련번호(3)_sig.cer	RA+기관코드+기관명+일련번호(3)_env.cer
LRA	저장위치	[Windows] 하드디스크레이블명[1]/\GPKI\Certificate\class1 [Unix/Linux] 사용자계정[2]//gpki/Certificate/class1 [Unix/Linux] (이동식디스크를 마운트한 디렉토리)[3]//gpki/Certificate/class1/ [MacOS]사용자계정[2]/Library/Preferences/GPKI/Certificate/class1 [MacOS]/Volumes[4]/디스크명/Preferences/GPKI/Certificate/class1	
	개인키 파일명	LRA+기관코드+기관명+일련번호(3)_sig.key	LRA+기관코드+기관명+일련번호(3)_env.key
	인증서 파일명	LRA+기관코드+기관명+일련번호(3)_sig.cer	LRA+기관코드+기관명+일련번호(3)_env.cer

1) MS운영체제가 설치된 하드디스크
2) 사용자가 로그온한 계정
3) 이동식디스크
4) 기관명 : 전자관인 인증서 내 Subject DN 중 마지막 OU에 해당하는 값(최하위기관명)

7.4. 보안토큰 기반의 인증서 이용기술

보안토큰 내에 전자서명 인증서를 저장하고 사용하기 위하여 다음의 표준을 준용한다

- KCAC.TS.HSMU "보안토큰 기반의 공인인증서 이용기술 규격
- KCAC.TS.HSMU "보안토큰 기반의 공인인증서 저장형식 기술규격
- 보안토큰 API(PKCS#11) 프로파일

보안토큰에서 RSA 전자서명 알고리즘을 사용하기 위하여 객체 속성 템플릿을 준용하여야 한다.

RSA 공개키 객체(RSA Public Key Object Attribute)

속성	데이터 타입	내용	처리
CKA_MODULUS	Big integer	Modulus n	M
CKA_MODULUS_BITS	CK_ULONG	n의 길이(비트)	M
CKA_PUBLIC_EXPONENT	Big integer	Public exponent e	M

※ RSA공개키 객체 템플릿(C_GenerateKeyPair 함수 이용시) :

```
CK_OBJECT_CLASS class = CKO_PUBLIC_KEY;
CK_KEY_TYPE keyType = CKK_RSA;
CK_UTF8CHAR label[] =   An RSA public key object
CK_BYTE exponent[] = {...};
CK_ULONG bits = 1024;
CK_BYTE id[] = {123};
CK_BBOOL true = TRUE;
CK_BBOOL false = FALSE;
CK_ATTRIBUTE template[] = {
{CKA_CLASS, &class, sizeof(class)},
{CKA_KEY_TYPE, &keyType, sizeof(keyType)},
{CKA_TOKEN, &true, sizeof(true)},
{CKA_LABEL, label, sizeof(label)-1},
{CKA_ID, id, sizeof(id)},
{CKA_WRAP, &false, sizeof(false)},
{CKA_ENCRYPT, &false, sizeof(false)},
{CKA_MODULUS_BITS, &bits, sizeof(bits)},
{CKA_PRIVATE, false, sizeof(false)},
{CKA_VERIFY, true, sizeof(true)},
{CKA_PUBLIC_EXPONENT, exponent, sizeof(exponent)}
};
```

※ RSA공개키 객체 템플릿(C_CreateObject 함수 이용시) :

```
CK_OBJECT_CLASS class = CKO_PUBLIC_KEY;
```



```
CK_KEY_TYPE keyType = CKK_RSA;
CK_UTF8CHAR label[] =   An RSA public key object
```

```
CK_BYTE exponent[] = {...};
CK_BYTE modulus[] = {...};
CK_BYTE subject[] = {...};
CK_BYTE id[] = {123};
CK_BBOOL true = TRUE;
CK_BBOOL false = FALSE;
CK_ATTRIBUTE template[] = {
{CKA_CLASS, &class, sizeof(class)},
{CKA_KEY_TYPE, &keyType, sizeof(keyType)},
{CKA_TOKEN, &true, sizeof(true)},
{CKA_LABEL, label, sizeof(label)-1},
{CKA_ID, id, sizeof(id)},
{CKA_WRAP, &false, sizeof(false)},
{CKA_ENCRYPT, &false, sizeof(false)},
{CKA_MODULUS, modulus, sizeof(modulus)},
{CKA_SUBJECT, subject, sizeof(subject)},
{CKA_PRIVATE, false, sizeof(false)},
{CKA_VERIFY, true, sizeof(true)},
{CKA_PUBLIC_EXPONENT, exponent, sizeof(exponent)}
};
```

RSA 개인키객체(RSA Private Key Object Attribute)

