KSKSKSKS
KSKSKSK
KSKSKS
KSKSK
KSKS
KSK
KS

KS X ISO/IEC 19790

KS

정보기술 — 보안기술 — 암호모듈 보안 요구사항

KS X ISO/IEC 19790:2015

산업통상자원부 국가기술표준원

2015년 8월 4일 개정

http://www.kats.go.kr

심 의 : 정보기술 기술심의회

	성 명	근 무 처	직 위
(회 장)	김 형 준	한국전자통신연구원	센 터 장
(위 원)	강 현 국	고려대학교	교 수
	김 재 성	한국인터넷진흥원	수 석
	류 관 희	충북대학교	교 수
	박 춘 식	서울여자대학교	교 수
	박 호 진	한국전자통신연구원	책 임
	오 경 희	TCA 서비스	대 표
	전 진 옥	비트컴퓨터	대 표
	정 혁	한국전자통신연구원	책 임
	정 혜 정	평택대학교	교 수
(간 사)	배 승 호	국가기술표준원 표준정책국 전기전자표준과	

개정 작성 : 암호모듈 연구위원회

	성 명	근 무 처	직 위
(위원장)	최 희 봉	국가보안기술연구소	책임연구원
(위 원)	이 훈 재	동서대학교	교 수
	이 옥 연	국민대학교	교 수
	홍 석 희	고려대학교	교 수
	최 명 길	중앙대학교	교 수
	염 용 진	국민대학교	교 수
	한 상 윤	국가보안기술연구소	선임연구원
(간 사)	배 승 호	국가기술표준원	연 구 사

표준열람 : 국가표준종합정보센터 (http://www.standard.go.kr)

제 정 자 : 산업통상자원부 국가기술표준원장　　제　　정 : 2007년 12월 26일
개　　정 : 2015년 8월 4일　　국가기술표준원 고시　제 2015-0342 호
심　　의 : 산업표준심의회 정보기술 기술심의회
원안작성협력 : 암호모듈 연구위원회

목 차

개 요

이 표준은 2012년 제2판으로 발행된 ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules를 기초로, 기술적 내용 및 대응국제표준의 구성을 변경하지 않고 작성한 한국산업표준이다.

한국산업표준

KS X ISO/IEC 19790:2015

정보기술 — 보안기술 — 암호모듈 보안 요구사항

Information technology — Security techniques — Security requirements for cryptographic modules

1 적용범위

이 표준은 컴퓨터와 통신 시스템 내 중요 정보를 보호하는 보안 시스템에서 사용하는 암호모듈을 위한 보안 요구사항을 명시한다. 이 표준은 넓은 범위의 중요 데이터(예: 행정 정보, 자금 이체 정보, 생명 보호 정보, 개인 신상 정보, 정부가 사용하는 중요한 정보)와 다양한 응용 환경(예: 보호되는 시설, 사무실, 이동식 매체, 전혀 보호되지 않는 장소)에 따라, 적용하고자 하는 암호모듈을 4가지 보안수준으로 구분한다. 이 표준은 11개 요구사항 영역별 4개의 보안수준을 명시하며, 각 보안수준은 이전 보안수준보다 높은 보안수준을 나타낸다(보안수준 1: 가장 낮은 수준, 보안수준 4: 최고 높은 수준).

이 표준은 보안을 제공하는 암호모듈이 충족해야 하는 보안 요구사항을 명시하며, 암호모듈이 이 표준에 적합하다고 해서 특정 모듈이 안전하거나 정보를 보호하는 모듈이 정보 소유자에게 충분하고 수용할 만하다고 보장하지는 않는다. 따라서 암호모듈 운영자는 보호해야 할 정보에 적합한 보안기능들을 사용해야 하고, 사용자는 잔존 위협들을 인지하고 있어야 한다.

2 인용표준

다음의 인용표준은 이 표준의 적용을 위해 필수적이다. 발행연도가 표기된 인용표준은 인용된 판만을 적용한다. 발행연도가 표기되지 않은 인용표준은 최신판(모든 추록을 포함)을 적용한다.

이 표준의 **부속서** C와 D, E, F에서 나열된 문서

3 용어와 정의

이 문서의 목적을 위하여 다음의 용어와 정의를 적용한다.

3.1
접근통제목록 (access control list, ACL)
대상물에 대한 접근 허용 목록

3.2
관리자 안내서 (administrator guidance)
암호관리자 또는 기타 관리자가 암호모듈의 정확한 구성, 유지보수 및 관리를 위해 사용되는 문서

3.3
검증기관 (approval authority)
암호모듈 시험 결과를 확인하고 검증필 암호모듈로 승인하는 업무를 담당하는 기관

3.4
검증대상 데이터 인증기술 (approved data authentication technique)
검증대상 암호알고리즘 목록에 포함된 전자서명, 메시지 인증 코드 또는 키 해시(예: HMAC)

3.5
검증대상 무결성기술 (approved integrity technique)
검증대상 암호알고리즘 목록에 포함된 해시, 메시지 인증 코드 또는 전자서명

3.6
검증대상 동작모드 (approved mode of operation)
검증대상 암호알고리즘을 사용하는 서비스를 적어도 하나 포함하는 서비스의 집합. 비보안 서비스도 포함할 수 있다.

비고 1 CBC 등과 같은 검증대상 암호알고리즘의 동작모드와 혼동하지 않는다.
비고 2 비검증대상 암호알고리즘 혹은 프로세스는 제외한다.

3.7
검증대상 암호알고리즘 (approved security function)
블록 암호, 스트림 암호, 대칭/비대칭 키 암호알고리즘, 메시지 인증 코드, 해시함수뿐만 아니라 난수 발생기, 개체 인증 및 SSP 생성/설정과 같은 알고리즘. 검증기관이 선정한 암호알고리즘을 검증대상 암호알고리즘이라 하며 그 외 암호알고리즘을 비검증대상 암호알고리즘이라 한다.

부속서 C에서 참조되는 암호알고리즘

3.8
비대칭 암호기술 (asymmetric cryptographic technique)
공개키와 개인키의 연관된 변환을 이용하는 암호기술

비고 주어진 공개키에 의한 변환으로부터 제한된 시간과 계산 능력하에서 개인키에 의한 변환을 유도하는 것이 계산 불가능한 특성을 갖는다.

3.9
생체인식 (biometric)
운영자의 신원을 인식하거나 또는 주장된 신원을 검증하는 데 사용되는 측정 가능하고 물리적 특성을 갖는 개인의 행동적 특성

3.10
우회 능력 (bypass capability)
부분적 암호 기능 또는 전체적 암호 기능을 우회할 수 있는 서비스 능력

3.11
인증서 (certificate)
인증기관(CA)의 개인키나 비밀키를 이용하여 위조될 수 없도록 만들어진 개체의 데이터

비고 검증기관이 발행한 모듈 검증서와 혼동하지 않는다.

3.12
손상 (compromise)
핵심 보안매개변수의 인가되지 않은 노출, 변경, 대체, 사용 또는 공개 보안매개변수의 인가되지 않은 노출, 변경, 대체

3.13
조건부 자가시험 (conditional self-test)
명세된 조건이 발생할 때 암호모듈이 수행하는 시험

3.14
기밀성 (confidentiality)
중요 정보가 인가되지 않은 개체로부터 수정, 노출, 대체되지 않는 성질

3.15
형상관리시스템 (configuration management system, CMS)
암호모듈의 하드웨어, 소프트웨어 및 개발 문서에서 이루어진 변경을 통제함으로써 보안 특성 및 보증을 관리하는 시스템

3.16
제어 정보 (control information)
모듈 동작을 지시하기 위해 암호모듈에 입력되는 정보

3.17
핵심 보안매개변수 (critical security parameter, CSP)
노출되거나 변경되면 암호모듈의 보안을 손상시킬 수 있는 보안 관련 정보(예: 비밀키/개인키, 패스워드나 개인식별번호와 같은 인증 데이터)

보기 비밀키 및 개인키 및 패스워드, PIN, 인증서 등과 같은 인증 데이터

비고 CSP는 평문으로 또는 암호화되어 존재할 수 있다.

3.18
암호관리자 (crypto officer)
암호모듈의 초기화 또는 관리 기능을 수행하기 위해 암호모듈에 접근하는 개체 또는 프로세스

3.19
암호알고리즘 (cryptographic algorithm)
암호키를 포함할 수 있는 입력에 대하여 출력을 생성하는 정의된 계산 절차

3.20
암호경계 (cryptographic boundary)
암호모듈의 명시적으로 정의된 연속 경계(하드웨어, 소프트웨어 및/또는 펌웨어 구성 요소의 집합). 암호모듈의 모든 구성 요소를 포함한다.

3.21
암호 해시함수 (cryptographic hash function)
임의의 길이를 갖는 이진 문자열을 고정 길이를 갖는 이진 문자열에 매핑하는 함수로, 동일한 해시 값을 갖는 두 개의 다른 값을 찾는 것이 계산적으로 불가능한 함수

3.22
암호키 (cryptographic key)
암호 변환(암호화, 복호화, 인증 코드 연산, 서명 생성, 서명 검증 등)을 실행하기 위한 암호알고리즘에 사용되는 매개변수

보기 암호 변환에는 암호화, 복호화, 암호 검증 기능 연산, 서명 생성, 서명 검증 등을 포함하지만 이에 국한하지 않는다.

3.23
암호키 구성 요소 (cryptographic key component)
평문 CSP를 만들거나 또는 암호 기능을 수행하기 위해 검증대상 암호알고리즘에서 다른 키 구성 요소와 사용되는 매개변수

3.24
암호모듈 (cryptographic module)
암호알고리즘(암호알고리즘과 키 생성을 포함)을 구현한 하드웨어, 소프트웨어 및/또는 펌웨어의 집합. 암호경계 내에 포함되어 있다.

3.25
암호모듈 보안정책 (cryptographic module security policy)
이 표준의 요구사항으로부터 유도된 규칙과 검증기관이 추가한 규칙을 포함하여 암호모듈을 운영할 때 준수해야 할 보안 규칙의 명세

비고 **부속서** B 참조

3.26
데이터 경로 (data path)
데이터가 전달되는 물리적 또는 논리적 경로

비고 물리적 데이터 경로는 여러 개의 논리적 데이터 경로에 의해 공유될 수 있다.

3.27
제한 기능 동작 (degraded operation)
오류 상태에서 정상 상태로 복귀할 때 알고리즘, 보안기능, 서비스 또는 프로세스의 전체 집합 중 일부 집합만이 사용 가능하거나 또는 구성 가능한 운영

3.28
차분전력 분석 (differential power analysis, DPA)
암호연산과 상관관계가 있는 정보를 추출하기 위해 암호모듈의 전력 소비 변화를 분석

3.29
전자서명 (digital signature)
적절히 구현되었을 때 다음의 서비스를 제공하는 데이터의 암호학적 변환의 결과

- 발신 인증
- 데이터 무결성
- 서명자 부인 봉쇄

3.30
직접 주입 (direct entry)
키보드 등과 같은 장치를 이용하여 SSP 또는 키 구성 요소를 암호모듈에 입력

3.31
개별 서명 (disjoint signature)
코드의 전체 세트를 함께 나타내는 한 개 이상의 서명

3.32
전자기 방사 (electromagnetic emanations, EME)
정보 처리 장치에 의해 전송, 수신 또는 처리되는 정보를 탈취하여 분석하면 잠재적으로 노출시킬 수 있는 신호

3.33
전자적 주입 (electronic entry)
전자식 방법을 사용하여 암호모듈에 SSP 혹은 키 구성 요소를 주입

비고 키의 운영자는 주입되는 키의 값을 알지 못한다.

3.34
포괄 서명 (encompassing signature)
코드의 전체 세트에 대한 단일 서명

3.35
암호화된 키 (encrypted key)
평문 상태인 키를 숨기기 위해서, 키 암호용 키와 검증대상 암호알고리즘을 사용하여 암호화된 암호키

비고 키는 보호된 것으로 간주한다.

3.36
개체 (entity)
사람, 그룹, 장치 또는 프로세스

3.37
엔트로피 (entropy)
폐쇄 시스템 내 무질서, 난수성, 변화성을 측정

비고 난수 X의 엔트로피는 X 관찰로부터 얻을 수 있는 정보량의 수학적 측정값이다.

3.38
환경장애보호 (environmental failure protection, EFP)
모듈의 정상 동작 범위를 벗어난 환경 조건에서 암호모듈의 보안 손상을 보호하는 기능 사용

3.39
환경장애시험 (environmental failure testing, EFT)
모듈의 정상 동작 범위를 벗어난 환경 조건에서 암호모듈의 보안 손상이 발생하지 않음을 보증하는 특정 방법 사용

3.40
오류탐지코드 (error detection code, EDC)
데이터로부터 계산된 값으로, 의도되지 않은 데이터 변경을 탐지하도록 설계된 정보의 부가 비트로 구성된 값

3.41
실행 가능한 코드양식 (executable form)
모듈의 운영환경에 의해 소프트웨어 또는 펌웨어가 관리 및 통제되는 코드양식이며, 컴파일(예: 비소스 코드, 객체 코드 혹은 적기 컴파일 코드)이 필요 없는 코드양식

3.42
고장 유도 (fault induction)
과도 전압, 방사, 레이저 또는 클럭 왜곡 기술을 적용하여 하드웨어의 동작 변경을 유도하는 기술

3.43
유한상태모델 (finite state model, FSM)
유한한 입력 사건 집합, 유한한 출력 사건 집합, 유한한 상태 집합에 대하여 상태와 입력을 출력에 매핑하는 함수, 상태와 입력을 상태에 매핑하는 함수, 초기 상태를 서술한 명세서로 구성되며, 순차적으로 동작하는 수학적 모델

3.44
펌웨어 (firmware)
암호경계 내 하드웨어에 저장된 암호모듈의 실행 코드. 변경 불가 또는 제한된 운영환경에서 실행 중 동적으로 작성되거나 변경될 수 없다.

보기 저장 하드웨어에는 PROM, EEPROM, FLASH, HDD 등이 포함되지만 이에 국한하지 않는다.

3.45
펌웨어 모듈 (firmware module)
펌웨어 단독으로 구성된 모듈

3.46
기능명세 (functional specification)
운영자에게 보이는 포트와 인터페이스를 상위 수준으로 명시한 문서 및 암호모듈의 동작 방법을 상위 수준으로 명시한 설명

3.47
기능시험 (functional testing)
기능명세에서 정의된 바와 같이 암호모듈 기능을 시험

3.48
하드/경도 (hard/hardness)
금속 또는 다른 재료의 파손 또는 긁힘, 곡손에 대한 상대적 저항. 물리적으로 강하고 견고하며 내구력이 있는 상태

비고 또 다른 물체에 의해 관통될 재료의 상대적 저항

3.49
하드웨어 (hardware)
프로그램과 데이터를 처리하기 위해 사용된 암호경계 내 물리적 장치/구성 요소

3.50
하드웨어 모듈 (hardware module)
기본적으로 하드웨어로 구성되고 또한 펌웨어도 포함될 수 있는 모듈

3.51
하드웨어 모듈 인터페이스 (hardware module interface, HMI)
요청된 서비스 일부분으로서 모듈의 암호경계로 입력되거나 출력되는 매개변수를 포함하여, 하드웨어 모듈 서비스를 요청하는 데 사용되는 명령어의 전체 집합

3.52
해시값 (hash value)
암호학적 해시함수의 출력값

3.53
하이브리드 모듈 (hybrid module)
소프트웨어 구성 요소 또는 펌웨어 구성 요소와 하드웨어 구성 요소의 합성 부분으로 암호경계를 정의하는 모듈

3.54
하이브리드 펌웨어 모듈 인터페이스 (hybrid firmware module interface, HFMI)
요청된 서비스 일부분으로서 모듈의 암호경계로 입력되거나 출력되는 매개변수를 포함하여, 하이브리드 펌웨어 모듈 서비스를 요청하는 데 사용되는 명령어의 전체 집합

3.55
하이브리드 소프트웨어 모듈 인터페이스 (HSMI, hybrid software module interface)
요청된 서비스 일부분으로서 모듈의 암호경계로 입력되거나 출력되는 매개변수를 포함하여, 하이브리드 소프트웨어 모듈 서비스를 요청하는 데 사용되는 명령어의 전체 집합

3.56
입력 데이터 (input data)
암호모듈로 입력되는 정보로서 검증대상 암호알고리즘에 의한 변환 혹은 계산에 사용할 수 있는 정보

3.57
무결성 (integrity)
데이터가 비인가 및 미탐지 방법으로 변경 또는 삭제되지 않았음을 나타내는 속성

3.58
인터페이스 (interface)
논리적 정보 흐름을 위해 모듈에 접근할 수 있는 암호모듈의 논리적 출입 포인트

3.59
키 합의 (key agreement)
두 명 이상의 참가자가 정보를 이용해 키를 도출하는 SSP 설정 절차. 상대방의 참여 없이 키값을 독립적으로 사전에 결정하지 못한다.

3.60
키 암호화 키 (key encryption key, KEK)
키를 암호화 또는 복호화하는 데 사용하는 암호키

3.61
키 로더 (key loader)
하나 이상의 평문 SSP, 키 구성 요소 또는 암호화된 SSP, 키 구성 요소를 저장할 수 있는 능력을 가지며, 요청 시 암호모듈에 전송할 수 있는 독립 저장 장치

비고 키 로더는 수동으로 동작된다.

3.62
키 관리 (key management)
보안정책에 의거한 키 요소의 생성, 등록, 인증, 등록 취소, 분배, 설치, 저장, 보존, 폐기, 유도 및 파기에 대한 관리

3.63
키 전송 (key transport)
키를 자동화 방식을 사용하여 하나의 개체에서 다른 개체로 안전하게 전송하는 것.

3.64
제한된 운영환경 (limited operational environment)
소프트웨어/펌웨어 로드 시험을 성공적으로 통과하도록 통제된 펌웨어 변경만을 수용하도록 설계된 운영환경

3.65
상세 수준 시험 (low-level testing)
암호모듈의 개별 구성 요소 또는 구성 요소 그룹과 그 물리적 포트와 논리적 인터페이스를 시험

3.66
유지보수 역할 (maintenance role)
물리적 또는 논리적 유지보수 서비스를 수행하는 역할

보기 유지보수 서비스는 하드웨어와/또는 소프트웨어 진단이 포함되지만 이에 국한하지 않는다.

3.67
수동 (manual)
사람(운영자)의 조작을 요구

3.68
메시지 인증 코드 (message authentication code, MAC)
사고나 고의로 데이터 변경이 발생하였을 경우 이를 탐지하기 위해 대칭키를 사용하여 데이터를 체크섬한 값이며, 검증대상 암호알고리즘을 이용하여 생성되며 메시지를 인증하기 위한 인증값

보기 해시 기반 메시지 인증 코드

3.69
마이크로코드 (microcode)
실행 가능한 프로그램 명령에 대응되는 프로세서 명령

보기 어셈블러 코드

3.70
최소 엔트로피 (minimum entropy)
최악 상태의 샘플 엔트로피 추정치 결정 시 유용한 엔트로피의 한계

3.71
변경 가능한 운영환경 (modifiable operational environment)
통제되지 않은 소프트웨어(즉, 신뢰할 수 없는)를 포함할 수 있는 기능적 변경을 수용하도록 설계된 운영환경

3.72
다중 요소 인증 (multi-factor authentication)
최소 두 가지의 독립적 인증 요소를 갖는 인증

비고 1 인증 요소는 한 개체의 신원을 인증 또는 검증하는 데 사용되는 정보 및 프로세스의 일부이다.
비고 2 독립적 인증 요소 분류: 본인이 알고 있는 것, 본인이 소유하고 있는 것, 본인의 특성

3.73
다중칩 내장 암호모듈 (multiple-chip embedded cryptographic module)
그 안에 두 개 이상의 집적회로 칩이 서로 연결되어 있고 물리적으로 보호되지 않은 봉함 또는 제품 내 내장된 물리적 형체

보기 어댑터와 확장 보드

3.74
다중칩 독립형 암호모듈 (multiple-chip standalone cryptographic module)
그 안에 두 개 이상의 집적회로 칩이 서로 연결되어 있고 전체 봉함이 물리적으로 보호되는 물리적 형체

보기 암호 라우터 또는 안전한 무선

3.75
비관리자 안내서 (non-administrator guidance)
암호모듈을 검증대상 동작모드에서 운영하기 위해 사용자와/또는 그 외 비관리자가 사용하는 문서

비고 비관리자 안내서는 암호모듈의 암호알고리즘을 서술하고 있으며 암호모듈을 안전하게 사용하는 정보 및 절차를 서술하고 있다. 비관리자 안내서는 훈령, 지침 및 경고를 포함한다.

3.76
비침투 공격 (non-invasive attack)
모듈 암호경계 내 구성 요소와 직접적인 물리적 접촉 없이 암호모듈에서 수행할 수 있는 공격

비고 암호모듈 상태를 변경 또는 교체하지 않는 공격

3.77
변경 불가능한 운영환경 (non-modifiable operational environment)
펌웨어 교체를 허용하지 않도록 설계된 운영환경

3.78
비보안 관련 (non-security relevant)
이 표준 범위 내에서 다루지 않는 요구사항으로, 암호모듈의 운영에 간섭하거나 방해하지 않는 암호

경계 내에 있는 하드웨어, 펌웨어, 소프트웨어 구성 요소

3.79
정상 동작 (normal operation)
알고리즘, 서비스 또는 프로세스의 전체 집합을 사용할 수 있거나 구성을 설정할 수 있는 동작

3.80
불투명 (opaque)
빛(즉, 400 nm～750 nm 파장 범위의 가시 스펙트럼 범위 내 빛)이 통과할 수 없고, 투명하지 않고, 가시 스펙트럼 내에서 반투명으로 보이지 않음.

3.81
운영환경 (operational environment)
모듈이 안전하게 운영할 수 있는 운영체제 및 하드웨어 플랫폼으로 구성된 모든 소프트웨어와 하드웨어 집합

3.82
동작 상태 (operational state)
운영자가 서비스 또는 기능을 요청하고 암호모듈의 데이터 출력 인터페이스를 통하여 데이터가 출력될 수 있는 상태

3.83
운영자 (operator)
한 개 이상 역할을 수행할 권한을 갖는 개인 또는 그 개인을 대신하여 작동하는 프로세스(주체)

3.84
출력 데이터 (output data)
암호모듈이 수행한 후 만들어진 정보 또는 계산 결과

3.85
부식 방지 (passivation)
반도체 교차점 또는 표면, 구성 요소 또한 검출 및 보호 수단을 포함하기 위해 제조된 집적회로의 반응 과정의 효과

보기 이산화규소 또는 인 유리

비고 부식 방지는 회로의 행태를 수정할 수 있다. 부식 방지 재료는 기술에 따라 좌우된다.

3.86
패스워드 (password)
신원을 인증 또는 접근 권한을 검증하는 데 사용되는 문자열

보기 문자, 숫자, 기타 기호

3.87
개인식별번호 (personal identification number, PIN)
신원을 인증하는 데 사용되는 번호 코드

3.88
물리적 보호 (physical protection)

물리적 수단을 사용하여 암호모듈, CSP 및 PSP를 보호하는 것.

3.89
평문키 (plaintext key)
암호화되지 않은 암호키 또는 보호용으로 사용할 수 없는 비검증대상 방식에 의해 난독화된 암호키

3.90
포트 (port)
암호모듈에 접근하는 데 제공되는 물리적/논리적 입구와 출구

3.91
동작 전 자가시험 (pre-operational self-test)
암호모듈에 전원이 들어온 시간 또는 인스턴스화된(전원 꺼짐, 리셋, 리부팅, 처음 시작, 정전 후) 시간과 동작 상태로 천이된 시간 사이에 수행되는 시험

비고 인스턴스화란 컴퓨터 내에서 실행시킬 수 있는 실행 파일을 만드는 것을 말한다.

3.92
개인키 (private key)
비대칭 암호알고리즘과 함께 사용되며, 하나의 개체(개인키를 사용하는 주체)와 유일하게 결합되는 암호키. 공개되어서는 안 된다.

비고 비대칭 서명 시스템의 경우 개인키는 서명 변환을 정의한다. 비대칭 암호화 시스템의 경우 개인키는 복호화 변환을 정의한다.

3.93
생산 등급 (production-grade)
운영 명세를 만족하도록 시험되었던 제품, 구성 요소 또는 소프트웨어

3.94
공개키 (public key)
비대칭 암호알고리즘과 함께 사용되며, 하나의 개체(공개키를 사용하는 주체)와 유일하게 결합되는 암호키. 공개가 가능하다.

비고 1 비대칭 서명 시스템의 경우 공개키는 검증 변환을 정의한다. 비대칭 암호화 시스템의 경우 공개키는 암호화 변환을 정의한다. '공개적으로 알려진' 키는 누구에게나 공개될 필요는 없다. 이 키는 사전에 명시된 그룹의 모든 회원에게만 공개될 수 있다.
비고 2 이 표준에서 공개키는 CSP에서 제외한다.

