무선 키분배 알고리즘 규격

Wireless Key Distribute Algorithm Specification

2001. 8 (ver1.21)

한국정보보호진흥원

목 차

1.목적 79

2. 서명용 알고리즘(Signature Algorithms) 79

2.1 RSA 79

2.2 ECDSA 79

2.3 공개키 정보(Subject Public Key Information) 80

2.4 ECC 커브 81

2.5 암호화 알고리즘 82

2.6 해쉬 알고리즘 82

부록1. 무선 전자서명인증관리체계에서 지원하는 알고리즘의 커브 파라메터 84

무선 키 분배 알고리즘 규격
Wireless Key Distribute Algorithm Specification

1.목적

본 규격에서는 키분배인증서 서명에 지원되는 알고리즘과 해쉬에 대하여 기술하며 관련 표준을 명시한다.

2. 서명용 알고리즘(Signature Algorithms)

서명용 알고리즘은 인증기관이 키분배인증서를 생성하는 경우에 사용된다.

이를 위하여 전자서명인증관리체계에서 지원하는 키분배인증서 서명용 알고리즘은 다음과 같다.

2.1 RSA

RSA는 소인수 분해 문제의 어려움에 기반한 알고리즘으로 Rivest, Shamir, 및 Adleman 등이 개발하였다.

RSA의 구현은 인증서버, CP, 단말기의 생성과 검증을 Mandatory로 한다.

RSA의 사용 가능한 전자서명 방식에 대한 OID 정의는 다음과 같다.

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

RSA에서 지원하는 키의 길이는 1024비트 이상이어야 한다.

2.2 ECDSA

ECDSA는 타원곡선(elliptic curve)상에서 group을 정의하고 이에 대한 이산대수 계산의 어려움에 근거를 두고 있다. 타원 곡선 상에서의 이산대수 문제는 일반적인 군에서 정의되는 이산대수 문제보다 훨씬 어려우며, 이에 따라, 작은 키로도 RSA보다 높은 비도를 유지할 수 있다. ECDSA는 2000년 2월 8일에 발표된 FIPS 186-2 DSS에 새롭게 포함된 내용으로 타

원곡선 전자서명 알고리즘이다.

ECDSA의 구현은 인증서버, CP, 단말기의 생성과 검증을 Mandatory로 한다.

ECDSA의 사용 가능한 전자서명 방식에 대한 OID 정의는 다음과 같다.

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

ECDSA에서 지원하는 키의 길이는 160비트 이상이어야 한다.

2.3 공개키 정보(Subject Public Key Informa

2.3.1 공개키 알고리즘(Subject Public Key Algorithms)

공개키 알고리즘은 인증서가 포함하고 있는 공개키가 사용될 알고리즘이다.

이를 위하여 전자서명 인증관리체계에서 지원하는 공개키 알고리즘은 다음과 같다.

2.3.1.1 RSA

RSA의 사용 가능한 공개키 알고리즘에 대한 OID 정의는 다음과 같다.

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

RSA에서 지원하는 키의 길이는 1024비트 이상이어야 한다.

2.3.1.2 ECDH

ECDH는 타원곡선(elliptic curve)상에서 DH 키분배 알고리즘이다.

ECDH의 사용 가능한 공개키 알고리즘에 대한 OID 정의는 다음과 같다.

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

3. ECC 커브

ECC 커브는 ECDSA, ECDH 등에서 사용되는 ECC 커브이다.

이를 위하여 무선 전자서명인증관리체계에서 지원하는 ECC 커브에 대한 ASN.1 코드는 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,
 }
```

※ WTLS 3번 커브

```
sect163k1 : { iso(1) identified-organization(3) secg(132) curve(0)
              ellipticCurve 1 }
```

※ WTLS 5번 커브

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

※ WTLS 7번 커브

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

※ 커브구현

구분 \ 커브	WTLS 5번	WTLS 7번	WTLS 3번	FIPS 186-2	X9.62
인증 서버	M	M	M	H	H
CP 서버	M	M	M	O	O
단말기	M	O	O	O	O

M: Mandatory, O: Optional, H: Highly Recommend

4. 암호화 알고리즘

지원 가능한 암호화 알고리즘은 다음과 같다.

4.1 SEED

128비트 블록 암호알고리즘(SEED)은 128비트 암호키를 이용하여 메시지를 블록 단위로 암·복호화하는 알고리즘으로 데이터의 기밀성 등과 같은 기능을 제공하기 위해 사용될 수 있다.

SEED에서 지원하는 키의 길이는 128비트이어야 한다.

4.2 TripleDES

TripleDES에서 지원하는 키의 길이는 168비트이어야 한다.

5. 해쉬 알고리즘

해쉬 알고리즘은 기본적으로 메시지 인증에 사용되며 전자서명 알고리즘과 함께 전자서명 생성 및 검증에 사용된다.

지원 가능한 해쉬 알고리즘은 다음과 같다.

5.1 SHA-1

"Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard"에서 정의하고 있는 SHA-1은 미국 정부에서 개발하였으며 임의의 입력값에 대하여 160비트 해쉬값을 출력한다.

SHA-1에 대한 OID의 정의는 다음과 같다.

```
id-SHA1 OBJECT IDENTIFIER ::= {
  iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26
}
```

부록1. 무선 전자서명인증관리체계에서 지원하는 알고리즘의 커브 파라메터

1. 목적

무선 전자서명인증관리체계에서 지원하는 전자서명 알고리즘의 커브파라메터에 대하여 기술하며 관련 규격을 명시한다.

이를 위하여 전자서명인증관리체계에서 지원하는 알고리즘의 커브 파라메터 다음과 같다.

2. WTLS 권고 커브

○ 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

○ 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

3. X9.62 권고 커브

Field 2^163

f = 08 00000000 00000000 00000000 00000000 00000107

curve E : y^2 + xy = x^3 + ax^2 + b

○ ID c2pnb163v1 (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

○ 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

○ 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

4. FIPS 186-2 권고 커브

Degree 163 Binary Field

T = 4

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

○ Curve K-163 (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

○ 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