전자서명인증체계 OID 가이드라인

Object Identifier Guideline for the Electronic Signature Certification System

V1.7

2019년 4월

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

< 목 차 >

1. 개요 1

2. 가이드라인의 구성 및 범위 1

3. 관련 표준 및 규격 1
3.1 국외 표준 및 규격 1
3.2 국내 표준 및 규격 2
3.3 기타 2

4. 정의 2
4.1 전자서명법 용어의 정의 2
4.2 용어의 정의 3
4.3 용어의 효력 3

5. 약어 3

6. OID 정의 및 표현형식 4
6.1 정의 4
6.2 표현형식 4

7. 국내 전자서명인증체계를 위한 OID 구조 및 형식 5
7.1 OID 구조 6
7.2 OID 형식 6
7.3 전자서명인증체계 OID 표 8

부록 1. 전자서명인증체계 OID 표 9
부록 2. 가이드라인 연혁 13

전자서명인증체계 OID 가이드라인
Object Identifier Guideline for the Electronic Signature Certification System

1. 개요

본 가이드라인은 전자서명인증체계에서 공인인증기관이 제공하는 PKI 공인인증서비스의 상호연동을 위하여 국내에서 독자적으로 정의한 객체 식별자(OID)를 규정함으로써 공인인증서비스에서 사용되고 있는 객체를 고유하게 식별할 수 있도록 한다.

2. 가이드라인의 구성 및 범위

본 가이드라인은 전자서명인증체계에서 공인인증기관 및 가입자 소프트웨어가 이용자에게 호환성 있는 유·무선 PKI 인증서비스를 제공하는데 있어 필요한 OID를 명시하고 있으며 크게 세 부분으로 구성되어 있다.

첫 번째로 OID에 대한 정의와 표현형식을 기술한다.

두 번째로 국내 전자서명인증체계를 위한 OID의 구조와 형식에 대하여 기술한다.

세 번째로 부록에서는 국내 전자서명인증체계에서 독자적으로 정의한 OID를 규정하고 이에 따르는 명칭과 설명을 기술하고 있다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[X660] ITU-T Recommendation X.660(1992) ¦ ISO/IEC9834-1:1993, Information Technology - Open Systems Interconnection - Procedures For The Operation Of OSI Registration Authorities: General Procedures3

[X680]	ITU-t Recommendation X.660(2002) ¦ ISO/IEC8824-1:2003, Information technology - Abstract Syntax -Notation One(ASN.1) : Specification of basic notation
[RFC1778]	IETF, RFC1778, The String Representation of Standard Attribute Syntaxes, 1995
[RFC2119]	IETF, RFC2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
[ISO6523]	ISO6523(1984), Data Interchange-Structure for the identification of organizations
[ISO3166]	ISO3166(1997), Codes for the representation of names of countries and their subdivisions-Part1: Country codes

3.2 국내 표준 및 규격

해당사항 없음

3.3 기타

해당사항 없음

4. 정의

4.1 전자서명법 용어의 정의

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

가) 인증서
나) 공인인증서
다) 공인인증기관

라) 전자서명인증체계
마) 가입자
바) 가입자 설비(가입자 소프트웨어)

4.2 용어의 정의

해당사항 없음

4.3 용어의 효력

본 가이드라인에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 전자서명 알고리즘을 생성하거나 처리하는데 따라야 할 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

본 규격에서는 다음의 약어가 이용된다.