3.95
공개키 인증서 (public key certificate)
개체를 유일하게 식별하는 데이터, 개체의 공개키를 포함하고 있으며, 신뢰할 수 있는 인증기관이 전자식으로 서명하여 공개키와 개체를 결합한 것.

3.96
공개키 (비대칭) 암호알고리즘 [public key (asymmetric) cryptographic algorithm]
공개키와 개인키 두 키 쌍을 사용하는 암호알고리즘

비고 이 두 키 쌍은 공개키로부터 개인키를 유도하는 것이 계산적으로 불가능하다는 속성을 지닌다.

3.97
공개 보안매개변수 (public security parameter, PSP)
변경되는 경우 암호모듈의 보안을 손상시킬 수 있는 보안 관련 공개 정보

보기 공개키, 공개키 인증서, 자체 서명된 인증서, 카운터와 관련되어 있으며, 내부에 일자와 시간 정보를 유지하고 있는 일회용 패스워드

비고 PSP는 변경될 수 없거나 또는 모듈이 변경을 결정한다면 보호된 것으로 간주한다.

3.98
난수 발생기 (random bit generator, RBG)
통계적으로 독립되고 편중되지 않은 이진수열을 출력하는 장치 또는 알고리즘

비고 암호 응용을 위해 사용되는 난수 발생기는 일반적으로 0과 1의 비트열을 생성하며, 이 수열은 난수 블록으로 결합될 수 있다. 난수 발생기는 결정론적 방식과 비결정론적 방식으로 분류된다. 결정론적 난수 발생기는 씨드키(seed key)라고 부르는 초기값으로부터 비트열을 생성하는 알고리즘으로 구성되어 있으며, 비결정론적 난수 발생기는 예측 불가능한 물리적 소스에 의존하는 출력을 생성한다.

3.99
탈부착 덮개 (removable cover)
손상 없이 암호모듈의 물리적 구성물에 접근할 수 있는 물리적 수단

3.100
역할 (role)
암호모듈 서비스에 대한 사용자 접근 권한 또는 제한 사항을 사용자와 연관하여 정의한 보안 속성

비고 1개 이상의 서비스가 역할에 연관될 수 있다. 역할은 1명 이상의 사용자에 연관될 수 있고, 사용자는 1개 이상의 역할을 맡을 수 있다.

3.101
역할 기반 접근통제 (role-based access control, RBAC)
객체에 대한 접근을 역할에 기초하여 허가하는 것.

3.102
런타임 환경 (runtime environment)
컴퓨터가 가동되고 있는 동안 프로세스 또는 프로그램에 소프트웨어 서비스를 제공하는 가상 머신 상태

비고 운영체제 자체 또는 운영체제하에서 가동하는 소프트웨어가 될 수 있다. 런타임 환경의 기본적인 목표는 '플랫폼 독립적' 프로그램의 목적을 수행하는 것이다.

3.103
비밀키 (secret key)
비밀키 암호알고리즘과 함께 사용되며, 하나 또는 여러 개체에게 유일하게 결합되는 암호키. 공개되어서는 안 된다.

3.104
씨드키 (seed key)
난수 발생기를 초기화하기 위해 사용하는 비밀값

3.105
자가시험 (self-tests)
암호모듈에 의해 실행되는 운영 전 및 조건부 시험

3.106
중요 데이터 (sensitive data)
사용자가 보호하고자 하는 데이터

3.107
중요 보안매개변수 (sensitive security parameters, SSP)
핵심 보안매개변수(CSP)와 공개 보안매개변수(PSP)

3.108
서비스 (service)
운영자가 외부에서 암호모듈이 수행할 수 있는 동작과 기능을 불러냄.

3.109
서비스 입력 (service input)
특정 동작이나 기능을 초기화하거나 달성시키기 위해 암호모듈에 사용된 모든 데이터 또는 통제 정보

3.110
서비스 출력 (service output)
서비스 입력에 의해 초기화되거나 달성되는 동작 또는 기능으로부터 출력되는 모든 데이터 및 상태 정보

3.111
단순 전력 분석 (simple power analysis, SPA)
암호 운영과 상관관계가 있는 정보 추출을 위해 암호모듈의 전력 소비와 관련하여, 암호 명령 실행 (또는 개별 명령 실행) 패턴의 직접(일차적으로 시각) 분석

3.112
단일칩 암호모듈 (single-chip cryptographic module)
그 안에서 단일 집적회로(IC) 칩을 독립형 장치로 사용하거나 또는 물리적으로 보호되지 않는 봉함 또는 제품 내 내장된 물리적 형체

보기 단일 집적회로(IC) 칩 또는 단일 IC칩 장착 스마트카드

3.113
소프트웨어 (software)
변경 가능한 운영환경에서 동작되는 암호경계 내의 프로그램과 데이터 구성 요소. 일반적으로 삭제 가능한 매체에 저장되며 실행 중 동적으로 기록되거나 변경될 수 있다.

보기 삭제 가능한 매체에는 솔리드 상태 메모리와 하드 드라이브 등을 포함하지만 이에 국한하지는 않는다.

3.114
소프트웨어 모듈 (software module)
소프트웨어로만 구성된 모듈

3.115
소프트웨어/펌웨어 로드 시험 (software/firmware load test)
암호모듈에 의해 실행할 수 있게 되기 전 반드시 성공해야 하는 소프트웨어 또는 펌웨어에 대하여 실시되는 일련의 시험

비고 소프트웨어 또는 펌웨어가 완전한 이미지 대체물이고 모듈 파워 사이클링 후에만 실행할 수 있으면 적용하지 않는다.

3.116
소프트웨어/펌웨어 모듈 인터페이스 (software/firmware module interface, SFMI)
요청된 서비스의 일부로, 모듈의 암호경계로 입력되거나 출력되는 매개변수를 포함하여 소프트웨어 모듈 또는 펌웨어 모듈의 서비스를 요청하기 위해 사용하는 명령어 집합

3.117
지식 분산 (split knowledge)
암호키를 여러 가지 키 구성 요소로 분산하는 과정. 원래 키의 정보를 개별적으로 공유하지 않는다. 분산된 키 구성 요소는 분리된 개체에 의해 계속해서 암호모듈로 입력 또는 출력될 수 있고, 원래 암호키를 재구성하기 위해 결합될 수 있다.

비고 키 구성 요소의 전부 또는 부분집합이 조합될 때 필요할 수 있다.

3.118
SSP 설정 (SSP establishment)
하나 또는 여러 개체 사이에 공유된 SSP를 사용할 있도록 만드는 절차

비고 SSP 설정에는 SSP 합의, SSP 전송, SSP 입력 또는 출력을 포함한다.

3.119
상태 정보 (status information)
운영 특성 또는 암호모듈의 상태를 표시하기 위하여 암호모듈로부터 출력되는 정보

3.120
강도가 높은 (strong)
평균 또는 기대치보다 큰 강도 또는 파워를 갖거나 공격을 견딜 수 있도록 견고하게 제작되어 쉽게 당하지 않는 상태

3.121
대칭키 암호기술 (symmetric cryptographic technique)
암호화와 복호화 모드에서 동일한 비밀키를 사용하는 암호화 기법. 비밀키 암호기술이라고도 한다.

3.122
탬퍼 검출 (tamper detection)
암호모듈의 물리적 보안을 손상시키기 위한 시도가 행해졌다는 것을 자동으로 검출하는 것.

3.123
탬퍼 증거 (tamper evidence)
암호모듈의 물리적 보안을 손상시키기 위한 시도가 행해졌다는 것에 대한 외부 표시

3.124
탬퍼 대응 (tamper response)
탬퍼 검출이 이루어졌을 때 암호모듈이 취하는 자동 조치

3.125
신뢰 채널 (trusted channel)
보호되지 않은 평문 CSP, 키 구성 요소, 인증 데이터를 안전하게 통신하기 위해 암호모듈과 발송자 또는 수신자 간에 설정된 신뢰되고 안전한 통신 링크

비고 모듈의 정의된 입력 혹은 출력 포트와 종단점 단말 사이의 통신 링크에서의 신뢰된 채널은 적합하지 않은 운영자/개체, 프로세스 또는 다른 장치에 의한 도청, 물리적 혹은 논리적 템퍼링을 보호한다.

3.126
사용자 (user)
암호 서비스를 받기 위해서 암호모듈에 접근하는 개인 또는 개인을 대신해서 작동하는 프로세스(주체)에 의해 취해진 역할

3.127
검증된 (validated)
검증기관에 의해 시험된 적합성을 보증

3.128
검증기관 (validation authority)
시험기관의 암호모듈 시험 결과를 검증하는 기관

3.129
벤더 (vendor)
암호모듈 검증을 신청하는 개체, 그룹 혹은 연합체

비고 벤더는 암호모듈을 직접 설계 또는 개발하였는지 여부와 상관없이 모든 관련 문서와 설계 증빙 서류에 접근할 수 있어야 한다.

3.130
제로화 (zeroisation)
데이터 복원을 방지하기 위하여 저장 장치의 내용물을 변경하거나 삭제함으로써 데이터, 보호되지 않은 SSP를 소거하는 방법

4 약어

이 문서의 목적 상 다음의 약어를 적용한다.

API	Application Program Interface
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining-Message authentication code
ECB	Electronic Codebook
HDL	Hardware Description Language
IC	Integrated Circuit
PROM	Programmable Read-Only Memory
RAM	Random Access Memory

URL Uniform Resource Locator

5 암호모듈 보안수준

다음 부속 조항은 4가지 보안수준을 개략적으로 설명한다. 본 절에 제시된 예들은 보안 요구사항이 어떻게 충족되는지 설명하기 위한 것으로, 각 보안수준의 전체 보안 요구사항을 나타내는 것은 아니다. 이 표준에서 기술된 모듈은 암호모듈을 나타낸다. 암호기술은 4가지 보안수준 모두에서 동일하게 적용된다. 각 보안수준은 모듈 자체(예: 내부 구성 요소와 동작에 대한 접근과 인식) 보호 수준 및 모듈 내에서 관리되는 SSP 보호 수준을 나타내며 단계적으로 증가한다. 각 보안 요구사항은 [xx.yy]로 식별하여야 하며, 여기서 xx는 조항, yy는 그 조항 안에서의 번호 색인을 나타낸다.

5.1 보안수준 1

보안수준 1은 가장 낮은 수준의 보안을 제공하며, 암호모듈의 기본 보안 요구사항을 명세하고 있다(예: 암호모듈은 최소한 1개 이상의 검증대상 암호알고리즘 또는 검증대상 중요 보안매개변수 설정 방식을 사용해야 한다). 소프트웨어 또는 펌웨어 모듈은 변경 불가능하거나, 제한적인 또는 변경 가능한 운영환경에서 동작될 수 있다. 보안수준 1 하드웨어 암호모듈은 생산 등급 구성 요소에 필요한 기본 요구사항보다 높은 보안수준의 물리적 보안 메커니즘이 요구되지 않는다. 구현된 비침투 공격에 대한 대응 방법 및 기타 공격에 대한 대응 방법을 문서화한다. 보안수준 1 암호모듈의 예는 개인 컴퓨터(PC)에서 발견될 수 있는 하드웨어 암호 보드 또는 모바일 장치나 일반용 컴퓨터에서 실행할 수 있는 암호화 툴킷이다.

암호모듈의 운영환경이 물리적 보안, 네트워크 보안과 관리적 절차 등과 같은 보안 통제가 모듈 외부에서 제공되는 경우, 보안수준 1 암호모듈을 보안 응용에 적용하는 것이 적합하다. 예를 들어, 보안수준 1 암호모듈의 구현은 모듈 SSP에 대해서 더 높은 보안수준을 가지며, 더 높은 보증 수준을 갖는 모듈보다 비용 측면에서 효과적일 수 있다. 암호모듈 환경이 사용 기관의 전체 보안에 중요하게 영향을 미칠 경우, 위의 사항은 사용 기관이 보안 요구사항을 충족시킬 수 있는 암호 솔루션을 선택할 수 있게 한다.

5.2 보안수준 2

보안수준 2는 보안수준 1의 물리적 보안 메커니즘보다 보안성을 향상시킨 탈부착 덮개에 도포, 봉인 또는 도난 방지 잠금장치를 사용하거나 개구부에 도포, 봉인 또는 도난 방지 잠금장치를 사용하는 등 탬퍼 증거를 요구한다.

코팅 또는 봉인을 모듈에 부착하여 모듈의 내부 SSP에 물리적으로 접근할 경우 코팅 또는 봉인이 파손되어야 한다. 비인가된 물리적 접근으로부터 보호하기 위하여 탬퍼 증거용 실(seal) 또는 도난 방지 잠금장치는 덮개 또는 개구부에 설치된다.

보안수준 2는 역할 기반 인증을 요구한다. 보안수준 2 암호모듈은 운영자가 특정 역할을 맡을 권한과 역할에 대응하는 서비스를 수행하는 권한이 있는지를 인증한다.

보안수준 2 암호모듈은 역할 기반 접근 통제 기능을 가지며, 변경 가능한 운영환경에서 실행될 수 있는 소프트웨어 암호모듈이 될 수 있다. 또한 위의 소프트웨어 암호모듈은 신규 그룹을 정의하고 접근통제목록(예: ACL)을 통한 제한적인 권한을 할당할 수 있는 견고한 메커니즘이 구현되어 있어야 하며, 한 명의 사용자를 한 개 이상의 그룹에 할당할 수 있는 기능을 가져야 하고, 비인가된 실행, 변경 및 암호 소프트웨어의 읽기를 방지해야 한다.

5.3 보안수준 3

보안수준 3은 보안수준 2의 탬퍼 증거를 갖는 물리적 보안 메커니즘보다 보안성을 향상시켜, 암호모듈의 내부 SSP에 대한 비인가된 접근을 방어하기 위한 대책을 요구한다. 보안수준 3에서 요구되는 물리적 보안 메커니즘은 암호모듈에 대한 직접적인 물리적 접근, 사용 또는 변경과 그리고 환기구멍이나 이음새 부분의 틈을 통한 탐침을 높은 확률로 탐지하고 대응해야 한다. 물리적 보안 메커니즘은 강력한 봉쇄물을 사용하고, 암호모듈의 탈부착 덮개 또는 개구부 개방 시 모든 CSP를 제로화하는 탬퍼 탐지 회로 또는 대응 회로를 사용할 수 있다.

보안수준 3은 보안수준 2에 명시된 역할 기반 인증 메커니즘에 보안성을 향상시킨 신원 기반 인증 메커니즘을 요구한다. 암호모듈은 운영자의 신원을 인증하고, 신원이 확인된 운영자가 특정 역할과 해당 서비스를 수행할 권한이 있는지 확인한다.

보안수준 3은 수동으로 설정되는 CSP가 암호화되거나 신뢰된 채널을 통하거나 또는 주입과 출력에 분산 지식 절차가 사용되어야 함을 요구한다.

보안수준 3은 환경 조건인 전압 및 온도가 정상 동작 범위를 벗어났을 때 암호모듈이 보안 손상되지 않는 것을 요구한다. 암호모듈은 전압 및 온도가 정상 동작 범위를 벗어났을 때 이를 탐지하고, CSP를 제로화하는 특수 환경장애보호 장치를 포함하거나, 보안을 손상시킬 가능성이 있는 정상 동작 범위 밖에서 암호모듈이 동작될 때 암호모듈의 보안이 영향받지 않음을 보증하는 견고한 환경장애 시험을 수행하는 기능을 포함해야 한다(예: 공격자가 암호모듈의 방어 대책을 공격하기 위해 암호모듈을 정상 동작 범위 밖에서 동작시킬 수 있다).

보안수준 3 암호모듈에 구현된 **7.8**의 비침투 공격 대응 방법은 보안수준 3 측정 지수에 따라 시험된다.

소프트웨어 암호모듈에 해당하는 보안 요구사항에서 보안수준 3이 없는 경우가 있으므로, 소프트웨어 암호모듈이 전체로 받을 수 있는 최고 높은 보안수준은 보안수준 2이다.

보안수준 3 모듈은 형상 관리 자동화, 상세 설계, 상세 수준의 시험 및 벤더가 생성한 인증 정보를 사용한 운영자 인증 등을 보안수준 2에 추가한 생명주기 보증을 요구한다.

5.4 보안수준 4

보안수준 4는 이 표준의 최고 높은 수준을 나타낸다. 보안수준 4는 보안수준 4보다 낮은 보안수준의 모든 보안 특징을 포함하고 확장된 특성을 포함한다.

보안수준 4에서 SSP가 모듈 내부에 저장되어 있을 때, 외부 전원이 모듈에 공급됨과 관계없이 물리적 보안 메커니즘은 모든 물리적 접근에 의한 비인가 공격 시도를 완벽하게 탐지 및 대응할 수 있는 암호모듈의 겉봉함을 제공해야 한다. 보안수준 4는 암호모듈의 봉함에 대한 모든 침투 공격이 높은 확률로 탐지되고, 탐지 즉시 모든 보호하지 않은 SSP가 제로화되는 요구사항이어야 한다. 보안수준 4 암호모듈은 물리적으로 보호되지 않은 환경에서 안전하게 운영될 수 있다.

보안수준 4는 운영자를 인증할 경우 다중체계 인증을 요구한다. 다음의 세 가지 속성 중 최소한 두 가지를 요구한다.

- 패스워드 등과 같은 기억하거나 알고 있는 요소
- 물리적 키나 토큰 등의 소유하는 요소
- 생체 정보 등과 같은 물리적인 속성

보안수준 4는 암호모듈의 보안을 손상시킬 가능성이 있는 정상 동작 범위 밖에서 모듈이 동작될 때 암호모듈의 보안이 영향받지 않음을 합리적으로 보증할 수 있는, 즉 전압과 온도 동작 범위를 탐지하고 CSP를 제로화할 수 있는 특수 환경 보호 특성을 요구한다.

보안수준 4 암호모듈에 구현된 **7.8**의 비침투 공격 대응 방법은 보안수준 4의 측정 지수에 따라 시험된다.

소프트웨어 암호모듈에 해당하는 보안 요구사항에서 보안수준 4가 없는 경우가 있으므로, 소프트웨어 암호모듈이 전체로 받을 수 있는 최고 높은 보안수준은 보안수준 2이다.

보안수준 4 모듈의 설계는 사전 조건과 사후 조건 간의 일치성과 기능명세서에 의해 검증된다.

6 기능적 보안 목적

이 표준은 암호모듈을 안전하게 설계하고 구현하는 보안 요구사항을 명세한다. 보안 요구사항은 보안 목적의 보안수준 1부터 시작하여 단계적으로 높아진다. 다음과 같은 상위 수준의 기능적 보안 목적으로부터 보안 요구사항은 도출된다.

- 중요 정보를 보호하기 위해 검증대상 보호 함수를 채택하고 정확하게 구현한다.
- 비인가된 운영이나 사용으로부터 암호모듈을 보호한다.
- CSP를 포함한 암호모듈의 내용물 등이 인가되지 않은 상태로 노출되는 것을 방지한다.
- SSP의 비인가된 변경, 대체, 추가, 삭제 등을 포함하여 암호모듈과 암호알고리즘의 비인가된 변경과 탐지되지 않는 변경을 방지한다.
- 암호모듈의 동작 상태에 대한 정보를 제공한다.
- 암호모듈이 검증대상 동작 상태에서 적절하게 수행됨을 보증한다.
- 모듈 동작 시 오류를 탐지하고 및 오류로부터 발생되는 SSP 손상을 방지한다.
- 암호모듈의 설계, 배포 및 구현이 적합함을 보증한다.

7 보안 요구사항

7.1 일반사항

여기서는 이 표준을 준수하는 암호모듈이 충족해야 하는 보안 요구사항을 명세한다.

보안 요구사항은 암호모듈의 설계 및 구현에 관련된 영역으로 구성된다. 이 영역은 ① 암호모듈 명세, ② 암호모듈 인터페이스, ③ 역할, 서비스 및 인증, ④ 소프트웨어/펌웨어 보안, ⑤ 운영환경, ⑥ 물리적 보안, ⑦ 비침투 보안, ⑧ 중요 보안매개변수 관리, ⑨ 자가시험, ⑩ 생명주기 보증, ⑪ 기타 공격에 대한 대응을 포함한다.

표 1은 각 영역에서의 보안 요구사항을 요약하고 있다.

여기서 언급한 각 영역의 보안 요구사항에 대하여 암호모듈을 시험한다. 암호모듈은 각 영역별로 독립적인 보안수준을 부여받는다. 몇몇 영역은 단계적으로 증가하는 보안수준을 가지며, 상위 수준의 보안 요구사항은 하위 수준의 보안 요구사항을 포함한다. 암호모듈은 각 보안 영역의 모든 보안 요구사항을 충족하면 최고 보안수준을 받는다. 암호모듈 명세, 유한상태모델 및 자가시험 등 여러 단계의 보안수준을 제공하지 않는 영역의 경우, 해당 영역의 보안수준은 암호모듈 전체 보안수준과 같은 보안수준을 부여받는다.

암호모듈은 각 영역에 대해 독립적인 보안수준을 받을 수 있을 뿐만 아니라 암호모듈 전체에 대한 보안수준을 받는다. 암호모듈 전체에 대한 보안수준은 각 영역에서 받은 독립적인 보안수준 중 가장 낮은 보안수준으로 결정된다.

이 표준의 다수 보안 요구사항들은 **부속서** A와 B에 요약된 특정 문서 요구사항들이다. 암호모듈이 독립적으로 검증 및 평가 스킴을 수행할 때 사용자 및 설치 설명서, 설계 명세, 생명주기 문서 등을 포함하는 모든 문서는 제공되어야 한다.

부속서 C, D, E, F는 검증대상 암호알고리즘, 검증대상 중요 보안매개변수 설정 방법, 검증대상 인증 메커니즘 및 비침투 공격에 대한 대응 시험방법과 관련된 참고 문서를 제공한다.

표 1 – 각 영역별 보안 요구사항 요약

<table>
<tr><th></th><th>보안수준 1</th><th>보안수준 2</th><th>보안수준 3</th><th>보안수준 4</th></tr>
<tr><td>암호모듈 명세</td><td colspan="4">암호모듈, 암호경계, 검증대상 암호알고리즘, 정상 동작모드 및 제한 기능 동작 모드의 명세. 모든 하드웨어, 소프트웨어, 펌웨어 구성 요소를 포함하는 암호모듈에 대한 서술. 모든 서비스는 검증대상 알고리즘이나 검증대상 프로세스를 사용하고 있는 검증대상 상태의 정보를 제공해야 함.</td></tr>
<tr><td>암호모듈 인터페이스</td><td colspan="2">필수 또는 선택적 인터페이스. 모든 논리적, 물리적 인터페이스 명세 및 모든 입출력 데이터 경로 명세</td><td colspan="2">신뢰 채널</td></tr>
<tr><td>역할, 서비스 및 인증</td><td>필수 또는 선택적 역할 및 서비스의 논리적 분리</td><td>역할 기반 또는 신원 기반 운영자 인증</td><td>신원 기반 운영자 인증</td><td>다중체계 인증</td></tr>
<tr><td>소프트웨어/펌웨어 보안</td><td>검증대상 무결성 기술, 정의된 SFMI, HFMI 및 HSMI.
실행 코드</td><td>검증대상 전자서명 혹은 메시지 인증 코드 기반 무결성 시험</td><td colspan="2">검증대상 전자서명 기반 무결성 시험</td></tr>
<tr><td>운영환경</td><td>변경 불가능한, 제한적 또는 변경 가능한.
SSP 관리</td><td>변경 가능한.
역할 기반 또는 임의적 접근 관리.
감사 메커니즘</td><td colspan="2"></td></tr>
<tr><td>물리적 보안</td><td>생산 등급 구성 요소</td><td>변조-증거.
불투명 덮개 또는 봉함</td><td>덮개와 개구부에 대한 변조 탐지 및 대응. 강도 높은 봉함 또는 도포. 직접적인 탐침에 대한 보호. EFP 또는 EFT</td><td>변조 탐지 및 대응 겉봉함. EFP. 오류 주입 공격에 대한 대응</td></tr>
<tr><td rowspan="2">비침투 보안</td><td colspan="4">모듈은 부속서 F의 비침투 공격에 대응하도록 설계함.</td></tr>
<tr><td colspan="2">부속서 F에서 명세한 대응 기술의 문서화 및 유효성</td><td>대응 시험</td><td>대응 시험</td></tr>
<tr><td rowspan="3">중요 보안매개변수 관리</td><td colspan="4">난수 발생기, SSP의 생성, 설정, 주입, 출력, 저장 및 제로화</td></tr>
<tr><td colspan="4">검증대상 기술을 이용한 자동화된 SSP 전송 또는 SSP 합의</td></tr>
<tr><td colspan="2">수동으로 설정된 SSP는 평문 형태로 입력되거나 출력될 수 있음.</td><td colspan="2">수동으로 설정된 SSP는 신뢰된 채널을 통한 암호화 형태 또는 지식 분산 과정을 사용하여 입력되거나 출력될 수 있음.</td></tr>
</table>

표 1 – 각 영역별 보안 요구사항 요약(계속)

<table>
<tr><th colspan="2"></th><th>보안수준 1</th><th>보안수준 2</th><th>보안수준 3</th><th>보안수준 4</th></tr>
<tr><td colspan="2" rowspan="2">자가시험</td><td colspan="4">정상 동작 전: 소프트웨어/펌웨어 무결성, 우회 및 핵심 기능시험</td></tr>
<tr><td colspan="4">조건부: 암호알고리즘, 키쌍 일치성, 소프트웨어/펌웨어 로드, 수동 주입, 조건부 우회 및 핵심 기능시험</td></tr>
<tr><td rowspan="8">생명주기 보장</td><td>형상 관리</td><td>암호모듈, 구성 요소 및 개발 문서의 형상관리시스템. 각각은 생명주기 동안 유일하게 식별되고 추적되어야 함.</td><td colspan="3">자동화 형상관리시스템</td></tr>
<tr><td>설계</td><td colspan="4">보안 특성을 갖는 모든 서비스를 시험할 수 있도록 설계된 모듈</td></tr>
<tr><td>FSM</td><td colspan="4">유한상태모델</td></tr>
<tr><td>개발</td><td>주석 처리된 소스 코드.
설계도 또는 HDL</td><td colspan="2">소프트웨어 고급 언어.
하드웨어 고급 명세 언어</td><td>모듈 구성 요소로 주입되는 사전 상태 조건과 구성 요소 완성 시 성공이 예측되는 사후 상태 조건을 주석 처리한 문서</td></tr>
<tr><td>시험</td><td colspan="2">기능시험</td><td colspan="2">상세 수준 시험</td></tr>
<tr><td>배포 및 운영</td><td>초기화 절차</td><td colspan="2">배포 절차</td><td>벤더가 생성한 인증 정보를 사용하여 운영자 인증</td></tr>
<tr><td>안내서</td><td colspan="4">관리자 및 비관리자 안내서</td></tr>
<tr><td colspan="2">기타 공격에 대한 대응</td><td colspan="3">현재 시험 요구사항을 시험할 수 없는 공격에 대한 대응 방법의 명세</td><td>시험 요구사항을 시험할 수 있는 공격에 대한 대응 방법의 명세</td></tr>
</table>

7.2 암호모듈 명세

7.2.1 암호모듈 명세의 일반 요구사항

암호모듈은 검증대상 암호알고리즘이나 프로세서를 사용하여 최소한 한 개 이상의 암호 서비스를 구현하고 암호경계 내에 포함된 하드웨어나 소프트웨어, 펌웨어 또는 이들의 결합 형태이어야 한다[02.01].

