암호 알고리즘 규격

Encryption Algorithm Scheme Specification

v1.21

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

KCAC.TS.ENC v1.21

목 차

암호 알고리즘 규격
Encryption Algorithm Specification

1. 개 요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계 유·무선 공인인증서비스에서 사용되는 암호 알고리즘 규격을 정의한다.

2. 규격의 구성 및 범위

본 규격은 전자서명인증체계의 유·무선 공인인증서비스에서 사용되는 암호화 알고리즘을 나열하고 각각의 구현에 따른 요구사항을 정의한다.

첫 번째로 SEED 암호화 알고리즘 구현을 통한 전자서명키 암·복호화를 위한 키 및 초기 벡터 생성 방안 등을 마련하고, 전자서명인증체계에서 이를 구분하기 위하여 사용되는 식별명칭을 규정한다. (단, 본 규격은 [PKCS5]에서 정의하고 있는 PBKDF1 키 생성 함수를 사용할 경우만을 다룬다)

두 번째로 3-DES 암호화 알고리즘 구현 요구사항을 규정한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[PKCS5]	RSA Laboratories, PKCS#5(1999), *Password-Based Cryptography Standard*
[PKCS8]	RSA Laboratories, PKCS#8(1993), *Private-Key Information Syntax Standard*
[3-DES]	NIST, FIPS PUB 46-3(1999), *DATA ENCRYPTION STANDARD(DES)*

3.2 국내 표준 및 규격

[KCAC.TG.OID]	KISA, KCAC.TG.OID, *전자서명인증관리체계 OID 가이드라인* v1.30, 2008년

3.3 기타

해당사항 없음

4. 정의

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

4.1 전자서명법 용어 정의

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

가) 공인인증서
나) 공인인증기관
다) 가입자

4.2 용어의 정의

가) 유선 공인인증서비스 : 인터넷 기반의 전자거래를 위해 공인인증서를 이용하는 서비스
나) 무선 공인인증서비스 : 무선 단말기 기반의 전자거래를 위해 공인인증서를 이용하는 서비스
다) 인증기관 식별자 : 인증서 DN의 O(Organization) 값

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 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) PBES : Password Based Encryption Scheme, 패스워드 기반의 키 암호화 기법
나) PBKDF : Password Based Key Derivation Function, 패스워드 기반의 키 추출 함수
다) DK : Derived Key, 추출키
라) IV : Initial Vector, 초기 벡터
마) OID : Object Identifier, 객체 식별자

6. SEED 블록 암호 알고리즘을 위한 암호화 키(K) 및 초기 벡터(IV) 생성

공인인증시스템 및 가입자 설비는 가입자의 전자서명키가 패스워드 기반으로 암호화되어 저장될 수 있도록 SEED 블록 암호알고리즘을 구현할 것을 권고한다.

패스워드 기반의 안전한 전자서명키 암호화을 위해서는 [PKCS5]에서 정의한 PBES1 암호화 기법을 이용할 수 있다. PBES1는 PBKDF1 키생성 함수와 블록 암호화 알고리즘을 사용해야 한다. 이 장에서는 PBES1에서 정의하고 있

지 않은 SEED 블록 암호화 알고리즘을 사용하기 위하여 암호화 키(K)와 초기 벡터(IV)를 생성하는 방법을 정의한다.

6.1. PBKDF1

8 바이트의 솔트(salt)와 아이터레이션 카운트(iteration count)를 선택하고, PBKDF1에 패스워드(P), 솔트(S), 아이터레이션 카운트(c)를 적용하여 20 바이트의 추출키(DK)를 생성한다.

```
DK = PBKDF1(P, S, c, 20)
```

6.2. 암호화 키(K) 생성

생성된 추출키(DK)에서 처음 16바이트를 암호화 키(K)로 정의한다.

```
K = DK<0 . . 15>
```

6.3. 초기 벡터(IV) 생성

초기 벡터(IV)의 생성은 아래 두 가지 방식으로 이루어진다.

첫 번째, 추출키(DK)와 상관없이 16바이트의 초기 벡터(IV)는 아래와 같은 값(Hexadecimal로 표현)으로 고정하여 사용한다.

```
IV = 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35
(※ IV는 스트링값 "0123456789012345")
```

두 번째, 추출키(DK)에서 암호화 키(K)를 제외한 나머지 4바이트를 SHA-1으로 해쉬하여 20바이트의 값(DIV)을 생성하고, 그 중 처음 16바이트를 초기 벡터(IV)로 정의한다.

```
DIV = Hash(DK<16 .. 19>)
IV = DIV <0 .. 15>
```

6.4. 메시지 패딩(padding)

SEED 블록 암호화 알고리즘 적용에 필요한 메시지 패딩(padding)은 [PKCS5]

PBES1에서 정의한 방법을 사용하되 PS(padding String)은 16-(‖M‖ mod 16) 바이트의 길이로 구성된다. (‖M‖: 메시지의 길이(바이트))

```
‖M‖ mod 16=15일 때, PS = 01
‖M‖ mod 16=14일 때, PS = 02 02
                ...
‖M‖ mod 16=0일 때, PS = 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10
```

7. 객체 식별자(OID) 정의

생성된 암호화 키(K), 초기 벡터(IV)와 SEED 블록 암호화 알고리즘을 이용하여 암호화된 개인키 정보(Encrypted private-key information)는 [PKCS8]을 준수하여 아래와 같이 정의된다.

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
    encryptedAlgorithm        EncryptionAlgorithmIdentifier
    encryptedDate             EncrypedData }
```

EncryptedAlgorithmIdentifier는 암호화 알고리즘 객체 식별자(OID)와 함께 PBKDF1와 관련된 파라미터인 솔트(S)와 아이터레이션 카운트(c)로 구성된다.

현재, 전자서명인증체계에서 SEED 블록 암호화 알고리즘을 이용한 패스워드 기반의 개인키 암호화에 사용되는 객체 식별자(OID)는 6.3절의 초기 벡터(IV) 구현방법에 따라 두 가지로 구분하여 사용해야 하고, 가입자 소프트웨어는 이를 처리해야 한다.

1) 첫 번째, IV = "123456789012345"로 고정하여 초기 벡터를 사용할 때

```
id-seedCBC OBJECT IDENTIFIER ::= {1 2 410 200004 1 4}
```

2) 두 번째, DIV = Hash(DK<16 .. 19>), IV = DIV <0 .. 15>를 이용하여 초기 벡터(IV)를 사용할 때

```
id-seedCBCWithSHA1 OBJECT IDENTIFIER ::= {1 2 410 200004 1 15}
```


8. 3-DES 블록 암호화 알고리즘 요구사항

공인인증시스템 및 가입자 설비는 가입자의 전자서명키가 패스워드 기반으로 암호화되어 저장될 수 있도록 3-DES 블록 암호 알고리즘을 구현하여야 한다.

3-DES 구현에 관련된 암호화 키 생성, 초기 백터 생성, 메시지 페딩, 개별 식별자 (OID)정의 등은 [3-DES]를 참조한다.

부록 1. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2004년 6월	・“SEED 알고리즘을 이용한 패스워드 기반의 개인키 암호화 기술규격” 제정
v1.10	2007년 4월	・“암호 알고리즘 규격”으로 규격명 변경 ・3-DES 블록암호 알고리즘 구현 요구사항 추가
v1.20	2008년 10월	・관련 국내 표준 및 규격 갱신 내용 반영 ・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.21	2009년 9월	・공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정