전자서명 알고리즘 규격

Digital Signature Algorithm Specification

v1.30

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

1. 개요 ····· 1
2. 규격의 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 용어 정의 ····· 2
4.2 용어의 정의 ····· 3
4.3 용어의 효력 ····· 3
5. 약어 ····· 3
6. RSA ····· 4
6.1 전자서명키 ····· 4
6.2 서명 대상 ····· 4
6.3 서명 생성 ····· 5
7. KCDSA ····· 5
8. ECDSA ····· 5
8.1 전자서명키 ····· 6
8.2 서명 대상 및 생성 ····· 8
8.3 서명값 구조 ····· 8
9. 부칙 ····· 9

부록 1. ECDSA 알고리즘의 커브 파라미터 ····· 10
부록 2. 규격의 연혁 ····· 16

전자서명 알고리즘 규격
Digital Signature Algorithm Specification

1. 개요

전자서명 알고리즘은 인증서 또는 CRL(인증서 효력정지 및 폐지목록)을 생성하는 경우와 전자문서에 전자서명을 하는 경우에 사용된다. 본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계의 공인인증기관이 유·무선 공인인증서비스를 제공하는데 있어 필수적으로 요구되는 전자서명 알고리즘 및 해당 전자서명 알고리즘의 구현 방법을 정의한다.

2. 규격의 구성 및 범위

본 규격은 공인전자서명인증체계 유·무선 공인인증서비스에서 사용되는 전자서명 알고리즘을 정의하기 위한 것으로 다음과 같이 두 부분으로 나누어진다.

첫 번째로 유·무선 공인인증서비스에서 사용되는 전자서명 알고리즘을 나열하고 각각의 구현에 따른 요구사항을 정의한다.

두 번째로 부록에서는 전자서명 알고리즘의 하나인 ECDSA 알고리즘의 권고 커브 파라미터를 정의한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[PKCS1] RSA, PKCS#1 v2.0, *RSA Cryptography Standard*, October 1, 1998

[X9.31] ANSI, X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry(ANSI)*, 1998

[X9.62] ANSI, X9.62-1999, *Public Key Cryptography for the Financial Services Industry : The Elliptic Curve Digital Signature Algorithm(ECDSA),* 1999

[SHA-1] NIST, FIPS PUB 180-1, *National Institute of Standards and Technology,* 1994

[SHA-2] NIST, FIPS PUB 180-3, National Institute of Standards and Technology, 2008

[RFC2119] IETF, RFC2119, *Key words for use in RFCs to Indicate Requirement Levels,* March 1997

3.2 국내 표준 및 규격

[TTA-120001/R1] TTA, TTAS.KO-12.0001/R1, *부가형 전자서명 방식 표준 - 제2부 : 인증서 기반 전자서명 알고리즘*, 2002

[KCAC.TS.CTL] KISA, KCAC.TS.CTL, v1.40, *인증기관간 상호연동을 위한 CTL 기술규격*, 2009

[KCAC.TS.CERTPROF] KISA, KCAC.TS.CERTPROF, v1.70, *전자서명 인증서 프로파일 규격*, 2009

3.3. 기타

[KCAC.TG.OID] KISA, KCAC.TG.OID, v1.30, *"전자서명인증체계 OID 가이드라인"*, 2008

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) 인증서
나) 인증기관
다) 공개키
라) 가입자

4.2 용어의 정의

본 규격을 위하여 다음과 같은 용어들을 정의한다.

가) 유선 공인인증서비스 : 인터넷 기반의 전자거래를 위해 공인인증서를 이용하는 서비스
나) 무선 공인인증서비스 : 무선 단말기 기반의 전자거래를 위해 공인인증서를 이용하는 서비스

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) TCI : Trusted Certificate Authority Information, 최상위인증기관 신뢰 정보
나) ASN.1 : Abstract Syntax Notation One, 추상적 구문 표기
다) CP : Contents Provider, 콘텐츠 제공자
라) CRL : Certificate Revocation List, 인증서 효력정지 및 폐지목록

6. RSA

RSA는 소인수 분해 문제의 어려움에 기반한 알고리즘으로, 공인인증시스템과 가입자 설비는 RSA 전자서명키 생성 및 전자서명 생성·검증 기능을 제공하여야 한다.