A.2.2에 명세된 요구사항을 충족하는 개발 문서가 제출되어야 한다[02.02].

7.2.2 암호모듈 유형

암호모듈은 다음과 같은 모듈 유형 중 한 가지로 정의되어야 한다[02.03].

- 하드웨어 모듈은 하드웨어 경계를 이용하여 암호경계가 구분될 수 있도록 명세화된 모듈이다. 하드웨어 암호경계 안에 펌웨어 또는 소프트웨어를 포함할 수 있으며, 이때 펌웨어 또는 소프트웨어는 운영체제도 포함할 수 있다.
- 소프트웨어 모듈은 변경 가능한 운영환경에서 실행하는 소프트웨어 구성 요소(한 개 또는 여러 개의 구성 요소)들이며, 암호경계는 소프트웨어 경계를 이용하여 구분될 수 있도록 명세화된 모듈이다. 소프트웨어 구성 요소가 실행되는 연산 플랫폼 및 운영체제는 정의된 소프트웨어 모듈 경계 외부

에 있다.

- 펌웨어 모듈은 제한되거나 변경이 불가능한 운영환경에서 실행하는 펌웨어 구성 요소들이며, 암호경계는 펌웨어 경계를 이용하여 구분될 수 있도록 명세화된 모듈이다. 펌웨어 구성 요소가 실행되는 연산 플랫폼 또는 운영체제는 정의된 펌웨어 모듈 경계 외부에 있지만 펌웨어 모듈과 항상 결합된 형태이어야 한다.
- 하이브리드 소프트웨어 모듈은 소프트웨어 구성 요소 및 하드웨어 구성 요소를 조합한 유형이며, 소프트웨어 구성 요소는 하드웨어 모듈 경계와 분리되어야 한다. 소프트웨어 구성 요소가 실행되는 연산 플랫폼 및 운영체제는 정의된 하이브리드 소프트웨어 모듈 경계의 외부에 있다(예: 소프트웨어 모듈과 하드웨어 모듈의 조합은 하이브리드 하드웨어 모듈로 분류된다).
- 하이브리드 펌웨어 모듈은 펌웨어 구성 요소 및 하드웨어 구성 요소를 조합한 유형이며, 펌웨어 구성 요소는 하드웨어 모듈 경계와 분리되어야 한다. 펌웨어 구성 요소가 실행되는 연산 플랫폼 또는 운영체제는 정의된 하이브리드 펌웨어 모듈 경계의 외부에 있지만 항상 하이브리드 펌웨어 모듈과 결합된 형태이어야 한다(예: 펌웨어 모듈과 하드웨어 모듈의 조합은 하이브리드 펌웨어 모듈로 분류된다).

하드웨어와 펌웨어 모듈은 **7.7**, **7.8**의 적용 가능한 모든 보안 요구사항을 만족해야 한다[02.04].

변경 가능한 환경에서 실행하는 소프트웨어 모듈의 경우, **7.7**의 물리적 보안 요구사항은 선택 사항이며, **7.8**의 비침투 보안 요구사항은 적용 가능한 모든 보안 요구사항을 만족해야 한다[02.05].

하이브리드 모듈의 경우, **7.5**, **7.6**, **7.7**, **7.8**의 적용 가능한 모든 보안 요구사항을 만족해야 한다[02.06].

7.2.3 암호경계

7.2.3.1 암호경계의 일반 요구사항

암호경계는 암호모듈의 모든 구성 요소의 경계에 의해서 설정되는 통합 경계(즉, 하드웨어 구성 요소, 소프트웨어 구성 요소 및 펌웨어 구성 요소의 집합)이어야 한다[02.07]. 해당 표준의 요구사항들은 암호모듈의 암호경계 내의 모든 알고리즘, 프로세스 및 구성 요소에 적용되어야 한다[02.08]. 암호경계는 암호모듈(즉, 이 표준의 범위 내에 있는 보안에 관련된)의 모든 알고리즘, 모든 프로세서 및 모든 구성 요소를 반드시 포함해야 한다[02.09]. 검증대상 동작모드에 사용되는 비보안 알고리즘, 비보안 프로세서 또는 비보안 구성 요소는 암호모듈의 검증대상 동작을 방해하거나 손상시키지 않는 방법으로 구현되어야 한다[02.10].

암호모듈의 명칭은 암호경계 내에 있는 구성 요소만의 조합을 의미하도록 정해져야 하며, 암호경계 내에 있는 구성 요소의 조합보다 더 큰 범위의 제품이나 구성 요소의 조합을 의미하는 명칭이 되지 않아야 한다[02.11]. 암호모듈은 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소 각각에 대하여 최소한 특정 버전 정보는 가져야 한다[02.12].

암호경계 외부에 있는 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 암호모듈의 검증대상 동작을 방해하거나 손상을 초래하지 않도록 구현되어야 한다. 암호경계 외부에 있는 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 해당 표준의 보안 요구사항을 적용받지 않는다[02.13]. 보안 요구사항에 해당하지 않는 하드웨어, 소프트웨어 또는 펌웨어는 **부속서 A**의 요구사항을 충족하도록 명세되어야 한다[02.14].

7.2.3.2 암호경계 정의

하드웨어 암호모듈의 암호경계는 다음과 같이 범위를 명확히 정해야 한다[02.15].

- 하드웨어 구성 요소의 집합은 다음을 포함할 수 있다.
  - ① 회로 보드, ② 회로 기판 또는 ③ 구성 요소 간을 배선으로 연결하는 기타 표면실장 부품 등을 포함하는 물리적 구조
  - 준주문형 IC(semi-integrated circuit), 주문형(custom) IC, 일반 상용(common) IC, 프로세서, 메모리, 전원 공급기, 변환기 등과 같은 능동 전기 소자
  - 봉함, 매몰재 혹은 캡슐화 물질, 커넥터 및 인터페이스 등과 같은 물리적 구조
  - 운영체제를 포함할 수 있는 펌웨어
  - 상기에 기재되지 않은 기타 구성 요소들

소프트웨어 암호모듈의 다음 사항에 대한 암호경계의 범위가 명확히 정해져야 한다[02.16].

- 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
- 메모리에 저장되어 있으며 한 개 또는 그 이상의 처리기에 의해 실행되는 암호모듈의 인스턴스 생성

펌웨어 암호모듈의 다음 사항에 대한 암호경계의 범위가 명확히 정해져야 한다[02.17].

- 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
- 메모리에 저장되어 있으며 한 개 또는 그 이상의 처리기에 의해 실행되는 암호모듈의 인스턴스 생성

하이브리드 암호모듈의 암호경계는 다음과 같아야 한다[02.18].

- 모듈의 하드웨어 구성 요소 경계와 이 구성 요소와 별도로 분리되어 있는 소프트웨어 구성 요소 경계와의 조합
- 모듈의 하드웨어 구성 요소 경계와 이 구성 요소와 별도로 분리되어 있는 펌웨어 구성 요소 경계와의 조합
- 각 구성 요소의 모든 포트와 인터페이스의 집합을 포함

하드웨어 모듈과 분리된 소프트웨어나 펌웨어 구성 요소와 조합된 하드웨어 모듈은 내장된 소프트웨어나 펌웨어를 포함할 수 있다.

7.2.4 동작모드

7.2.4.1 동작모드 일반적인 요구사항

운영자는 검증대상 동작모드에서 암호모듈을 동작시킬 수 있어야 한다[02.19]. 검증대상 동작모드는 검증대상 암호알고리즘이나 프로세스를 이용한 한 개 이상의 서비스를 포함한 서비스 집합으로 정의된다. 여기서 이들 서비스와 프로세스는 **7.4.3**에 명세되어 있다[02.20].

비검증대상 암호알고리즘이나 프로세스뿐만 아니라 **7.4.3**에 명세되지 않은 기타 서비스도 검증대상 동작모드에서 운영자가 사용할 수 없어야 한다. 단, 비검증대상 암호알고리즘이나 검증대상 프로세스의 일부분이면서 검증대상 프로세스의 비보안 관련 동작일 경우는 비검증대상 암호알고리즘이 사용될 수 있다(예: 검증대상 동작모드에서 수행되는 비검증대상 알고리즘 또는 비검증대상 키 생성 알고리즘으로 생성된 키는 데이터나 CSP를 알기 어렵게 하기 위해 사용될 수 있지만, 그 결과는 검증대상 암호알고리즘으로 보호되기 이전까지는 보호되지 않은 평문으로 취급되고, 비보안 관련 기능을 제공하는 것으로 간주된다)[02.21].

7.2.4.2 정상 동작

정상 동작은 알고리즘의 집합, 서비스 또는 프로세스가 사용 가능하거나 구성 가능한 상태를 말한다.

CSP는 검증대상 서비스 및 동작모드와 비검증대상 서비스 및 동작모드에서 독립적으로 분리되어야 한다(예: 상호 공유되거나 접근할 수 없어야 한다)[02.22]. 검증대상 난수 발생기의 출력은 난수 발생기 씨드를 비검증대상 동작모드로 접근할 수 없는 한 그 씨드를 제로화하지 않고 비검증대상 알고리즘이나 프로세스에 제공될 수 있다.

모듈의 보안정책은 검증대상 동작모드와 비검증대상 동작모드에서 제공하는 모든 서비스의 집합을 정의해야 한다[02.23].

모든 서비스들은 검증대상 동작모드에서 검증대상 암호알고리즘이나 프로세스를 사용할 때 각 서비스에 대한 표시기를 제공해야 한다. 여기서 이들 서비스와 프로세스는 **7.4.3**에 명세되어 있다[02.24].

7.2.4.3 제한 기능 동작

모듈이 오류 상태로 들어간다면 암호모듈은 제한 기능 동작을 지원하기 위해 설계될 수 있다. 암호모듈이 제한 기능 동작 상태로 동작하기 위해서는 다음이 적용되어야 한다[02.25].

- 오류 상태를 벗어난 후에만 제한 기능 동작으로 전환되어야 한다[02.26].
- 모듈이 재구성되고 제한 기능 동작 상태로 진입했을 때 상태 정보를 제공해야 한다[02.27].
- 오동작을 일으킨 메커니즘이나 기능은 분리되어야 한다[02.28].
- 제한 기능 동작 진입 후 모든 조건부 알고리즘 자가시험은 암호알고리즘이 처음 동작하기 전에 수행되어야 한다[02.29].
- 비동작 알고리즘이나 프로세스를 사용하려는 경우 서비스는 표시기를 제공해야 한다[02.30].

암호모듈은 모든 동작 전 자가시험을 성공적으로 통과할 때까지 제한 기능 동작 상태로 남아 있어야 한다[02.31]. 암호모듈은 제한 기능 동작 상태를 벗어나기 위한 조건처럼 모든 동작 전 자가시험의 확실한 진단을 수행해야 한다. 암호모듈이 동작 전 자가시험을 실패한다면 모듈은 제한 기능 동작에 진입할 수 없다[02.32].

7.3 암호모듈 인터페이스

7.3.1 암호모듈 인터페이스 일반 요구사항

암호모듈은 모든 논리적 정보 흐름이 암호경계의 입출구로 식별되는 물리적 접근 지점과 논리적 인터페이스에 제한되도록 해야 한다[03.01]. 암호모듈 논리적 인터페이스들은 한 개의 물리적 포트를 공유하더라도 서로 구별되어야 하며(예: 입력 데이터와 출력 데이터가 동일한 포트를 통해 입출력될 수 있다), 하나 이상의 물리적 포트(예: 입력 데이터가 직렬 및 병렬 포트 모두를 통해 들어올 수 있다.)로 분산하여 사용될 수 있다. 암호모듈의 소프트웨어 구성 요소의 API는 하나 이상의 논리적 인터페이스로 정의될 수 있다[03.02].

A.2.3의 요구사항을 충족하는 개발 문서를 제출해야 한다[03.03].

7.3.2 인터페이스의 유형

- **하드웨어 모듈 인터페이스(HMI)**: 요청된 서비스의 일부처럼 모듈의 암호경계에 들어가거나 나가는 매개변수를 포함한 하드웨어 모듈의 서비스를 요청하기 위해 사용하는 인터페이스 전체 집합
- **소프트웨어 또는 펌웨어 모듈 인터페이스(SFMI)**: 요청된 서비스의 일부처럼 모듈의 암호경계에 들어가거나 나가는 매개변수를 포함한 소프트웨어 또는 펌웨어 모듈의 서비스를 요청하기 위해 사용하는 인터페이스 전체 집합

- **하이브리드 소프트웨어 또는 하이브리드 펌웨어 모듈 인터페이스(HSMI 또는 HFMI)**: 요청된 서비스의 일부로 모듈의 암호경계에 들어가거나 나가는 매개변수를 포함한 하이브리드 소프트웨어 또는 하이브리드 펌웨어 모듈의 서비스를 요청하기 위해 사용하는 인터페이스 전체 집합

7.3.3 인터페이스 정의

암호모듈은 다음과 같은 5개의 인터페이스를 갖는다('입력'과 '출력'은 암호모듈의 관점에서 표시된다)[03.04].

1. **데이터 입력 인터페이스** 암호모듈에 입력되고 모듈에 의해 처리되는(평문 데이터, 암호문 데이터, SSP, 다른 모듈로부터의 상태 정보를 포함한) 모든 데이터(제어 입력 인터페이스를 통해 들어오는 제어 데이터는 제외)는 데이터 입력 인터페이스를 통해 입력되어야 한다[03.05]. 데이터는 모듈이 자가시험(**7.10**)을 수행하는 동안 데이터 입력 인터페이스를 통해 그 모듈로 입력할 수 있다.

2. **데이터 출력 인터페이스** (평문 데이터, 암호문 데이터, SSP를 포함한) 암호모듈에서 출력되는 모든 데이터(상태 출력 인터페이스를 통해 출력되는 상태 데이터와 제어 출력 인터페이스를 통해 출력되는 제어 데이터 제외)는 데이터 출력 인터페이스를 통해 출력되어야 한다[03.06]. 수동 키를 주입하는 상태, 동작 전 자가시험 상태, 소프트웨어/펌웨어를 로드하는 상태 및 제로화하는 상태 또는 암호모듈이 오류 상태에 있을 때는 '데이터 출력' 인터페이스를 통과하는 모든 데이터 출력은 금지되어야 한다[03.07].

3. **제어 입력 인터페이스** 암호모듈의 동작을 제어하는 데 사용되는 모든 입력 명령, 신호(예: 클럭 입력) 및 제어 데이터(함수 호출과 스위치, 버튼 및 키보드 같은 수동 제어 장치를 포함하는)는 '제어 입력' 인터페이스를 통해 입력되어야 한다[03.08].

4. **제어 출력 인터페이스** 암호모듈의 동작 상태를 제어하거나 표시하는 모든 출력 명령, 신호 및 제어 데이터(예: 다른 모듈에 입력시키는 제어 명령)는 '제어 출력' 인터페이스를 통해 출력되어야 한다[03.09]. 개발 문서의 보안정책에 서술된 예외 사항 이외의 오류 상태에 있을 때, '제어 출력' 인터페이스를 통한 암호모듈의 모든 제어 출력은 금지되어야 한다[03.10].

5. **상태 출력 인터페이스** 암호모듈의 상태를 표시하기 위해 사용되는 모든 출력 신호, 표시기(예: 오류 표시기) 및 상태 데이터[응답 코드 및 (디스플레이, 표시기 램프 같은) 시각 신호, (버저, 톤, 벨 소리 같은) 소리, (진동 같은) 기계적 신호와 같은 물리적 표시기]는 "상태 출력" 인터페이스를 통해서 출력되어야 한다. 상태 출력은 암시적이거나 명시적일 수 있다[03.11].

소프트웨어 암호모듈을 제외한 모든 모듈은 다음과 같은 인터페이스를 가져야 한다[03.12].

- **전원 인터페이스** 암호모듈에 공급되는 모든 외부 전력은 전원 인터페이스를 통과하여 공급되어야 한다[03.13]. 모든 전원이 암호모듈의 암호경계 내에서 내부에서 공급되거나 유지될 때, 전원 인터페이스는 필요하지 않다(예: 내장 배터리).

암호모듈은 입력에 사용되는 데이터, 제어 정보 및 전원과 출력에 사용되는 데이터, 제어 정보 및 상태 정보, 출력 전원을 구별해야 한다[03.14].
암호모듈 명세는 모든 입력의 가변 길이를 제한하는 것과 같이 입력 데이터와 제어 정보의 형식을 명확하게 명세해야 한다[03.15].

7.3.4 신뢰 채널

신뢰 채널은 안전하게 보호하지 않은 평문 CSP와 키 구성 요소, 인증 데이터를 통신하기 위해 암호

모듈과 송신자 또는 수신자 간 설정된 링크이다. 신뢰 채널은 원치 않은 운영자/개체 또는 과정, 기타 장치에 의한 또한 모듈의 정의된 입력 또는 출력 포트 간, 의도된 송신자 또는 수신자 종단 간의 통신 링크를 따라 발생하는 도청은 물론 물리적 또는 논리적 변조로부터 보호한다.

보안수준 1, 2

보안수준 1, 2의 경우 신뢰 채널에 대한 요구사항은 없다.

보안수준 3

보안수준 3의 경우

- 암호모듈과 송신자(또는 수신자) 종단 간의 보호되지 않은 평문 CSP, 키 구성 요소, 인증 데이터의 전송을 위하여 암호모듈은 신뢰 채널을 구현해야 한다[03.16].
- 신뢰 채널은 통신 링크에서 인가되지 않은 변경, 교체, 노출을 방지해야 한다[03.17].
- 신뢰 채널에 사용되는 물리적 포트는 다른 모든 포트들과 물리적으로 분리되거나[03.18], 신뢰 채널에 사용된 논리적 인터페이스는 다른 모든 인터페이스와 논리적으로 분리되어야 한다[03.19].
- 신원 기반 인증은 신뢰 채널을 이용하는 모든 서비스에 적용되어야 한다[03.20].
- 신뢰 채널을 사용할 때 상태 표시기를 제공해야 한다[03.21].

보안수준 4

보안수준 4는 보안수준 3의 보안 요구사항에 추가하여 신뢰 채널을 이용하는 모든 서비스에 다중체계 신원 기반 인증이 적용되어야 한다[03.22].

7.4 역할, 서비스 및 인증

7.4.1 역할, 서비스 및 인증 일반 요구사항

암호모듈은 운영자에게 인가된 역할을 지원하고 각 역할에 상응하는 서비스를 제공해야 한다[04.01]. 한 명의 운영자가 복수 역할을 맡을 수도 있다. 암호모듈이 복수 운영자가 모듈을 동시에 이용하는 것을 지원하는 경우, 암호모듈은 내부적으로 각 운영자의 역할과 이에 상응하는 서비스를 분리하여 유지할 수 있어야 한다[04.02]. 운영자는 CSP와 PSP가 변경 또는 공개, 대체되지 않는 경우, 서비스를 수행하도록 인가된 역할을 맡을 필요가 없다(예: 상태 표시, 자가시험 및 모듈의 보안에 영향을 주지 않는 기타 서비스).

인증 메커니즘은 모듈에 접근하는 운영자를 인증하기 위해, 운영자가 요청된 역할을 맡고 그 역할 내 서비스를 수행하도록 권한을 위임받았음을 검증하기 위해 암호모듈 내부에서 요구될 수 있다.

A.2.4를 만족하는 개발 문서가 제출되어야 한다[04.03].

7.4.2 역할

암호모듈은 적어도 하나의 암호관리자 역할을 지원해야 한다[04.04]. 암호관리자 역할은 암호 초기화나 관리 기능 및 일반 보안 서비스를 수행하는 역할이어야 한다(예: 암호모듈의 초기화, PSP와 CSP의 관리, 감사 기능)[04.05].

암호모듈은 사용자 역할을 지원할 수도 있다. 암호모듈이 사용자 역할을 지원하면, 사용자 역할은 암호 기능과 검증대상 암호알고리즘을 포함한 일반 보안 서비스를 수행하는 것이다[04.06].

암호모듈은 유지보수 역할을 지원할 수도 있다. 유지보수 역할은 물리적 또는 논리적 유지보수 서비스[예: 서비스 덮개 열기, 빌트인 자가시험(BIST) 등과 같은 진단 수행] 동안 담당하는 역할이다. 모든 보호되지 않은 SSP는 암호모듈이 유지보수 역할로 들어가거나 혹은 벗어날 때 제로화되어야 한다[04.07]

암호모듈은 위에서 명시한 역할 외 다른 역할을 지원할 수도 있다.

7.4.3 서비스

7.4.3.1 서비스 일반 요구사항

서비스는 모듈에서 수행되는 모든 동작, 서비스, 기능으로 정의된다[04.08]. 서비스 입력은 특정 서비스, 동작 또는 기능을 시작하거나 동작하기 위해 암호모듈로 입력되는 데이터 입력과 제어 입력으로 구성된다[04.09]. 서비스 출력은 서비스 입력에 의해 시작 또는 수행되는 서비스, 동작 및 기능으로부터 얻어지는 데이터 출력, 제어 출력과 상태 출력으로 구성된다[04.10]. 각 서비스 입력의 결과로 서비스 출력이 생성된다[04.11].

암호모듈은 운영자에게 다음 서비스를 제공해야 한다[04.12].

1. 모듈의 버전 정보 표시. 암호모듈은 검증 기록과 관련된 명칭 또는 모듈 식별자 그리고 버전 정보(예: 하드웨어, 소프트웨어 또는 펌웨어 버전 정보)를 출력해야 한다[04.13].
2. 상태 표시. 암호모듈은 현재 상태 정보를 출력해야 한다[04.14]. 이것은 서비스 요청에 대응한 상태 표시가 포함될 수 있다.
3. 자가시험 수행. 암호모듈은 **7.10.2**에 명세된 대로 동작 전 자가시험을 수행해야 한다[04.15].
4. 검증대상 암호알고리즘 수행. **7.2.4**에 명시된 대로 검증대상 동작모드에서 사용되는 검증대상 암호알고리즘을 적어도 한 개 이상 수행해야 한다[04.16]
5. 제로화 수행. 암호모듈은 **7.9.7**에 명시된 대로 파라미터의 제로화를 수행해야 한다[04.17].