가) OID : Object Identifier, 객체 식별자
나) ISO : International Organization for Standardization, 국제표준화 기구
다) CTL : Certificate Trust List, 인증서 신뢰 목록
라) NPKI : National Public Key Infrastructure, 전자서명인증체계
마) ASN.1 : Abstract Syntax Notation One, 추상 구문 표기법션

6. OID의 정의 및 표현형식

6.1 정의

OID는 국가 및 기관에서 보유하고 있는 전자적인 객체를 명확하게 식별하기 위하여 국제적으로 유일하게 할당한 갑이다

6.2 표현형식

OID 타입과 값의 ASN.1 형식은 다음과 같다.

```
OjectIdentifierType ::=OBJECT IDENTIFIER

ObjectIdentifierValue ::=  " { "ObjIdComponentsList" }"
                ¦          " { "DefinedValue ObjIDComponentsList" }"

ObjectComponentsList ::= ObjIdComponents
                ¦          ObjIdComponents ObjIdComponentsList

ObjComponents ::= NameForm
                  ¦ NumberForm
                  ¦ NameAndNumberForm
                  ¦ DefinedValue
```

o NameForm ::= identifier

NameForm은 ITU-T Rec. X.660 ¦ ISO/IEC 9834-1(부록 A~C)에서 정의된 식별자(identifier)중에서 하나가 된다.

예) { ido member-body }

o NumberForm ::= number ¦ DefinedValue

NumberForm의 DefinedValue는 정수 타입이며 음이 아닌 값으로 할당된다. number는 OID 구성요소에 할당된 숫자 값이다.

예) { 1 2 410 200004 }

o NameAndNumberForm ::= identifier "("NumberForm")"

identifier는 숫자 값이 OID 구성요소로 할당될 때 나타난다.

예) { iso member-body korea(410) kisa(200004) }

o DefinedValue : relative OID 타입

relative OID는 알려진 객체 식별자와 관련된 위치에 의해서 한 객체를 정의하는 값으로, 시작 노드는 알려진 "ObjIdComponents"에 의해 나타내어지고, 해당 "ObjIdComponents"는 시작 노드와 함께 그 다음 노드로부터의 아크 집합만을 나타낸다. (아크는 OID 계층구조의 각 구성요소를 지칭)

예) { korea 200004 }

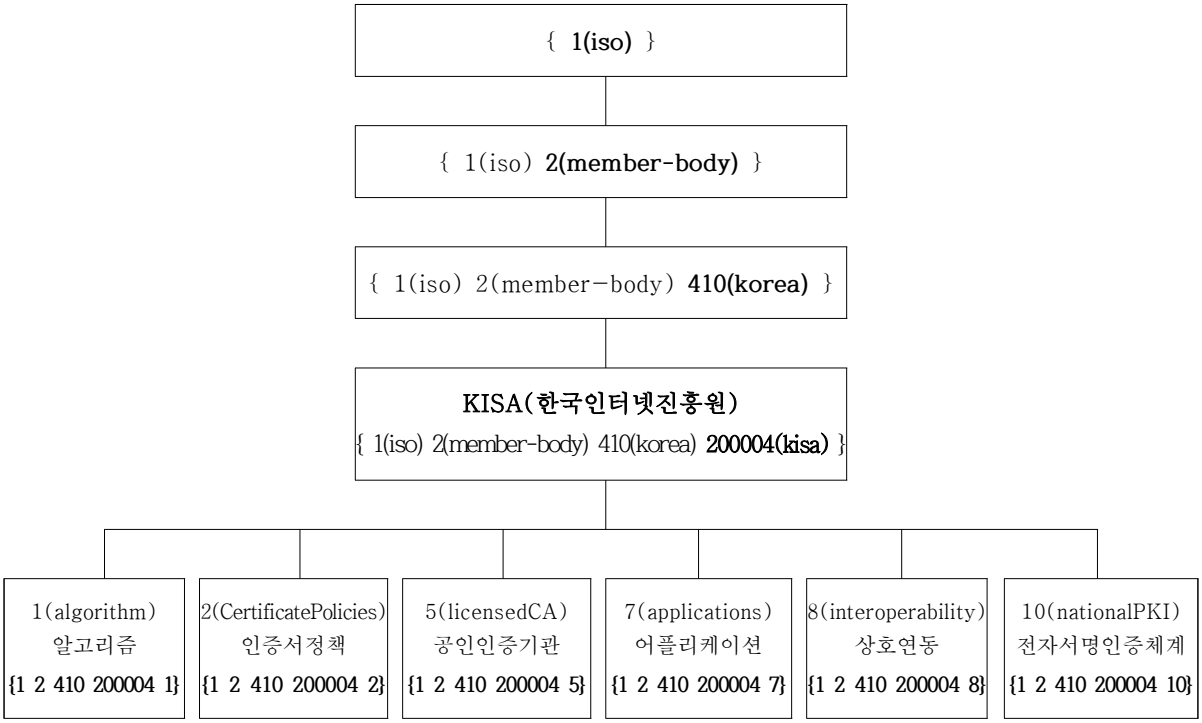
* korea OBJECT IDENTIFIER ::= { iso member-body 410 }으로 미리 정의