6.1 전자서명키

RSA 전자서명키 생성을 위한 난수 및 소수, 전자서명키의 생성은 [X9.31]을 준용해야 한다. RSA 공개키 알고리즘이 인증서에 포함되는 경우 해당 RSA 공개키 알고리즘에 대한 OID(Object Identifier) 는 다음과 같다.

```
rsaEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
                rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
```

6.2 서명 대상

RSA로 전자서명을 생성하는 경우 전자서명 대상으로는 서명대상 메시지의 해쉬값과 DigtestInfo 구조체가 있다.

메시지 해쉬값은 전자서명 하고자 하는 메시지를 SHA-1으로 해쉬한 160비트 값 또는 SHA-256으로 해쉬한 256비트 값이다. [KCAC.WTLSCert]에서 정의한 WTLS 인증서의 signature 필드, [KCAC.TS.TCI]의 TCI 구조체 signature 필드를 생성하는 경우에는 서명대상으로 메시지 해쉬값을 사용해야 한다.

DigestInfo 구조체는 서명하고자 하는 메시지를 SHA-1 또는 SHA-256으로 해쉬한 후 이 해쉬값을 [PKCS1]에서 정의된 DigestInfo 형태로 변환하여 서

명하는 방식이다. DigestInfo의 ASN.1 형태는 다음과 같으며 여기서 Digest는 서명하고자 하는 메시지에 대한 SHA-1 160비트 또는 SHA-256 256비트 해쉬값이다.

```
DigestInfo ::= SEQUENCE
{
        digestAlgorithm  AlgorithmIdentifier,
        Digest           OCTET STRING }
```

[KCAC.WALSP]에서 정의한 SignedContents의 signature 필드 및 전자서명인증체계에서 사용되는 인증서와 CRL의 signature 필드를 생성하는 경우에는 서명대상으로 위의 DigestInfo 구조체를 사용해야 한다.

6.3 서명 생성

RSA를 사용한 전자서명 생성 및 검증은 [PKCS1]을 준용해야 한다. SHA-1 또는 SHA-256을 사용한 RSA 전자서명 알고리즘에 대한 OID는 다음과 같다.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

sha256WithRSAEncryption OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
```

7. KCDSA

KCDSA는 국내에서 개발된 알고리즘으로 [TTA-120001/R1]를 준용한다. 공인인증시스템은 KCDSA 전자서명키 생성 및 전자서명 생성·검증 기능을 제공할 것을 권고한다. 가입자 설비는 KCDSA 전자서명키 생성 및 전자서명 생성·검증 기능을 제공하여야 한다. KCDSA를 사용한 전자서명 방식에 대한 OID는 [KCAC.TG.OID]를 준용해야 한다.

8. ECDSA

ECDSA는 타원곡선 전자서명 알고리즘으로, 무선 공인인증서비스 제공을 위한

공인인증시스템 및 가입자 설비는 모두 ECDSA 전자서명키 생성 및 전자서명 생성·검증 기능을 제공하여야 한다. 유선 공인인증서비스 제공을 위한 가입자 설비는 ECDSA 전자서명키 생성 및 전자서명 생성·검증 기능을 제공할 것을 권고한다.

8.1 전자서명키

ECDSA 전자서명키 생성을 위한 난수 및 소수, 전자서명키의 생성은 [X9.62]를 준용해야 한다. ECDSA에서 사용되는 ECC 커브에 대한 ASN.1 형태는 다음과 같다.