암호모듈은 위에서 명시한 서비스 외에 검증대상 및 비검증대상 동작모드에서의 서비스, 운영 또는 기능을 제공할 수 있다. 특정 서비스는 한 개 이상의 역할에서 제공할 수 있다(예: 키 주입 서비스는 사용자 역할과 암호관리자 역할에서 제공할 수 있다).

7.4.3.2 우회 기능

우회 기능은 암호 기능 또는 프로세스를 부분적 또는 전체적으로 피하는 서비스 기능이다. 암호모듈이 특정 데이터나 상태값을 암호로 보호된 형태(예: 암호문)로 출력할 수 있고, 또한 이들을 (모듈의 설정이나 운영자 개입의 결과로) 보호되지 않은 형태(예: 평문)로도 출력할 수 있다면 우회 기능이 정의되어 있어야 한다[04.18].

암호모듈이 우회 기능이 구현된 경우

- 암호모듈에 우회 기능이 구현된 경우, 인가된 역할의 사용자만이 우회 기능을 설정할 수 있다[04.19].
- 단순한 오류로 인한 평문 데이터의 의도하지 않은 유출을 방지하기 위해, 우회 기능을 활성화하는 두 개의 독립된 내부 조치가 요구되어야 한다[04.20]. 두 개의 독립된 내부 조치가 우회 기능만을 수행하는 전용 소프트웨어 혹은 하드웨어를 동작할 수 있어야 한다(예: 두 개의 다른 소프트웨어 또는 하드웨어 플래그를 설정하고 그중 하나는 사용자가 시작시키도록 한다)[04.21].
- 그 모듈은 다음과 같이 우회 기능의 상태를 표시해야 한다[04.22].
  1. 우회 기능이 비활성화 상태이고 모듈은 암호 처리만을 제공한다(예: 평문의 암호화).

2. 우회 기능이 활성화 상태이고 모듈은 암호 처리를 제외한 서비스만 제공한다(평문을 암호화하지 않음).
3. 우회 기능이 선택적으로 활성화, 비활성화되며 일부 서비스는 암호 처리와 함께 또한 일부 서비스는 암호 처리 없이 제공한다(예: 복수 통신 채널을 가진 모듈의 경우, 평문 데이터는 각 채널 설정에 따라 암호화되거나 또는 암호화되지 않는다).

7.4.3.3 자가 초기화된 암호 출력 기능

자가 초기화된 암호 출력 기능은 외부 운영자 요청 없이 암호 운영 및 기타 검증대상 보안기능 또는 SSP 관리 기술을 수행할 수 있는 모듈의 기능이다. 자가 초기화된 암호 출력 기능은 암호관리자에 의해 설정되고 이러한 설정은 모듈의 리셋, 재부팅 또는 전원 재인가 시 보존되어야 한다[04.23].

암호모듈에 자가 초기 암호 출력 기능이 구현된 경우

- 단순 오류로 인한 의도하지 않은 출력을 방지하기 위해 두 개의 독립된 내부 조치가 필요하다[04.24]. 두 개의 독립된 내부 조치를 통해서만 암호 출력 기능을 조정하는 전용 소프트웨어 혹은 하드웨어를 동작시킬 수 있어야 한다(예: 두 개의 서로 다른 소프트웨어 또는 하드웨어 플래그를 설정하고 그중 하나는 사용자가 시작시키도록 한다)[04.25].
- 모듈은 그 기능이 활성화되었는지 상태를 표시해야 한다[04.26].

7.4.3.4 소프트웨어/펌웨어 로드

암호모듈이 소프트웨어나 펌웨어를 외부로부터 로드하는 기능을 가지고 있으면 다음과 같은 요구사항을 만족해야 한다[04.27].

- 로드되는 소프트웨어나 펌웨어의 검증을 유지하기 위해서 로드되어 암호모듈에 사용되기 전에 소프트웨어 또는 펌웨어는 검증기관에 의해 검증받아야 한다[04.28].
- 데이터 출력 인터페이스를 통한 데이터 출력은 소프트웨어 또는 하드웨어에 대한 로드와 로드 시험이 성공된 후 실행되어야 한다[04.29].
- **7.10.3.4**에 명시된 소프트웨어/펌웨어 로드 시험은 로드된 코드가 실행될 수 있기 전에 수행되어야 한다[04.30].
- **7.10.2**에 명시된 사전 동작 시험이 성공적으로 완료되기 전까지 모든 로드 또는 변경된 검증대상 암호알고리즘의 실행을 보류해야 한다[04.31].
- 모듈의 버전 정보는 새로 로드된 소프트웨어 또는 펌웨어의 추가 및 업데이트를 반영하여 변경되어야한다(**7.4.3**)[04.32].

새로운 소프트웨어 또는 펌웨어 로드로 전체 이미지가 대체되면, 이 전체 이미지는 검증을 유지하기 위해 검증기관의 신규 검증이 필요한 완전히 새로운 모듈로 간주된다[04.33]. 새로운 소프트웨어 또는 펌웨어 이미지는 전원 인가 리셋을 통해 모듈 전환이 완료된 후 실행되어야 한다[04.34]. 새로운 이미지가 실행되기 전에 모든 SSP는 제로화되어야 한다[04.35].

7.4.4 인증

운영자의 모듈 접근을 인증하고 운영자가 요구되는 역할을 담당하고 그 역할 내 서비스를 수행하도록 인가받았음을 검증하기 위해 암호모듈 내 인증 메커니즘이 필요할 수 있다. 다음과 같은 유형의 메커니즘을 암호모듈로의 접근을 관리하기 위해 사용한다.

역할 기반 인증: 암호모듈이 역할 기반 인증 메커니즘을 지원하면, 운영자는 암시적 또는 명시적으로

하나 이상의 역할을 선택해야 하고[04.36], 선택된 역할(또는 역할들의 집합)이 잘 부여되었는지 확인해야 한다[04.37]. 암호모듈은 운영자의 개별 신원을 인증을 요구하지 않는다. 역할의 선택과 선택된 역할의 부합하는 인증은 결합시킬 수 있다. 암호모듈이 운영자의 역할 변경을 허용하는 경우, 암호모듈은 그 운영자가 이전에 인증받지 않은 역할을 인증해야 한다[04.38].

신원 기반 인증: 암호모듈이 신원 기반 인증 메커니즘을 지원하면, 암호모듈은 운영자가 개별적이고 유일하게 식별되는 것을 요구해야 한다[04.39]. 운영자에 의해 선택된 1개 이상의 암시적 또는 명시적 역할을 요구해야 한다[04.40]. 또한, 운영자가 선택된 역할을 맡을 권한이 있는지 여부와 함께, 운영자의 신원을 인증해야 한다[04.41]. 운영자 신원 인증, 역할 선택과 선택된 역할의 부합하는 인증은 결합시킬 수 있다. 암호모듈이 운영자의 역할 변경을 허용하는 경우, 이전에 인증받지 않았던 역할을 수행하는 식별된 운영자를 인증해야 한다[04.42].

암호모듈은 인증된 운영자에게 인가받은 역할 내에서 허용된 모든 서비스를 수행하도록 허용하거나 각 서비스별 또는 서비스의 여러 집합을 위한 별도의 인증을 요구하기도 한다. 암호모듈이 리셋, 재부팅, 전원 재인가 후 모듈은 운영자를 인증해야 한다[04.43].

지식이나 소유(예: 패스워드, PIN, 암호키 등), 소유(예: 물리적 키, 토큰 등), 개인 특징(예: 생체인식) 등을 포함하여 지원된 인증 메커니즘의 구현을 위해 암호모듈은 다양한 유형의 인증 데이터를 요구할 수 있다. 암호모듈 내의 인증 데이터는 인가되지 않은 사용, 노출, 변경 및 대체로부터 보호되어야 한다[04.44]. 검증대상 보호함수는 인증 메커니즘의 일부로 사용될 수 있다.

인증 메커니즘의 초기화는 특수 처리를 보장할 수 있다. 운영자가 암호모듈에 최초로 접근하였을 때, 암호모듈이 운영자를 인증하기 위한 데이터를 가지고 있지 않다면, 암호모듈에 대한 접근을 통제하고 인증 메커니즘을 초기화하기 위해 다른 인가된 방법(예: 통제 절차, 제품 출하 시 설정된 인증 데이터 또는 기본적으로 설정된 인증 데이터)이 사용되어야 한다[04.45]. 모듈을 통제하는 데 기본 설정 인증 데이터가 사용될 경우, 최초 인증 후 기본 설정 인증 데이터는 교체되어야 한다[04.46]. 기본적으로 설정된 인증 데이터는 제로화 요구사항을 만족시키지 않아도 된다(**7.9.7**).

인증 메커니즘은 여러 인증 속성으로 구성된 메커니즘 그룹일 수 있으며, 각 속성이 공동으로 이 조항의 요구사항을 만족시킬 수 있다. 암호모듈이 운영자를 인증하는 데 암호알고리즘을 사용할 경우, 이들 암호알고리즘은 검증대상 암호알고리즘이어야 한다[04.47].

- 모듈은 **부속서** E에 명시된 대로 검증대상 인증 메커니즘을 구현해야 한다[04.48].
- 검증대상 인증 메커니즘의 보안 강도는 보안정책 문서에 명시되어야 한다(**부속서** B)[04.49].
- 검증대상 인증 메커니즘을 수행할 때마다, 모듈은 인증 객체의 보안 강도를 충족시켜야 한다[04.50]. 1분 동안 검증대상 인증 메커니즘을 사용하기 위해 여러 번 시도를 할 경우, 모듈은 인증 객체의 보안 강도를 충족해야 한다[04.51].
- 검증대상 인증 메커니즘은 요구사항에 적합하게 모듈에 구현되어야 하며, 문서로 규정한 통제 절차 또는 보안 규칙(예: 패스워드 크기 제한)에 의존하지 않아야 한다[04.52].
- 보안수준 2에서 소프트웨어 암호모듈의 경우, 운영체제가 인증 메커니즘을 구현할 수도 있다. 운영체제에 인증 기능이 구현되어 있을 때, 인증 메커니즘은 이 조항의 요구사항을 충족해야 한다[04.53].
- 인증을 수행하는 동안 운영자는 피드백되는 인증 데이터를 인식할 수 없어야 한다(예: 패스워드가 입력될 때 눈으로 볼 수 없어야 한다)[04.54]. 중요하지 않은 글자는 실제 인증 데이터에 표시할 수도 있다.
- 인증을 수행하는 동안 운영자에게 피드백되는 정보가 요구되는 인증 메커니즘 강도를 약화시켜서는 안 된다[04.55].

보안수준 1

보안수준 1의 경우, 암호모듈은 모듈로의 접근 통제를 위한 인증 메커니즘을 요구하지 않는다. 암호모듈이 인증 메커니즘을 제공하지 않는 경우에도, 운영자는 암호모듈에서 암시적 또는 명시적으로 1개 이상의 역할을 맡아야 한다[04.56].

보안수준 2

보안수준 2의 경우, 암호모듈은 암호모듈 접근 통제를 위해 최소한 역할 기반 인증 메커니즘을 사용해야 한다[04.57].

보안수준 3

보안수준 3의 경우, 암호모듈은 암호모듈 접근 통제를 위해 신원 기반 인증 메커니즘을 사용해야 한다[04.58].

보안수준 4

보안수준 4의 경우, 암호모듈은 암호모듈 접근 통제를 위해 다중체계 신원 기반 인증 메커니즘을 사용해야 한다[04.59].

7.5 소프트웨어/펌웨어 보안

암호모듈은 하드웨어 또는 소프트웨어, 펌웨어, 하이브리드 모듈 중 하나로 정의한다(**7.2.2**). 해당 절의 요구사항은 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소에 적용되어야 한다[05.01].

하드웨어 내에서 완전하게 실행되는 암호모듈은 이 표준의 소프트웨어/펌웨어 보안 요구사항의 대상이 아니다.

검증대상 무결성기술을 위해 사용되는 공개 검증키 또는 키 메시지 인증키는 모듈 코드 내에 있을 수 있지만 SSP로 간주하지 않는다.

A.2.5를 만족하는 개발 문서가 제출되어야 한다[05.02].

보안수준 1

보안수준 1의 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소에는 다음과 같은 요구사항이 적용되어야 한다[05.03].

- 모든 소프트웨어와 펌웨어는 **7.11.7**의 요구사항을 만족해야 하며, 설치 전에 변경되어서는 안 된다[05.04].
- 검증대상 무결성 기법을 사용하는 암호 메커니즘은 모듈의 정의된 암호경계 내에서 다음 중 한 가지 방법으로 모든 소프트웨어 구성 요소와 펌웨어 구성 요소에 적용해야 한다[05.05].
  - 암호모듈 자체로 무결성 검증
  - 다른 검증대상 암호모듈의 검증대상 동작모드에서 무결성 검증
- 무결성 시험 실패 시, 모듈은 오류 상태로 전환되어야 한다[05.06]. 검증대상 무결성기술은 단일 인증 코드/서명, 또는 복수 인증 코드/서명으로 구성되며, 복수 인증 코드 또는 서명은 어느 하나라도 실패할 경우 모듈은 오류 상태로 전환되어야 한다[05.07]. 무결성기술 메커니즘의 예상하는 참조 출력은 데이터로 간주할 수 있지만 그 자체는 무결성기술의 대상이 아니다. 소프트웨어 또는 펌웨

어 무결성 시험 중 임시로 생성된 값은 무결성 시험이 완료되면 모듈에 의해 제로화되어야 한다[05.08].

- 운영자는 **7.3.2**에 명세한 HMI 또는 SFMI, HSMI, HFMI 서비스를 통해서 들어온 요청에 따라 검증대상 무결성기술을 수행할 수 있어야 한다[05.09].
- 암호모듈과 (**7.4.3**에 명세된) 서비스의 (**7.3.3**에 명세된) 모든 데이터 입력, 제어 입력, 데이터 출력, 제어 출력 및 상태 출력은 정의된 HMI 또는 SFMI, HFMI, HSMI를 통해 이뤄져야 한다[05.10].
- 소프트웨어 또는 펌웨어 모듈의 경우, 로드된 소프트웨어 또는 펌웨어 이미지가 유효성이 검증된 모듈 이미지의 완전히 대체하거나 또는 오버레이가 아닌 경우, 그 대체물 또는 오버레이가 새로운 모듈을 구성하기 때문에 소프트웨어/펌웨어 로드 시험은 적용할 수 없다(NA).

  로드된 소프트웨어 또는 펌웨어가 ① 검증대상 암호모듈과 연계 또는 결합되는 경우 또는 ② 검증대상 암호모듈을 변경하는 경우 ③ 검증대상 암호모듈을 실행시키는 핵심 부분인 경우에 해당하지만 검증대상 모듈을 완전히 대체하거나 오버레이가 아닌 경우, 로드된 소프트웨어 또는 펌웨어는 소프트웨어/펌웨어 로드 시험이 적용되어야 하고, 이 시험은 검증대상 모듈에 의해 수행되어야 한다[05.11].

보안수준 2

보안수준 1의 요구사항 외에, 다음과 같은 요구사항은 보안수준 2에 대한 암호모듈의 소프트웨어와 펌웨어 구성 요소에 적용되어야 한다[05.12].

- 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소는 실행 형태[예: 소스 형태가 아닌 코드, 오브젝트 코드 또는 적시(just-in-time) 컴파일 코드]의 코드만 포함해야 한다[05.13].

- HMI, SFMI, HFMI 또는 HSMI 인터페이스를 통한 서비스 중에서 운영자가 실행 코드를 검사할 수 있어서는 안 된다[05.14].

- 검증대상 전자서명 또는 키 메시지 인증 코드는 모듈의 정의된 암호경계 내 모든 소프트웨어와 펌웨어에 적용할 수 있어야 한다[05.15]. 계산된 결과가 성공을 확인할 수 없다면, 무결성 시험은 실패이며 모듈은 오류 상태로 전환되어야 한다[05.16].

보안수준 3, 4

보안수준 1, 2의 요구사항 외에, 다음 요구사항은 보안수준 3과 4에 대한 암호모듈의 소프트웨어 구성 요소 및 펌웨어 구성 요소에 적용된다[05.17].

검증대상 전자서명을 사용하는 암호 메커니즘은 암호모듈에 대하여 정의된 암호경계 내의 모든 소프트웨어 구성 요소 및 펌웨어 구성 요소에 적용되어야 한다[05.18]. 계산된 결과가 성공을 확인할 수 없다면 무결성 시험은 실패이며 모듈은 오류 상태로 전환되어야 한다[05.19].

전자서명 기술은 단일 서명 또는 복수 서명으로 구성되며, 복수 서명 중 어느 하나라도 실패할 경우 모듈이 오류 상태로 전환되어야 한다[05.20]. 개인 서명키는 모듈의 외부에 존재해야 한다[05.21].

7.6 운영환경

7.6.1 운영환경 일반 요구사항

암호모듈의 운영환경은 운영할 모듈에 요구되는 소프트웨어와/또는 펌웨어, 하드웨어의 관리를 지칭한다. 소프트웨어 또는 펌웨어, 하이브리드 모듈의 운영환경에는 적어도 모듈 구성 요소와 컴퓨팅 플

랫폼, 그 컴퓨팅 플랫폼상에서 소프트웨어 또는 펌웨어 실행을 관리 또는 허용하는 운영체제를 포함한다. 하드웨어 모듈은 모듈 내에 내부 소프트웨어 또는 펌웨어의 실행을 허용하는 운영체제로 구성된 운영환경을 가질 수 있다. 운영체제는 해당되는 경우 가상 머신(시스템과/또는 프로세스)과 런타임 환경(예: Java 런타임 환경－JRE)이 포함된 것으로 간주한다.

범용 운영환경은 소프트웨어와 펌웨어 구성 요소를 관리하고 또한 워드프로세서 등 범용 응용 소프트웨어를 포함하여 시스템과 운영자 프로세스/스레드를 관리하는 시중의 범용 운영체제(예: 자원 관리자)의 사용을 지칭한다.

운영환경은 변경 불가 또는 제한적, 변경 가능한 환경일 수 있다.

다음의 조항은 이 세 가지 운영환경을 명시한다.

1. **변경 불가능한 운영환경**: 운영자 또는 프로세스에 의한 모듈 구성 요소 또는 컴퓨팅 플랫폼, 운영체제의 변경을 방지하는 방식으로 설계 또는 구성한다. 이 환경은 프로그래밍할 수 없는 컴퓨팅 플랫폼이나 소프트웨어 또는 펌웨어의 추가적인 로드를 방지하는 하드웨어 모듈 내 펌웨어 모듈 운영으로 구성할 수 있다.

2. **제한적 운영환경**: 운영자 또는 프로세스에 의한 모듈 구성 요소 또는 컴퓨팅 플랫폼, 운영 시스템의 통제된 변경을 허용하는 방식으로 설계 또는 구성한다. 이 환경은 추가 펌웨어의 추가적 로드가 **7.4.3.4**에서 명시된 펌웨어 로드 요구사항을 만족하는 경우 프로그래밍 가능한 하드웨어 모듈 내에서 운영되는 펌웨어가 될 수 있다.

3. **변경 가능한 운영환경**: 기능을 추가/삭제/변경하도록 구성할 수 있는 운영환경을 지칭하고/또는 범용 운영체제 기능(예: 컴퓨터 운영체제, 구성 가능한 스마트카드 운영체제, 프로그램 가능한 소프트웨어의 사용)을 포함할 수 있다. 운영자 또는 프로세스가 소프트웨어 구성 요소를 변경할 수 있고/또는 운영자 또는 프로세스가 정의된 소프트웨어 또는 펌웨어, 하이브리드 모듈의 일부가 아닌 소프트웨어(예: 워드프로세서)를 로드 및 실행할 수 있으면 운영체제는 변경 가능한 운영환경으로 간주한다.

   변경 가능한 운영환경은 다음의 특징을 지닌다.

   운영환경 내에서 기능을 추가 또는 변경할 수 있다. 그러한 기능이 운영환경에 의해 간섭이 차단되지 않는 한 암호모듈의 운영을 간섭하지 않는다고 장담할 수는 없다.

   운영환경의 신뢰되는 부분에 속하지 않는 같은 운영환경에서 운영되는 어떤 기능도 암호모듈의 정의된 인터페이스를 거치지 않고는 SSP로 접근하지 못하도록 요구된다.

   그러므로 운영환경에게 운영 중 암호모듈은 CSP 관련 암호모듈에서 정보를 얻을 수도 없고 CSP 또는 PSP, 암호모듈 자체가 제공하는 인터페이스를 거치지 않는 암호모듈의 실행 흐름을 변경할 수 없는 운영환경 내 다른 기능과 분리하는 기능을 제공하도록 요구된다.
   코드와 데이터가 담긴 암호모듈을 정확하게 보호하기 위해(예: 암호모듈에 있는 내부 프로세스 간의 특정 통신 금지, 암호모듈의 SSP 또는 코드가 들어 있는 파일로의 제한적 접근적 권리 부여) 운영환경의 특정 구성이 요구될 수 있다.

다음의 표는 운영환경의 몇 가지 예를 제공한다.

표 2 – 운영환경의 예

형상 예	운영환경
코드 로딩을 허용하지 않는 컴퓨팅 플랫폼 운영자에 의한 컴퓨팅 플랫폼, 운영체제 또는 암호모듈의 형상 변경을 허용하지 않는 컴퓨팅 플랫폼	변경 불가
표준에서 요구하는 적용 가능한 모든 요구사항을 만족하고, 인증된 추가 코드의 로딩을 허용하는 운영체제를 포함한 컴퓨팅 플랫폼	제한적
표준의 소프트웨어 또는 펌웨어 로딩 요구사항을 만족하지 않고, 코드의 로딩을 허용하는 컴퓨팅 플랫폼	변경 가능
보안 보호 기법 제거를 허용한 운영자가 운영체제를 다시 설정할 수 있는 코드가 있는 컴퓨팅 플랫폼	변경 가능

변경 불가능한 또는 제한적인 환경의 경우, 변경 불가 또는 제한적 환경을 유지하는 관리 구성 요소에 컴퓨팅 플랫폼, 운영 시스템, 암호모듈 자체의 속성이나 상기 모두를 포함할 수 있다.

변경 불가능한 또는 제한적인 환경에서 실행하는 코드는 이 표준에서 펌웨어로 지칭한다. 변경 가능한 환경에서 실행하는 코드는 이 표준에서 소프트웨어로 지칭한다.

변경 불가능한 운영환경 또는 제한적 운영환경인 경우, **7.6.2**의 운영체제 요구사항을 적용해야 한다[06.01].

변경 가능한 운영환경인 경우, **7.6.3**의 운영체제 요구사항을 적용해야 한다[06.02].

A.2.6에 명시된 요구사항을 만족하는 개발 문서를 제공해야 한다[06.03].

7.6.2 제한적인 운영환경 또는 변경 불가능한 운영환경의 요구사항

보안수준 1

암호모듈이 **7.7**의 보안수준 1인 경우, **7.6.3**의 보안수준 1 요구사항이 적용되어야 한다[06.04].

보안수준 2, 3, 4

추가적인 요구사항이 없다.

7.6.3 변경 가능한 운영환경의 요구사항

보안수준 1

다음의 요구사항을 보안수준 1의 운영체제에 적용한다.

- 암호모듈의 각 인스턴스는 암호모듈 자신의 SSP를 제어해야 한다[06.05].
- 운영환경은 응용 프로그램의 데이터가 운영환경 내의 프로세스 메모리에 있거나 영구 저장소에 저장되는 것과 상관없이 인가되지 않은 CSP에 대한 접근과, 제어되지 않는 보안매개변수의 변경을 방지함으로써 각각의 응용 프로세스가 독립적으로 동작할 수 있도록 하는 기능을 제공해야 한다[06.06]. 이는 암호모듈과 운영체제의 신뢰되는 부분에 의해서 CSP와 SSP로의 직접 접근이 제한된다는 것을 말한다. 운영환경 설정에 대한 제한 사항은 암호모듈의 보안정책 문서에 서술되어야 한다[06.07].

- 암호모듈에 인해 생성된 프로세스는 해당 암호모듈에 의해서만 소유되어야 하며, 외부 프로세스/운영자는 소유할 수 없다[06.08].

비고 이 요구사항은 관리자 설명서 및 절차에 의해 시행될 수 없으며, 암호모듈 자체에 의해 수행되어야 한다.

보안수준 2

보안수준 1의 요구사항 외에, 보안수준 2에서 운영환경은 다음과 같은 요구사항이나 관련 검증기관이 인정하는 조건들을 충족시켜야 할 것이다[06.09].