7. 국내 전자서명인증체계를 위한 OID 구조 및 형식

국내에서 보유하고 있는 전자객체에 대해서 국제 표준에 따른 고유한 OID를 부여하는 것이 필수적으로 요구됨에 따라, 전자서명인증체계에서 독자적으로 정의한 알고리즘, 전자적인 객체 등에 대한 OID를 다음의 구조와 형식으로 기술한다.

7.1 OID 구조

<국내 전자서명인증체계 OID 구조>



※ 이하 아크에 대한 정의는 부록1의 참조

o (algorithm) 알고리즘 : 국내 알고리즘의 OID로 활용됨
※ 향후 알고리즘에 부여될 OID 체계는 { 1 2 410 200004 1 101}부터 부여함(예, KCDSA 개정, SEED 개정 등)
o (certificatePolicies) 인증서 정책 : KISA 인증서 정책 OID로 활용됨
o (licensedCA) 공인인증기관 : 국내 공인인증기관 OID로 활용됨
o (applications) 어플리케이션 : 국내 어플리케이션 OID로 활용됨
o (interoperability) 상호연동 : 국내 상호연동을 위한 OID로 활용됨
o (nationalPKI) 전자서명인증체계 : 전자서명인증체계의 OID로 활용됨
※ 향후 NPKI에서 사용되는 PKI 관련 객체들에 대한 OID가 할당됨

7.2 OID 형식

□ ISO 계열

o 국내 전자서명인증체계는 ISO 계열의 OID 구조를 가짐
o ISO로부터 국내 member-body에 할당된 루트 OID는 {iso(1) member-body(2) korea(410)}임
- “korea(410)” 의 authority는 국내의 개체들에 대하여 OID 할당

※ member-body(2) 다음의 아크에서는 ISO 3166에서 규정한 세자리 숫자의 국가코드가 나오며 이것은 그 국가에 있는 ISO National Body를 정의한 것임

□ 한국인터넷진흥원(KISA)

o KISA의 기관 OID는 공인인증 OID체계의 루트 OID로 활용됨
- KISA의 루트 OID는 {1 2 410 200004 }로 정의
- 아크 200004는 ISO의 국내 Member-Body로부터 KISA에 할당
- 200004 이하의 아크는 KISA에서 할당

□ 알고리즘(algorithm)

o 국내 알고리즘의 OID로 활용됨
- 알고리즘 OID는 {1 2 410 200004 1 }로 정의
- 아크 1 이하는 알고리즘 OID 할당 요청 시 KISA에서 부여
  ※ 기존 부여받은 알고리즘에서 파생되는 OID는 해당 아크 이하로 할당됨

※ 향후 알고리즘에 부여될 OID 체계는 알고리즘 기반으로 "101번" 부터 부여하여 사용함 (예, KCDSA 개정판(101), SEED 개정판(102) 등)임

□ 인증서 정책(certificatePolices)

o KISA 인증서 정책 OID로 활용됨
- 인증정책 OID는 {1 2 410 200004 2 }로 정의
- 아크 2 이하는 KISA의 인증서 정책 OID를 정의함