```
ecpkParameters ::= CHOICE {
        ecParameters   ECParameters,
        namedCurve   OBJECT IDENTIFIER,
        implicitlyCA   NULL }
ecParameters ::= SEQUENCE {
        version         ECPVer,
        fieldID         FieldID,
        curve           Curve,
        base            ECPoint,
        order           INTEGER,
        cofactor        INTEGER      OPTIONAL,
 }
```

전자서명인증체계에서 지원하는 ECDSA 알고리즘 커브 파라미터는 부록 1.을 준용한다. 무선 공인인증시스템 및 CP 서버, 단말기에서 구현해야 하는 커브는 다음과 같다.

구분 \ 커브	c2pnb 163v1	secp 160r1	sect 163k1	sect 233k1	sect 233r1	secp 224r1	FIPS 186-3	X9.62
무선 공인인증 시스템	M	M	M	M	M	M	R	R
CP 서버	M	M	M	M	M	M	O	O
단말기	M	O	O	O	O	M	O	O

무선 공인인증시스템은 sect163k1, c2pnb163v1, secp160r1를 모두 구현해야 하며, 각각에 대한 OID는 다음과 같다.

o sect163k1 커브 (WTLS 3번 커브)

sect163k1 : { iso(1) identified-organization(3) certicom(132) curve(0) 1}

o c2pnb163v1 커브 (WTLS 5번 커브)

c2pnb163v1 : { iso(1) member-body(2) us(840) ANSI-X9-62(10045) curves(3) characteristicTwo(0) 1 }

o secp160r1 커브 (WTLS 7번 커브)

secp160r1 : { iso(1) identified-organization(3) certicom(132) curve(0) 8 }

가입자 공인인증서의 전자서명키를 2,048비트로 상향 조정하는 시점부터 ECDSA 전자서명키 생성에 sect233k1, sect233r1, secp224r1 커브를 추가로 구현해야 하며, 각각에 대한 OID는 다음과 같다.

o sect233k1 커브 (WTLS 10번 커브)

sect233k1 : { iso(1) identified-organization(3) certicom(132) curve(0) 26 }

o sect233r1 커브 (WTLS 11번 커브)

sect233r1 : { iso(1) identified-organization(3) certicom(132) curve(0) 27 }

o secp224r1 커브 (WTLS 12번 커브)

secp224r1 : { iso(1) identified-organization(3) certicom(132) curve(0) 33 }

무선 공인인증시스템에서 FIPS 186-3 및 X9.62 커브 구현은 권고사항이며, 각각에 대한 OID는 부록1을 참조한다.

가입자 공인인증서의 전자서명키를 2,048비트로 상향 조정하는 시점부터는 ECDSA 전자서명키 생성에 sect233k1, sect233r1, secp224r1커브 또는 FIPS 186-3의 K-233, B-233커브를 이용하여야 한다.

ECDSA 공개키 알고리즘이 인증서에 포함되는 경우 해당 ECDSA 알고리즘에 대한 OID는 다음과 같다.

```
id-ecPublicKey OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ANSI-X9-62(10045)
    id-public-key-type(2) 1 }
```

8.2 서명 대상 및 생성

ECDSA에 의한 전자서명에서 서명 대상은 전자서명하고자 하는 전자문서의 SHA-1에 의한 160비트 해쉬값 또는 SHA-256에 의한 256비트 해쉬값이다. 이 해쉬값은 [X9.62]를 준용하여 전자서명되며 그 결과값으로 r과 s를 생성해야 한다. SHA-1 또는 SHA-256 해쉬 후 ECDSA를 사용한 전자서명 방식에 대한 OID는 다음과 같다.

```
ecdsa-with-SHA1 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ANSI-X9-62(10045) signature(4) 1 }