- 모든 암호 소프트웨어, SSP, 제어 정보 및 상태 정보는 역할 기반 접근 통제나 최소한 임의 접근 통제를 제공하는 운영체제의 통제를 따라야 한다. 여기서 임의적 접근 통제란, 예를 들면 새 그룹을 정의하고 대응되는 제한적 권한을 접근통제목록(ACL)을 통해 할당하는 메커니즘을 갖고, 각 사용자를 하나 이상의 그룹에 배정한다[06.10]. 운영체제는 인가되지 않은 ① 실행, ② 변경, ③ SSP, 제어 정보 및 상태 정보의 읽기를 방지하도록 설정되어야 한다[06.11].
- 평문 데이터, 운영체제의 암호 소프트웨어, SSP, 인증 데이터를 보호하기 위한 접근통제 메커니즘은
  - 역할이 어떻게 정의되는지 저장된 암호화 소프트웨어에 대한 독점적 실행 권한에 대한 제한적 허용이 어떻게 정의된 역할과 관계되는지 정의하고 적용하도록 설정되어야 한다[06.12].
  - 일련의 역할이나 그룹에게 암호경계 내에 저장된 암호모듈 소프트웨어[암호 프로그램, 암호 데이터(예: 암호 감사 데이터), SSP, 평문 데이터]를 변경할 수 있는 제한적 접근을 정의하고 역할이나 그룹이 이를 실행할 수 있도록 설정해야 한다[06.13].
  - 일련의 역할이나 그룹에게 암호 데이터(예: 암호 감사 데이터), CSP, 평문 데이터를 읽을 수 있는 제한적 접근을 정의하고, 역할이나 그룹이 이를 실행할 수 있도록 설정해야 한다[06.14].
  - 일련의 역할이나 그룹에게 SSP를 입력할 수 있는 제한적 권한을 정의하고 역할이나 그룹이 이를 실행할 수 있도록 설정해야 한다[06.15].
- 다음의 명세는 역할이나 지정된 그룹의 권한과 보안정책에서 정의하는 서비스와 일치해야 한다[06.16].
  - 유지보수 역할을 지원하지 않을 때 운영체제는 모든 운영자와 실행 중인 다른 프로세스들이 암호 프로세스(예: 암호 프로그램 이미지의 로드 및 실행)를 변경하는 것을 방지해야 한다[06.17]. 이 경우에서 가동 중인 프로세스는 운영체제에 의해 소유되지 않았거나 초기화되지 않은(즉, 운영자-초기화) 프로세스 또는 암호를 지칭한다.
  - 운영체제는 사용자 역할 또는 사용자 그룹의 프로세스가 다른 프로세스가 소유한 SSP나 시스템 SSP에 대한 읽기 또는 쓰기 권한을 획득하는 것을 방지해야 한다[06.18].
  - 위의 요구사항을 충족시키는 운영체제의 설정은 관리자 지침에 구체적으로 명세해야 한다[06.19]. 관리자 지침은 콘텐츠를 보호하기 위하여 운영체제 구성에 대하여 기술해야 한다[06.20].

운영체제를 위한 식별과 인증 메커니즘은 **7.4.3**의 요구사항에 부합되고 모듈 보안정책에 명세되어야 한다[06.21].

모든 암호 소프트웨어와 SSP, 제어, 상태 정보는 다음의 제어를 만족해야 한다[06.22].

- 최소한 다음의 속성을 가지는 운영체제[06.23]
  - 운영체제는 각각의 감사 이벤트의 감사 메커니즘을 시간과 같이 제공해야 한다[06.24]. 암호모듈은 감사 기록의 일환으로 SSP를 포함하지 않아야 한다[06.25].
  - 암호모듈은 다음의 이벤트들을 운영체제의 감사 메커니즘에 의해 기록해야 한다[06.26].
    - 암호 데이터와 SSP의 변경, 접근, 삭제, 추가
    - 암호관리자 기능을 위해 유효하지 않은 입력을 제공하려는 시도

  - 암호관리자 역할에서/로부터 운영자의 추가 또는 삭제(이 역할이 암호모듈에 의해 관리된다면)
  - 보안 관련 암호관리자 기능의 사용
  - 암호모듈과 관련된 인증 데이터에 접근하기 위한 요청
  - 암호모듈과 관련된 인증 메커니즘(예: 로그인)의 사용
  - 암호관리자 권한에 대한 요청
- 운영체제의 감사 메커니즘은 다음의 운영체제 관련 이벤트를 감사할 수 있어야 한다[06.27].
  - 감사 흔적을 저장하는 감사 데이터에 대한 모든 운영자 읽기 또는 쓰기 접근
  - 암호 데이터 또는 SSP를 저장하기 위해 암호모듈을 사용하는 파일에 대한 접근
  - 암호관리자 역할에서/로부터 운영자의 추가 또는 삭제(이 역할이 운영환경에 의해 관리된다면)
  - 인증 데이터 관리 메커니즘 사용을 위한 요청
  - 현 보안수준에서 신뢰 채널이 제공될 때, 신뢰 채널 기능을 사용하기 위한 요청과 요청의 수락 여부
  - 현 보안수준에서 신뢰 채널이 제공될 때, 개시자의 신원과 신뢰 채널의 대상
- 운영체제는 보안정책에 인정된 운영자 외의 운영자가 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터를 변경하지 못하게 설정되어야 한다[06.28].

• 암호모듈이 검증대상 운영 모드로 작동하는지와 관계없이, 위의 요구사항을 충족하도록 설정된 운영체제만 이 보안수준에 사용되어야 한다[06.29]. 감사 기록은 검증대상 보호함수를 사용하여 무단 변경으로부터 보호해야 한다.

7.7 물리적 보안

7.7.1 물리적 보안 형체

암호모듈은 모듈 내용물에 대한 비인가된 물리적 접근을 제한하고 설치 시 모듈의 비인가된 사용이나 변경(모듈 전체 내용물 교체 포함)을 방어하기 위하여 물리적 보안 메커니즘을 사용해야 한다[07.01]. 암호경계 내의 모든 하드웨어, 소프트웨어, 펌웨어, 데이터 구성 요소 및 SSP를 보호해야 한다[07.02].

암호모듈이 컴퓨팅 플랫폼에서 제공되는 물리적 보안이 유일하게 소프트웨어로만 완전히 구현되어 있다면, 이 표준의 물리적 보안 요구사항의 대상이 아니다.

이 조항의 요구사항은 하드웨어 모듈, 펌웨어 모듈, 그리고 하드웨어와 펌웨어 조합모듈의 구성 요소에 적용되어야 한다[07.03].

이 조항의 요구사항은 모듈의 정의된 물리적 경계에 적용할 수 있어야 한다[07.04].

물리적 보안 요구사항은 다음 세 가지 정의된 암호모듈의 물리적 형체에 대하여 명시한다.

1. **단일칩 암호모듈(single-chip cryptographic modules)** 단일 집적회로(IC) 칩이 독립 장치로 사용되거나 또는 물리적으로 보호되지 않는 일부 다른 모듈이나 봉함 내부에 탑재될 수 있는 물리적 개체이다. 단일칩 암호모듈의 예로는 단일 IC칩 또는 단일 IC칩으로 구성된 스마트카드를 포함한다.

2. **다중칩 내장형 암호모듈(multiple-chip embedded cryptographic modules)** 둘 또는 그 이상의 IC칩들이 상호 연결되고, 또한 물리적 보호가 적용되지 않는 봉함이나 제품의 내부에 내장된 물리적 구현을 말한다. 다중칩 탑재 암호모듈의 예로는 어댑터와 확장 보드를 포함한다.

3. **다중칩 독립형 암호모듈(multiple-chip standalone cryptographic modules)** 둘 또는 그 이상 IC칩들이 상호 연결되고, 또한 물리적 보호가 전체적으로 적용된 봉함 내부에 내장되는 것을 말한다.

다중칩 독립 암호모듈의 예로는 보안 라우터, 암호 무선 통신 기기 또는 USB 토큰을 포함한다.

암호모듈의 물리적 보안 메커니즘에 따라 다음에 대하여 물리적으로 접근, 사용 또는 변경하고자 하는 비인가된 시도가 탐지될 확률이 높아야 한다[07.05].

- 시각적 흔적을 남기는 계속된 시도(즉, 변조-증거)
- 접근 시도 도중

암호모듈은 CSP 를 보호하기 위하여 적절하고 즉각적 조치가 취해야 한다[07.06].

표 3은 4가지 보안수준에 각각에 대해 모든 형체에 대한 일반적인 요구사항과 3가지 형체에 대한 물리적인 보안 요구사항에 대한 요약이다. 각 보안수준에 따른 형체별 물리적 보안 요구사항은 동일 수준에서의 일반 요구사항과 이전 수준의 형체별 요구사항을 한층 강화시킨다.

표 3 – 암호모듈에 대한 물리적 보안 요구사항 요약

	모든 형체에 대한 일반 요구사항	**단일칩**	**다중칩 내장형**	**다중칩 독립형**
보안수준 1	생산 등급 구성 요소. 표준 부식 방지. 유지보수 접근 인터페이스에 접속할 때 절차적 또는 자동 제로화	추가 요구사항 없음.	생산 등급 봉함 또는 제거 가능 덮개	생산 등급 봉함 또는 제거 가능 덮개
보안수준 2	변조-증거. 가시적 스펙트럼 내 불투명 또는 반투명화. 환기구나 틈새를 통하여 직접 관측 방지	칩이나 봉함에 대한 변조-증거 코팅	개구부나 제거 가능 덮개를 위한 변조-증거 캡슐화 재료, 또는 변조-증거 봉인/따개 방지 잠금장치가 있는 봉함	개구부나 제거 가능 덮개를 위한 변조-증거 캡슐화 재료, 또는 변조-증거 봉인/따개 방지 잠금장치가 있는 봉함
보안수준 3	변조 응답 및 제로화 회로. 유지보수 접근 인터페이스 접근 시 자동으로 제로화. 환기구나 틈새를 통한 탐침 방어. 온도 및 전압용 EFP 또는 EFT	칩상의 견고한 변조-증거 코팅 또는 강력한 제거-방지 및 침투 방지 봉함	견고한 변조-증거 캡슐화 재료 또는 강력한 봉함	견고한 변조-증거 캡슐화 재료 또는 강력한 봉함
보안수준 4	변조 검출 및 응답 겉봉함. 온도 및 전압용 EFP. 오류 유도 방지	칩상의 견고한 제거-방지 코팅	제로화 기능을 갖는 변조 검출 및 응답 겉봉함	제로화 기능을 갖는 변조 검출 및 응답 겉봉함

일반적으로, 보안수준 1은 요구사항의 기준 설정을 제공한다. 보안수준 2는 변조-증거 메커니즘과 모듈 내 핵심 영역의 내부 운영에 관한 정보를 수집 못하게 하는 기능(불투명성)을 추가로 요구한다. 보안수준 3은 제거 가능 덮개와 개구부에 대한 변조 검출 및 응답 메커니즘과 개구부나 입력 지점을 통한 직접 탐침 메커니즘을 갖는 강하고 견고한 절연 또는 비절연 봉함을 사용토록 추가 요구한다. 환경장애보호(EFP) 기능 또는 환경장애시험(EFT) 기능이 보안수준 3에서 요구된다. 보안수준 4는 전체 봉함 또는 중요 부분 손상에 대한 변조 검출 및 응답 메커니즘을 갖는 절연 또는 비절연의 강한/견고한 봉함을 사용토록 추가 요구한다. 환경장애보호 기능(EFP) 및 오류 유도 공격에 대한 방어 기능이 보안수준 4에서 요구된다.

암호모듈이 물리적인 접근이 허용되도록 설계할 때, 유지보수 접근 인터페이스에 대한 보안 요구사항이 명시된다(예: 모듈 벤더나 기타 인가된 개인에 의해).

변조 검출과 변조 응답은 변조-증거에 대한 대체 수단이 아니다.

A.2.7의 요구사항을 충족하는 개발 문서를 제출해야 한다[07.07].

7.7.2 물리적 보안 일반 요구사항

다음 요구사항은 모든 물리적 형체에 적용되어야 한다[07.08].

- 개발 문서는 암호모듈의 물리적 보안 메커니즘을 구현한 물리적 형체와 보안수준을 명세하여야 한다[07.09].
- 물리적 보안 목적을 위해 중요 데이터를 짧은 시간 내에 제로화해야 한다. 탐지 후 제로화 도중 중요 데이터가 탈취되지 않도록 해야 한다[07.10].
- 암호모듈이 모듈의 내용물에 대한 물리적 접근이 필요한 유지보수 역할을 포함하거나, 또는 그 모듈이 물리적 접근이 허용되도록 설계되어 있다면(예: 모듈 벤더나 기타 인가된 개인), 이때
  - 유지보수 접근 인터페이스가 정의되어야 한다[07.11].
  - 유지보수 접근 인터페이스는 제거 가능 덮개나 개구부까지도 포함해서 암호모듈 내용물에 대한 모든 물리적 접근 경로를 포함해야 한다[07.12].
  - 유지보수 접근 인터페이스 내에 포함된 제거 가능 덮개나 개구부는 적절한 물리적 보안 메커니즘을 사용하여 보호되어야 한다[07.13].

보안수준 1

다음 요구사항은 보안수준 1에 대한 모든 암호모듈에 적용하여야 한다[07.14].

- 암호모듈은 표준 부식 방지 기술(예: 환경적 또는 기타 물리적 손상을 보호하기 위하여 모듈 회로에 적용된 절연 코팅 또는 봉인 코팅)을 포함한 생산 등급 구성 요소로 구성되어야 한다[07.15].
- 물리적 유지보수를 수행할 때, 운영자가 제로화를 절차에 따라 실행하거나 또는 암호모듈이 제로화를 자동으로 실행해야 한다[07.16].

보안수준 2

보안수준 1에 대한 일반 요구사항에 외에, 다음 요구사항은 보안수준 2의 모든 암호모듈에 적용되어야 한다[07.17].

- 모듈에 물리적 접근을 시도할 때 암호모듈은 변조-증거(예: 덮개, 봉함 및 봉인)를 제공하여야 한다[07.18].
- 모듈의 핵심 영역에 대한 내부 동작 정보 수집을 방지하기 위하여 변조-증거 물질, 코팅 또는 봉함은 육안(가시광선 파장 범위 400 nm～750 nm의 빛)으로 볼 수 없는 불투명 또는 반투명이어야 한다[07.19].
- 만일 암호모듈에 환기구나 틈새가 있다면, 직접 육안 관찰을 통하여 모듈의 내부적 구조나 구성 요소 등과 관련된 정보의 수집을 방지할 수 있도록 모듈이 제작되어야 한다. 육안 관찰은 모듈의 내부 구조나 구성 요소를 볼 수 있도록 인공 광원을 사용할 수 있다[07.20].

보안수준 3

보안수준 1과 2에 대한 일반 요구사항 외에, 다음 요구조건들은 보안수준 3에 대한 모든 암호모듈에

적용되어야 한다[07.21].

- 암호모듈에 개구부나 제거 가능 덮개가 포함되어 있거나 유지보수 접근 인터페이스가 정의되어 있다면, 그 모듈은 변조 대응 및 제로화 기능을 포함해야 한다[07.22]. 개구부가 열리거나 덮개가 제거될 때 또는 유지보수 접근 인터페이스가 사용될 때, 암호모듈의 변조 대응 및 제로화 기능이 모든 비보호된 SSP를 즉각 제로화시켜야 한다[07.23]. 보호되지 않은 SSP가 암호모듈 내부에 있을 때 변조 대응 및 제로화 기능이 작동 상태를 유지해야 한다[07.24].
- 암호모듈에 환기구나 틈새가 있다면, 모듈은 봉함 내부로 탐지되지 않는 탐침을 방지(예: 한 개의 연계 탐침기에 의한 탐침 방지)하는 방식으로 제작되어야 한다[07.25].
- 강도 또는 경도가 높은 절연 또는 비절연의 봉함, 코팅 또는 매몰재는 모듈이 동작 중이거나 저장 및 배포될 때의 온도 범위(설계 명세)에서 강도와 경도가 유지되어야 한다[07.26].
- 변조-증거 봉인이 있는 경우, 봉인은 고유 번호로 할당되거나 또는 독립적으로 식별 가능(예: 고유 번호가 있는 증거 테이프 또는 고유 식별 가능한 홀로그램 봉인)해야 한다[07.27].
- 암호모듈은 EFP 특징을 포함하고 있거나 또는 EFT를 적용해야 한다[07.28].

보안수준 4

보안수준 1, 2와 3에 대한 일반 요구사항에 추가하여, 다음 요구사항은 보안수준 4에 해당하는 모든 암호모듈에 적용되어야 한다[07.29].

- 암호모듈은 경도가 높은 불투명 제거-방지 코팅에 의해 보호되거나 변조 대응 및 제로화 기능을 갖는 변조 탐지 겉봉함에 의해 보호되어야 한다[07.30].
- 암호모듈은 EFP 특징을 포함하고 있어야 한다[07.31].
- 암호모듈은 오류 유도 공격에 대한 보호 기술을 제공하여야 한다[07.32]. 오류 유도 대응 기술과 대응 측정 지수들은 **부속서** B에서 명시된 바와 같이 문서화되어야 한다[07.33].

7.7.3 물리적 보안 형체에 따른 물리적 보안 요구사항

7.7.3.1 단일칩 암호모듈

7.7.2에서 명시한 일반 보안 요구사항 외에, 다음의 요구사항은 단일칩 암호모듈에 적용되어야 한다.

보안수준 1

단일칩 암호모듈에는 추가적인 보안수준 1의 요구사항이 없다.

보안수준 2

보안수준 1의 요구사항 외에, 다음 요구사항들은 보안수준 2의 단일칩 암호모듈에 적용되어야 한다. [07.34].

- 암호모듈을 직접 관찰, 탐침 또는 조작하는 것을 방지하는 목적과 모듈을 변조 또는 제거하려는 시도에 대한 증거를 제공하는 목적을 얻기 위하여, 변조-증거 코팅(예: 변조-증거 부식 방지물 또는 부식 방지층 위에 도포한 변조-증거 물질) 또는 변조-증거 봉함이 암호모듈에 처리되어 있어야 한다[07.35].

보안수준 3

보안수준 1, 2의 요구사항 외에, 다음 요구사항들은 보안수준 3의 단일칩 암호모듈에 적용되어야 한

다[07.36].

- 모듈은 경도가 높은 불투명 변조-증거 코팅(예: 부식 방지층을 덮고 있는 경도가 높은 불투명 에폭시) 처리가 되어 있어야 한다[07.37].
- 봉함을 제거하려는 시도 시 또는 침투하려는 시도 시, 암호모듈에 높은 확률로 심각한 손상(즉, 모듈 기능의 정지)을 주도록 봉함이 구현되어야 한다[07.38], [07.39].

보안수준 4

보안수준 1, 2, 3의 요구사항 외에, 다음 요구사항들은 보안수준 4의 따른 단일칩 암호모듈에 적용되어야 한다[07.40].

- 모듈에서 코팅을 벗겨 내거나 들추어 내려는 시도가 있을 때 모듈을 높은 확률로 심각한 손상(즉, 모듈 기능의 정지)을 주도록, 높은 경도 및 접착성을 갖는 제거-방지용 불투명 코팅으로 처리되어야 한다[07.41].
- 모듈의 코팅을 녹일 때 높은 확률로 모듈 자체를 녹이거나 모듈에 심각한 손상(즉, 모듈 기능의 정지)을 줄 수 있도록 제거-방지 코팅이 용해 특성을 가져야 한다[07.42].

7.7.3.2 다중칩 내장형 암호모듈

7.7.2에 명시된 일반 보안 요구사항 외에, 다음의 요구사항들이 다중칩 내장형 암호모듈에 적용되어야 한다.

보안수준 1

암호모듈에 봉함이나 제거 가능 덮개가 처리되어 있다면, 생산 등급의 봉함 또는 제거 가능 덮개가 사용되어야 한다[07.43].

보안수준 2

보안수준 1의 요구사항 외에, 다음의 요구사항은 보안수준 2의 다중칩 내장형 암호모듈에 적용하여야 한다[07.44].

- 모듈 구성 요소는 직접 관찰을 방지하고 모듈 구성 요소를 변조하거나 제거하려는 시도를 할 때 증거를 제공하는 변조-증거 코팅 또는 매몰재[예: 에칭 방지 코팅 또는 비정상 표기(bleeding) 페인트]로 표면 처리되어야 한다[07.45].
- 모듈은 개구부나 제거 가능 덮개를 포함할 수 있는 금속으로 된 또는 경도가 높은 플라스틱으로 된 생산 등급 봉함 내부에 포함되어야 한다[07.46].
- 봉함이 개구부나 제거 가능 덮개를 포함한다면, 개구부 또는 덮개는 물리적 또는 논리적 열쇠를 활용하여 따개 방지용 기계 잠금장치로 잠그거나[07.47], 변조-증거 봉인(예: 증거 표시 테이프 또는 홀로그램 봉인)으로 보호되어야 한다[07.48].

보안수준 3

보안수준 1, 2의 요구사항 외에, 다음 요구사항들은 보안수준 3의 다중칩 내장형 암호모듈에 적용되어야 한다[07.49].

- 암호모듈 내부에 포함된 회로의 다중칩 형체는 봉함을 제거하려는 시도 시 또는 침투하려는 시도 시 높은 확률로 모듈에 심각한 손상(즉, 모듈 기능의 정지)을 주는 경도 높은 코팅 또는 매몰재(예:

경도 높은 에폭시 물질)로 표면 처리되어야 한다[07.50].
- 모듈은 강도 높은 봉함에 내장되어야 한다[07.51].

이때 봉함을 제거하거나 침투하려는 시도 시 높은 확률로 모듈에 심각한 손상(즉, 모듈 작동의 기능 정지)을 줄 것이다.

보안수준 4

보안수준 1, 2, 3의 요구사항 외에, 다음 요구사항은 보안수준 4의 다중칩 내장형 암호모듈에 적용되어야 한다[07.52].

- 모듈 구성품은 강도 높고 경도가 높은 절연 또는 비절연 봉함에 내장되어야 한다[07.53]. SSP에 충분한 범위까지 접근하기 위한 매몰재 혹은 봉함 자르기, 드릴하기, 밀링하기, 갈아내기, 태우기, 용해하기 또는 분해하기 등의 변조를 탐지하는 겉봉함(예: 꼬불한 모양의 도체로, 휠 수 있는 절연막 인쇄 회로 또는 전선 묶음으로 둘러싼 패키지 또는 휘지 않고 쉽게 부러지는 회로 또는 강도 높은 봉함)에 의해 봉함은 포장되어야 한다[07.54], [07.55].
- 모듈은 변조 탐지 겉봉함을 지속적으로 감시해서 변조가 탐지되면 보호되지 않은 모든 SSP를 즉시 제로화해야 하는 변조 대응 및 제로화 회로를 포함해야 한다[07.56], [07.57], [07.58]. 암호모듈 내부에 보호되지 않은 SSP가 포함되어 있을 때 변조 대응 회로는 항상 작동 상태를 유지해야 한다[07.59].

7.7.3.3 다중칩 독립형 암호모듈

7.7.2에서 명시된 일반 보안 요구사항 외에, 다음의 요구사항들이 다중칩 독립형 암호모듈에 적용되어야 한다.

보안수준 1

암호모듈은 개구부 또는 제거 가능 덮개를 포함할 수 있는 금속으로 된 또는 경도가 높은 플라스틱으로 된 생산 등급 봉함에 모듈 전체가 내장되어야 한다[07.60].

보안수준 2

보안수준 1의 요구사항 외에, 다음 요구사항은 보안수준 2의 다중칩 독립형 암호모듈에 적용되어야 한다[07.61].

- 암호모듈의 봉함이 개구부 또는 제거 가능 덮개를 포함한다면 개구부 또는 덮개는 물리적 또는 논리적 키를 적용한 따개 방지 기계 잠금장치로 잠금이 되거나[07.62], 변조-증거 봉인(예: 증거 테이프 또는 홀로그램 봉인)으로 보호되어야 한다 [07.63].

보안수준 3

보안수준 1, 2의 요구사항 외에, 다음 요구사항은 보안수준 3의 다중칩 독립형 암호모듈에 적용되어야 한다[07.64].

- 모듈은 봉함을 제거하려는 시도 시 또는 침투하려는 시도 시 높은 확률로 모듈에 심각한 손상(예: 모듈의 작동 정지)을 주는 강도 높은 봉함에 내장되어 있어야 한다[07.65].

보안수준 4

보안수준 1, 2, 3의 요구사항 외에, 다음 요구사항은 보안수준 4의 다중칩 독립형 암호모듈에 적용되어야 한다[07.66].