□ 공인인증기관(licencedCA)

o 국내 공인인증기관 OID로 활용됨
- 공인인증기관의 OID는 {1 2 410 200004 5 }로 정의
- 아크 5 이하에는 공인인증기관의 기관명에 대한 OID가 할당됨
  ※ 금융결제원과 한국무역정보통신은 별도의 OID체계를 가짐[부록 1. 참조]

□ 어플리케이션(application)

o 국내 어플리케이션 OID로 활용됨
- 확장명칭형식(othername) OID는 {1 2 410 200004 7 }로 정의
- 아크 7 이하에는 특정 어플리케이션에 대하여 알고리즘을 제외한 OID가 할당됨

□ 상호연동

o 국내 상호연동을 위한 OID로 활용됨
- 상호연동 OID는 {1 2 410 200004 8 }로 정의
- 아크 8 이하에는 상호연동을 위해 CTL 등에 대한 OID가 할당됨

□ 전자서명인증체계(nationalPKI)

o 전자서명인증체계의 OID로 활용됨
- 전자서명인증체계 OID는 {1 2 410 200004 10 }로 정의
- 아크 10 이하에는 향후 NPKI에서 사용되는 PKI 관련 객체들에 대한 OID가 할당됨

7.3 전자서명인증체계 OID 표

[부록 1. 전자서명인증체계 OID]에서 국내 전자서명인증체계에서 독자적으로 정의하고 있는 OID의 명칭과 설명을 기술한다.