속성	데이터 타입	내용	처리
CKA_MODULUS	Big integer	Modulus n	M
CKA_PUBLIC_EXPONENT	Big integer	Public exponent e	M
CKA_PRIVATE_EXPONENT	Big integer	Private exponent d	M
CKA_PRIME_1	Big integer	Prime p	M
CKA_PRIME_2	Big integer	Prime q	M
CKA_EXPONENT_1	Big integer	Private exponent d modulo p-1	M
CKA_EXPONENT_2	Big integer	Private exponent d module p-2	M
CKA_COEFFICIENT	Big integer	CRT coefficient q^{-1} mod p	M

※ RSA 개인키 객체 템플릿(C_GenerateKeyPair 함수 이용시) :

```
CK_OBJECT_CLASS class = CKO_PRIVATE_KEY;
CK_KEY_TYPE keyType = CKK_RSA;
CK_UTF8CHAR label[] =   "LABEL 명"
CK_BYTE id[] = {123};
CK_BBOOL true = TRUE;
CK_BBOOL false = FALSE;
CK_ATTRIBUTE template[] = {
{CKA_CLASS, &class, sizeof(class)},
KCAC.TS.HSMU v2.00

{CKA_KEY_TYPE, &keyType, sizeof(keyType)},
{CKA_TOKEN, &true, sizeof(true)},
{CKA_LABEL, label, sizeof(label)-1},
{CKA_ID, id, sizeof(id)},
{CKA_SENSITIVE, &true, sizeof(true)},
{CKA_DECRYPT, &false, sizeof(false)},
{CKA_SIGN, &true, sizeof(true)},
{CKA_UNWRAP, &false, sizeof(false)},
{CKA_PRIVATE, &true, sizeof(true)},
};
```

※ RSA 개인키 객체 템플릿(C_CreateObject 함수 이용시) :

```
CK_OBJECT_CLASS class = CKO_PRIVATE_KEY;
CK_KEY_TYPE keyType = CKK_RSA;
CK_UTF8CHAR label[] =   "LABEL 명"
CK_BYTE subject[] = {...};
CK_BYTE id[] = {123};
CK_BYTE modulus[] = {...};
CK_BYTE publicExponent[] = {...};
CK_BYTE privateExponent[] = {...};
CK_BYTE prime1[] = {...};
CK_BYTE prime2[] = {...};
CK_BBOOL true = TRUE;
CK_BBOOL false = FALSE;
CK_BYTE exponent1[] = {...};
CK_BYTE exponent2[] = {...};
CK_BYTE coefficient[] = {...};
```

```
CK_ATTRIBUTE template[] = {
{CKA_CLASS, &class, sizeof(class)},
{CKA_KEY_TYPE, &keyType, sizeof(keyType)},
{CKA_TOKEN, &true, sizeof(true)},
{CKA_LABEL, label, sizeof(label)-1},
{CKA_SUBJECT, subject, sizeof(subject)},
{CKA_ID, id, sizeof(id)},
{CKA_SENSITIVE, &true, sizeof(true)},
{CKA_SIGN, &true, sizeof(true)},
{CKA_UNWRAP, &false, sizeof(false)},
{CKA_DECRYPT, &false, sizeof(false)},
{CKA_PRIVATE, &true, sizeof(true)},
{CKA_MODULUS, modulus, sizeof(modulus)},
{CKA_PUBLIC_EXPONENT, publicExponent, sizeof(publicExponent)},
{CKA_PRIVATE_EXPONENT, privateExponent, sizeof(privateExponent)},
{CKA_PRIME_1, prime1, sizeof(prime1)},
{CKA_PRIME_2, prime2, sizeof(prime2)},
KCAC.TS.HSMU  v2.00

{CKA_EXPONENT_1, exponent1, sizeof(exponent1)},
{CKA_EXPONENT_2, exponent2, sizeof(exponent2)},
{CKA_COEFFICIENT, coefficient, sizeof(coefficient)}
}
```

