情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

신 암호모듈 검증기준 FIPS PUB 140-3의 변경 내용 분석

고갑승*, 배익환*, 최성자*, 이강수*†

요 약

정보시스템의 보호를 위한 정보보호 제품의 경우, CC를 바탕으로 하는 '정보보호시스템 평가제도'를 통해 평가 및 인증하며, 정보보호제품을 구현한 암호모듈의 경우, '암호모듈검증제도'(CMVP)를 통해 시험 및 검증한다. 본 글에서는 사실상의 국제기준인 미국 및 카나다의 CMVP의 새로운 검증기준 후보인 FIPS PUB 140-3의 변화내용을 분석한다. 또한, FIPS 140-1, FIPS 140-2, ISO/IEC 19790(즉, FIPS 140-2의 국제표준)의 내용과도 비교한다.

Ⅰ. 서 론

정보보호 기능은 모든 유형의 '정보시스템'이 가져야 할 기본이며 공통기능이 되었다. 또한, 정보시스템은 각종 정보보호 '제품' (예: 침입차단제품, 가상사설망 제품, 스마트카드 제품 등)을 통해 구현하며, 정보보호 제품은 보안 서비스를 제공하기위한 '암호모듈'을 통해 구현한다. 여기서, 암호모듈은 보안서비스를 제공하기 위한 보안 프로토콜, 보안 매커니즘 및 암호 알고리즘이며 하드웨어, 소프트웨어 또는 펌웨어로 구현된다.

따라서, 정보시스템의 전체 보안성을 평가 및 보증하기 위해서는 시스템을 구성하고 있는 정보보호 제품 및 암호모듈을 평가해야한다. 정보보호 제품의 '평가 및 인증' (evaluation & certification)은 국내·외적으로 국제공통기준인 CC(Common Criteria, ISO/IEC 15408)에 기반한 평가인증 체계를 통해 실시하며, 암호모듈의 '시험과 검증' (test & verification)은 CMVP(Cryptographic Module Verification Program)를 통해 실시한다. CMVP는 미국과 캐나다에서 운영 중인 암호검증체계이며 NIST FIPS 140-1(과거)과 NIST FIPS 140-2(현재) 기준과 이 기준으로부터 유도한 구체적인 시험기준인 DTR(derived test requirement)을 기반으로 하여 시험 및 검증한다.

FIPS 140-2는 사실상의 국제표준이며, 실제 암호모듈 검증을 위한 국제기준인 ISO/IEC 19790은 FIPS 140-2와 거의 동일하다. 또한, 아직 투표단계인 ISO/IEC 24759는 ISO/IEC 19790을 위한 시험기준인 DTR에 해당한다. 미국의 CMVP는 우리나라와 일본의 암호모듈검증 체계의 모델이 되었으며, 향후, CCRA처럼 'CMVP 상호인정(CMVP RA) 제도'가 실시될 것으로 예상된다.

이와 같은 배경에서, 본 논문에서는 CMVP의 새로운 기준 후보인 FIPS 140-3의 변화내용을 분석한다. 또한, CMVP와 관련된 각국의 각종 기준의 차이를 명확히 하고 CC와 CMVP와의 차이점도 제시한다.

본 글을 이용하면, CC 전문가에게는 CMVP를 쉽게 이해할 수 있으며, CMVP 전문가에게는 CC를 쉽게 이해할 수 있다.

본 글의 2장에서는 각 국의 CMVP의 기준을 조사한 결과와 CC와의 개념상의 유사점과 차이점을 보인다. 3장에서는 FIPS 140-3의 변화 내용을 보이며 기존의 기준(즉, FIPS 140-1, FIPS 140-2와 ISO/IEC 19790)의 차이점도 제시한다. 4장에서는 분석과 결론을 맺는다.

Ⅱ. CMVP 기준의 분류

2.1. CMVP의 종류

미국의 CMVP의 기준이 된 모체는 Federal Standard 1027이며 이는 DES 사용 장비의 일반 보안요구사항이

*한남대학교 컴퓨터공학과(kabseung@se.hannam.ac.kr, ikanir@se.hannam.ac.kr, irecomm@dreamwiz.com, †gslee@eve.hannam.ac.kr)

며 하드웨어 중심이며 제한적이었다. 따라서, 이를 대체하기위해 FIPS 140 기준을 제정하였다.

• FIPS 140-1 (1994년 1월)은 벤더(개발자)에게 융통성을 부여하고 하드웨어 중심이며 소프트웨어로 구현된 암호모듈도 암호모듈로 간주하기 시작하였다[1, 2].

• FIPS 140-2 (2001년 5월)에서는 FIPS 140-1을 재구성하고 요구사항을 명확히 하였고 벤더나 검증자를 위한 DTR을 개발하였고 설계보증 개념을 추가하였다[3, 4]. ISO/IEC 19790 (2006년 3월)은 FIPS 140-2를 국제표준화한 것이며 내용을 일부 변경하였다[5, 6].

• FIPS 140-3은 2007년 7에 초안이 발표되었다[7]. 우리나라와 일본도 미국의 CMVP를 기반으로 하여 제도를 운영하고 있다[8, 9, 10, 11]. [표 1]은 CMVP와 관련된 각 국의 각종 기준간의 관계를 체계화한 것이다.

DTR은 FIPS 140-2를 기준으로 하여 시험 및 검증을 할 때, 각 보안요구사항 영역(area) 별로 '시험항목'

〔표 1〕 CMVP 기준의 분류

기준별 / 국가별	암호모듈 검증기준 (CMVP)			암호모듈 시험기준 (DTR)		
	기준명	발행년도	상태	기준명	발행년도	상태
미국 및 카나다 (CMVP)	NIST FIPS 140-1	1994.1	폐지	DTR for FIPS FIPS 140-1	1995.3	최종
	NIST FIPS 140-2	2001.5	현재 표준	DTR for FIPS FIPS 140-2	2004.3	초안
	NIST FIPS 140-3	2007.7	초안 (07.10까지 컴멘트 접수)	N/A	N/A	N/A
국제	ISO/IEC 19790	2006.3	현재 표준	ISO/IEC 24759	2007.5	FCD (07.9.14까지 투표)
우리나라 (KCMV)	암호검증기준 V1.2 (FIPS 140-2 참조)	2006.11	현재 표준	암호시험기준 V1.0 (DTR 참조)	2007.3	표준
	KS X ISO/IEC 19790	2007년말	공람중	KS X ISO/IEC 24759	2007년말	공람중
일본 (JCMVP)	JIS X 19790 (당분간 '암호모듈평가기준 제 0.1판, 2005년 3월 (FIPS 140-2의 번역) 사용	2007.3	현재 표준	JIS X 5091 (암호모듈시험기준 제 0.1판, 2005년 3월 (DTR의 번역)	2007.3	현재 표준

(즉, 벤더(개발자)가 제출해야할 문서이며 벤더의 행동(assertion)을 정의하고, 시험항목을 위해 '제출문서' 을 명세함) 및 '시험절차'(즉, 시험자가 행할 시험절차)를 상세히 명세한 문서이다. NIST의 CMVP체계에서는 DTR에 따라 시험을 실시할 때의 지침을 별도의 '구현