- 암호모듈의 봉함은 덮개 스위치(예: 마이크로 스위치, 자기장 홀 효과 스위치, 영구자석 구동기 등), 움직임 검출기(예: 초음파, 적외선 또는 마이크로웨이브) 또는 보안수준 4에 명시된 기타 변조 탐지 메커니즘과 같은 변조 탐지 메커니즘을 사용하는 변조 탐지 겉봉함을 포함해야 한다[07.67]. 변조 탐지 메커니즘은 SSP에 충분한 범위까지 접근하기 위한 잘라내기, 드릴하기, 밀링하기, 갈아내기, 태우기, 용해하기 또는 분해하기와 같은 공격에 대응해야 한다[07.68].
- 암호모듈은 변조 탐지 겉봉함을 지속적으로 감시하고 변조 탐지 시 보호되지 않은 모든 SSP를 즉시 제로화해야 하는 변조 응답 및 제로화 기능을 포함해야 한다[07.69], [07.70], [07.71]. 보호되지 않는 SSP가 암호모듈 내부에 포함되어 있을 때 변조 대응 및 제로화 회로 기능이 작동 상태를 유지하고 있어야 한다[07.72].

7.7.4 환경장애보호/시험

7.7.4.1 환경장애보호/시험 일반 요구사항

전자 기기 및 회로는 특정 환경 조건 범위 내에서 운영할 수 있도록 설계한다. 명시된 정상 운영 전압 및 온도 범위에서 우발적 또는 고의적으로 벗어나는 경우, 암호모듈의 보안을 손상시킬 수 있는 비정상적인 운영이나 전자 기기 및 회로 고장을 야기할 수 있다. 환경장애보호(EFP) 특성을 충족하거나 환경장애시험(EFT)을 충족하는 모듈을 구축함으로써 암호모듈 보안이 극한 환경 조건에서도 손상되지 않는다는 것을 합리적으로 보장할 수 있다.

보안수준 1, 2의 경우, 모듈은 환경장애보호(EFP) 특성 또는 환경장애시험(EFT)을 요구하지는 않는다. 보안수준 3에서 모듈은 환경장애보호(EFP) 특성을 충족하거나 환경장애시험(EFT)을 충족해야 한다[07.73]. 보안수준 4에서 모듈은 환경 시험 보호(EFP) 특성을 적용하고 있어야 한다[07.74].

7.7.4.2 환경장애보호 특징

환경장애보호(EFP) 특성은 모듈의 안전성을 손상시킬 수 있는 모듈의 정상 동작 범위 밖일 때의 비정상 환경 조건들(우발적 또는 고의적)로부터 암호모듈을 보호해야 한다[07.75].

동작 온도 및 동작 전압이 규정된 정상 동작 범위를 벗어날 때 암호모듈은 이를 감시하고 정확하게 대응해야 한다[07.76].

온도 또는 전압이 암호모듈의 정상 동작 범위를 벗어난다면, 보호 기능은 다음 둘 중에 하나를 수행해야 한다[07.77].

- 동작 진행을 방지하기 위해 암호모듈을 정지함.
- 보호되지 않은 모든 SSP를 즉시 제로화함.

7.7.4.3 환경장애시험 절차

환경장애시험(EFT)은 온도 및 전압이 모듈의 정상 동작 범위를 벗어났을 때 환경 조건(우발적 또는 고의적)이 모듈의 안전성을 손상하지 않음을 보장하기 위해, 암호모듈을 분석하고 시뮬레이션하고 시험하는 절차를 포함해야 한다[07.78].

동작 온도 및 동작 전압이 모듈에 오류를 일으킬 만큼 정상 동작 범위를 벗어난다면, 어떠한 순간에서라도 암호모듈의 안전성이 손상되지 않음을 EFT는 입증해야 한다[07.79], [07.80].

시험 온도 범위는 정상 동작 범위 안의 임의 온도에서부터 ① 모듈을 동작하지 못하도록 정지시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 최저 온도(즉, 최저 추운 온도)까지 지정되어야 한다. 또한 시험 온도 범위는 정상 동작 범위 안의 임의의 온도에서부터 ① 모듈을 정지시키거나 오류 상태로 전환하거나 또는 ② 보호되지 않은 모든 SSP를 제로화시키는 최고 온도(즉, 최고 뜨거운 온도)까지 지정되어야 한다[07.81].

시험 온도 범위는 섭씨 −100°부터 +200°까지(화씨 −150°부터 +400°까지) 지정되어야 한다[07.82]. 그러나 ① 모듈이 작동되지 못하도록 중단하거나, ② 보호되지 않은 모든 SSP가 즉시 제로화되거나, 또는 ③ 모듈이 고장 상태에 진입하자마자 그 시험(EFT)은 중단되어야 한다[07.83]. 모듈의 물리적 경계는 제외시키고, 중요한 구성 요소와 핵심 장치에서의 온도가 내부에서 감시되어야 한다[07.84].

시험 전압 범위는 정상 동작 전압 범위 내 임의의 전압으로부터 ① 작동하지 못하도록 모듈을 중지시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 저전압까지 점진적으로 낮출 수 있어야 한다[07.85]. 또한 시험 전압 범위는 정상 동작 전압 범위 내의 임의 전압으로부터 ① 작동하지 못하도록 모듈을 중단시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 고전압까지 점차적으로 높일 수 있어야 한다[07.86].

7.8 비침투 보안

비침투 공격은 물리적으로 모듈을 변경하거나 침투하지 않고 모듈의 핵심 보안매개변수 정보를 획득함으로써 암호모듈을 손상시키려고 시도한다. 모듈은 이러한 유형의 공격을 완화하기 위한 다양한 방법을 실행할 수 있다. 이 표준에서 다루는 관련 보안기능별 비침투 공격 완화 방법은 **부속서** F를 참조한다.

암호모듈이 비침투 공격으로부터 모듈의 보호하지 않은 SSP를 보호하는 데 **부속서** F에서 기술한 비침투 공격 완화 방법을 실행하지 않으면 이 하부 조항은 적용하지 않는다.

암호모듈이 모듈의 SSP를 보호하기 위해 **부속서** F에서 기술하지 않은 비침투 공격 완화 방법을 실행하면 그 기법은 **7.12**의 요구사항을 만족해야 한다[08.01].

암호모듈이 모듈의 SSP를 보호하기 위해 **부속서** F에서 기술한 비침투 공격 완화 방법을 실행하면 그 기법은 다음의 요구사항을 만족해야 한다[08.02].

A.2.8에 명세한 개발 문서가 제공되어야 한다[08.03].

보안수준 1, 2

보안수준 1, 2의 경우, 개발 문서는 **부속서** F에 언급된 암호모듈 CSP의 보호를 위한 암호모듈에 적용된 모든 비침투 공격에 대한 완화 방법을 명세해야 한다[08.04]. 문서에는 각 공격 완화 기법의 효과성 증빙 자료를 수록하여야 한다[08.05].

보안수준 3

보안수준 1, 2의 요구사항 외에 보안수준 3의 경우, 암호모듈이 **부속서** F에서 기술한 바와 같이 보안수준 3을 위해 검증대상 비침투 공격 완화 방법을 만족하는지 시험해야 한다[08.06].

보안수준 4

보안수준 4의 경우, 암호모듈이 **부속서** F에 기술한 바와 같이 보안수준 4를 위해 검증대상 비침투 공격 완화 방법을 만족하는지 시험해야 한다[08.07].

7.9 중요 보안매개변수 관리

7.9.1 중요 보안매개변수 관리 일반 요구사항

중요 보안매개변수(SSP)는 핵심 보안매개변수(CSP)와 공개 보안매개변수(PSP)로 구성된다. SSP 관리를 위한 보안 요구사항은 모듈에서 사용하는 SSP의 전체 생명주기를 포괄한다. SSP 관리에는 난수 발생기(RBG)와 SSP 생성, SSP 설정, SSP 주입/출력, SSP 저장, 보호하지 않은 SSP 제로화를 포함한다.

암호화된 CSP는 검증대상 암호알고리즘을 사용하여 암호화된 CSP를 지칭한다. 비검증대상 암호알고리즘으로 암호화되거나 난독화된 CSP는 이 표준의 범위 내에서 보호하지 않은 평문으로 간주한다.

CSP는 암호모듈 내에서 인가되지 않은 접근, 사용, 노출, 변경 및 대체로부터 보호되어야 한다[09.01].

PSP는 암호모듈 내에서 인가되지 않은 변경과 대체로부터 보호되어야 한다[09.02].

암호모듈은 생성, 주입되거나 출력되는 SSP를 지정된 개체(사람, 그룹, 역할 또는 프로세스)와 연계시켜야 한다[09.03].

패스워드의 해시값, 난수 발생기의 상태 정보 및 키 생성 중간값은 제로화를 위한 보호된 CSP로 간주되어야 한다[09.04].

A.2.9에 명세된 요구사항을 충족하는 개발 문서가 제공되어야 한다[09.05].

7.9.2 난수 발생기

암호모듈은 난수 발생기와 난수 발생기의 체인을 포함하거나 단독으로 난수 발생기일 수 있다. 검증대상 난수 발생기는 **부속서** C 목록에서 찾을 수 있다.

검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 난수가 요구된다면, 이를 제공하기 위해 검증대상 난수 발생기가 사용되어야 한다[09.06].

엔트로피가 암호모듈의 암호경계 외부에서 수집된다면, 엔트로피 입력으로 생성된 데이터는 CSP로 간주되어야 한다[09.07].

7.9.3 중요 보안매개변수 생성

모듈은 내부적으로 SSP를 생성하거나 또는 모듈로 입력된 SSP에서 유도할 수 있다.

검증대상 난수 발생기의 출력을 이용하는 SSP 생성을 손상하는 행위(예를 들면, 결정론적 난수 발생기를 초기화하는 시드값 추측)는 적어도 생성된 SSP의 값을 전수 조사로 찾는 만큼의 연산량을 필요로 해야 한다[09.08].

① 검증대상 난수 발생기를 이용하여 모듈에서 생성되거나 ② 모듈에 주입된 다른 SSP로부터 유도된 것으로, 검증대상 암호알고리즘 또는 SSP 설정에 사용되는 SSP는 **부속서** D의 목록에 제시된 검증대상 SSP 생성 방법을 사용해야 한다[09.09].

7.9.4 중요 보안매개변수 설정

SSP 설정은 다음으로 구성할 수 있다.

- 자동화된 SSP 전송 또는 SSP 합의 방법
- 직접 또는 전자적 방법을 통한 수동 SSP 주입 또는 출력

자동화된 SSP 설정은 **부속서** D에 검증대상으로 정의된 방법을 사용해야 한다[09.10]. SSP의 수동 설정은 **7.9.5**의 요구사항을 충족해야 한다[09.11].

7.9.5 중요 보안매개변수의 주입 및 출력

중요 보안매개변수는 수동으로 모듈에 주입되거나 외부로 출력되는 경우 ① 직접적으로(예: 키보드, 숫자 패드, 화면 출력) 또는 ② 전자식으로(예: 스마트카드, 토큰, PC 카드, 전자식 키 저장 장치, 모듈의 운영체제) 수행된다. SSP가 수동으로 모듈에 주입되거나 외부로 출력되는 경우, 주입 또는 출력은 HMI, SFMI, HFMI 또는 HSMI(**7.3.2**) 인터페이스를 사용해야 한다[09.12].

SSP가 모듈에 주입되거나 모듈 외부로 출력되는 경우, 암호를 사용하여 보호되는 모든 SSP는 검증대상 암호알고리즘을 이용하여 암호화되어야 한다[09.13].

직접 주입되는 SSP의 경우, 주입되는 값은 육안 검증을 허용하고 정확성을 향상시키기 위해서 임시적으로 표시되어야 한다. 암호화된 SSP가 직접 모듈에 주입되는 경우, SSP가 평문으로 표시되지 않아야 한다[09.14]. 직접 주입되는 (평문이거나 암호화된) SSP는 암호모듈에 주입되는 동안 **7.10.3.5**에 정의된 조건부 수동 주입 시험을 이용하여 정확한 주입 여부가 확인되어야 한다[09.15].

중요 정보를 의도치 않게 출력하는 것을 방지하기 위하여, CSP가 평문으로 출력되는 경우 두 개의 독립된 내부 조치가 있어야 한다[09.16]. 이러한 정의된 두 개의 독립된 내부 조치는 CSP 출력 설정에만 전용으로 사용되어야 한다[09.17].

무선 접속을 통한 전자식 주입 또는 출력의 경우, CSP, 키 구성 요소 및 인증 데이터는 암호화되어야 한다[09.18].

수동으로 주입되는 PSP는 암호적으로 인증될 필요는 없다.

보안수준 1, 2

평문 CSP와 키 구성 요소, 인증 데이터는 암호모듈의 다른 물리적 포트와 논리적 인터페이스를 공유하는 물리적 포트와 논리적 인터페이스를 거쳐 주입 및 출력할 수 있다.

소프트웨어 암호모듈 또는 하이브리드 소프트웨어 모듈의 소프트웨어 구성 요소의 경우, CSP, 키 요소 및 인증 데이터가 운영환경 내에서 관리되고 **7.6.3**의 요구사항을 충족한다면, 평문이거나 암호화된 형식으로 입출력될 수 있다[09.19].

보안수준 3

보안수준 1, 2 외에 보안수준 3의 경우, CSP, 키 요소 및 인증 데이터가 암호모듈에 주입되거나 외부로 출력될 때 암호화되거나 신뢰 채널을 통해야 한다[09.20].

평문으로 된 비밀 정보 CSP와 개인키는 암호모듈에 주입되거나 외부로 출력될 때 지식 분산 기법 또는 신뢰 채널을 이용해야 한다[09.21].

암호모듈이 지식 분산 기법을 사용한다면, 각 키 구성 요소의 입력과 출력을 위해 개별적인 신원 기반 운영자 인증을 채택해야 한다[09.22]. 또한, 원본 암호키를 재구성하기 위해서는 적어도 두 개의 키 구성 요소가 요구되어야 한다[09.23].

보안수준 4

보안수준 3 외에 보안수준 4의 경우, 암호모듈은 키 구성 요소가 입·출력할 때 각 키 구성 요소에 대해 개별적으로 운영자를 다중체계 신원 기반 인증해야 한다[09.24].

7.9.6 중요 보안매개변수 저장

모듈 내 저장된 SSP는 평문이나 암호화된 형태로 저장할 수 있다. 암호모듈 내부에 저장되는 모든 SSP는 SSP를 지정한 개체(예: 운영자, 역할, 프로세스)와 연계되어야 한다[09.25].

인가되지 않은 운영자가 평문 CSP에 접근하는 것은 금지되어야 한다[09.26]. 인가되지 않은 운영자에 의한 PSP 변경은 금지되어야 한다[09.27].

7.9.7 중요 보안매개변수의 제로화

암호모듈 내부에서 보호되지 않은 모든 SSP와 키 구성 요소를 제로화하는 방법을 제공해야 한다[09.28]. 임시로 저장된 SSP와 모듈에 의해 소유된 다른 저장된 값은 미래 용도로 더 이상 필요 없을 때 제로화하여야 한다.

제로화된 SSP는 복구되거나 재사용될 수 없어야 한다[09.29].

보안수준 4를 제외하고 보호된 PSP의 제로화, 암호화된 CSP의 제로화, (이 표준의 요구사항을 만족하는) 추가 내장형 검증필 암호모듈 내에서 물리적으로 또는 논리적으로 보호된 CSP의 제로화는 요구하지 않는다.

인증 프록시(예: 모듈 초기화 키인 CSP) 과정에 어쩔 수 없이 평문 데이터로 보여지는 경우 SSP는 제로화 요구사항을 만족시킬 필요가 없다.

단지 **7.10**의 자가시험에만 사용하는 매개변수는 제로화 요구사항을 만족할 필요가 없다.

보안수준 1

보호하지 않은 SSP의 제로화는 모듈 운영자와 모듈의 독립적인 컨트롤(예: 하드 드라이브의 포맷, 재진입 중 모듈의 파괴)에 의해서 절차적으로 수행된다.

보안수준 2, 3

암호모듈은 보호되지 않는 SSP의 제로화를 수행해야 한다(예: 모두 0 또는 1로 덮어 쓰거나 난수로 채우기)[09.30]. 제로화 수행 시 보호되지 않은 SSP를 보호되지 않은 다른 SSP로 덮어쓰는 것을 방

지해야 한다[09.31]. 일시적으로 사용되는 SSP는 더 이상 필요하지 않게 되면 제로화되어야 한다[09.32]. 암호모듈은 제로화가 완료되었을 때 상태 표시를 출력해야 한다[09.33].

보안수준 4

보안수준 2, 3의 요구사항 외에 다음의 요구사항을 충족해야 한다[09.34].

- 제로화는 즉각적으로 중단 없이 수행되어야 한다[09.35]. 또한 충분히 짧은 시간에 수행되어 중요 정보가 제로화의 시작과 종료 사이에 복구될 수 없도록 해야 하며[09.36],
- 평문이든 암호화되어 있든 모든 SSP는 제로화되면 공장 출하 상태로 회귀되어야 한다[09.37].

7.10 자가시험

7.10.1 자가시험 일반 요구사항

자가시험이 수행되어야 한다. 또한 성공 또는 실패 판정이 암호모듈에 의해서만 결정되며, 외부의 제어, 외부로부터 제공되는 테스트 벡터, 예상 출력값, 운영자 관여, 또는 모듈이 검증대상 동작모드에 있는지 비검증대상 동작모드에 있는지 여부와 무관하게 수행되어야 한다[10.1], [10.02].

암호모듈이 출력 인터페이스를 통해 데이터를 출력되기 이전에, 암호모듈이 동작 전 자가시험을 수행해야 하며 수행 결과가 성공해야 한다[10.03].

적용되는 암호알고리즘이나 프로세스가 호출될 때, 조건부 자가시험이 수행되어야 한다(즉, 사용되는 암호알고리즘에 대해 자가시험이 요구된다)[10.04].

알고리즘 표준(**부속서** C～E)에 대해 적용되는 모든 자가시험은 암호모듈 자체 내에서 구현될 수 있어야 한다[10.05]. 검증대상 암호알고리즘, SSP 설정 방법, 인증 메커니즘에 대하여 알고리즘 표준(**부속서** C～E)에 대한 자가시험은 표준(**부속서** C～E)에 명세된 방법에 따라 구현되어야 한다[10.06].

암호모듈은 이 표준에서 명시한 시험 외 다른 동작 전 또는 조건부 핵심 기능시험을 수행할 수 있다.

암호모듈이 자가시험에 실패한다면 오류 상태로 전환되어야 한다[10.7]. 그리고 **7.3.3**에 명세된 방식으로 오류 표시를 출력해야 한다[10.8]. 암호모듈이 오류 상태에서 암호 연산을 수행하지 않아야 하고 제어 출력 인터페이스와 데이터 출력 인터페이스를 통한 제어 출력 및 데이터 출력을 수행하지 않아야 한다[10.09]. 암호모듈은 함수 또는 알고리즘과 관련된 자가시험이 반복 수행되어 성공적으로 통과될 때까지 자가시험이 실패한 함수와 알고리즘에 관련된 어떠한 기능도 사용하지 않아야 한다[10.10]. 암호모듈이 자가시험 실패에 대하여 오류 상태를 출력하지 않는다면, 모듈이 오류 상태에 진입했는지를 암시적으로 보안정책 문서(**부속서** B)에 서술된 명백한 절차를 통해 결정할 수 있어야 한다[10.11].

보안수준 3, 4에서, 암호모듈은 인가된 운영자만 접근할 수 있는 오류 로그를 관리해야 한다[10.12]. 오류 로그는 적어도 가장 최근에 발생한 오류 이벤트에 대한 정보(예: 실패한 자가시험의 종류)를 제공해야 한다[10.13].

A.2.10에 명세된 문서 요구사항이 충족되어야 한다[10.14].

7.10.2 동작 전 자가시험

7.10.2.1 동작 전 자가시험 일반 요구사항

암호모듈에 전원이 인가되는 시점 또는 (전원 꺼짐, 리셋, 리부팅, 콜드스타트, 전원 인터럽트 등이 발생한 후) 인스턴스화되는 시점과 암호모듈이 동작 상태로 천이되기 직전 시점 사이에 암호모듈에 의해 동작 전 시험이 수행되고 성공적으로 통과되어야 한다[10.15].

암호모듈은 해당하는 경우 다음과 같은 동작 전 자가시험을 수행해야 한다[10.16].

- 동작 전 소프트웨어/펌웨어 무결성 시험
- 동작 전 우회 기능시험
- 동작 전 핵심 기능시험

7.10.2.2 동작 전 소프트웨어/펌웨어 무결성 시험

암호경계 내부의 모든 소프트웨어와 펌웨어 구성 요소는 **7.5**에 정의된 요구사항을 만족하는 검증대상 무결성 검증 기술을 이용하여 검증되어야 한다[10.17]. 검증이 실패하면 동작 전 소프트웨어/펌웨어 무결성 시험이 실패한다[10.18]. 이 표준의 보안 요구사항에서 제외된 소프트웨어나 펌웨어, 재구성이 불가능한 메모리에 저장된 실행 가능 코드는 동작 전 소프트웨어/펌웨어 무결성 시험을 실시할 필요가 없다.

하드웨어 암호모듈이 소프트웨어 또는 펌웨어를 포함하지 않는 경우, 모듈에는 동작 전 자가시험으로 **7.10.3.2**에 따라 적어도 하나의 암호알고리즘 자가시험이 구현되어야 한다[10.19].

동작 전 소프트웨어/펌웨어 무결성 시험을 위해 사용되는 검증대상 무결성 검증 기술에 사용되는 암호알고리즘은 우선 **7.10.3.2**에 따른 암호알고리즘 자가시험을 통과해야 한다[10.20].

7.10.2.3 동작 전 우회 기능시험

암호모듈에 우회 기능이 구현되는 경우, 우회 기능을 활성화하기 위해 필요한 통제 로직이 정확히 동작하는지 보증해야 한다[10.21].

암호모듈은 다음과 같은 방법에 의해 데이터 경로를 검증해야 한다[10.22].

- 우회 기능 스위치가 암호 프로세스를 지원하도록 설정되는 경우, 암호모듈이 우회 기능을 통하여 전달되는 데이터가 암호에 의해 처리되는지 검증을 수행함.
- 우회 기능 스위치가 암호 프로세스를 지원하지 않도록 설정되는 경우, 암호모듈이 우회 기능을 통하여 전달되는 데이터가 암호에 의해 처리되지 않는지 검증을 수행함.

7.10.2.4 동작 전 핵심 기능시험

암호모듈의 안전한 운영을 위해 동작 전 시험에서 시험해야 하는 핵심적인 보안기능이 있을 수 있다[10.23]. 동작 전 시험에 포함되는 핵심 기능에 대하여 개발 문서에 명세해야 한다[10.24].

7.10.3 조건부 자가시험

7.10.3.1 조건부 자가시험 일반 요구사항

다음 시험에 대하여 개발 문서에 명세된 조건이 발생하면 암호모듈에 의해 조건부 자가시험이 수행되어야 한다[10.25].

– 암호알고리즘 자가시험, 암호키 쌍 일치 시험, 소프트웨어/펌웨어 로드 시험, 수동 주입 시험, 조건부 우회 기능시험 및 조건부 핵심 기능시험

7.10.3.2 조건부 암호알고리즘 시험

암호알고리즘 시험은 **부속서** C~E에 명세된 목록 중 모듈에 구현된 검증대상 암호알고리즘에 대하여 모든 암호 기능(예: 암호알고리즘, SSP 설정 방법, 인증)이 수행되어야 한다[10.26]. 암호알고리즘이 최초로 사용되기 이전에 조건부 자가시험이 수행되어야 한다[10.27].

암호알고리즘 자가시험에는 기지 답안 시험(known-answer test), 비교 시험(comparison test), 오류탐지 시험(fault-detection test)이 있다.

기지 답안 시험은 결과를 생성하기 위해 암호알고리즘이 동작에서 알고 있는 입력 벡터(예: 데이터, 키 정보, 임의 길이의 상수)로 구성한다. 결과는 알고 있는 예상 출력 결과값과 비교한다.

시험의 수행으로 계산된 출력값이 이미 알고 있는 정답과 일치하지 않으면 암호알고리즘의 기지 답안 자가시험은 실패로 판정된다[10.28].

알고리즘의 자가시험은 암호모듈에서 지원하는 검증대상 키 길이, 모듈의 크기, DSA용 소수 또는 타원 곡선의 각각에 대하여 최소한 가장 작은 것을 사용해야 한다[10.29].

알고리즘이 다중 운영 모드(예: ECB, CBC)를 지원하는 경우, 자가시험에서 암호모듈이 지원하거나 검증기관이 지정하는 최소한의 한 개 이상의 운영 모드가 선택되어야 한다[10.30].

기지 답안 검사의 예:

- 일방향 함수: 입력 테스트 벡터가 예상되는 값과 일치하는 출력을 생성해야 한다[10.31].
  (예: 해시, 키를 사용한 해시, 메시지 인증, 엔트로피 벡터가 고정된 난수 발생기, SSP 합의)
- 가역 함수: 전방향 또는 역방향 기능이 모두 자가시험을 통과해야 한다[10.32].
  (예: 대칭키 암호화 및 복호화, SSP 전송용 암호화 및 복호화, 전자서명의 생성과 검증)

비교 시험은 암호알고리즘을 두 번 이상 독립적으로 구현한 후 두 개 이상 구현물의 출력값을 비교한다. 출력값이 일치하지 않으면 암호알고리즘의 비교 자가시험은 실패로 판정된다[10.33].