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4)
    ecdsa-with-SHA2(3) 2 }
```

8.3 서명값 구조

8.2에서 생성된 전자서명값 r과 s값은 연접(concatenate) 또는 ASN.1 구조로 구성된다.

첫 번째로 연접구조는 [WTLS]에서 정의되었으며 서명값인 정수 r과 s를 [X9.62]에서 정의된 Integer-to-Octet-String 변환 규칙에 의해 문자열(옥텟스트링) R과 S로 변환한 후 이를 연접하여 서명값 구조를 생성한다. 이때 생성된 서명값 구조(Sig)를 기호로 표시하면 다음과 같다.

Sig : R | S

위의 구조는 [KCAC.WTLSCert]에서 정의한 WTLS 인증서의 signature 필드, [KCAC.WALSP]에서 정의한 SignedContents의 signature 필드 및 [KCAC.TS.TCI]의 TCI 구조체에 포함되는 signature 필드에 사용해야 한다. SignedContents가 유선환경과 호환성을 가지기 위해서는 CP에서 서명값 연접구조를 ASN.1 구조로 변환하여 사용해야 한다.

두 번째 ECDSA 서명값 구조인 ASN.1 구조는 [X9.62]에 명시된 방법으로 정수 r과 s를 ASN.1 구조체인 ECDSA-Sig-Value 형태로 변환하여 사용하는 방법이다. ECDSA-Sig-Value 구조체의 ASN.1 형태는 다음과 같다.