〔표 2〕 CMVP와 CC간의 개념의 대응

CC 3.1	CMVP (FIPS 140-2)
기능 클래스 (10종) • 보안감사, 통신, 암호지원, 사용자데이터보호, 식별 및 인증, 보안관리, 프라이버시, TSF보호, 자원활용, TOE접근, 안전한 경로/채널	승인된 암호 알고리즘 • 승인된 보호함수, 난수발생기, 키설정 기법
보증 클래스 (8종) • PP평가, ST평가, 개발, 설명서, 생명주기지원, 시험, 취약성평가, 합성	요구사항 영역 (10종) • 암호모듈명세, 암호모듈 포트와 인터페이스, 역할-서비스-인증, 유한상태기계, 물리적보안, 운영환경, 암호키관리, 자가시험,설계보증, EMC/EMI, 기타공격에 대한 대응
보증 패밀리 • 보증 클래스당 1개 이상 • 예: '생명주기지원' 클래스내의 '형상관리능력' 패밀리 ALC_CMC)	부영역 • 영역당 1개 이상) • 예: '역할-서비스-인증' 영역내의 '역할'
보증 컴포넌트 • 보증패밀리당 1개 이상 • 예: ALC_CMC 패밀리내의 컴포넌트 ALC_CMC.1)	
보증 엘리먼트 • 보증컴포넌트당 1개 이상 • 예: ALC_CMC.1 컴포넌트내의 개발자요구사항 ALC_CMC.1.D	시험항목 (assertions) • 부영역당 1개 이상 • 예: '역할-서비스-인증' 영역내의 '역할' 부영역내의 'AS03.07'
평가수준 • Evaluation Assurance Level 1 ~ 7	평가수준 • Security Level 1 ~ 4 (※FIPS 140-3에서는 5까지)
종속관계 (dependencies)	없음
개발자요구사항 (developer action elements) • 예: ADV_TDS.2.1D	시험항목 (assertions) • 예: AS05.01
증거요구사항 (content and presentation elements) • 예: ADV_TDS.2.1C	제출문서 (required vendor information) • 예: VE05.01.01
평가자요구사항 (evaluator action elements) • 예: ADV_TDS.2.1E	시험절차 (required test procedure) • TE05.01.01
평가자 공통요구사항 • 모든 보증컴포넌트마다 공통이며 " .*.1E 평가자는 제공된 정보가 모든 증거요구사항을 만족하는지 확인해야한다." 임	시험자 공통 사항 • "제출문서를 검증하는 업무" 임
보안목표명세서 (ST)	암호모듈 보안정책
	• FIPS 140-1에서는 TCSEC으로 평가된 OS 권장 • FIPS 140-2(ISO/IEC 19790)에서는 CC로 평가된 OS 권장

지침'으로 발표하고 있다[12]. 사실, CMVP의 참여자(개발자, 벤더, 평가자, 검증자 등)에게는 FIPS 140-2보다는 DTR이 필요한 문서이다.

2.2. CMVP와 CC와의 관계

CMVP는 정보시스템의 하위수준인 암호모듈을 시험 및 검증하기위한 것이고, CC는 상위수준인 정보보호 제품이나 시스템을 평가 및 인증하기 위한 제도이지만, 둘 사이에는 공통점이 많다[13]. [표 2]는 CC V.3.1과 CMVP (FIPS 140-2, ISO/IEC 19790)간의 개념상의 대응을 보인다.

CC와 CMVP 모두 평가대상물(제품 또는 암호모듈)의 보안기능과 보증수준을 별도의 차원으로 보고 있다. 예컨대, CC의 경우, 보안기능은 많지만 보증수준이 낮은(예: EAL1) 제품도 있고, 보안기능은 1가지이지만 보증수준이 높은(예: EAL7) 제품도 있다. 또한, CMVP의 경우, 많은 수의 '승인된(approved)' 보안함수를 최저등급(1등급)으로 평가할 수 도 있고(Open SSL처럼 대부분의 소프트웨어로 구현된 암호 라이브러리가 여기에 해당됨), 한 가지 암호알고리즘(예: AES)만을 최고 보안등급(SL4)로 검증할 수 있다.

CMVP는 CC에 비해 계층성이 부족하다. 즉, CC의 요구사항은 클래스-패밀리-컴포넌트-엘리먼트로 계층구조화 되어있지만, CMVP에서는 영역과 부영역 및 시험항목(assertion)에 대응한다. CC의 보증 엘리먼트별 개발자요구사항, 증거요구사항, 평가자요구사항 및 평가자 공통요구사항은, CMVP에서 시험항목, 제출문서, 시험절차 및 시험자 공통사항에 각각 대응한다. 특히, CC에서 특정 제품에 대한 보안요구사항명세서에 해당하는 '보안목표'는 CMVP에서는 '암호모듈보안정책'에 해당한다.

Ⅲ. 변화 내용

3.1 개요

3.1.1. 목차의 변화

[표 3]은 CMVP의 각 기준의 목차의 차이를 보인다. ISO/IEC 19790은 FIPS 140-2를 국제문서화한 것이므로 큰 변화는 없지만, FIPS 140-3은 많은 변화가 있음을 알 수 있다.

3.1.2. 관련 법의 변화

FIPS 140-2는 "Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106"에 근거를 두고 있지만, FIPS 140-3은 이것과 FISMA로 알려진 "Federal Security Management Act of 2002(Public Law 107-347)"에 근거를 두고 있다.

3.1.3. 보안 등급의 변화

FIPS 140-2와 ISO/IEC 19790은 다음과 같이 4개 등급으로 되어 있다.

- 1등급: 비평가 OS, 물리적 보안 없음
- 2등급: 불법조작-증거, 역할기반 인증, OS는 EAL2
- 3등급: 물리적 보안 메커니즘, 불법조작-발견/대응, 제로화, 신분기반 인증, 포트와 인터페이스, 안전한 경로, OS는 EAL3
- 4등급: 물리적 보안 메커니즘, 작동범위(전압, 온도), 환경 보안. OS는 EAL4

그러나 FIPS 140-3은 다음과 같이 5개 등급으로 되어있다.

- 1등급: FIPS 140-2와 동일
- 2등급: OS는 DAC 및 감사메커니즘 제공(EAL2 없음) 추가됨
- 3등급: 안전한 채널, 지식분산, 타이밍 분석 공격, OS는 EAL3 운영자에 의한 공격방지기능, 안전한 채널을 통한 통신 및 감사기능(EAL3 없음), 생명주기보증(형상관리, 하위수준 시험, 벤더가 제공한 인정정보를 사용한 운영자인증)
- 4등급: two-factor 인증, 단순전력분석(SPA), 차분전력분석(DPA), 모듈비활성시 CSP보안강화, OS는 감사기능 강화, 전제-후제조건 및 기능명세간의 대응성을 비정형적으로 증명
- 5등급 추가: 모듈비활성시CSP 및 PSP보안강화, EFP 메커니즘, 비가시적 방사 시험, 전자기 방출 공격, 전제-후제조건 및 기능명세간의 대응성을 비정형적으로 증명하고 정형모델로 검증

〔표 3〕 CMVP 기준의 목차 비교

FIPS 140-1 (1994년 1월)	FIPS 140-2 (2001년 5월)	ISO/IEC 19790 (2006년 3월)	FIPS 140-3 (2007년 7월)
1. 개요 ▪4개 등급 정의	1. 개요 ▪4개 등급 정의	1. 범위	1. 개요 ▪5개 등급 정의
2. 용어와 약자	2. 용어와 약자	2. 참고문헌 3. 용어와 정의 4. 약어	2. 용어와 약자
		5. 암호모듈 보안수준 4개 등급 정의	
3. 보안기능 목적	3. 보안기능 목적	6.	3. 보안기능 목적
4. 보안 요구사항	4. 보안 요구사항	7.	4. 보안 요구사항
4.1 암호모듈	4.1 암호모듈 명세	7.1	4.1 암호모듈 명세 ▪암호모듈 유형 ▪암호 범위 ▪다중 승인된 동작모드 ▪노후된 기능성 ▪모듈 보안강도
4.2 모듈 인터페이스	4.2 암호모듈 포트와 인터페이스	7.2	4.2 암호모듈 물리적 포트 및 논리적 인터페이스
4.3 역할과 서비스	4.3 역할, 서비스 및 인증	7.3	4.3 역할, 인증 및 서비스
4.4 유한상태기계 모델	4.4 유한상태 모델	7.4	4.10 생명주기 보증 ▪ 유한상태모델
4.5 물리적 보안 ▪단일칩 암호모듈 ▪다중칩 내장 암호모듈 ▪다중칩 독립 암호모듈 ▪EFP/EFT	4.5 물리적 보안 ▪일반 물리적 보안요구사항 ▪단일칩 암호모듈 ▪다중칩 내장 암호모듈 ▪다중칩 독립 암호모듈 ▪EFP/EFT	7.5	4.6 물리적보안 ▪일반 물리적 보안요구사항 ▪단일칩 암호모듈 ▪다중칩 내장 암호모듈 ▪다중칩 독립 암호모듈 ▪EFP/EFT
4.6 소프트웨어 보안	-	-	**4.4** 소프트웨어 보안 **(※내용다름)**
4.7 OS 보안	4.6 운영환경 ▪OS 요구사항	7.6	4.5 운영환경 ▪변경가능 운영환경을 위한 OS 요구사항
4.8 암호키 관리 ▪키 생성 ▪키 저장 ▪키 분배 ▪키 파기 ▪키 주입 및 출력 ▪키 검색(archiving)	4.7 암호키 관리 ▪난수발생기 ▪키 주입 및 출력 ▪키 생성 ▪키 저장 ▪키 설정 ▪키 재로화	7.7	4.8 SSP 관리 ▪난수발생기 ▪SSP 주입 및 출력 ▪SSP 생성 ▪SSP 저장 ▪SSP 설정 ▪SSP 제로화
4.9 암호 알고리즘 (※ 내용없음)	-	-	-
4.10 EMI/EMC	4.8 EMI/EMC	없음	없음
4.11 자가시험 ▪전원인가 시험: 암호알고리즘, 소프트웨어/펌웨어 무결성, 핵심기능, 통계적 난수 발생기 ▪조건부시험: 쌍일치 일관성, 소프트웨어/펌웨어 로드, 수동 키주입, 연속난수발생기	4.9 자가시험 ▪전원인가시험: 암호알고리즘, 소프트웨어/펌웨어 무결성, 핵심기능 ▪조건부시험: 쌍일치 일관성, 소프트웨어/펌웨어 로드, 수동 키주입, 연속난수발생기, 우회	7.8	4.9 자가시험 ▪운영전 자가시험 ▪조건부 자가시험 ▪핵심기능 시험
-	-	-	**4.7** 물리적보안: **Non-Invasive** 공격 ▪타이밍공격 ▪단순전력분석 ▪차분전력분석
-	4.10 설계보증 ▪ 형상관리 ▪ 지침 문서 ▪ 배포와 운영 ▪ 개발	7.9	**4.10** 생명주기 보증 ▪형상관리 ▪배포와 운영 ▪개발 ▪지침문서 ▪벤더시험
-	-	-	4.10 생명주기 보증 ▪ 설계
-	4.11 기타 공격에 대한 대응(mitigation) ▪ 전력분석 ▪ 타이밍 분석 ▪ 고장유도 ▪ TEMPEST	G:	4.11 기타공격에 대한 대응
A: 문서요구사항 요약	A: 문서요구사항 요약	A:	부록 A: 문서 요약 요구사항
B: 소프트웨어개발 방법 권고	B: 소프트웨어개발 방법 권고	F:	부록 B: 소프트웨어개발 방법 권고
C: 선택 참고문헌	C: 암호모듈 보안정책	C:	부록 C: 암호모듈 보안정책
D: 선택 관련문헌	D. 참고문헌	참고문헌	부록 D: 선택 참고문헌
-	E. 응용가능 URL		-
-	별책부록 A: 승인된 보안기능(함수)	D: 승인된 보안기능	-
-	별책부록 B: 승인된 보호프로파일	C: 승인된 보호프로파일	-
-	별책부록 C: 승인된 난수생성기		-
-	별책부록 D: 승인된 키설정 기법	E: 승인된 키설정방법	-