오류 탐지 시험은 암호알고리즘 구현 범위 내에서 오류 탐지 메커니즘들의 통합된 구현을 포함한다. 만약 오류가 탐지되면 암호알고리즘에 대한 오류 탐지 자가시험은 실패로 판정된다[10.34].

7.10.3.3 조건부 암호키 쌍 일치 시험

암호모듈이 공개키, 비밀키 쌍을 생성한다면, **부속서** C~E의 암호알고리즘 명세에 따라 생성된 공개키, 비밀키 쌍에 대하여 암호키 쌍 일치 시험을 수행해야 한다[10.35].

7.10.3.4 조건부 소프트웨어/펌웨어 로드 시험

암호모듈이 외부에서 소프트웨어 또는 펌웨어를 로드하는 기능이 있을 때, **7.4.3.4**에 추가하여 다음 요구사항이 충족되어야 한다[10.36].

- 암호모듈은 로드되는 소프트웨어 또는 펌웨어의 유효성 확인을 위해 검증대상 인증기술을 구현해야 한다[10.37].
- 참조될 인증키는 소프트웨어 또는 펌웨어가 로드되기 이전에 독립적으로 암호모듈에 로드되어야

한다[10.38].
- 적용된 검증대상 인증기술이 성공적으로 검증되어야 한다[10.39]. 그렇지 않으면 소프트웨어/펌웨어 로드 시험은 실패로 판정된다[10.40]. 소프트웨어/펌웨어 로드 시험의 실패 시 로드된 소프트웨어 또는 펌웨어는 사용될 수 없어야 한다[10.41].

7.10.3.5 조건부 수동 주입 시험

SSP 또는 키 구성 요소가 수동으로 암호모듈에 직접 주입되거나, 인간 운영자가 입력값을 잘못 주입하여 오류가 유발될 수 있는 경우, 다음과 같은 수동 주입 시험이 수행되어야 한다[10.42].

- SSP 또는 키 구성 요소에 오류탐지코드(EDC)가 적용되어야 한다[10.43]. 또는 중복 입력으로 주입되어야 한다[10.44].

EDC가 사용된다면 EDC는 적어도 16비트의 길이를 가져야 한다[10.45]. EDC 검증이 실패하거나 반복 입력된 값이 일치하지 않으면 해당 시험 항목은 실패로 판정된다[10.46].

7.10.3.6 조건부 우회 기능시험

암호모듈에 암호 처리 없이 서비스를 제공하는 우회 기능이 구현되어 있다면(예: 모듈을 통해 평문이 전송되는 경우), 다음과 같은 우회 기능시험이 수행되어 암호모듈의 구성 요소 가운데 단 하나라도 실패하는 경우 의도하지 않은 평문의 출력이 방지됨을 확인해야 한다[10.47].

암호모듈이 서로 배타적인 우회 서비스나 암호 서비스 중 하나만을 선택할 때, 암호 기능을 제공하는 서비스가 올바르게 동작하는지 시험해야 한다[10.48].

암호 처리를 지원하는 서비스와 암호 처리를 지원하지 않는 서비스를 제공하는 경우, 암호모듈이 우회 서비스와 암호 서비스를 자동적으로 선택할 수 있다면, 암호모듈은 전환 과정 통제 메커니즘이 변경될 때(예: IP 송신/수신 주소 테이블) 암호 처리를 지원하는 서비스의 정확한 동작을 시험해야 한다[10.49].

암호모듈이 우회 기능을 통제하는 내부 정보를 유지한다면, 암호모듈은 통제 정보의 변경이 진행되는 즉시 검증대상 인증기술로 통제 정보의 무결성을 검증해야 한다[10.50]. 그리고 통제 정보의 변경 직후 검증대상 인증기술을 이용하여 새로운 무결성 검증값을 생성해야 한다[10.51].

7.10.3.7 조건부 핵심 기능시험

암호모듈의 안전한 운영에 핵심적인 보안기능이 있으면 조건부 자가시험에 반영되어야 한다[10.52].

7.10.3.8 주기적인 자가시험

보안수준 1, 2

암호모듈에 대한 주기적 시험의 요청이 있으면 암호모듈은 동작 전 또는 조건부 자가시험을 실행해야 한다. 주기적 자가시험을 시작하기 위해 요청할 수 있는 수단은 제공되는 서비스 요청, 리셋, 리부팅 또는 반복적인 전원 인가 등이다[10.53].

보안수준 3, 4

보안수준 1, 2의 요구사항 외에, 암호모듈은 정해진 시간 간격마다 자동적으로, 외부 입력 또는 외부

제어에 무관하게, 동작 전 자가시험 또는 조건부 자가시험을 수행해야 한다[10.54]. 동작 전 자가시험 또는 조건부 자가시험을 반복하는 동안 암호모듈의 동작을 중단(interrupt)하게 만드는 시간 간격과 조건에 대한 정보를 보안정책 문서(**부속서** B)에 명세해야 한다(예: 모듈이 중단할 수 없는 핵심적인 서비스를 수행하고 있을 때 동작 전 자가시험을 실시할 시간이 도래한 경우, 자가시험은 다음 번으로 연기된다)[10.55].

7.11 생명주기 보증

7.11.1 생명주기 보증 일반 요구사항

생명주기 보증은 암호모듈의 설계, 개발, 운영, 수명의 종료 기간 동안 암호모듈 벤더에 의해 적절한 사용을 나타내며, 모듈이 적절히 설계, 개발, 시험, 구성, 배포, 설치, 폐기되고 있음을 보증하며, 적절한 운영자 안내서가 제공되고 있음을 보장하는 것을 지칭한다. 형상 관리, 설계, 유한상태모델, 개발, 시험, 배포, 운영, 지침 문서를 위한 보안 요구사항을 명시한다.

A.2.11에 명세된 개발 문서가 제공되어야 한다[11.01].

7.11.2 형상 관리

형상 관리는 암호모듈 벤더가 구현한 형상관리시스템을 위한 요구사항을 명시하고, 암호모듈과 관련 문서의 개선, 변경 과정에서 규율과 통제를 요구함으로써 암호모듈의 무결성이 보존된다는 보장을 제공한다. 형상관리시스템은 암호모듈과 관련 문서의 우발적이거나 고의적인 변경을 방지하고, 암호모듈과 관련 문서의 변경 이력을 추적한다.

보안수준 1, 2

다음의 보안 요구사항은 보안수준 1, 2의 암호모듈에 적용해야 한다[11.02].

- 형상관리시스템은 암호모듈 및 암호경계 내의 모듈 구성 요소를 개발하기 위해 사용되어야 하고, 또한 암호모듈과 관련된 개발 문서를 개발하기 위해 사용되어야 한다[11.03].
- 암호모듈과 관련된 문서를 구성하고 있는 각 형상 항목(예: 암호모듈, 모듈 하드웨어 부품, 모듈 소프트웨어 구성 요소, 모듈 HDL, 사용자 안내서, 보안정책 문서, 기타)에 대한 개별 버전은 유일한 식별자가 할당되어 표시되어야 한다[11.04].
- 형상관리시스템은 검증필 암호모듈(validated module) 생명주기 전체 동안 발생하는 개별 형상 항목을 ① 식별, ② 버전 또는 개정에 대한 변경을 추적하고 유지하여야 한다[11.05].

보안수준 3, 4

보안수준 1, 2의 요구사항 외에, 자동화된 형상관리시스템을 사용하여 형상 항목이 관리되어야 한다[11.06].

7.11.3 설계

설계는 암호모듈의 기능명세를 다루는 공학적인 해결책이다. 설계는 암호모듈의 기능명세가 보안정책서에서 기술한 의도된 기능에 상응한다는 점을 보장하려는 의도를 갖고 있다.

암호모듈이 제공하는 보안 관련 서비스를 시험할 수 있도록 암호모듈이 설계되어야 한다[11.07].

7.11.4 유한상태모델

암호모듈 동작은 유한상태모델을 사용하여 명세되어야 한다. 유한상태모델은 ① 상태 천이도, ② 상태 천이표와 상태 설명으로 구성된다[11.08]. 암호모듈이 해당 표준의 모든 요구사항을 충족할 수 있도록 FSM을 상세하게 서술하여야 한다[11.09].

암호모듈의 FSM은 최소한 다음 동작 상태 및 오류 상태를 포함해야 한다[11.10].

- 전원 켜진 상태/전원 꺼진 상태: 전원 꺼진 상태는 전원이 모듈에 공급되지 않아서 대기 상태(휘발성 메모리 유지)가 되거나 비휘발성 메모리에 동작 상태가 유지되어 있는 상태(예: 동면 상태)이다. 전원 켜진 상태는 주전원, 보조 전원 또는 백업 전원이 모듈에 공급되는 상태이다. 해당 상태는 암호모듈에 공급되는 전력원과 별개의 상태이다. 소프트웨어 모듈에서 전원 켜진 상태는 암호모듈의 실행 가능한 이미지를 프로그램 실행 메모리에 로드하는 상태이다.
- 초기화 상태: 암호모듈이 검증대상 동작 상태로 천이하기 전 암호모듈을 초기화하는 상태
- 암호관리자 상태: 암호관리자 서비스가 실행되는 상태(예: 암호 초기화, 안전한 관리 및 키 관리)
- CSP 주입 상태: CSP를 암호모듈에 주입하는 상태
- 사용자 상태: (사용자 역할이 구현된 경우) 인가된 사용자가 보안 서비스, 암호 동작 또는 다른 검증대상 기능을 암호모듈이 수행하게 하는 상태
- 검증대상 동작 상태: 검증대상 암호알고리즘이 수행되는 상태
- 자가시험 상태: 암호모듈이 자가시험을 수행하고 있는 상태
- 오류 상태: 암호모듈에서 오류가 발생한 상태(예: 자가시험 실패). 암호모듈의 한 개 오류 상태는 한 가지 이상의 오류 조건으로부터 발생할 수 있다. 오류 상태는 암호모듈의 유지보수, 서비스나 수리를 요구하는 “심각한 오류”(예: 장비의 오작동으로 발생하는 오류)와 모듈의 초기화나 재설정을 요구하는 “단순한 오류”를 포함한다. 암호모듈의 유지보수, 서비스나 수리가 필요한 심각한 오류 상태를 제외하고, 모든 오류 상태로부터 복구 가능해야 한다[11.11].

암호모듈 서비스, 암호알고리즘 사용, 오류 상태, 자가시험 또는 운영자 인증은 별개의 상태로 정의되어야 한다[11.12].

암호관리자를 제외한 역할은 다른 암호모듈 상태에서 암호관리자 상태로 변경할 수 없다[11.13].

암호모듈에는 다음과 같은 기타 상태를 포함될 수 있다(이에 국한된 것은 아님).

- 우회 상태: 정상적으로는 암호 양식으로 출력되어야 하지만, 모듈 형상이나 운영자 개입의 결과로 특정 데이터나 상태 항목이 평문으로 출력되는 상태
- 대기 상태: 암호모듈이 휴면 중인 상태(예: 저전력 또는 중지, 동면 중)

7.11.5 개발

적절한 개발 과정은 모듈 기능명세와 보안정책서에 상응하게 암호모듈이 구현되어 있으며, 암호모듈을 유지보수할 수 있으며, 유효성이 검증된 암호모듈을 재사용할 수 있음을 보장한다. 이 조항은 기능명세에서 구현물까지 발췌한 다양한 수준에서 암호모듈의 보안기능을 나타내는 보안 요구사항을 명시한다.

보안수준 1

다음 요구사항은 보안수준 1에 해당하는 암호모듈에 적용되어야 한다[11.14].

- 암호모듈이 소프트웨어나 펌웨어를 포함한다면, 컴파일하여 실행 형태로 변환하는 데 사용된 소스

코드, 언어 참고 자료, 컴파일러, 컴파일러 버전과 컴파일러 옵션, 링커와 링커 옵션, 런타임 라이브러리와 런타임 라이브러리 설정, 구성 설정, 빌드 프로세스와 방법, 빌드 옵션, 환경 변수, 모든 다른 리소스 등은 형상관리시스템을 사용하여 추적되어야 한다[11.15].

- 암호모듈이 소프트웨어나 펌웨어를 포함한다면, 소프트웨어나 펌웨어가 암호모듈의 설계와 일치함을 나타내는 주석을 소스 코드에 달아야 한다[11.16].
- 암호모듈이 하드웨어를 포함한다면 개발 문서는 해당 사항이 있는 경우, 회로도(schematics) 혹은 하드웨어 서술 언어(HDL)를 명세해야 한다[11.17].
- 암호모듈이 하드웨어를 내장한다면, HDL은 하드웨어와 암호모듈의 설계가 일치함을 나타내도록 주석 처리해야 한다[11.18].
- 소프트웨어 암호모듈, 펌웨어 암호모듈, 하이브리드 암호모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여
  - 벤더가 개발 단계에서 무결성 및 인증 기법 메커니즘의 결과 코드를 계산하여 이 결과 코드를 소프트웨어 모듈 혹은 펌웨어 모듈에 결합해야 한다. 여기서 무결성 및 인증 메커니즘은 **7.5**와 **7.10**에서 명세되어 있다[11.19].
  - 개발 문서는 소스 코드를 실행 파일 형태로 컴파일하는 컴파일러, 구성 설정 및 방법을 명세해야 한다[11.20].
  - 제품을 생산할 수 있는 개발 도구(예: 컴파일러)를 사용하여 암호모듈을 개발해야 한다[11.21].

보안수준 2와 3

보안수준 1의 요구사항 외에, 다음의 요구사항은 보안수준 2와 3의 암호모듈에 적용되어야 한다[11.22].

- 모든 소프트웨어 또는 펌웨어는 상위 수준의 언어로 구현되어야 한다[11.23]. 또는 암호모듈의 성능이 중요하거나 상위 수준 언어를 사용할 수 없어 하위 수준 언어(예: 어셈블리 언어 또는 마이크로코드)를 사용하는 경우 근거가 제공되어야 한다[11.24].
- 암호모듈에 내장된 맞춤형 집적회로는 고급 하드웨어 기술 언어(HDL)(예: VHDL 또는 Verilog)를 사용하여 구현되어야 한다[11.25].
- 암호모듈의 기능과 실행과 관련이 없는 코드, 매개변수, 기호를 사용하지 않는 방식으로 소프트웨어 암호모듈 또는 펌웨어 암호모듈 및 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소를 설계하고 구현해야 한다[11.26].

보안수준 4

보안수준 1, 2, 3의 요구사항 외에, 다음의 요구사항을 보안수준 4 암호모듈에 적용해야 한다[11.27].

- 각 암호모듈 하드웨어 구성 요소 및 암호모듈 소프트웨어 구성 요소에 대하여, 개발 문서는 ① 암호모듈 구성 요소, 기능 또는 절차를 정확하게 실행시키기 위해 시작 단계에서 요구되는 사전 조건과 ② 암호모듈 구성 요소, 기능 또는 절차의 실행이 정확히 완료된 경우 예측되는 사후 조건을 명세하는 주석을 서술해야 한다[11.28]. 사전 조건과 사후 조건은 암호모듈 구성 요소와 기능, 절차의 가동이 완벽하고 모호하지 않게 충분히 상세히 나타내는 표기법을 사용하여 명시할 수 있다.

7.11.6 벤더 시험

이 조항은 암호모듈 내 구현된 보안기능시험의 포함 여부를 확인하고, 암호모듈이 모듈 보안정책서와 기능명세에 의거하여 가동되고 있음을 암호모듈의 벤더 시험을 통해 보장한다.

보안수준 1, 2

보안수준 1, 2의 경우, 개발 문서는 암호모듈에 대하여 수행된 기능시험을 명시해야 한다[11.29].

소프트웨어 암호모듈, 펌웨어 암호모듈 또는 하이브리드 암호모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여 벤더는 현재 자동화 보안 진단 도구(예: 버퍼 오버플로 탐지)를 사용해야 한다[11.30].

보안수준 3, 4

개발 문서는 암호모듈에 대하여 수행된 상세 수준의 시험 절차와 결과를 명세화해야 한다[11.31].

7.11.7 배포 및 운영

이 조항은 암호모듈의 안전한 배포와 설치, 시작을 위한 보안 요구사항을 명시하고, 모듈이 안전하게 인가된 운영자에게 전달되고 안전한 방식으로 설치, 시작되었음을 보장한다.

보안수준 1

개발문서는 암호모듈의 안전한 설치, 초기화 및 시동을 위한 절차를 명세화해야 한다[11.32].

보안수준 2, 3

보안수준 1의 요구사항 외에, 개발 문서는 암호모듈 버전들이 인가된 운영자에게 배포, 설치, 초기화되는 동안 안전성 유지에 필요한 절차를 명세화해야 한다[11.33]. 해당 절차는 암호모듈이 인가받은 운영자에게 운송, 설치, 초기화되는 동안 변조 탐지 방법을 명세화해야 한다[11.34].

보안수준 4

보안수준 1, 2, 3의 요구사항 외에 이 절차는 인가받은 운영자가 벤더가 제공한 운영자 특성에 맞는 인증 데이터를 사용하여 암호모듈을 인증할 것을 요구해야 한다[11.35].

7.11.8 수명의 종료

이 조항은 암호모듈을 더 이상 사용하지 않거나 운영자가 향후 사용할 의사가 없을 때 보안 요구사항을 명시한다.

보안수준 1, 2

보안수준 1과 2의 경우, 개발 문서는 암호모듈의 안전한 소거 절차를 명세해야 한다[11.36]. 소거는 중요 정보(예: SSP, 사용자 데이터 등)를 모듈에서 제거하여 다른 운영자에게 전달되지 않게 하거나 또는 폐기하는 과정이다.

보안수준 3, 4

보안수준 1, 2의 요구사항 외에, 개발 문서는 암호모듈을 안전하게 파기하는 데 필요한 절차를 명세해야 한다[11.37].

7.11.9 안내서

이 조항의 요구사항은 암호모듈을 사용하는 모든 개체가 모듈을 검증대상 동작모드로 관리 및 사용하기 위한 정확한 안내와 절차를 갖도록 보장하기 위한 것이다.

안내서는 관리자 안내서와 비관리자 안내서로 구성된다.

관리자 안내서는 다음을 명세해야 한다[11.38].

- 암호관리자와 다른 관리자 역할에 사용할 수 있는 암호모듈의 관리 기능, 보안 이벤트, 보안매개변수(해당되면 매개변수값), 물리적 포트와 논리적 인터페이스
- 독립된 운영자 인증 메커니즘이 기능적으로 독립을 유지하기 위해 요구되는 절차
- 검증대상 동작모드에서 암호모듈을 관리하는 방법에 대한 절차
- 암호모듈의 안전한 운영과 관련된 사용자 동작에 대한 가정 사항

비관리자 안내서는 다음을 명세해야 한다[11.39].

- 암호모듈 사용자가 사용할 수 있는 검증대상 및 비검증대상 암호알고리즘, 물리적 포트, 논리적 인터페이스
- 암호모듈의 검증대상 동작모드에 대한 모든 사용자의 책임

7.12 기타 공격에 대한 대응

이 표준에서는 정의되지 않은 암호모듈의 공격에 대한 취약성은 모듈 유형과 구현, 구현 환경에 의해 좌우된다. 그 같은 공격은 적대적인 환경(예: 공격자가 모듈의 인가된 운영자일 수 있는)에서 구현된 암호모듈에는 특히 문제가 될 수 있다. 이러한 공격은 일반적으로 물리적으로 모듈 외부에 있는 출처에서 획득한 정보의 분석에 의존한다. 모든 경우에서, 공격은 암호모듈 내 CSP에 관한 일부 지식을 알기 위해 시도된다.

A.2.12에 명세된 보안 요구사항을 충족하는 개발 문서가 제출되어야 한다[12.01].

보안수준 1, 2, 3

암호모듈이 이 표준 내 어디서도 명세되지 않은 하나 이상의 특정 공격에 대응하도록 설계되었다면 개발 문서는 모듈이 대응하도록 설계된 공격을 열거해야 한다[12.02]. 공격 완화에 사용되는 보안 메커니즘의 존재와 적절한 기능은 요구사항과 관련 시험 개발 시 그 유효성을 검증할 것이다.

보안수준 4

보안수준 1, 2, 3의 요구사항 외에, 다음 보안 요구사항은 보안수준 4 암호모듈에 적용되어야 한다[12.03].

- 이 표준 내 어디서도 명세되지 않은 특정 공격들에 대한 대응 기법이 요구되면, 개발 문서는 공격에 대응하기 위한 방법과 대응 기술의 효과를 시험하는 방법을 명세해야 한다[12.04].

부속서 A
(규정)

문서 요구사항

A.1 목적

이 부속서는 암호모듈에 요구되는 최소한 문서 내용을 명시한다[A.01].

A.2 항목

A.2.1 일반사항

일반적인 문서 요구사항은 명시하지 않았다.

A.2.2 암호모듈 명세

- 모듈 유형 명세(하드웨어, 소프트웨어, 펌웨어, 하이브리드 소프트웨어 또는 하이브리드 펌웨어 모듈)(보안수준 1, 2, 3, 4)
- 모듈 경계 명세(보안수준 1, 2, 3, 4)
- 암호모듈의 하드웨어, 소프트웨어 및 펌웨어 구성 요소 명세와 모듈의 물리적 형상 설명(보안수준 1, 2, 3, 4)
- 이 표준의 보안 요구사항에서 제외된 암호모듈의 하드웨어 및 소프트웨어, 펌웨어 구성 요소 명세와 그러한 제외의 이론적 근거 설명(보안수준 1, 2, 3, 4)
- 암호모듈의 물리적 포트와 논리적 인터페이스(보안수준 1, 2, 3, 4)
- 암호모듈의 수동 또는 논리적 제어, 물리적 또는 논리적 상태 표시, 적용 가능한 물리적, 논리적, 전기적 특징(보안수준 1, 2, 3, 4)
- 암호모듈에 의해 사용되는 모든 검증대상 및 비검증대상 암호알고리즘 목록과 모든 검증대상 및 비검증대상 운영 모드 명세(보안수준 1, 2, 3, 4)
- 마이크로프로세서와 입력/출력 버퍼, 평문/암호문 버퍼, 관리 버퍼, 키 저장, 작업 메모리, 프로그램 메모리를 포함한 암호모듈의 주요 하드웨어 구성 요소와 구성 요소 간 상호연결을 보여 주는 블록 다이어그램(보안수준 1, 2, 3, 4)
- 암호모듈의 하드웨어 및 소프트웨어, 펌웨어 설계 명세(보안수준 1, 2, 3, 4)
- 모든 보안 관련 정보(보안수준 1, 2, 3, 4)
  - (평문 및 암호화된) 비밀 및 개인 암호키
  - 인증 데이터(예: 패스워드, PIN)
  - CSP
  - PSP
  - 공개 또는 변경으로 암호모듈 보안에 해를 미칠 수 있는 기타 보호 정보(예: 감사 이벤트, 감사 데이터)
- 제한 기능 동작모드 지원 방법 명세(보안수준 1, 2, 3, 4)
- 이 표준의 요구사항에서 도출된 규칙과 벤더가 부여한 추가 요구사항에서 도출된 규칙을 포함한 암호모듈 보안정책(보안수준 1, 2, 3, 4)

A.2.3 암호모듈 인터페이스

- 물리적, 논리적 데이터 입력과 데이터 출력, 관리 입력, 관리 출력, 상태 출력, 전원 인터페이스 및 물리적, 논리적 인터페이스(보안수준 1, 2, 3, 4)
- 신뢰 채널 인터페이스(보안수준 3, 4)
- 오류 상태 동안 제어 출력 인터페이스를 막지 않을 경우, 예외와 그 이론적 근거(보안수준 1, 2, 3, 4)

A.2.4 역할, 서비스, 인증

- 암호모듈이 지원하는 모든 인가받은 역할(보안수준 1, 2, 3, 4)
- 암호모듈이 제공하는 검증대상 및 비검증대상 서비스, 운영 및 기능명세. 각 서비스에서 서비스 입력과 그에 상응하는 서비스 출력, 그 서비스를 수행할 수 있는 인가받은 역할 명세(보안수준 1, 2, 3, 4)
- 다음의 모듈이 제공하는 모든 서비스 명세(보안수준 1, 2, 3, 4)
  - 운영자가 인가받은 역할이 필요하지 않음.
  - 암호모듈이 제공하는 서비스가 암호키와 다른 CSP를 변경 또는 공개, 대체하지 않음.
  그렇지 못할 경우, 모듈의 보안에 영향을 제공함.
- 암호모듈이 지원하는 인증 메커니즘(복수 인증 메커니즘 사용을 지지하는 이론적 근거 포함), 지원된 인증 메커니즘 실행에 요구되는 인증 데이터 유형, 최초의 모듈 접근 관리와 인증 메커니즘, 인증 메커니즘의 초기화 방법, 모듈이 지원하는 인증 메커니즘의 강도(보안수준 2, 3, 4)
- 버전 정보, 상태 표시, 자가시험과 검증대상 보안기능 수행, 제로화 수행의 결과를 보여 주는 모듈 서비스 명세(보안수준 1, 2, 3, 4)
- 우회 메커니즘(보안수준 1, 2, 3, 4)
- 소프트웨어 또는 펌웨어 로드 메커니즘(보안수준 1, 2, 3, 4)
- 자가 초기화된 운영 출력 기능 관리 및 인터페이스(보안수준 1, 2, 3, 4)