```
ECDSA-Sig-Value ::= SEQUENCE
{       r INTEGER,
        s INTEGER     }
```

전자서명인증체계내 인증서 및 CRL의 signature 필드는 구조체는 이 구조를 사용해야 한다.

9. 전자서명 알고리즘의 안전성 확보

가입자 공인인증서는 공인인증체계의 전자서명키를 상향 조정하는 시점부터 전자서명 알고리즘은 2048 비트(RSA, KCDSA) 또는 224 비트(ECDSA) 이상을 사용하여야 하며, 전자서명 메시지에 256비트 이상의 출력값을 가지는 해쉬 알고리즘을 사용하여야 한다. 다만, 발급된 가입자 공인인증서는 유효기간 내에서 사용 가능 하며, 공인인증서 생성에 사용한 동일한 해쉬 알고리즘을 전자서명에 사용할 수 있다.

공인인증체계의 전자서명키를 상향 조정하는 시점은 미래창조과학부가 별도로 고시하여 정한날로 한다.

부록1. ECDSA 알고리즘의 커브 파라미터

1. WTLS 권고 커브

1. WTLS 권고 커브

1.1 Assigned number 5

Assigned number	5
Basic	Yes
Field size	163
Irreducible polynomial	x^163 + x^8 + x^2 + x + 1
Elliptic curve E	y^2 + xy = x^3 + ax^2 + b; over GF(2^163)
Seed	D2C0FB15 760860DE F1EEF4D6 96E67687 56151754
Parameter a	07 2546B543 5234A422 E0789675 F432C894 35DE5242
Parameter b	00 C9517D06 D5240D3C FF38C74B 20B6CD4D 6F9DD4D9
Generating point G	07 AF699895 46103D79 329FCC3D 74880F33 BBE803CB, 01 EC23211B 5966ADEA 1D3F87F7 EA5848AE F0B7CA9F (~ y_p = 01)
Order of G	04 00000000 00000000 0001E60F C8821CC7 4DAEAFC1
Cofactor K	02

1.2 Assigned number 7

Assigned number	7
Basic	Yes
Field size	160
Elliptic curve E	y^2 = x^3 + ax + b; over GF(p)
Prime P	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFF
Seed	S = 1053CDE4 2C14D696 E6768756 1517533B F3F83345 r = 2DA6C4D7 0B90FF91 2E725E25 E90AF631 C18F0D2F
Parameter a	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC
Parameter b	1C97BEFC 54BD7A8B 65ACF89F 81D4D4AD C565FA45
Generating point G	4A96B568 8EF57328 46646989 68C38BB9 13CBFC82, 23A62855 3168947D 59DCC912 04235137 7AC5FB32 (~ y_p = 00)
Order of G	01 00000000 00000000 0001F4C8 F927AED3 CA752257
Cofactor K	01

1.3 Assigned number 3

Assigned number	3
Basic	No
Field size	163
Irreducible polynomial	x^163 + x^7 + x^6 + x + 1
Elliptic curve E	y^2 + xy = x^3 + ax^2 + b; over GF(2^163)
Parameter a	01
Parameter b	01
Generating point G	02 FE13C053 7BBC11AC AA07D793 DE4E6D5E 5C94EEE8, 02 89070FB0 5D38FF58 321F2E80 0536D538 CCDAA3D9 (~ y_p = 01)
Order of G	04 00000000 00000000 00020108 A2E0CC0D 99F8A5EF
Cofactor K	02

1.4 Assigned number 10

Assigned number	10
Basic	No
Field size	233
Irreducible polynomial	x^233 + x^74 + 1
Elliptic curve E	y^2 + xy = x^3 + ax^2 + b; over GF(2^233)
Parameter a	0000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Parameter b	0000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
Generating point G	0172 32BA853A 7E731AF1 29F22FF4 149563A4 19C26BF5 0A4C9D6E EFAD6126, 01DB 537DECE8 19B7F70F 555A67C4 27A8CD9B F18AEB9B 56E0C110 56FAE6A3 (~ y_p = 00)
Order of G	80 00000000 00000000 00000000 00069D5B B915BCD4 6EFB1AD5 F173ABDF
Cofactor K	04

1.5 Assigned number 11

Assigned number	11
Basic	No
Field size	233
Irreducible polynomial	x^233 + x^74 + 1
Elliptic curve E	y^2 + xy = x^3 + ax^2 + b; over GF(2^233)
Seed	74D59FF0 7F6B413D 0EA14B34 4B20A2DB 049B50C3
Parameter a	0000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
Parameter b	0066 647EDE6C 332C7F8C 0923BB58 213B333B 20E9CE42 81FE115F 7D8F90AD
Generating point G	00FA C9DFCBAC 8313BB21 39F1BB75 5FEF65BC 391F8B36 F8F8EB73 71FD558B, 0100 6A08A419 03350678 E58528BE BF8A0BEF F867A7CA 36716F7E 01F81052 (~ y p = 01)
Order of G	0100 00000000 00000000 00000000 0013E974 E72F8A69 22031D26 03CFE0D7
Cofactor K	02

1.6 Assigned number 12

Assigned number	12
Basic	No
Field size	224
Elliptic curve E	y2 = x3 + ax + b; over GF(p)
Prime P	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 00000000 00000001
Seed	BD713447 99D5C7FC DC45B59F A3B9AB8F 6A948BC5
Parameter a	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFE
Parameter b	B4050A85 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943 2355FFB4