3.1.4. 용어의 변화

FIPS 140-2에서 암호키, 비밀키, 개인키 등을 ISO/IEC 19790과 FIPS 140-3에서는 CSP (주요보안매개변수)로 통일했고 비 보안 자료를 PSP (공개보안매개변수)로 칭한다. 또한, CSP와 PSP를 합하여 SSP (비밀보안매개변수)로 칭한다. 또한, 용어명이 같아도 정의가 대폭 변경되었다.

- ISO/IEC 19790에서 추가된 용어는 "승인기관, 승인된 ISO/IEC, 승인된 OS, 승인된 보호프로파일, 비대칭 암호 기법, 인증서, 유지보수역할, 보호막, 제품수준(production-grade, 대칭 암호 기법, trust anchor" 이며, 삭제된 용어는 "자동 키 전송, EMC/EMI, HMAC, 공개키(비대칭) 암호 알고리즘, TEMPEST, 검증 기관"이다.
- FIPS 140-3에서 추가된 용어는 "허용된 보안 기능, 승인된 자료 인증 기법, 우회 기능, 조건부 시험, 형상관리시스템(CMS), 암호 알고리즘, 암호 해쉬 기능, 암호적으로 보호된 CSP/PSP/SSP, EME, 전자적 키 전송, Electrostatic discharge (ESD), Hard/hardness, 하드웨어 모듈, 하이브리드 모듈, 구현 지침, 키 동의, 논리적 보호, 메시지인증코드, Min-엔트로피, 변경가능 운영환경, 모듈 소프트웨어 인터페이스(MSI), 다중칩 내장 암호모듈, 다중칩 독립 암호모듈, Non-invasive 공격, 변경불가능 운영환경, 불투명, 운영환경, 보호막, 운영 전 시험, 제품수준(production-grade), 공개보안매개변수(PSP), 방사 hardening, 보안강도, 비밀 자료, 비밀보안매개변수(SSP), 서비스 입력, 서비스 출력, 서비스, 단일칩 암호모듈, 소프트웨어 모듈, 강한, 안전한 채널, Two-factor 인증, 검증된"이다. 삭제된 용어는 "자동 키 전송, EMC/EMI, 실체, 엔트로피, 펌웨어, 해쉬-기반 메시지인증코드(HMAC), 수동 키 전송, 보호프로파일, 평가대상물(TOE), TEMPEST, TOE 보안기능(TSF), TOE 보안정책(TSP), 안전한 경로" 이다. 특히, '펌웨어'라는 용어를 전혀 사용하지 않고 하드웨어와 소프트웨어로만 분류하고 있다. 또한, Trusted Path는 Trusted Channel로 변경하였다.

3.1.5. 보안요구사항의 목적의 변화

FIPS 140-2와 ISO/IEC 19790은 7가지이지만, FIPS 140-3은 '암호모듈의 적절한 설계, 배포 및 구현을 보증하기 위함'을 추가하여 8가지이다.

3.1.6. 암호모듈 보안정책의 변화

FIPS 140-2와 ISO/IEC 19790에서는 10가지 요구사항 영역에 없는 것(예: 식별 및 인증정책, 접근통제 정책)을 명세해야하지만 FIPS 140-3에서는 11가지 영역(즉, 명세, 포트와 인터페이스, 역할-서비스-인증, 소프트웨어 보안, 운영환경, 물리적 보안, 물리적 보안-Non-Invasive 공격, SSP 관리, 자가시험, 생명주기 보증, 기타공격의 대응)을 모두 포함하고 있다.

3.2. 보안요구사항 영역별 변화

3.2.1. 암호모듈 명세

- FIPS 140-2: 문서화 요구사항 있음
- ISO/IEC 19790: 암호모듈 범위(범위)에 논리적 범주 포함
- FIPS 140-3
  - 문서화 요구사항 삭제됨
  - 암호모듈유형: 하드웨어모듈, 소프트웨어모듈, 하이브리드 모듈
  - 암호 '범위'의 정의를 간략화(즉, 모듈의 운영을 위해 제공된 프로세서와 기타 하드웨어 컴포넌트)
  - '다중 승인된 동작모드' 요구사항 5가지 추가
  - '노후된 기능성' 지원 요구사항 4가지 추가
  - '모듈의 보안강도' 요구사항 추가

140-2	1	2	3	4
암호모듈 명세	▪ 암호모듈 명세, 암호범위, 승인된 알고리즘, 승인된 동작모드. 암호모듈의 설명, 모든 하드웨어, 소프트웨어, 및 펌웨어 컴포넌트 포함 ▪ 모듈 보안정책 설명			

140-3	1	2	3	4	5
암호모듈 명세	▪ 모듈, 범위, 승인된 알고리즘s 및 승인된 동작모드의 명세 ▪ 모듈 하드웨어 및 소프트웨어의 기술 ▪ 모듈의 문서화				
	▪ 보안정책은 승인된 동작모드를 정의	▪ 모듈의 승인된 동작모드를 표시			

3.2.2. 암호모듈 포트 및 인터페이스

- FIPS 140-2: 4종의 인터페이스: 자료입력, 자료출력, 제어입력, 상태출력
- ISO/IEC 19790: 동일
- FIPS 140-3
  - 논리적 인터페이스: 동일
  - 입·출력 시'안전한 채널' 추가

140-2	1	2	3	4
암호모듈 포트 및 인터페이스	• 요구되고 선택적인 인터페이스 • 모든 인터페이스 및 모든 입력 및 출력 자료 경로의 명세		• 다른 자료 포트와 논리적으로 격리된 CSP를 위한 자료포트	

140-3	1	2	3	4	5
암호모듈 논리적 포트 및 물리적 인터페이스	• 요구된 및 선택적 인터페이스 • 모든 인터페이스 및 모든 입력 및 출력 자료 경로의 명세		• 다른 포트와 인터페이스로부터 안전한 채널을 사용한 물리적으로 격리되거나 논리적으로 격리된 CSP의 입력 및 출력		