부록1. 인증기관 인증서 프로파일

구분	필드명	ASN.1 Type	주요 정보	
			Admin name	값
기본필드	Version	INTEGER	인증서 종류	x.509 v3
	Serial Number	INTEGER		-
	Issuer		-	-
	- type	OID		
	- value	printableString 또는utf8String		
	Validity		유효기간	10년
	- notBefore	UTCTime		
	- notAfter	UTCTime		
	Subject		-	-
	- type	OID		
	- value	BIT STRING		
	Subject Public Key Info		-	-
	- algorithm	OID		
	- subjectPublicKey	BIT STRING		
	Extensions	Extensions	-	-
			해쉬알고리즘	sha256
			서명알고리즘	sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		keyIdentifier
	- authorityCertIssuer	Seneral Name		authorityCertIssuer
	- authorityCertSerialNumber	INTEGER		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	Key Identifier
	Key Usage	BIT STRING		keyCertSign, CRLSign
	Certificate Policy			
	- policyIdentifier	OID		1.2.410.100001.5.3.1.1 1.2.410.100001.5.3.1.3 1.2.410.100001.5.3.1.5 1.2.410.100001.5.3.1.7 1.2.410.100001.5.3.1.9
	- policyQualifiers			-
	--PolicyQualifierId	OID		-
	--Qualifier			-
	--CPSuri			-
	---UserNotice			-
	----NoticeReference	SEQUENCE		-
	----NoticeReference	SEQUENCE		-
	----ExplicitText	BMPString		-
	Policy Mappings		-	
	-issuerDomainPolicy	OID		-
	-subjectDomainPolicy	OID		-
	Subject Alternative Names	otherName	-	-
	Issuer Alternative Names	otherName	-	-
	Basic Constraints		Basic Constraints	-
	-cA	True		subject type = CA
	-pathLenConstraint	INTEGER		path LengthConstraint=0
	Policy Constraints		Policy Constraints	
	-requireExplicitPolicy	INTEGER		requireExplicitPolicy=0
	-inhibitPolicyMapping	INTEGER		-
	Name Constraints		-	

	-permittedSubtrees			-
	-excludedSubtrees			-
	Extended Key Usage		-	-
	CrlDistributionPoint		CrlDistributionPoint	
	-distributionPoint	DistributionPoin tName		full name: URL=ldap://cen.dir.go.kr:389/cn =GPKIRootCA1,ou=GPKI,o=Gove rnment of Korea, c=KR?authorityRevocationlist;bina ry
	-reasons	ReasongFlags		-
	-cRLIssuer	GeneralNames		-
	Authority Information Access		-	
	-accessMethod	OID		-
	-accessLocation	General Name		-

※ 교육부 행정전자서명 인증기관(CA)의 키는 FIPS 140-2 Level 3 인증 HSM 장비에서 생성합니다. 또한 공개지수의 값은 3 이상의 홀수입니다.

부록2. 등록기관 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	27개월	유효기간	27개월
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	KCDSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	KCDSAWithSHA256		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerial Number	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.3		PolicyIdentifier=1.2.410.100001.5.3.1.3
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	----NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-

	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolicy	OID		-		-
	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080

부록3. OCSP용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	40일	유효기간	40일
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	RSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	sha256WithRSAEncryption		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerial Number	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment, dataEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.7		PolicyIdentifier=1.2.410.100001.5.3.1.7
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	----NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-
	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolicy	OID		-		-

	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	OcspNoCheck		-	-	-	-
	-ocspNoCheck	OID		-		-
	-value	Octet String		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080

부록4. 개인용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	27개월	유효기간	27개월
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	KCDSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	KCDSAWithSHA256		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerialNumber	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment, dataEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.3		PolicyIdentifier=1.2.410.100001.5.3.1.3
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	----NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-
	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolicy	OID		-		-

	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080

부록5. 전자관인용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	27개월	유효기간	27개월
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	KCDSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	KCDSAWithSHA256		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerial Number	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment, dataEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.1		PolicyIdentifier=1.2.410.100001.5.3.1.1
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	---NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-
	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolic	OID		-		-

	y					
	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080

부록6. 서버용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	27개월	유효기간	27개월
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	KCDSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	KCDSAWithSHA256		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerial Number	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment, dataEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.7		PolicyIdentifier=1.2.410.100001.5.3.1.7
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	----NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-
	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolic	OID		-		-

	y					
	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080

부록7. 특수목적용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	15개월	유효기간	15개월
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	KCDSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	KCDSAWithSHA256		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerialNumber	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment, dataEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.5		PolicyIdentifier=1.2.410.100001.5.3.1.5
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	----NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-
	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolicy	OID		-		-

	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080

부록8. SSL용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책	
			Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-
	Issuer		-	-
	- type	OID		
	- value	printableString 또는 utf8String		
	Validity		유효기간	27개월
	- notBefore	UTCTime		
	- notAfter	UTCTime		
	Subject		-	-
	- type	OID		
	- value	BIT STRING		
	Subject Public Key Info			
	- algorithm	OID	키종류	RSA
	- subjectPublic Key	BIT STRING	-	
	Extensions	Extensions	-	-
			해쉬 알고리즘	sha256
			서명 알고리즘	sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier
	- authorityCertIssuer	Seneral Name		authorityCertIssuer
	- authorityCertSerial Num ber	INTEGER		authorityCertSeri alNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, keyEncipherment
	Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.9
	- policyQualifiers			-
	--PolicyQualifierId	OID		-
	--Qualifier			-
	--CPSuri			-
	---UserNotice			-
	----NoticeReference	SEQUENCE		-
	----NoticeReference	SEQUENCE		-
	----ExplicitText	BMPString		-
	Policy Mappings		-	
	-issuerDomainPolicy	OID		-
	-subjectDomainPolic	OID		-