부록 1. 전자서명인증체계 OID 표

{1(iso) 2(member-body) 410(korea) 200004(kisa) 1(algorithms) } 이하 노드

OID							명칭	설명	규격
200004							kisa	한국인터넷진흥원	
200004	1						algorithm	알고리즘	
200004	1	1					kcdsa	KCDSA 전자서명 알고리즘	1.1, 1.2
200004	1	2					has160	HAS160 해쉬 알고리즘	
200004	1	3					seedECB	SEED 블록암호 알고리즘 - ECB모드	1.1, 1.2, 2.1, 2.3
200004	1	4					seedCBC	SEED 블록암호 알고리즘 - CBC모드	
200004	1	5					seedOFB	SEED 블록암호 알고리즘 - OFB모드	
200004	1	6					seedCFB	SEED 블록암호 알고리즘 - CFB모드	
200004	1	7					seedMAC	SEED 블록암호 알고리즘 - MAC	
200004	1	8					kcdsaWithHAS160	HAS160 해쉬 후 KCDSA 전자서명	1.1, 1.2, 2.1, 2.2, 2.3
200004	1	9					kcdsaWithSHA1	SHA-1 해쉬 후 KCDSA 전자서명	
200004	1	10					seedECBWithHAS160	HAS160 해쉬로 키 추출 후 SEED ECB로 암호화	
200004	1	11					seedCBCWithHAS160	HAS160 해쉬로 키 추출 후 SEED CBC로 암호화	
200004	1	12					seedOFBWithHAS160	HAS160 해쉬로 키 추출 후 SEED OFB로 암호화	
200004	1	13					seedCFBWithHAS160	HAS160 해쉬로 키 추출 후 SEED CFB로 암호화	
200004	1	14					seedECBWithSHA1	SHA-1 해쉬로 키 추출 후 SEED ECB로 암호화	1.1, 1.2, 2.1, 2.2, 2.3
200004	1	15					seedCBCWithSHA1	SHA-1 해쉬로 키 추출 후 SEED CBC로 암호화	
200004	1	16					seedOFBWithSHA1	SHA-1 해쉬로 키 추출 후 SEED OFB로 암호화	
200004	1	17					seedCFBWithSHA1	SHA-1 해쉬로 키 추출 후 SEED CFB로 암호화	
200004	1	20					rsaWithHAS160	HAS160 해쉬 후 RSA 전자서명	1.1, 1.2, 2.1, 2.2
200004	1	21					kcdsa1	KCDSA1 전자서명 알고리즘	
200004	1	22					kcdsa1WithHAS160	HAS160 해쉬 후 KCDSA1 전자서명	
200004	1	23					kcdsa1WithSHA1	SHA-1 해쉬 후 KCDSA1 전자서명	
200004	1	24					ecdsaWithHAS160	HAS160 해쉬 후 ECDSA 전자서명	
200004	1	25					fork256	FORK256 해쉬 알고리즘	2.1, 2.2, 2.3
200004	1	26					kcdsaWithFORK256	FORK256 해쉬 후 KCDSA 전자서명	
200004	1	27					kcdsaWithSHA256	SHA256 해쉬 후 KCDSA 전자서명	
200004	1	28					seedECBWithFORK256	FORK256 해쉬로 키 추출 후 SEED ECB로 암호화	
200004	1	29					seedCBCWithFORK256	FORK256 해쉬로 키 추출 후 SEED CBC로 암호화	
200004	1	30					seedOFBWithFORK256	FORK256 해쉬로 키 추출 후 SEED OFB로 암호화	
200004	1	31					seedCFBWithFORK256	FORK256 해쉬로 키 추출 후 SEED CFB로 암호화	
200004	1	32					seedECBWithSHA256	SHA256 해쉬로 키 추출 후 SEED ECB로 암호화	
200004	1	33					seedCBCWithSHA256	SHA256 해쉬로 키 추출 후 SEED CBC로 암호화	
200004	1	34					seedOFBWithSHA256	SHA256 해쉬로 키 추출 후 SEED OFB로 암호화	
200004	1	35					seedCFBWithSHA256	SHA256 해쉬로 키 추출 후 SEED CFB로 암호화	
200004	1	36					rsaWithFORK256	FORK256 해쉬 후 RSA 전자서명	
200004	1	37					kcdsa1WithFORK256	FORK256 해쉬 후 KCDSA1 전자서명	
200004	1	38					kcdsa1WithSHA256	SHA256 해쉬 후 KCDSA1 전자서명	
200004	1	39					ecdsaWithFORK256	FORK256 해쉬 후 ECDSA 전자서명	
200004	1	40					kcdsaWithSHA224	SHA224 해쉬 후 KCDSA 전자서명	
200004	1	41					kcdsa1WithSHA224	SHA224 해쉬 후 KCDSA1 전자서명	
200004	1	100					ecc	타원곡선 전자서명 알고리즘	2.1
200004	1	100	1				id-fieldType	유한체	
200004	1	100	1	1			prime-field	소수체	
200004	1	100	1	2			characteristic-two-field	이진 확장체	
200004	1	100	1	2	3		id-characteristic-two-field-basis	이진 확장체에서의 기저의 종류	
200004	1	100	1	2	3	1	gnBasis	가우스 정규기저	