3.2.3. 역할, 서비스 및 인증

- FIPS 140-2
  - 역할종류: 사용자, 암호관리자, 유지보수
  - 서비스 종류: 상태보이기, 자가시험 실행, 승인된 보호함수 실행
  - 우회기능 상태: 비활성(암호기능 작동), 활성(암호기능 작동안함) '활성 및 dedicated'
  - 운영자 인증 종류: 역할기반, 신분기반
- ISO/IEC 19790: 동일
- FIPS 140-3
  - 역할 종류 중 유지보수 역할 삭제
  - 서비스 종류: 모듈 버전번호 보이기, 제로화 추가됨
  - 우회기능 기능: '활성 및 dedicated' 상태 삭제됨
  - '외부 소프트웨어로딩' 요구사항 4개 추가
  - 'OS가 인증기능을 구현했다면, OS의 인증 메커니즘은 본 요구를 충족할 것' 추가됨
  - '디폴트 인증 자료' 사용 시 2개 지침 추가됨: 처음인증을 대체해야함, 배포된 모듈마다 유일해야 함
  - 인증강도 요구사항 추가: 100만 ==> 1억, 모듈 구현에 의해 충족되어야하며 문서화된 절차적 제어나 보안 규칙에 의존하지 않아야함. '사전공격'에 대비해 패스워드를 만들 것
  - 수준 4,5에서 two-factor 신분기반 인증을 강화

140-2	1	2	3	4
역할, 서비스 및 인증	• 요구되고 선택적인 역할과 서비스 간의 논리적 분리	• 역할기반 또는 신분기반 운영자 인증	• 신분기반 운영자 인증	

140-3	1	2	3	4	5
역할, 서비스 및 인증	• 모듈의 역할 및 서비스의 정의	• 역할기반 또는 신분기반 인증	• 신분기반 운영자 인증	• Two-factor 인증	

3.2.4. 소프트웨어 보안

- FIPS 140-2: 없음
- ISO/IEC 19790: 없음
- FIPS 140-3
  - 1등급: 실행가능 코드, 승인된 무결성 기술, MSI, 읽기와 수정의 제한, 언로드 시 제로화, 포맷 체크
  - 2등급: 전자서명기반 무결성 시험
  - 3등급: 소프트웨어 무결성 시험 시작을 위한 MSI (모듈 소프트웨어 인터페이스) 명령
  - 4등급: CSP와 무결성 시험 소프트웨어 코드의 암-복호
  - 5등급: PSP와 무결성 시험 소프트웨어 코드의 암-복호

140-2	1	2	3	4
없음				

140-3	1	2	3	4	5
보안	• 실행가능 코드, 승인된 무결성 기법, MSI, 읽기 및 수정 제한, 언로드시 제로화, 포맷체크	• 전자서명기반 무결성 시험.	• 소프트웨어 무결성 시험을 개시하기 위한 NSI명령 • 해쉬값 제로화	• CSP 및 무결성 시험 코드의 암호 및 복호화	• PSP 및 무결성 시험 코드의 암호 및 복호화

3.2.5. 유한상태기계

- FIPS 140-2
  - 표현법: 전태전이도, 상태전이표

- 표현내용: 상태, 전이, 입력사건, 출력사건
- 상태종류: 전원 on/off, 암호관리자, 키/CSP 주입, 사용자, 자가 시험, 오류, 우회, 유지보수

■ ISO/IEC 19790: 동일

■ FIPS 140-3

- '생명주기 보증'에 포함됨
- 표현법: '상태 기술' 추가
- 표현내용: 입력사건에 입력 자료와 제어 입력을 포함, 출력사건에 내부모듈조건, 자료 출력, 상태 출력 포함
- 상태종류 추가분: 일반 초기화, CSP 주입(명칭 변경), 승인된, Quiescent(모듈의 휴지 상태), (유지보수 상태 삭제됨)

140-2	1	2	3	4
유한상태 모델	• 유한상태모델 명세 • 요구된 상태 및 선택적 상태 • 상태전이도 및 상태 전이의 명세			

140-3	1	2	3	4	5
생명주기 보증(FSM)	• 유한상태모델				

3.2.6. 물리적보안

■ ISO/IEC 19790

- 1등급: 유지용 접근인터페이스에 접근 시 자동적 제로화 (3등급에서 이동)
- (EFP/EFT) 전압에 대한 시험요구 추가
- non-invasive-공격: 없음

■ FIPS 140-3

[공통]

- 유지용 접근인터페이스에 접근 시 자동적 제로화 (3등급) 삭제
- 2등급: 가시광선에 대해 불투명 커버링 추가
- 3등급: 통풍 openings를 통한 프로빙 방어
- 4등급: 견고한 불투명 제거-내성 코팅
- 5등급: electrostatic discharge 및 전자기 방사 유도 고장에 대한 고장 내인성, 비가시광선에 불투명(X선, MRI 등)

[단일칩]

- 거의 동일함
- 2등급: '가시광선에 대한 불투명' 요구사항 삭제됨
- 5등급: 요구사항 없음

[다중 내장]

- 3등급: '강한 외장' 추가
- 5등급: 불법조작-발견 및 대응회로 자체 및 CSP의 보호기능 추가(불능화 시)

[다중 독립]

- 2등급: '가시광선에 대한 불투명' 요구사항 삭제됨, 증거 테입이나 입체도형 봉인은 유일한 번호를 부여
- 2등급: '강한 외장' 추가
- 5등급: 불법조작-발견 및 대응회로 자체 및 CSP의 보호기능 추가(불능화 시)

[EFP/EFT]

- 5등급: 온도와 전압에 대한 EFP적용 할 것
- 온도에 대한 시험요구 상세화
- 전압에 대한 시험요구 추가

[non-invasive-공격]

- FIPS 140-2의 '기타공격의 대응' 의 일부 내용 포함
- 1,2등급: 없음
- 3등급: 타이밍 공격
- 4등급: 단순전력분석(SPA)(SPA) 공격, 차분전력분석(DPA) 공격.
- 5등급: 전자기 방출 공격

140-2	1	2	3	4
물리적보안	• 제품수준 장비	• 락이나 불법조작근거	• 덮개나 문을 위한 불법조작 발견 및 대응	• 불법조작-발견 및 대응 외장 • EFP 또는 EFT

140-3	1	2	3	4	5
물리적보안	• 제품수준(production grade) 컴포넌트	• 불법조작증거 • 불투명 덮개나 외장	• 탈착식 덮개 및 문에 불법조작 대응 및 제로화 회로 • 프로빙으로부터 보호하는 벤트 • 견고한 불투명 코팅이나 외장	• 온도 및 전압을 위한 EFP나 EFT • 다중칩 모듈을위한 불법조작 발견 및 제로화 회로	• 온도 및 전압을 위한 EFP • 비가시적 방사 시험에 대해 불투명 • 불법조작 발견 및 제로화 회로 불능화의 보호

3.2.7. 물리적보안 (non-invasive-공격)

■ FIPS 140-2: 없음 (※ '기타공격의 대응'에 타이밍공격과 SPA/DPA 포함)

■ ISO/IEC 19790: 없음

■ FIPS 140-3

- FIPS 140-2의 '기타공격의 대응'의 일부 내용 포함
- 1, 2등급: 없음
- 3등급: 타이밍 공격
- 4등급: 단순전력분석(SPA)(SPA) 공격, 차분전력분석(DPA) 공격.
- 5등급: 전자기 방출 공격

140-2	1	2	3	4
없음				

140-3	1	2	3	4	5
물리적보안-Non-invasive 공격	• 추가요구사항 없음		• 타이밍 분석 공격으로부터 CSP의 보호	• SPA 및 DPA공격으로부터 CSP의 보호.	• EME 공격으로부터 CSP의 보호

3.2.8. 운영환경

■ ISO/IEC 19790
- 2등급: 저장된 감사 데이터는 공인안된 접근을 방어해야한다.
- 3등급: 감사메커니즘에 '실패적인 자체 시험 운영' 및 '탬퍼-발견의 고지' 추가

■ FIPS 140-3
- 용어: "범용 운영환경" 용어 삭제, 제한된(정적 변경불가능 가상) 운영환경 ==> 변경불가능 운영환경
- 1등급: '모듈 운영 중 타 프로세스가 보안자료에 접근 하는것 방지' 삭제됨. 세션 시작과 종료 시 CSP를 제로화 추가. 다중 동시운영자 적용 시 강제적 접근통제. 등급 2에 있던 OS의 접근통제 메커니즘 요구사항이 등급 1로 이동. OS의 형상은 '보안관리자 지침'에 명세해야함.
- 2등급: OS의 EAL2요구사항 삭제. 모듈 외부에 저장된 감사정보도 승인된 암호메커니즘을 적용. '보안정책'에 운영자의 식별 및 인증을 OS가 할지 개발자가 제공 코드가 할지 명세
- 3등급: OS의 EAL3요구사항 삭제. OS는 모듈 소프트웨어, SSP 및 감사 자료의 수정 방지기능 가질 것. 운영자와 모듈간의 안전한 채널 형성 (Trusted Path 용어 제거). OS는 이들 기능을 영구적으로 가질 것
- 4, 5등급: OS의 EAL4요구사항 삭제. 감사기능은 영구적이고 감사기능 및 자료의 보호(운영자의 공격에 대한 보호)

