전자서명키 보호 기술규격

Cryptographic Key Protection Specification

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명키 보호 기술규격

Cryptographic Key Protection Specification

1. 개 요

본 규격에서는 전자서명법 상에서 구축된 전자서명인증체계에서 공인인증기관이 제공하는 키 관리설비에 적용되는 전자서명키 보호기술 관련 표준 및 규격을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [FIPS140-2]의 보안등급 3을 준용하여 전자서명키 관리에 적용되어야 하는 기술사항을 정의하고 있다. 따라서, [FIPS140-2]와 [FIPS140-1]의 보안등급 3이상 인증을 받은 전자서명키 관리 암호모듈은 본 규격을 모두 만족하는 것으로 간주한다.

본문에서는 전자서명키를 보호하기 위한 일반적 요구사항과 공인인증기관에 적용된 전자서명 생성키를 보호하기 위한 기술적 요구사항들을 명시하고 있다.

본 규격에 정의된 전자서명키 관리 설비에 대한 보안요구사항은 추후 관련 법규 및 지침이 제정되면 그 법규 및 지침을 준수한다. 본 규격은 암호모듈내의 전자서명키 관리에 해당하는 부분만을 정의한다.

3. 관련 표준

3.1 국외 참조권고 및 표준

[FIPS140-2] NIST FIPS PUB 140-2 (2001), *Security Requirements for Cryptographic Modules, NIST(National Institute of Standards and Technology, US)*

[DTR] NIST DTR(2004. 03. 02), *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*

[WD19790] ISO/IEC 2nd Working Group Draft 19790 [SC 27 N 3807] *Information Technology-Secuirty Techniques-Security Requirements for Cryptographic Modules (2004. 04)*

3.2 국내 표준 및 규격

해당사항 없음

4. 정의

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) 전자서명생성키

4.2 용어의 정의

본 규격에서 적용되는 용어의 정의는 다음과 같다.

가) 암호모듈 : 암호기술을 하드웨어·소프트웨어·펌웨어 등의 형태로 구현한 장치
나) 중요보안파라메터 : 비밀키, 전자서명키, ID/PW, PIN, Credentials 등과 같이 공개나 수정에 의해 암호모듈의 보안성을 무너뜨릴 수 있는 보안관련 정보

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 전자서명키 관리설비의 요구사항 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

해당사항 없음

6. 전자서명키 관리 보안 요구사항

6.1 일반적 암호모듈 요구사항

전자서명키 관리에 대한 보안 요구 사항은 암호모듈에서 사용되는 전자서명키와 그 외 중요보안파라메터들의 생성 및 삭제 등 생명주기에 적용된다.

본 규격에서 의미하는 전자서명키 관리는 난수생성 및 키 생성, 설정, 분배, 입출력, 저장 및 삭제를 포함한다.

전자서명생성키 및 그 외 중요보안파라메터는 인가되지 않은 노출, 변경 그리고 치환으로부터 암호모듈 내에서 보호되어야 하며, 전자서명검증키는 인가되지 않은 변경 및 치환으로부터 암호모듈 내에서 보호되어야 한다.

암호모듈 명세서는 암호모듈에서 이용되는 모든 전자서명키 및 그 외 중요보안파라메터를 규정해야 한다.

6.2 난수 생성기

암호모듈은 전자서명키 생성 등의 연산을 위해 난수 생성기를 사용할 수 있으며, 이 경우 전자서명인증체계 난수 생성기 시험에 통과하여야 한다.

초기벡터(Initial Vector) 및 초기값 키(Seed Key)는 같은 값을 가져서는 안되다.

암호모듈 명세서는 암호모듈에 이용되는 모든 난수생성기 각각을 설명하여야 한다.

6.3 키 생성

암호모듈은 내부적으로 전자서명키를 생성할 수 있다. 이 경우 전자서명키 생성은 전자서명인증체계에서 정의된 암호 알고리즘을 사용하여야 하며, 동 체계에서 정의된 키 생성 방법을 이용해 생성되어야 한다.

암호모듈 명세서는 암호모듈에 이용되는 키 생성 방법을 규정해야 한다.

6.4 키 설정

키 설정이라 함은 키 전송이나 키 동의 등의 방법을 통하여 생성된 비밀키 및 전자서명키를 정당한 객체가 소유하는 것을 말한다.

키 설정은 SSL, TLS, IPSec등 공개키 알고리즘이 프로토콜에 적용된 자동화된 방법과 수동으로 전달된 키를 주입장치(Loading Device)를 이용하여 설정하는 수동의 방법 또는, 자동화된 방법과 수동방법의 조합에 의해 수행될 수 있다. 키 설정 방법이 암호모듈에 이용되고 있는 경우에는, 전자서명인증체계에서 정의된 키 설정 기술만이 사용되어야 한다.