200004	1	100	1	2	3	2	tpBasis	삼항다항식 기저	
200004	1	100	1	2	3	3	ppBasis	오항다항식 기저	
200004	1	100	1	3			odd-characteristic-extension-field	홀소수 확장체	
200004	1	100	2				id-publickKeyType	키형태	
200004	1	100	2	1			id-ecPublicKey	타원곡선 공개키	
200004	1	100	3				ellipticCurves	타원곡선	
200004	1	100	3	0			c-TwoCurve	GF(2m)상의 타원곡선	
200004	1	100	3	0	1		eC2M163R	f(x)=x163+x7+x6+x3+1, 임의의 곡선	
200004	1	100	3	0	2		eC2M163K	f(x)=x163+x7+x6+x3+1, Koblitz 곡선	
200004	1	100	3	0	3		eC2M193R	f(x)=x193+x15+1, 임의의 곡선	
200004	1	100	3	0	4		eC2M233R	f(x)=x233+x74+1, 임의의 곡선	
200004	1	100	3	0	5		eC2M233K	f(x)=x233+x74+1, Koblitz 곡선	
200004	1	100	3	0	6		eC2M283R	f(x)=x283+x12+x7+x5+1, 임의의 곡선	
200004	1	100	3	0	7		eC2M283K	f(x)=x283+x12+x7+x5+1, Koblitz 곡선	
200004	1	100	3	0	8		eC2M409R	f(x)=x409+x87+1, 임의의 곡선	
200004	1	100	3	0	9		eC2M409K	f(x)=x409+x87+1, Koblitz 곡선	
200004	1	100	3	0	10		eC2M571R	f(x)=x571+x10+x5+x2+1, 임의의 곡선	
200004	1	100	3	0	11		eC2M571K	f(x)=x571+x10+x5+x2+1, Koblitz 곡선	
200004	1	100	3	1			primeCurve	GF(p) 상의 타원곡선	
200004	1	100	3	1	1		eCP160R	[log2p]=160, 임의의 곡선	
200004	1	100	3	1	2		eCP160K	[log2p]=160, Koblitz 곡선	
200004	1	100	3	1	3		eCP192R	[log2p]=192, 임의의 곡선	
200004	1	100	3	1	4		eCP192K	[log2p]=192, Koblitz 곡선	
200004	1	100	3	1	5		eCP224R	[log2p]=224, 임의의 곡선	
200004	1	100	3	1	6		eCP224K	[log2p]=224, Koblitz 곡선	
200004	1	100	3	1	7		eCP256R	[log2p]=256, 임의의 곡선	
200004	1	100	3	1	8		eCP256K	[log2p]=256, Koblitz 곡선	
200004	1	100	3	1	9		eCP384R	[log2p]=384, 임의의 곡선	
200004	1	100	3	1	10		eCP384K	[log2p]=384, Koblitz 곡선	
200004	1	100	3	1	11		eCP512R	[log2p]=512, 임의의 곡선	
200004	1	100	3	1	12		eCP512K	[log2p]=512, Koblitz 곡선	
200004	1	100	3	2			c-extensionCurve	GF(pm) 상의 타원곡선	
200004	1	100	3	2	1		eCP16M11R	p=216-129, f(x)=x11-3, 임의의 곡선	
200004	1	100	3	2	2		eCP16M11K	p=216-129, f(x)=x11-2, Koblitz 곡선	
200004	1	100	3	2	3		eCP16M13R	p=216-15, f(x)=x13-2, 임의의 곡선	
200004	1	100	3	2	4		eCP16M13K	p=216-15, f(x)=x13-3, Koblitz 곡선	
200004	1	100	3	2	5		eCP16M17R	p=216-17, f(x)=x17-2, 임의의 곡선	
200004	1	100	3	2	6		eCP16M17K	p=216-17, f(x)=x17-2, Koblitz 곡선	
200004	1	100	3	2	7		eCP32M05R	p=232-1, f(x)=x7-2, 임의의 곡선	
200004	1	100	3	2	8		eCP31M07R	p=231-1, f(x)=x7-3, 임의의 곡선	
200004	1	100	3	2	9		eCP31M07K	p=231-1, f(x)=x7-3, Koblitz 곡선	
200004	1	100	3	2	10		eCP31M11R	p=231-1, f(x)=x11-3, 임의의 곡선	
200004	1	100	3	2	11		eCP31M11K	p=231-1, f(x)=x11-3, Koblitz 곡선	
200004	1	100	3	2	12		eCP61M03R	p=261-1, f(x)=x3-5, 임의의 곡선	
200004	1	100	3	2	13		eCP61M05R	p=261-3, f(x)=x5-3, 임의의 곡선	
200004	1	100	3	2	14		eCP61M05K	p=261-3, f(x)=x5-3, Koblitz 곡선	
200004	1	100	3	2	15		eCP61M07R	p=261-3, f(x)=x7-3, 임의의 곡선	
200004	1	100	3	2	16		eCP61M07K	p=261-3, f(x)=x7-3, Koblitz 곡선	
200004	1	100	4				id-ecSigType	서명형태	
200004	1	100	4	1			eckcdsa-with-HAS160	HAS160 해쉬 후 ECKCDSA 전자서명	
200004	1	100	4	2			eckcdsa-with-FORK256	FORM256 해쉬 후 ECKCDSA 전자서명	
200004	1	100	4	3			eckcdsa-with-SHA1	SHA-1 해쉬 후 ECKCDSA 전자서명	
200004	1	100	4	4			eckcdsa-with-SHA224	SHA224 해쉬 후 ECKCDSA 전자서명	
200004	1	100	4	5			eckcdsa-with-SHA256	SHA256 해쉬 후 ECKCDSA 전자서명	