140-2	1	2	3	4
운영환경	• 단일 운영자 • 실행가능 코드 • 승인된 무결성 기법	• 명세된 DAC 메커니즘과 감사기능을 가지고 EAL2로 평가된 PP	• '보안정책모델'을 가지고 '안전한 경로'가 추가되고 EAL3으로 평가된 참조된 PP	• '안전한 경로'가 추가 되고 EAL4로 평가된 참조된 PP

140-3	1	2	3	4	5
운영환경	• 단일사용자 OS 또는 재량적접근통제(DAC).	• 감사 메커니즘 • 재량적접근통제(DAC)	• 암호 소프트웨어, SSP 및 감사 자료 보호 • 안전한 채널 • 확장형 감사		• 확장형 감사 요구사항.

3.2.9. 암호키(SSP)관리

■ FIPS 140-2

■ ISO/IEC 19790

[난수발생기]
- 용어: 난수(RNG) ==> 랜덤비트(RBG)
- 엔트로피 소스시험 필요. RBG내의 결정적 컴포넌트를 시험. 발생기의 출력에 대해 연속적 난수발생기 시험(ISO/IEC 18031준수)

[키제로화]
- 인증 프록시 과정에 평문데이터를 노출하기위해 CSP가 사용된다면, 이들 제로화 할 필요가 없다.(예: 모듈 초기화 키)

■ FIPS 140-3

[난수발생기]
- 용어: 암호키 ==> SSP(= CSP + PSP)
- 엔트로피 시험. RBG내의 결정적 컴포넌트를 시험. 발생기의 출력에 대해 연속적 난수발생기 시험(ISO/IEC 18031준수)
  요구된 최소 엔트로피 값을 모듈에 제공하고 검증할 것

[키생성]
- 키 생성 ==> SSP생성
- SSP를 외부로부터 로드 가능
- 승인된 '난수발생기'를 이용해 승인된 'SSP 생성방법' 이용

[키설정]
- OTAS(radio communications 암호모듈) 삭제됨

- 전자적 SSP 설정방법(즉, SSP 전송 또는 SSP 동의체계)을 이용

[키주입과 출력]

- 소프트웨어모듈의 경우 추가(OS가 통제)
- 전자적 전송된 CSP 경우: 암호형태, 무결성 보호
- 전자적 전송된 PSP 경우: 무결성 보호
- 비전자적 전송된 PSP 경우: 평문으로
- 1, 2등급: 삭제됨(윗 문장과 중복)
- 3, 4, 5등급: 두 운영자가 동일한 신분을 갖지 않음에 대한 검증을 추가. SSP 주입과 출력 시 안전한 채널 활용

[키저장]

- 문서요구사항 4가지 추가(저장방법, 접근 보호 방법, 수정 보호방법, 엔티티와 연관 방법)
- PSP는 모듈외부의 무인가 운영자가 수정하지 말아야함 추가

[키제로화]

- 제로화를 등급별로 구체화 함
- 1, 2등급: 절차적이고 모듈의 제어(예: 모듈 파기 등)와 독립적일 것.
- 3등급: 모듈이 CSP의 제로화를 제거할 것
- 4등급: 없음
- 5등급: 모듈은 모든 PSP 제로화 방법 제공. PSP 제로화 방법 및 증거를 문서화. 임시 PSP도 제로화 할 것

140-2	1	2	3	4
암호키 관리	• 키 관리 메커니즘: 난수 및 키 생성, 키 설정, 키 분배 키 주입/출력, 키 저장 및 키 제로화			
	• 수동 전송방법을 사용해 전송된 비밀 및 개인키는 평문형태로 주입 또는 출력될 수 있음		• 수동 전송방법을 사용해 전송된 비밀 및 개인키는 암호화하거나 지식분산절차를 사용해 주입 또는 출력한다.	

140-3	1	2	3	4	5
SSP 관리	• 난수발생기, SSP 생성, SSP 설정, SSP 주입 및 출력, SSP 저장 및 CSP 제로화에 대한 요구사항				
	• 비전자적으로 전송된 SSP는 평문형태로 주입가능		• 비전자적으로 전송된 SSP는 암호 형태이거나 지식분산절차를 사용해 주입 또는 출력		• PSP의 제로화

3.2.10. EMI/EMC: ISO/IEC 19790 및 FIPS 140-3에서 삭제

140-2	1	2	3	4
EMI/EMC	• 47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable		• 47 CFR FCC Part 15. Subpart B, Class B (Home use).	

140-3	1	2	3	4	5
없음					

3.2.11. 자가시험

[전원인가시험] (=운영전 자가시험)

- FIPS 140-2
  - 암호알고리즘 시험
  - 소프트웨어/펌웨어 무결성 시험
  - 핵심기능 시험
- ISO/IEC 19790
  - 암호알고리즘 시험: 동일
  - 소프트웨어/펌웨어 무결성 시험: '소프트웨어/펌웨어 무결성 시험은 ROM에 저장된 데이터에는 적용하지 말아야한다'.
  - 핵심기능 시험: 동일
  - 난수발생기(RBG) 엔트로피 시험 추가
- FIPS 140-3
  - 자가시험 성공 전에는 모듈을 사용하지 말것 추가
  - '전원인가(전원인가) 시험' ==> '운영전 자가시험(운영전 자가시험)' 명칭 변경
  - 운영 전 자가시험의 시기 정의함: 전원 on 상태와 서비스를 위한 기능사용 사이
  - 벤더는 운영전 시험까지의 최소 경과시간을 명세해야함
  - '보안정책'에 시험실패시의 행동을 명세
  - 모듈의 운영 중단 관련 정책과 기간을 명세
  - 암호알고리즘 시험: 모든 승인 및 허용된 암호알고리즘에 대해 실시. 소프트웨어무결성 시험에서 사용한 승인된 자료인증 기법내의 보안기능에 대해서는 KAT가 불필요함
  - 소프트웨어/펌웨어 무결성시험(==> 소프트웨어 무결성시험): non-reconfigurable 메모리내의 코드는 시험할 필요 없음. 1등급에서 승인된

자료인증기법은 MAC이나 전자서명을 사용을 포함해야함. 2, 3, 4, 5등급에서 전자서명의 사용을 포함해야함

- 핵심기능 시험: 운영전 자가시험이 아니라 자기 시험내의 독립적인 항목으로 처리함. 2, 3, 4등급에서 전원인가나 조건 충족 시 시험할 것을 요구함
- 운영전 우회시험: 추가됨

[조건부 시험]

- FIPS 140-2
  - 암호키 쌍 일치 시험
  - 소프트웨어/펌웨어 로드 시험
  - 수동 키 주입 시험
  - 연속적인 난수발생기 시험
  - 우회 시험
- ISO/IEC 19790
  - 암호키 쌍 일치 시험: 세부내용삭제
  - 소프트웨어/펌웨어 로드 시험: 삭제
  - 수동 키 주입 시험: 동일
  - 연속적인 난수발생기 시험: '시험은 오직 RBG의 최소 강도(health)시험을 목적으로 한 것이며, 랜덤 생성의 품질을 나타내지는 않는다. RBG상에서의 모든 기타 시험은 ISO/IEC 18031에 따라 처리해야한다.' 추가
  - 우회시험: 동 FIPS 140-3
  - 조건부 시험 ==> 조건부 자가시험
  - 암호키 쌍 일치 시험: 키동의 시에 키를 사용할 때 요구사항 추가
  - 소프트웨어/펌웨어 로드 시험(소프트웨어 로드 시험) : 승인된 인증기법(MAC, 전자서명, HMAC 등)을 적용 ==> 승인된 전자서명 기법을 적용
  - 수동 키 주입 시험: 조건에서 '운영자의 실수에 의한 잘못된 주입'도 추가
  - 연속적인 난수발생기 시험: 16비트이상 블록 ==> 64비트 이상 블록. 시험대상에 'RBB 엔트로피 소스' 추가
  - 우회시험(==> 조건부 우회 시험): 내용 달라짐(간소화).
    우회용 정보의 변경시 무결성 검증으로 대체
  - RBB 엔트로피 소스 시험: 소스의 출력단에서 최소-엔트로피 평가 추가일