	y			
	Subject Alternative Names	otherName	-	dNSName = DOMAIN
	Issuer Alternative Names	otherName	-	-
	Basic Constraints		-	
	-cA	False		-
	-pathLenConstraint	INTEGER		-
	Policy Constraints		-	
	-requireExplicitPolicy	INTEGER		-
	-inhibitPolicyMapping	INTEGER		-
	Name Constraints		-	
	-permittedSubtrees			-
	-excludedSubtrees			-
	Extended Key Usage		-	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.epki.go.kr/인증서가 포함된 DP포인트.crl
	-distributionPoint	DistributionPointName		-
	-reasons	ReasongFlags		-
	-cRLIssuer	GeneralNames		-
	Authority Information Access		Authority Information Access	
	-accessMethod	OID		[1]Authority Info Access Access Method=인증 기관 발급자 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.epki.go.kr/EPKICA.cer [2]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.epki.go.kr:8081
	-accessLocation	General Name		

부록9. SCVP용 인증서 프로파일

구분	필드명	ASN.1 Type	Sign 인증서 정책		Km 인증서 정책	
			Admin Name	값	Admin Name	값
기본필드	Version	INTEGER	인증서 종류	x.509v3	인증서 종류	x.509v3
	Serial Number	INTEGER	-	-	-	-
	Issuer		-	-	-	-
	- type	OID				
	- value	printableString 또는 utf8String				
	Validity		유효기간	27개월	유효기간	27개월
	- notBefore	UTCTime				
	- notAfter	UTCTime				
	Subject		-	-	-	-
	- type	OID				
	- value	BIT STRING				
	Subject Public Key Info					
	- algorithm	OID	키종류	KCDSA	키종류	RSA
	- subjectPublic Key	BIT STRING	-			
	Extensions	Extensions	-			
			해쉬 알고리즘	sha256		sha256
			서명 알고리즘	KCDSAWithSHA 256		sha256WithRSAEncryption
Policy Constraints 확장필드	Authority Key Identifier		Authority Key Identifier		Authority Key Identifier	
	- keyIdentifier	OCTET STTING		KeyIdentifier		KeyIdentifier
	- authorityCertIssuer	General Name		authorityCertIssuer		authorityCertIssuer
	- authorityCertSerial Number	INTEGER		authorityCertSerialNumber		authorityCertSerialNumber
	Subject Key Identifier	OCTET STRING	Subject Key Identifier	keyIdentifier	Subject Key Identifier	keyIdentifier
	Key Usage	BIT STRING	Key Usage	digitalSignature, nonRepudiation	Key Usage	keyEncipherment, dataEncipherment
	Certificate Policy		Certificate Policy		Certificate Policy	
	- policyIdentifier	OID		PolicyIdentifier=1.2.410.100001.5.3.1.7		PolicyIdentifier=1.2.410.100001.5.3.1.7
	- policyQualifiers			-		-
	--PolicyQualifierId	OID		-		-
	--Qualifier			-		-
	--CPSuri			-		-
	---UserNotice			-		-
	----NoticeReference	SEQUENCE		-		-
	----NoticeReference	SEQUENCE		-		-

	----ExplicitText	BMPString		-		-
	Policy Mappings		-		-	
	-issuerDomainPolicy	OID		-		-
	-subjectDomainPolicy	OID		-		-
	Subject Alternative Names	otherName	-	-	-	-
	Issuer Alternative Names	otherName	-	-	-	-
	Basic Constraints		-		-	
	-cA	False		-		-
	-pathLenConstraint	INTEGER		-		-
	Policy Constraints		-		-	
	-requireExplicitPolicy	INTEGER		-		-
	-inhibitPolicyMapping	INTEGER		-		-
	Name Constraints		-		-	
	-permittedSubtrees			-		-
	-excludedSubtrees			-		-
	Extended Key Usage		-	-	-	-
	CrlDistributionPoint		-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.epki.go.kr:389/cn=인증서가 포함된 DP포인트,ou=CRL,ou=GPKI,o=Government of Korea,c=kr?certificateRevocationList;binary
	-distributionPoint	DistributionPointName		-		-
	-reasons	ReasongFlags		-		-
	-cRLIssuer	GeneralNames		-		-
	Authority Information Access		Authority Information Access		Authority Information Access	
	-accessMethod	OID		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)		Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)
	-accessLocation	General Name		Alternative Name: URL=http://ocsp.epki.go.kr:8080		Alternative Name: URL=http://ocsp.epki.go.kr:8080