200004	1	101					EncryptedPrivateKeyInfos	전자서명생성정보를 암호화한 형태	
200004	1	101	1				nfcObjectBasedEncryption	NFC 객체 인증을 통한 소유기반 암호화	
200004	1	101	2				fingerprintBasedEncryption	지문 인증을 통한 생체 기반 암호화	
200004	1	101	3				faceprintBasedEncryption	얼굴 인증을 통한 생체 기반 암호화	
200004	1	101	4				voiceprintBasedEncryption	화자 인증을 통한 생체 기반 암호화	
200004	1	101	5				eyeprintBasedEncryption	망막 인증을 통한 생체 기반 암호화	
200004	1	101	6				irisprintBasedEncryption	홍채 인증을 통한 생체 기반 암호화	
200004	1	101	7				handprintBasedEncryption	손바닥 인증을 통한 생체 기반 암호화	
200004	1	101	8				actofsigningBasedEncryption	서명 행위 인증을 통한 생체 기반 암호화	
200004	1	101	9				pinBasedEncryption	PIN 인증을 통한 암호화	
200004	1	101	10				patternBasedEncryption	PATTERN 인증을 통한 암호화	

{1(iso) 2(member-body) 410(korea) 200004(kisa) 2(certificatePolicies) } 이하 노드

OID							명칭	설명	규격
200004	2						certificatePolicies	인증서 정책	
200004	2	1					sign	전자서명	1.1, 1.2

{1(iso) 2(member-body) 410(korea) 200004(kisa) 5(licensedCA) } 이하 노드

OID							명칭	설명	규격
200004	5						licensedCA	공인인증기관 영역	
200004	5	1					signkorea	코스콤	-
200004	5	1	1	5			certificatePolicies	상호연동용 인증서(개인용)	
200004	5	1	1	7			certificatePolicies	상호연동용 인증서(법인·단체·개인사업자)	
200004	5	2					signgate	한국정보인증	
200004	5	2	1	1			certificatePolicies	상호연동용 인증서(법인·단체·개인사업자)	
200004	5	2	1	2			certificatePolicies	상호연동용 인증서(개인용)	
200004	5	3					niasign	한국정보화진흥원	
200004	5	3	1	1			certificatePolicies	상호연동용 인증서(기관용(공공기관))	
200004	5	3	1	2			certificatePolicies	상호연동용 인증서(법인용)	
200004	5	3	1	9			certificatePolicies	상호연동용 인증서(개인용)	
200004	5	4					crosscert	한국전자인증	
200004	5	4	1	1			certificatePolicies	상호연동용 인증서(개인용)	
200004	5	4	1	2			certificatePolicies	상호연동용 인증서(법인용)	
200004	5	5					initech	이니텍	
200004	5	5	1	1			certificatePolicies	상호연동용 인증서(개인용)	
200004	5	5	1	2			certificatePolicies	상호연동용 인증서(법인용)	
200005							kftc	금융결제원	
200005	1	1	1				certificatePolicies	상호연동용 인증서(개인용)	
200005	1	1	5				certificatePolicies	상호연동용 인증서(법인용)	
200012							ktnet	한국무역정보통신	
200012	1	1	1				certificatePolicies	상호연동용 인증서(개인용)	
200012	1	1	3				certificatePolicies	상호연동용 인증서(법인용)	

※ 금융결제원과 한국무역정보통신은 별도의 OID체계를 가짐

- 금융결제원 : {iso(1) member-body(2) korea(410) kftc(200005) }
- 한국무역정보통신 : {iso(1) member-body(2) korea(410) ktnet(200012) }