140-2	1	2	3	4
자가시험	• 전원인가 시험: 암호 알고리즘 시험, 소프트웨어/펌웨어 무결성 시험, 및 핵심 기능 시험 • 조건부 시험			

140-3	1	2	3	4	5
자가시험	• 운영전 자가시험: 소프트웨어 무결성 시험, 암호 알고리즘 시험, 및 운영전 우회 시험 • 조건부 자가시험: 쌍일치(pair-wise) 일관성 시험, 소프트웨어 로드 시험, 수동 키 주입 시험, 연속 RBG 시험, RBG 엔트로피 소스 시험, 및 조건부 우회 시험				

3.2.12. 설계보증

[형상관리]

- ISO/IEC 19790: 형상관리 기능을 좀 더 구체화
- FIPS 140-3
  - 설계보증 ==> 생명주기보증
  - 1,2등급: 신분과 버전의 변경을 추적하고 유지함. 형상관리 문서화 추가
  - 3, 4, 5등급: 자동화된 형상관리 요구

[설계]

- FIPS 140-2: 없음
- FIPS 140-3
  - 설계추가(FIPS 140-2의 '개발' 내용 일부 이동)
  - 1등급: 모듈과 보안정책 간 대응
  - 2등급: 기능명세
  - 3등급: 상세설계
  - 4등급: 전제조건과 후제조건 간 및 기능명세 간 대응의 비정형적 증명
  - 5등급: 전제조건과 후제조건 간 및 기능명세 간 대응의 비정형적 증명 및 정형모델

[개발]

- FIPS 140-2: FIPS 140-3에서 '설계'와 '개발'로 분산되었음
- ISO/IEC 19790: 개발보안문서 및 개발도구 문서 요구사항 추가
- FIPS 140-3
  - FIPS 140-2의 '개발'의 일부내용이 FIPS 140-3에서 '설계'로 이동함
  - 1등급: 모듈과 보안정책 간 대응 삭제
  - 2, 3등급: 비독점 언어 추가

[배포와 운영]

- ISO/IEC 19790: 동일
- FIPS 140-3
  - 2등급: 배포 중에 불법조작발견 추가
  - 3, 4, 5등급: 모듈의 인증 실시

[지침문서]

- FIPS 140-2: 암호관리자(암호-officer)지침, 사용자 지침
- ISO/IEC 19790: 동일
  - 관리자(administor) 지침: 암호관리자와 관리적 역할용 독립적 운영자인증 메커니즘의 유지 절차 추가
  - 비관리자(non-adm.) 지침: 사용자와 비관리적 역할용

[벤더시험]

- FIPS 140-2: 없음
- ISO/IEC 19790: 없음
- FIPS 140-3
  - '생명주기 보증'에 속함
  - 1, 2등급: 모듈의 기능시험(기능명세서대로)
  - 3, 4, 5등급: 하위수준(컴포넌트, 포트와 인터페이스 수준) 시험 절차 명세 및 결과

140-2	1	2	3	4
설계 보증	▪ 형상관리 (CM) ▪ 안전한 설치 및 생성 ▪ 설계 및 정책 대응 ▪ 지침문서	▪ CM 시스템 (FIPS 140-2) ▪ 안전한 분배 ▪ 기능 명세	▪ 고급언어 구현	▪ 정형적 모델 ▪ 상세 설명 (비정형적 증명) ▪ 전제조건 및 후제조건

140-3	1	2	3	4	5
생명주기 보증: 설계	▪ 모듈 및 보안 정책간의 대응	▪ 기능 명세	▪ 상세 설계	▪ 전제조건과 후제조건 및 기능명세간의 대응성의 비정형적 증명	▪ 정형적 모델 및 비정형적 정형모델 및 기능명세간의 대응성 증명

140-2	1	2	3	4
설계 보증	▪ 형상관리 (CM). ▪ 안전한 설치 및 생성 ▪ 설계 및 정책 대응 ▪ 지침문서	▪ CM 시스템 (FIPS 140-2) ▪ 안전한 분배 ▪ 기능al 명세	▪ 고급언어 구현	▪ 정형적 모델 ▪ 상세 설명 (비정형적 증명) ▪ 전제조건 및 후제조건

140-3	1	2	3	4	5
생명주기 보증: CMS	▪ 모듈, 컴포넌트 및 문서를 위한 CMS ▪ 각각은 생명주기를 통해 유일하게 식별되고 추적됨		▪ 자동 CMS		
생명주기 보증: 개발	▪ 주석을 단소스 코드, 도면 (schematics) 또는 HDL	▪ 소프트웨어 고급언어 ▪ 하드웨어 고급명세언어			
생명주기 보증: 벤더시험	▪ 기능 시험		▪ 하위수준 시험		
생명주기 보증: 배포 및 운영자	▪ 시동 절차	▪ 배포 절차	▪ 벤더가 제공한 인증정보를 이용한 운영자 인증		
생명주기 보증: 지침 문서	▪ 관리자(adm.) 및 non-관리자(adm.) 지침				

3.2.13. 기타공격에 대한 대응

- FIPS 140-2
  - 전력분석 공격(SPA, DPA)
  - 타이밍 분석
  - 고장유도 공격
  - TEMPEST
- ISO/IEC 19790
  - 7.10절에서 등급만 정의
  - 부록G에서 상세히 기술
  - 1, 2, 3등급과 4등급으로 구분
  - 전력분석 공격(SPA, DPA): 동일
  - 타이밍 분석: 동일
  - 고장유도 공격: 동일
  - TEMPEST: 삭제
- FIPS 140-3
  - 1, 2, 3등급: 대응할 모든 공격을 보안정책이나 지원문서에 열거함
  - 4, 5등급: 공격 대응방법과 그 효과성을 명세
  - 각종 공격사례(SPA, 타이밍 등) 삭제
  - '물리적보안(non-invasive 공격)'에 타이밍, SPA/DPA 공격을 이동시킴

140-2	1	2	3	4
기타공격에 대한 대응	▪ 현재 시험요구사항이 없는 기타공격에 대한 대응의 명세			

40-3	1	2	3	4	5
기타공격에 대한 대응	보안정책에 명세된 모든 대응 메커니즘 (※주의. 본문에는 1, 2, 3등급(대응할 모든 공격을 보안정책이나 지원문서에 열거함)과 4, 5등급(공격 대응방법과 그 효과성을 명세)으로 구분함)				

Ⅳ. 분석 및 결론

FIPS 140-2에서는 4등급이지만 FIPS 140-3은 5등급이다. FIPS 140-3은 그동안 발표된 자료에 의하면 6등급 평가기준이있지만, 최종적으로 5등급이 되었다. 부록 A와 B는 각각 FIPS 140-2와 FIPS 140-3의 등급을 정의한 것이다.

FIPS 140-2의 1, 2등급은 FIPS 140-3의 1, 2 등급과 매우 유사하다. FIPS 140-2의 3, 4등급은 FIPS 140-3의 3, 4, 5등급에 대응되지만, FIPS 140-3의 5등급의 경우 FIPS 140-2의 4등급과 정확히 대응이 되지 않으며 새로운 등급에 해당한다. 이런 문제는 2007년 11월까지 공개 검토과정을 통해 수정될 것으로 예상한다.

NIST에서는 2005년 1월부터 준비하여 2007년 7월 13일에 FIPS 140-3을 발표하였고 2007년 11월까지 공람한 후 2008년에는 FIPS 140-2를 대체할 것으로 예상된다.

한편, FIPS 140-2는 2006년에 이미 ISO/IEC 19790으로 국제표준화 하였고, FIPS 140-2의 DTR도 ISO/IEC 24759로 표준화할 예정이다. 즉, 미국 내에서는 FIPS 140-3을 표준화 할 것이며, 이에 따라 ISO/IEC 19790도 변경해야 할 것이다. 이런 복잡한 환경에서 수행해야 할 활동은 다음과 같다.