이 경우 전송되는 전자서명키는 6.5절의 키 입출력 요구사항을 만족해야한다. 특히, 전자서명키가 공유된 중간 값으로부터 유도되는 경우에 한하여, 공유된 값은 6.5절의 키 입출력 요구 사항을 만족할 필요는 없다.

암호모듈 명세서는 암호모듈에 이용되는 키 설정 방법을 규정해야 한다.

6.5 키 입력 및 출력

전자서명키는 암호모듈에 입력되거나 암호모듈로부터 출력될 수 있다. 만일 전자서명키가 암호모듈에 입력 또는 암호모듈로부터 출력되는 경우, 전자서명키 입출력은 인가된 운영자의 키보드 조작 등에 방법을 통한 직접적인 입출력 방법 또는 스마트카드/토큰, PC카드, 다른 전자적인 키 주입장치를 이용한 전자적 방법을 사용하여 수행되어야 한다.

초기값 키(Seed Key)가 키 생성 중에 입력되는 경우에는, 전자서명키와 같은 방법으로 입력되어야 한다.

암호모듈에 입출력되고 사용되는 모든 비밀키 및 전자서명키는 전자서명인증체계의 암호 알고리즘을 이용해 암호화되어야 한다. 전자서명검증키는 평문 형식으로 암호모듈에 입력되거나 출력될 수 있다. 암호모듈은 입력 또는 출력되는 전자서

명키와 비밀키를 사람, 그룹, 또는 프로세스 등 키 사용이 인가된 객체만 접근할 수 있도록 해야한다.

수동으로 입력되는 전자서명키는 정확성을 위해 암호모듈에 입력되는 과정 중에 검증되어야한다. 키 입력 중에 수동으로 입력되는 암호화된 전자서명키 값은, 시각적인 검증과 정확성을 향상시키기 위해 일시적으로 표시될 수 있다. 하지만, 전자서명키 평문 값은 표시되어서는 안되다.

암호모듈 명세서는 암호모듈에 이용되는 키 입력 방법 및 키 출력 방법을 규정해야 한다.

자동화된 키 설정 방법에 의해 설정된 비밀키 및 전자서명키 입출력은 암호화된 형식으로 수행되어야 한다.

수동의 방법을 이용해 설정된 비밀키와 전자서명키는 평문 형식으로 암호모듈에 입력 또는 출력될 수 있다. 이 경우 암호화된 형식 또는, 분산지식(Split Knowledge)의 방법을 이용하여 암호모듈에 입력 또는 암호모듈로부터 출력되어야 한다.

분산지식 방법이 이용되는 경우,

- 암호모듈은 비밀키 및 전자서명키의 입력 또는 출력시에 각각의 분산정보 관리자들을 별도로 인증해야 한다.
- 평문의 비밀키 및 전자서명키는 부주의로 인한 저장, 결합, 또는 그 외의 수단에 의해 위험에 노출될 수 있다. 따라서, 평문의 비밀키 및 전자서명키는 신뢰경로 또는 직접 접속된 케이블을 통하여 암호모듈에 입력 또는 출력되어야 한다.
- 원래의 비밀키 및 전자서명키를 재구성하기 위해 적어도 2 개 이상의 분산정보가 요구되어야 한다.
- 암호모듈 명세서는 n 개의 비밀키 및 전자서명키 분산정보가 원래의 키를 재구성하는데 필요한 경우, 어떠한 n-1 개의 키 분산정보도 원래 키 길이 이외에 어떠한 정보도 제공하지 않는다는 것을 증명해야 한다.
- 암호모듈 명세서는 암호모듈에 적용되는 분산지식 방법 및 절차를 규정해야 한다.

6.6 키 저장

암호모듈 내에 저장되어 있는 전자서명키는 평문의 형식 또는 암호화된 형식으로 저

장되어야 한다. 평문의 비밀키 및 전자서명키는 인가되지 않은 운영자에 의한 접근을 허용해서는 안되다.

암호모듈은 저장된 전자서명키와 비밀키를 사람, 그룹, 또는 프로세스 등 키 사용이 인가된 객체만이 접근할 수 있도록 해야한다.

암호모듈 명세서는 암호모듈에 이용되는 키의 저장 방법을 규정해야 한다.

6.7 키의 삭제

암호모듈은 암호모듈 내에서 평문의 비밀키 및 전자서명키, 그 외 보호되어 있지 않은 중요보안파라메터 모두를 삭제하기 위한 방법을 제공하여야 한다. 또한 안전한 장치에 내장되고 본 규격에 의해 검증된 모듈 안에서 물리적, 논리적으로 보호되는 암호화된 비밀키 및 전자서명키, 중요보안파라메터는 삭제하지 않아도 된다.

암호모듈 명세서는 암호모듈에 이용되는 키의 삭제 방법을 규정해야 한다.

부록 1. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2004년 8월	·“전자서명키 보호 기술규격” 제정
v1.10	2008년 10월	·관련 국내 표준 및 규격 갱신 내용 반영 ·법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.11	2009년 9월	·공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정