{1(iso) 2(member-body) 410(korea) 200004(kisa) 7(application) } 이하 노드

OID							명칭	설명	규격
200004	7						applications	어플리케이션 영역	
200004	7	1					smime	어플리케이션 중 smime 영역	-
200004	7	1	1				alg	smime용 알고리즘	
200004	7	1	1	1			cMSSEEDwrap	CMS에서 SEED 키 wrapping	
200004	7	1	2				kbims	바이오인식용 OID 정의	
200004	7	2					SecretBag	전자서명생성정보 암호화 확장	-
200004	7	3					NFC KeyFactorID	NFC 객체로부터 수집된 인자 값	-
200004	7	3	1				Tag Type	ISO 14443-A 기반 태그 타입	
200004	7	3	2				Technologies Available	NFC 객체가 지원하는 태그 기술 목록	
200004	7	3	3				Serial Number	NFC 객체의 시리얼 번호	
200004	7	3	4				ATQA (Answer To Request, Type A)	PICC Type A 의 요청에 대한 응답 값	
200004	7	3	5				SAK (Select acKnowledge, Type A)	PICC Type A 의 선택 승인 값	
200004	7	3	6				ATS (Answer To Select)	선택에 대한 응답 값	

{1(iso) 2(member-body) 410(korea) 200004(kisa) 8(interoperability) } 이하 노드

OID							명칭	설명	규격
200004	8						interoperability	상호연동 관련 OID 정의	
200004	8	1					ctl	살제 사용하지 않음(MS OID로 교체)	5.1
200004	8	1	1				subjectUsage	subject Usage 필드를 위한 OID 정의	
200004	8	1	1	1			electronic-civil-application	민원서비스에 사용되는 CTL 표시	
200004	8	1	2				oc	CTL을 위한 Object Class 정의	
200004	8	1	2	1			pkiCTL	PKI용 CTL 표시하는 Object Class	
200004	8	1	3				at	CTL을 위한 속성 정의	
200004	8	1	3	1			certificateTrustList	인증서 신뢰목록을 표시하는 속성	

{1(iso) 2(member-body) 410(korea) 200004(kisa) 10(nationalPKI)} 이하 노드

OID							명칭	설명	규격
200004	10						nationalPKI	국가 공개키 기반 기조	
200004	10	1					attributes	속성	1.5, 3.1
200004	10	1	1				kisa-identifyData	인증서 소유자의 부가 대체명칭	
200004	10	1	1	1			vid	가상 ID	
200004	10	1	1	2			encryptedVID	암호화된 가상 ID	
200004	10	1	1	3			randomNum	난수	
200004	10	1	2				kisa-HSM	보안토큰 식별자	6.3
200004	10	1	3				deviceCertificate	홈디바이스 인증서	-
200004	10	1	3	1			HRAInfo	홈RA 정보	
200004	10	1	3	2			HRAOwner	홈RA 소유자 정보	
200004	10	1	3	3			devDesc	디바이스 기능 설명	

부록 2. 가이드라인 연혁

버전	제·개정일	제·개정내역
v1.0	2003년 8월	o “전자서명인증체계 OID 가이드라인”으로 제정
v1.1	2007년 3월	o 홈디바이스 인증서 관련 OID를 추가하여 개정
v1.2	2007년 9월	o FORK256, SHA256 관련 OID를 추가하여 개정
v1.3	2008년 10월	o 법률 공포번호가 해당 법률 개정 시마다 변경되는 점을 고려하여 법령명으로 개정
v1.4	2013년 10월	o KCDSA, EC-KCDSA 관련 OID를 추가하여 개정
v1.5	2016년 5월	o 바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인 제정에 따른 OID를 추가하여 제정
v1.6	2017년 9월	o 신규 공인인증기관 지정에 따른 OID를 추가하여 개정
v1.7	2019년 4월	o 바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인 개정에 따른 신규 OID 추가