- 미국은 FIPS 140-3을 위한 DTR을 개발할 것이다.
- 각국마다 국가 암호정책에 따라 FIPS 140-3에 대한 승인된 보호함수를 지정할 것이다. 이는 FIPS 140-2와 유사할 것이다.
- '보안정책서'가 대폭 변했으므로, 벤더는 FIPS 140-3을 위한 새로운 '보안정책서'를 개발해야 할 것이다.
- 기존에 FIPS 140-1과 2로 검증된 800개의 암호모듈(4개 등급)에 대한 FIPS 140-3 (5개 등급)에 대한 대체 인정을 위한 기준이 마련되어야 한다.
- 국제기준인 ISO/IEC 19790 및 ISO/IEC 24759는 FIPS 140-2를 기반으로 하고 있으며 이를 FIPS 140-3에 맞도록 변경하거나 (제 1안), 또는 그대로 사용한다(제 2안).
- 우리나라(일본 포함)에서 FIPS 140-3의 수용정책: FIPS 140-3이 미국에서 공식 표준화될 때까지 KS X ISO/IEC 19790과 KS X ISO/IEC 24759를 사용한다.
- FIPS 140-3에 대한 시험 기술을 지속적으로 개발 및 축적한다.
- CC체계와 개념상 유사하므로, CC 평가체계와 연계한다.

본 글에서는 CMVP의 새로운 기준이 될 FIPS 140-3의 변화내용을 분석하였다. FIPS 140-3은 FIPS 140-2에 비해 대폭 변경하였다. 즉, 10년간의 CMVP 경험을 바탕으로 개정하였으며 암호모듈의 개발 생명주기에 대한 검증을 강화하고 있다. 예컨대, '소프트웨어 보안' 영역이 추가되었고 '벤더시험'과 부영역이 추가되었다. 특히, 4등급에서 5등급으로 변경한 점이 가장 큰 변화이다.

끝으로, FIPS 140-3은 확정된 것은 아니지만 향후 5년 정도 CMVP에서 사용될 신 기준 이므로, 우리나라도 FIPS 140-3에 나타난 기준에 대한 비용효과적인 시험 및 검증 방법을 개발해야 할 것이다.

참고문헌

[1] FIPS FIPS 140-1, Security Requirements for Cryptographic Modules, NIST, March January 1994.

[2] Derived Test Requirements for FIPS FIPS 140-1, Security Requirements for Cryptographic Modules, NIST, March 1995.

[3] FIPS FIPS 140-2, Security Requirements for Cryptographic Modules, NIST, March May 2001.

[4] Derived Test Requirements for FIPS FIPS 140-2, Security Requirements for Cryptographic Modules, Draft, NIST, March 2004.

[5] FIPS FIPS 140-3 (Draft), Security Requirements for Cryptographic Modules, NIST, July 2007.

[6] ISO/IEC 19790, Information technology- Security techniques - Security requirements for cryptographic modules, 2006.3.

[7] ISO/IEC FCD 24759, Information technology- Security techniques - Test requirements for cryptographic modules, Final comment draft, 2007.5.

[8] 암호검증기준, V 1.2, 암호검증기관, 2006. 11.

[9] 암호시험기준, V 1.0, 암호검증기관, 2007. 3.

[10] JIS X 19790 セキュリティ技術－暗号モジュールのセキュリティ要求事項.

[11] JIS X 5091 セキュリティ技術－暗号モジュールのセキュリティ試験要件.

[12] Implementation Guidance for FIPS FIPS 140-2 and the Cryptographic Module Validation Program, July 2007(update).

[13] CC Common Criteria for Information Technology Security Evaluation Part 1, 2, 3, Version 3.1, Revision 1, September 2006.

부록 A. FIPS 140-2와 ISO/IEC 19790의 보안등급 정의

보안등급 / 요구사항 영역	보안등급 1	보안등급 2	보안등급 3	보안등급 4
암호모듈 명세	▪ 암호모듈 명세, 암호범위, 승인된 알고리즘, 승인된 동작모드. 암호모듈의 설명, 모든 하드웨어, 소프트웨어, 및 펌웨어 컴포넌트 포함 ▪ 모듈 보안정책 설명			
암호모듈 포트 및 인터페이스	▪ 요구되고 선택적인 인터페이스 ▪ 모든 인터페이스 및 모든 입력 및 출력 자료 경로의 명세		▪ 다른 자료 포트와 논리적으로 격리된 CSP를 위한 자료포트	
역할, 서비스, 및 인증	▪ 요구되고 선택적인 역할과 서비스간의 논리적 분리	▪ 역할기반 또는 신분기반 운영자 인증	▪ 신분기반 운영자 인증	
유한상태모델	▪ 유한상태모델 명세 ▪ 요구된 상태 및 선택적 상태 ▪ 상태전이도 및 상태 전이의 명세			
물리적보안	▪ 제품수준 장비	▪ 락이나 불법조작 근거	▪ 덮개나 문을 위한 불법조작 발견 및 대응	▪ 불법조작-발견 및 대응 외장 ▪ EFP 또는 EFT
운영환경	▪ 단일 운영자 ▪ 실행가능 코드 ▪ 승인된 무결성 기법	▪ 명세된 DAC 메커니즘과 감사기능을 가지고 EAL2로 평가된 PP	▪ '보안정책모델'을 가지고 '안전한 경로'가 추가되고 EAL3으로 평가된 참조된 PP	▪ '안전한 경로'가 추가되고 EAL4로 평가된 참조된 PP
암호 키 관리	▪ 키 관리 메커니즘: 난수 및 키 생성, 키 설정, 키 분배 키 주입/출력, 키 저장 및 키 제로화			
	▪ 수동 전송방법을 사용해 전송된 비밀 및 개인키는 평문형태로 주입 또는 출력될 수 있음		▪ 수동 전송방법을 사용해 전송된 비밀 및 개인키는 암호화하거나 지식분산절차를 사용해 주입 또는 출력한다.	
EMI/EMC (FIPS 140-2)	▪ 47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable		▪ 47 CFR FCC Part 15. Subpart B, Class B (Home use)	
자가시험	▪ 전원인가 시험: 암호 알고리즘 시험, 소프트웨어/펌웨어 무결성 시험, 및 핵심 기능 시험 ▪ 조건부 시험			
설계보증	▪ 형상관리 (CM) ▪ 안전한 설치 및 생성 ▪ 설계 및 정책 대응 ▪ 지침문서	▪ CM 시스템 (FIPS140-2) ▪ 안전한 분배 ▪ 기능al 명세	▪ 고급언어 구현	▪ 정형적 모델 ▪ 상세 설명 (비정형적 증명) ▪ 전제조건 및 후제조건
기타공격에 대한 대응	▪ 현재 시험요구사항이 없는 기타공격에 대한 대응의 명세 (FIPS 140-2)			
	▪ 현재 시험요구사항이 없는 기타공격에 대한 대응의 명세 (19790)			▪ 시험요구사항이 있는 기타공격에 대한 대응의 명세 (19790)