A.2.5 소프트웨어/펌웨어 보안

- 사용된 검증대상 무결성 기법(보안수준 1, 2, 3, 4)
- 요청 시 운영자가 검증대상 무결성 기법을 수행하는 방법(보안수준 1, 2, 3, 4)
- 실행 가능 코드양식(보안수준 2, 3, 4)

A.2.6 운영환경

- 해당되는 경우 모듈이 사용한 운영 시스템을 포함하여 암호모듈을 위한 운영환경(보안수준 1, 2)
- 운영환경의 보안 규칙 또는 설정, 형상 제약 사항(보안수준 1, 2)
- 명세 요구사항에 의거하여 운영 시스템 구성을 위한 관리자 안내서 문서(보안수준 2)

A.2.7 물리적 보안

- 암호모듈의 물리적 보안 메커니즘이 구현된 물리적 형체와 보안수준. 모듈이 사용하는 물리적 보안 메커니즘(보안수준 1, 2, 3, 4)
- 암호모듈이 모듈 콘텐츠로의 물리적 접근을 요구하는 유지보수 역할을 포함하거나 또는 모듈이 물리적 접근을 허용하도록 설계된 경우, 유지보수 접근 인터페이스와 유지보수 접근 인터페이스가 접근될 때 CSP를 제로화하는 방법 기술(보안수준 1, 2, 3, 4)
- 암호모듈의 정상 동작 범위. 암호모듈이 사용하는 환경장애보호 특징 또는 수행한 환경장애시험 기술(보안수준 4)

- 사용된 고장 유도 완화 기법(보안수준 4)

A.2.8 비침투 보안

- **부속서** F에 명시된 바를 포함하여 사용된 비침투 공격 완화 기법(보안수준 1, 2, 3, 4)
- 사용된 공격 완화 기법의 영향 분석(보안수준 1, 2, 3, 4)

A.2.9 중요 보안매개변수 관리

- 암호모듈에 의해 사용되는 모든 CSP와 PSP(보안수준 1, 2, 3, 4)
- 모든 난수 발생기와 그 용도(보안수준 1, 2, 3, 4)
- 모듈에 의해 요구된 입력한 엔트로피 입력 매개변수별 최소 엔트로피(보안수준 1, 2, 3, 4)
- 암호모듈에 의해 적용된 각각의 난수 발생기(검증대상 및 비검증대상, 엔트로피 소스) 명세(보안수준 1, 2, 3, 4)
- 최소 엔트로피가 암호모듈의 암호경계 내에서 수집된 경우, 추정한 최소 엔트로피와 생성 방법(보안수준 1, 2, 3, 4)
- 난수 발생기를 이용하는 각 SSP 생성 방법(보안수준 1, 2, 3, 4)
- 모듈에 의해 사용되는 모든 SSP 설정 방법(보안수준 1, 2, 3, 4)
- 모듈에 의해 사용되는 각 SSP 생성 방법(보안수준 1, 2, 3, 4)
- 암호모듈에 의해 사용되는 키 생성 방법(검증대상 및 비검증대상)(보안수준 1, 2, 3, 4)
- 암호모듈에 의해 사용되는 SSP 설정 방법(보안수준 1, 2, 3, 4)
- 암호모듈에 의해 사용되는 키 주입 및 출력 방법(보안수준 1, 2, 3, 4)
- *n*개의 구성 요소가 원본 CSP가 되는 지식 분산 기법을 사용하는 경우, $n-1$개 구성 요소의 어떠한 조합도 원본 CSP의 길이 외 다른 어떤 정보도 제공하지 않음을 증명해야 함(보안수준 3, 4).
- 모듈에 의해 사용되는 지식 분산 절차(보안수준 3, 4)
- 모듈 내 저장된 SSP(보안수준 1, 2, 3, 4)
- 모듈 내 저장되었을 때 CSP가 비인가된 접근과 사용, 공개, 변경, 교체로부터 보호되는 방법(보안수준 1, 2, 3, 4)
- 모듈 내 저장되었을 때 PSP가 비인가된 변경과 교체로부터 보호되는 방법(보안수준 1, 2, 3, 4)
- 모듈이 그 모듈 내 저장된 PSP를 그 매개변수가 할당된 개체(운영자, 역할 또는 과정)와 연계시키는 방식 기술(보안수준 1, 2, 3, 4)
- 모듈이 사용한 제로화 방법과 이 방법이 제로화된 값의 복구와 재사용을 방지하는 방식에 관한 이론적 근거(보안수준 1, 2, 3, 4)

A.2.10 자가시험

- 동작 전 및 조건부 시험을 포함한 암호모듈에 의해 수행된 자가시험(보안수준 1, 2, 3, 4)
- 자가시험의 성공 및 실패 상태 표시(보안수준 1, 2, 3, 4)
- 모든 오류 상태 기술(보안수준 1, 2, 3, 4)
  - 자가시험 실패 시
  - 오류 상태로 들어갈 수 있는 조건과 대응
  - 오류 상태에서 나가 암호모듈의 정상 운영을 재기하는 데 필요한 조건과 방법(예: 모듈의 유지보수, 모듈 재시작, 자동적인 모듈 복구, 제한 기능 동작모드로 들어가기, 점검 및 수리를 받기 위해 모듈을 벤더로 반송된 경우 포함)
- 안전한 암호모듈의 운영에 중요한 모든 보안기능, 모듈에 의해 수행되는 적용 가능한 전원 인가 시험과 조건부 시험 식별(보안수준 1, 2, 3, 4)
- 암호모듈에서 우회 능력이 구현되었을 때, 상호 전환 절차를 확인할 수 있는 메커니즘이나 논리(보안수준 1, 2, 3, 4)

A.2.11 생명주기 보증

- 암호모듈에 사용한 형상관리시스템(보안수준 1, 2, 3, 4)
- 형상관리시스템이 관리하는 암호모듈, 모듈 구성 요소 및 모듈 관련 개발 문서(보안수준 1, 2, 3, 4)
- 암호모듈의 안전한 설치 및 생성, 시동을 위한 절차(보안수준 1, 2, 3, 4)
- 암호모듈을 인가받은 운영자에게 배포 및 전달하는 동안의 보안 유지 절차(보안수준 2, 3, 4)
- 암호모듈의 하드웨어와/또는 소프트웨어, 펌웨어 구성 요소 설계와 암호모듈의 보안정책, FSM 간 관련성(보안수준 1, 2, 3, 4)
- 암호모듈에 소프트웨어가 포함되면, 그 소프트웨어의 소스 코드와 소프트웨어의 모듈 설계와의 관련성을 분명하게 설명할 수 있는 코멘트 및 주석(보안수준 1, 2, 3, 4)
- 암호모듈에 하드웨어가 포함되어 있으면, 하드웨어 도식과/또는 HDL 목록(보안수준 1, 2, 3, 4)
- 기능적인 명세 기술－암호모듈, 암호모듈의 기능, 암호모듈의 외부 물리적 포트와 논리적 인터페이스, 그 물리적 포트와 논리적 인터페이스의 목적(보안수준 2, 3, 4)
- 상세 설계 명세－암호모듈의 주요 구성 요소의 내부 기능, 내부 구성 요소 인터페이스, 그 구성 요소 인터페이스의 목적(하나의 전체로 암호경계 내와 주요 구성 요소 내) 내부 정보 흐름(보안수준 3, 4)
- 암호모듈 설계와 기능명세 간의 관련성(사전 조건과 사후 조건 포함)(보안수준 4)
- 다음 사항으로 구성된 상태 천이 다이어그램과 상태 천이표를 사용하는 유한상태모델 기술(보안수준 1, 2, 3, 4)
  - 암호모듈 동작 및 오류 상태
  - 한 상태에서 다른 상태로의 전환
  - 한 상태에서 다른 상태로 전환되게 만드는 데이터 입력과 제어 입력을 포함한 입력 이벤트
  - 한 상태에서 다른 상태로 전환된 결과로, 내부 모듈 상태와 데이터 출력, 상태 출력을 포함한 출력 이벤트
- 소프트웨어 또는 펌웨어의 소스 코드 명세(보안수준 1, 2, 3, 4)
- 각 암호모듈 하드웨어 구성 요소 및 암호모듈 소프트웨어 구성 요소에 대하여, 개발 문서는 ① 암호모듈 구성 요소, 기능 또는 절차를 정확하게 실행시키기 위해 시작 단계에서 요구되는 사전 조건과 ② 암호모듈 구성 요소, 기능 또는 절차의 실행이 정확히 완료된 경우 예측되는 사후 조건을 명세하는 주석을 서술해야 한다(보안수준 4).
- 관리자 안내서는 다음을 명세해야 한다(보안수준 1, 2, 3, 4).
  - 암호관리자와 다른 관리자 역할에 사용할 수 있는 암호모듈의 관리 기능, 보안 이벤트, 보안매개변수(해당되면 매개변수값), 물리적 포트와 논리적 인터페이스
  - 독립된 운영자 인증 메커니즘이 기능적으로 독립을 유지하기 위해 요구되는 절차
  - 검증대상 동작모드에서 암호모듈을 관리하는 방법에 대한 절차
  - 암호모듈의 안전한 운영과 관련된 사용자 동작에 대한 가정 사항
- 비관리자 안내서는 다음을 명세해야 한다(보안수준 1, 2, 3, 4).
  - 암호모듈 사용자가 사용할 수 있는 검증대상 및 비검증대상 암호알고리즘, 물리적 포트, 논리적 인터페이스
  - 암호모듈의 검증대상 동작모드에 대한 모든 사용자의 책임

A.2.12 기타 공격의 완화

- 암호모듈이 이 표준에서는 명세되지 않은 하나 이상의 특정 공격에 대응하도록 설계되었다면 개발 문서는 해당 공격에 대한 대응 방법을 열거해야 한다(보안수준 1, 2, 3).
- 암호모듈에서 이 표준 어디서도 명세되지 않은 특정 공격들에 대한 대응 기법이 설계되었다면, 개발 문서는 공격에 대응하기 위한 방법과 대응 기술의 효과를 시험하는 방법을 명세해야 한다(보안수준 4).

부속서 B
(규정)

암호모듈 보안정책

B.1 일반사항

다음의 목록은 보안정책에서 제공해야 하는 요구사항을 요약한다[B.01].

해당 내용은 검증기관의 결정에 의해서 변경될 수 있다.

B.2 항목

B.2.1 일반사항

- 개별 조항의 수준과 전반적인 수준을 나타내는 표(표 설명)

B.2.2 암호모듈 명세

- 사용 환경을 포함한 모듈의 목적 및 용도
- 모듈을 묘사할 수 있는 다이어그램 또는 도식도, 사진. 하드웨어 모듈 사진 포함. 보안정책이 모듈의 복수 버전을 포괄하면, 각 버전을 별도로 나타내거나 나타낸 그림이 모든 버전을 대표하여 그림임을 설명하는 주석을 단다. 소프트웨어 또는 펌웨어 암호모듈의 경우, 보안정책에는 다음을 나타내는 블록 다이어그램을 포함시킨다.
  - 운영체제와 다른 지원 애플리케이션, 암호경계와 관련된 소프트웨어 또는 펌웨어 모듈의 논리적 객체 위치를 나타내어 논리적 객체와 암호경계 사이에 있는 모든 논리적, 물리적 층을 분명하게 정의
  - 소프트웨어 또는 펌웨어 모듈의 논리적 객체와 그 암호경계 내 있는 운영 시스템과 다른 지원 애플리케이션 간의 상호작용
- 모듈 설명
  - 모듈과 모든 구성 요소(하드웨어 또는 소프트웨어, 펌웨어)의 버전 제공/식별
- 하드웨어 또는 소프트웨어, 펌웨어, 하이브리드 지정
  - 소프트웨어와 펌웨어, 하이브리드 암호모듈의 경우, 모듈을 시험했던 운영체제의 목록과 그 모듈에 의해 사용할 수 있는 것으로 벤더가 확인한 운영체제 목록
- 모듈 설명 전체의 보안수준과 각 영역별 보안수준
- 모듈의 물리적, 암호경계에 관한 정확한 정의
  - 보안정책에 명시된 암호경계에서 제외된 하드웨어 또는 소프트웨어, 펌웨어
- 동작모드와 각 모드로의 선택 방법. 보안정책은 암호모듈 내 실행된 각 검증대상 동작모드와 각 동작모드의 구성 방법을 기술한다.
- 제한 기능 동작 설명
- 모든 보안기능 표(표 설명). 검증대상 서비스에서 키 강도 및 운영 모드(예: CBC, CCM) 포함
- 블록 다이어그램
- 전반적인 보안 설계 및 운영 규칙
- 해당되는 초기화 요구사항

B.2.3 암호모듈 인터페이스

- 모든 포트와 인터페이스(물리적, 논리적)를 나열한 표(표 설명)
- 다섯 개의 논리적 인터페이스에 따른 정보 정의
- 물리적 포트에 따른 데이터 명시
- 신뢰 채널 명시
- 오류 상태에서 제어 출력 인터페이스를 막지 않는 경우 기대 사항과 이론적 근거

B.2.4 역할, 서비스, 인증

- 모든 역할 명시
- 역할표(표 설명). 입력, 출력에 대한 서비스 명령어
- 해당 방법의 신원 또는 역할에 기반 여부와 상관없이 각 인증 방법 및 요구되는 방법 명시
- 인증 요구사항이 어떻게 만족되었는가?
- 우회 능력이 있으면, 두 가지 독립적 조치가 무엇이며 상태 확인 방법은?
- 자가 초기화된 암호 출력 기능이 있으면, 두 가지 독립적 조치가 무엇이며 상태 표시 방법은?
- 외부 소프트웨어 또는 펌웨어를 로드했으면, 모듈로의 무단 접근과 무단 사용을 막는 코드의 제어 및 분리에 대한 관리 명세
- 검증대상 또는 비검증대상, 보안 및 비보안 서비스 목록을 분리하여 작성
- 각 서비스별로 서비스 이름, 목적, 용도에 관한 간략한 설명(일부 경우 서비스 이름만으로도 이 같은 정보 제공함.)
  - 사용되거나 구현되어 있는 검증대상 보안기능 목록(알고리즘 또는 키 관리 기법, 인증 기법)
  - 서비스가 사용한 검증대상 보안기능과 관련된 SSP 목록
  - 서비스 사용 권한을 부여받은 각 운영자 역할별로 각각의 접근 권한 명시(모든 SSP로의 접근이 허용된 개인의 권리를 기술한 정보와 각 역할을 인증하는 데 사용한 방식 기술)
- 설치 과정과 암호 인증 메커니즘 설명.

B.2.5 소프트웨어/펌웨어 보안

- 사용한 검증대상 무결성 기법
- 운영자가 요구 시 무결성 시험을 초기화하는 방식
- 제공된 실행 가능 코드의 양식 및 각 구성 요소
- (모듈이 공개 소스일 경우) 코드를 실행 가능 포맷으로 편집하기 위해 필요한 컴파일러와 관리 매개변수

B.2.6 운영환경

- 운영환경(예: 변경 불가 또는 제한적, 변경 가능) 식별
- 운영체제와 시험 플랫폼 식별
- 각 해당 수준별로 요구사항 만족 방법 설명
- 벤더는 다른 운영체제에서의 포팅으로 해당 암호모듈이 정확하게 운영되지 못한다는 사실을 제공해야 함.
- 보안 규칙 또는 설정, 운영환경의 구성에 부가된 제약
- 운영환경의 구성에 부가된 제약

B.2.7 물리적 보안

암호모듈 형태(단일칩, 다중칩 내장, 다중칩 독립형)

- 모듈 내에서 실행되고 있는 물리적 보안 메커니즘(예: 변조-증거 봉인, 변조 방지 봉인, 잠금장치, 변조 대응 및 제로화 스위치, 알람 등)
- 운영자가 물리적 보안이 유지되고 있음을 보장하기 위해 요구되는 조치(예: 변조 방지 봉인의 주기적 확인, 변조 대응 및 제로화 스위치에 대한 시험)
  - 운영자가 모듈의 생명주기를 수정 또는 적용하려는 변조 방지 봉인이나 보안 장치가 필요한 모듈이 있다면, 그 정보를 기술한다. **B.2.2** 내에 참조할 사진/그림은 모듈 구성이나 설정 정보를 필요로 한다. 추가적인 사진이나 그림은 다른 설정 정보를 반영하기 위해 제공해야 한다.
  - 만약 필러 패널이 채워지지 않는 슬롯이나 개구부의 불투명 요구사항을 만족하기 위해 덮어야 한다면, 패널은 필요에 따라 변조 방지 봉인이 부착된 사진/그림이 있어야 한다. 필러 패널은 부품 리스트에 포함된다.
  - 사진/그림이 물리적 보안 요구사항을 만족시키기 위해서는 변조-증거 봉인 또는 보안 장비의 정확한 위치를 나타내야 한다.
  - 필요한 변조-증거 봉인이나 보안 장비의 총 개수를 표시해야 한다(예: 변조-증거 봉인 5개와 불투명 스크린 2개). 정확한 위치를 제공하는 사진/그림은 각 항목의 번호를 표시해야 하고, 표시된 총 개수와 동일해야 한다(실제 변조-증거 봉인 또는 보안 장비는 번호가 표시되지 않아야 한다).
  - 만약 변조-증거 봉인 또는 보안 장치가 모듈 공급업체에 의해 순서가 다시 정렬될 수 있는 부품이라면, 보안정책은 모듈 공급업체의 봉인, 보안 장비, 해당 보안 키트의 부품 번호를 나타내야 한다. 재구성 후 모듈의 운영자는 새로운 변조-증거 봉인이나 보안 장비의 제거와 설명을 요구할 것이다.
  - 운영자의 책임감 있는 역할 명시 ① 미사용된 봉인은 항상 보안에 유의하여 관리 ② 재구성(변조-증거 봉인이나 보안 장치가 제거되거나 설치되는 동안 및 모듈이 검증대상 상태로 돌아가는 동안의 보안 유지)처럼 모듈의 변경 사항을 직접 관리 및 관찰
  - 변조-증거 봉인이나 보안 장비가 제거되거나 설치되었다면, 표면이나 장비는 새로운 변조-증거 봉인이나 보안 장치가 적용되기 위한 준비할 수 있도록 지침서가 포함되어야 한다.
- 실행한 고장 유도 완화 방법 명시

B.2.8 비침투 보안

- 모듈이 모듈의 CSP를 비침투 공격으로부터 보호하기 위해 사용하는 **부속서** F에서 지칭된 모든 비침투 완화 기법 명시
- 모듈이 모듈의 CSP를 비침투 공격으로부터 보호하기 위해 사용하는 **부속서** F에서 지칭된 모든 비침투 완화 기법의 효과성 명시

비고 모듈이 모듈의 CSP를 비침투 공격으로부터 보호하기 위해 사용하는 **부속서** F에서 지칭된 모든 비침투 완화 기법의 효과성 기술하는 상세 설명의 수준이어야 한다.

B.2.9 중요 보안매개변수 관리

- 키 유형과 비트 강도, 보안기능, 키 생성 장소와 방법, 키 주입 및 출력 여부, SSP 생성 및 설정방법을 명시하고 관련 키를 나타내는 키 표시 제공
- 기타 SSP 표와 생성 방법 제시
- 검증대상 및 비검증대상 난수 발생기
- 난수 발생기 출력의 사용 기술
- 난수 발생기 엔트로피 소스
- 전자 및 수동 키 입출력 방법
- SSP 저장 방법
- 보호하지 않은 SSP 제로화 방법과 이론적 근거, 운영자 초기화 기능 명시

- 알고리즘 또는 키 길이가 검증대상 동작모드에서 비검증대상 동작모드로 변경되는 경우 해당 변경 기간 또는 시간 간격

B.2.10 자가시험

- 정의된 매개변수와 함께 운영 전 및 조건부 자가시험 목록 제공과 시험이 수행되는 동안의 조건 나열
- 주기적인 자가시험 반복을 위한 시간 동안 모듈의 운영을 방해하는 결과를 초래할 수 있는 조건에 관한 시간 기간과 정책 명시
- 모든 오류 상태와 상태 표시 기술
- 적용 가능할 경우, 운영 초기화에 대한 기술

B.2.11 생명주기 보증

- 모듈의 안전한 설치 및 초기화, 시동, 운영을 위한 절차 명시
- 유지보수 요구사항 명시
- 관리자 및 비관리자 가이드라인 제공(별도의 문서일 수 있다.)

B.2.12 기타 공격의 완화

- 완화한 기타 공격 명시
- 나열한 완화 기법의 효과성 기술
- 보안 관련 가이드라인 및 제약 사항

비고 기타 공격 완화를 위해 실행하는 보안 메커니즘을 기술하는 상세 설명의 수준이어야 한다.

부속서 C
(규정)

검증대상 암호알고리즘

C.1 목적

이 부속서에서는 검증기관이 선정한 검증대상 암호알고리즘을 제공한다. 검증대상 암호알고리즘은 블록 암호, 공개키 암호알고리즘, 전자서명, 메시지 인증 코드, 해시함수, 난수 발생기, 키 설정 방식 등으로 분류된다.

검증대상 암호알고리즘 목록은 암호모듈 검증기관이 별도로 제공한다.

부속서 D
(규정)

검증대상 중요 보안매개변수 생성 및 설정 방법

D.1 목적

이 부속서는 이 표준에 적용할 수 있는 검증대상 중요 보안매개변수 생성 및 설정 방법 목록을 제공한다.

D.1.1 중요 보안매개변수 생성

검증대상 중요 보안매개변수 생성 목록은 검증기관이 별도로 제공한다.

D.1.2 중요 보안매개변수 설정 방법

검증대상 중요 보안매개변수 설정 방법 목록은 검증기관이 별도로 제공한다.

부속서 E
(규정)

검증대상 인증 메커니즘

E.1 목적

이 부속서는 이 표준에 적용할 수 있는 검증대상 인증 메커니즘 목록을 제공한다.

E.1.1 인증 메커니즘

검증대상 인증 메커니즘은 검증기관이 별도로 제공한다.

부속서 F
(규정)

검증대상 비침투 공격 완화 방법

F.1 목적

이 부속서는 이 표준에 적용할 수 있는 검증대상 비침투 공격 완화 방법 목록을 제공한다.

F.1.1 비침투 공격 완화 방법

검증대상 비침투 공격 완화 방법 목록은 검증기관이 별도로 제공한다.

참고문헌

[1] KS Q ISO 10007:2003, 품질경영 — 구성 관리 지침

[2] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-2, May 25, 2001(with latest change notices)

[3] KS X ISO/IEC 27001, 정보기술 — 보안기술 — 정보보호 경영시스템 — 요구사항

KS X ISO/IEC 19790:2015
해 설

이 해설은 본체와 부속서에 규정·기재한 사항 및 이들과 관련된 사항을 설명하는 것으로 표준의 일부는 아니다.

1 개정의 취지

이 표준은 대응하는 국제표준 ISO/IEC 19790:2012(2nd Edition)가 개정됨에 따라 국내 표준을 개정한 것이다.

2 대응하는 표준과의 정합성

이 표준은 대응하는 국제표준 ISO/IEC 19790:2012와 비교하여 볼 때, 표면상으로 경미한 차이는 있지만 표준 내용에 관해서는 전체적으로 동등하다.

3 장래의 방침

이 표준은 관련 표준인 ISO/IEC 19790:2012와 동등한 것으로, 관련 표준이 개정되었을 경우에 한하여 이 표준을 개정한다.

한국산업표준	정보기술 — 보안기술 — 암호모듈 보안 요구사항
발간 • 보급	한 국 표 준 협 회 153-787 서울특별시 금천구 가산디지털1로 145 에이스하이엔드타워 3차(16층) ☎ (02)2624-0114 ☎ (02)2624-0148 http://www.kssn.net

KS X ISO/IEC 19790:2015

KSKSKS
SKSKS
KSKS
SKS
KS
SKS
KSKS
SKSKS
KSKSKS

Information technology — Security techniques — Security requirements for cryptographic modules

ICS 35.040

Korean Agency for Technology and Standards
http://www.kats.go.kr