Generating point G	B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6 115C1D21, BD376388 B5F723FB 4C22DFE6 CD4375A0 5A074764 44D58199 85007E34 (~ y_p = 00)
Order of G	FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D
Cofactor K	01

2. X9.62 권고 커브

Field 2^163
f = 08 00000000 00000000 00000000 00000000 00000107
curve E : y^2 + xy = x^3 + ax^2 + b

2.1 ID c2pnb163v1 (WTLS 5번커브)

SEED = D2C0FB15 760860DE F1EEF4D6 96E67687 56151754
a = 07 2546B543 5234A422 E0789675 F432C894 35DE5242
b = 00 C9517D06 D5240D3C FF38C74B 20B6CD4D 6F9DD4D9
Base point G(with point compression) :
0307 AF699895 46103D79 329FCC3D 74880F33 BBE803CB
Order of G :
n = 04 00000000 00000000 0001E60F C8821CC7 4DAEAFC1
h = 02

2.2 ID c2pnb163v2

SEED = 53814C05 0D44D696 E6768756 1517580C A4E29FFD
a = 01 08B39E77 C4B108BE D981ED0E 890E117C 511CF072
b = 06 67ACEB38 AF4E488C 407433FF AE4F1C81 1638DF20
Base point G(with point compression) :
0300 24266E4E B5106D0A 964D92C4 860E2671 DB9B6CC5
Order of G :
n = 03 FFFFFFFF FFFFFFFF FFFDF64D E1151ADB B78F10A7
h = 02

2.3 ID c2pnb163v3

SEED = 50CBF1D9 5CA94D69 6E676875 615175F1 6A36A3D8
a = 07 A526C63D 3E25A256 A007699F 5447E32A E456B50E
b = 03 F7061798 EB99E238 FD6F1BF9 5B48FEEB 4854252B
Base point G(with point compression) :
0202 F9F87B7C 574D0BDE CF8A22E6 524775F9 8CDEBDCB
Order of G :

n = 03 FFFFFFFF FFFFFFFF FFFE1AEE 140F110A FF961309
h = 02

3. FIPS 186-3 권고 커브

3.1 Degree 163 Binary Field

T = 4
p(t) = *t*^163+ *t*^7+ *t*^6+ *t*^3+ 1

3.1.1 Curve K-163 (WTLS 3번커브)

a = 1
r = 5846006549323611672814741753598448348329118574063
Polynomial Basis:
Gx = 2 fe13c053 7bbc11ac aa07d793 de4e6d5e 5c94eee8
Gy = 2 89070fb0 5d38ff58 321f2e80 0536d538 ccdaa3d9
Normal Basis:
Gx = 0 5679b353 caa46825 fea2d371 3ba450da 0c2a4541
Gy = 2 35b7c671 00506899 06bac3d9 dec76a83 5591edb2

3.1.2 Curve B-163

r = 5846006549323611672814742442876390689256843201587
Polynomial Basis:
b = 2 0a601907 b8c953ca 1481eb10 512f7874 4a3205fd
Gx = 3 f0eba162 86a2d57e a0991168 d4994637 e8343e36
Gy = 0 d51fbc6c 71a0094f a2cdd545 b11c5c0c 797324f1
Normal Basis:
s = 85e25bfe 5c86226c db12016f 7553f9d0 e693a268
b = 6 645f3cac f1638e13 9c6cd13e f61734fb c9e3d9fb
Gx = 0 311103c1 7167564a ce77ccb0 9c681f88 6ba54ee8
Gy = 3 33ac13c6 447f2e67 613bf700 9daf98c8 7bb50c7f

3.2 Degree 233 Binary Field

T = 2
p(*t*) = *t* 233 + *t* 74 + 1

3.2.1 Curve K-233 (10번커브)

a = 0

n = 3450873173395281893717377931138512760570940988862252126328087024741343

Polynomial Basis:

G x = 172 32ba853a 7e731af1 29f22ff4 149563a4 19c26bf5 0a4c9d6e efad6126

G y = 1db 537dece8 19b7f70f 555a67c4 27a8cd9b f18aeb9b 56e0c110 56fae6a3

Normal Basis:

G x = 0fd e76d9dcd 26e643ac 26f1aa90 1aa12978 4b71fc07 22b2d056 14d650b3

G y = 064 3e317633 155c9e04 47ba8020 a3c43177 450ee036 d6335014 34cac978

3.2.2 Curve B-233 (11번커브)

n = 690174634679056378743475586227702555583981273734501355\
5379383634485463

Polynomial Basis:

b = 066 647ede6c 332c7f8c 0923bb58 213b333b 20e9ce42 81fe115f 7d8f90ad

G x = 0fa c9dfcbac 8313bb21 39f1bb75 5fef65bc 391f8b36 f8f8eb73 71fd558b

G y = 100 6a08a419 03350678 e58528be bf8a0bef f867a7ca 36716f7e 01f81052

Normal Basis:

SEED = 74d59ff0 7f6b413d 0ea14b34 4b20a2db 049b50c3

b = 1a0 03e0962d 4f9a8e40 7c904a95 38163adb 82521260 0c7752ad 52233279

G x = 18b 863524b3 cdfefb94 f2784e0b 116faac5 4404bc91 62a363ba b84a14c5

G y = 049 25df77bd 8b8ff1a5 ff519417 822bfedf 2bbd7526 44292c98 c7af6e02

부록 2. 규격의 연혁

버전	제·개정일	제·개정내역
v1.00	2004년 9월	· "전자서명 알고리즘 규격"으로 제정
v1.10	2007년 4월	· 유·무선 전자서명 알고리즘 규격 통합
v1.20	2008년 10월	· 관련 국내 표준 및 규격 갱신 내용 반영 · 법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.30	2009년 9월	· 공인인증서 암호체계 고도화에 따른 알고리즘 변경 사항 반영