부록 B. FIPS 140-3의 보안등급 정의

보안등급 / 요구사항영역	보안등급 1	보안등급 2	보안등급 3	보안등급 4	보안등급 5
1. 암호모듈 명세	• 모듈, 범위, 승인된 알고리즘 및 승인된 동작모드의 명세 • 모듈 하드웨어 및 소프트웨어의 기술 • 모듈의 문서화				
	• 보안정책은 승인된 동작모드를 정의		• 모듈의 승인된 동작모드를 표시		
2. 암호모듈 포트 및 인터페이스	• 요구된 및 선택적 인터페이스 • 모든 인터페이스 및 모든 입력 및 출력 자료경로의 명세		• 다른 포트와 인터페이스로부터 안전한 채널을 사용한 물리적으로 격리되거나 논리적으로 격리된 CSP의 입력 및 출력		
3. 역할, 서비스 및 인증	• 모듈의 역할 및 서비스의 정의	• 역할기반 또는 신분기반 인증.	• 신분기반 운영자 인증	• Two-factor 인증	
4. 소프트웨어 보안	• 실행가능 코드, 승인된 무결성 기법, MSI, 읽기 및 수정 제한, 언로드 시 제로화, 포맷체크	• 전자서명기반 무결성 시험	• 소프트웨어 무결성 시험을 개시하기위한 NSI명령 • 해쉬값 제로화	• CSP 및 무결성 시험 코드의 암호 및 복호화	• PSP 및 무결성 시험 코드의 암호 및 복호화
5. 운영환경	• 단일사용자 OS 또는 재량적접근통제(DAC)	• 감사 메커니즘 • 재량적접근통제 (DAC)	• 암호 소프트웨어, SSP 및 감사 자료 보호 • 안전한 채널 • 확장형 감사	• 확장형 감사 요구사항	
6. 물리적 보안	• 제품수준(production grade) 컴포넌트	• 불법조작 증거. • 불투명 덮개나 외장	• 탈착식 덮개 및 문에 불법조작 대응 및 제로화 회로 • 프로빙으로부터 보호하는 벤트 • 견고한 불투명 코팅이나 외장	• 온도 및 전압을 위한 EFP나 EFT • 다중칩 모듈을 위한 불법조작 발견 및 제로화 회로	• 온도 및 전압을 위한 EFP • 비가시적 방사 시험에 대해 불투명 • 불법조작 발견 및 제로화 회로 불능화의 보호
7. 물리적 보안Non-invasive 공격	• 추가요구사항 없음		• 타이밍 분석 공격으로부터 CSP의 보호	• SPA 및 DPA 공격으로부터 CSP의 보호	• EME 공격으로부터 CSP의 보호
8. SSP 관리	• 난수발생기, SSP 생성, SSP 설정, SSP 주입 및 출력, SSP 저장 및 CSP 제로화에 대한 요구사항				
	• 비전자적으로 전송된 SSP는 평문형태로 주입 가능		• 비전자적으로 전송된 SSP는 암호 형태이거나 지식분산절차를 사용해 주입 또는 출력		• PSP의 제로화
9. 자가시험	• 운영전 자가시험: 소프트웨어 무결성 시험, 암호 알고리즘 시험, 및 운영 전 우회 시험 • 조건부 자가시험: 쌍일치(pair-wise) 일관성 시험, 소프트웨어 로드 시험, 수동 키 주입 시험, 연속 RBG 시험, RBG 엔트로피 소스 시험, 및 조건부 우회 시험				
10. 생명주기 보증 : CMS 설계 FSM 개발 벤더시험 배포 및 운영자 지침 문서	• 모듈, 컴포넌트 및 문서를 위한 CMS • 각각은 생명주기를 통해 유일하게 식별되고 추적됨		• 자동 CMS		
	• 모듈 및 보안정책간의 대응	• 기능 명세	• 상세 설계	• 전제조건과 후제조건 및 기능명세간의 대응성의 비정형적 증명	• 정형적 모델 및 비정형적 정형모델 및 기능명세간의 대응성 증명
	• 유한상태모델				
	• 주석을 단 소스 코드, 도면(schematics) 또는 HDL	• 소프트웨어 고급언어 • 하드웨어 고급명세언어			
	• 기능 시험		• 하위수준 시험		
	• 시동 절차	• 배포 절차	• 벤더가 제공한 인증정보를 이용한 운영자 인증		
	• 관리자(adm.) 및 비-관리자(adm.) 지침				
11. 기타공격에 대한 대응	• 보안정책에 명세된 모든 대응 메커니즘 (주의. 본문에는 1, 2, 3등급(대응할 모든 공격을 보안정책이나 지원문서에 열거함)과 4, 5등급(공격 대응방법과 그 효과성을 명세)으로 구분함)				

부록 C. 물리적 보안요구사항

등급	기준	모든 구현형태의 일반(공통) 요구사항	단일칩 암호모듈	다중칩 내장 암호모듈	다중칩 독립 암호모듈
1	140-2	• 제품등급 컴포넌트 (표준 보호막 가짐)	• 추가 요구사항 없음	• 가능하다면, 제품등급 외장이나 탈착식 덮개	• 제품등급 외장
	19790	• 제품등급 컴포넌트 (표준 보호막 가짐) • 유지보수용 접근 인터페이스에 접근시 자동적 제로화	상동	상동	상동
	140-3	• 제품등급 컴포넌트	상동	상동	상동
2	140-2	• 불법조작-증거 (예: 덥개, 외장 또는 봉인)	• 칩이나 와장에 불투명 불법조작-증거 코팅	• 문이나 탈착식 덥개를 위해 불법조작-증거 봉인이나 제거내성 잠금장치를 가진 불투명 외장 또는 물질로 캡슐화한 불투명 불법조작-증거	• 문이나 탈착식 덥개를 위해 불법조작-증거 봉인이나 제거내성 잠금장치를 가진 불투명 외장
	19790	상동	상동	상동	상동
	140-3	• 불법조작-증거 • 불투명 덥개	상동	상동	상동
3	140-2	• 유지보수용 접근 인터페이스에 접근시 자동적 제로화 • 불법조작 대응 및 제로화 회로. • 보호된 통풍구	• 칩상에 견고한 불투명 불법조작-증거 코팅 또는 • 강한 제거-내성 및 침투-저항 외장	• 다중칩 회로 구현형태를 견고한 불투명 포팅물질로 캡슐화 또는 • 응용가능한 다중칩 독립 보안등급 3 요구사항	• 다중칩 회로 구현형태를 견고한 불투명 포팅물질로 캡슐화 또는 • 제거/침투를 시도할때 심각한 손상을 야기하는 강한 외장
	19790	• 불법조작 대응 및 제로화 회로 • 보호된 통풍구	상동	상동	상동
	140-3	• 불법조작 대응 및 제로화 회로. • 프로빙으로부터 보호된 통풍구	상동	상동	상동
4	140-2	• 온도 및 전압을 위한 EFP나 EFT	• 칩상에 견고한 불투명 제거-내성 코팅	• 불법조작 대응 및 제로화 회로를 가진 불법조작 발견 외장	• 불법조작-대응 및 제로화 회로를 가진 불법조작-발견/대응 외장
	19790	상동	상동	상동	상동
	140-3	상동	상동	상동	상동
5	140-2				
	19790				
	140-3	• 온도 및 전압을 위한 EFP. • 비가시적 방사 시험에 대해 불투명(예: X선, MRI, 등) • ESD 및 방사 고장-유도	• 추가 요구사사항 없음	• 불법조작-발견/대응 회로 대응(mitigation).	

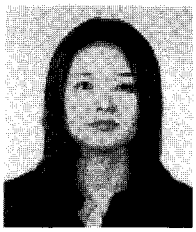
부록 D. DTR의 예: ISO/IEC 19790에 대한 DTR인 ISO/IEC 24759의 '물리적 보안' 영역내의 시험항목

AS06.16(등급 2, 3, 4): OS는 암호범위 내에 저장된 암호 소프트웨어를 운영자 및 실행 프로세스가 읽는 것을 막아야 한다.
[제출 문서]
VE06.16.01: 운영자 또는 실행 프로세스가 암호범위 내에 저장된 암호소프트웨어를 읽는 것을 OS가 어떻게 방지하는지 명세해야 한다.
[시험절차]
TE06.16.01: VE06.16.01에서 명세하는 정보를 제공했는지 확인하여야 한다.
TE06.16.02: 암호범위 내에 저장된 암호 소프트웨어를 읽는 시도를 해야 한다. 어떠한 운영자 또는 실행 프로세스도 암호범위 내에 저장된 암호 소프트웨어를 읽을 수 없다는 것을 검증하여야 한다.

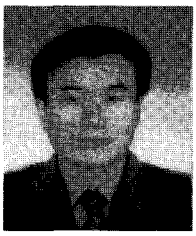
〈著者紹介〉

고 갑 승 (Kab-Seung Kou)
정회원
2005년 2월 : 영동대학교 컴퓨터공학과 학사
2007년 2월 : 한남대학교 대학원 컴퓨터공학과 석사
2007년 3월~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
<관심분야> 소프트웨어공학, 보안공학, 정보보호 컨설팅 및 위험분석

배 익 환 (Ik-Whan Bae)
2006년 2월 : 한남대학교 컴퓨터공학과 학사
2008년 2월 : 한남대학교 대학원 컴퓨터공학과 석사
<관심분야> 소프트웨어공학, 위험분석



최 성 자 (Sung-Ja Choi)
정회원
1991년 2월 : 한남대학교 학사
1997년 2월 : 한남대학교 대학원 석사
2005년 8월 : 한남대학교 대학원 박사
2006년 3월~현재 : 한남대학교 컴퓨터공학과 연구교수 (BK21 정보보안공학지역핵심사업팀)
<관심분야> 소프트웨어공학, 웹공학, 보안공학, 소프트웨어 시험



이 강 수 (Gang-Soo Lee)
종신회원
1981년 2월 : 홍익대학교 전자계산학과 학사
1983년 2월 : 서울대학교 대학원 계산학 전공 석사
1989년 2월 : 서울대학교 대학원 계산학전공 박사
1985년~1987년 : 국립한밭대학교 전자계산학과 전임강사
1992년~1993년 : 미국일리노이대학교 객원교수
1995년 : 한국전자통신연구원 초빙연구원
1987년~현재 : 한남대학교 컴퓨터공학과 교수
2006년 ~현재 : BK21 정보보안공학지역핵심사업팀장
<관심분야> 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