특 집

암호 모듈 평가 프로그램(CMVP) 분석과 소개

김 석 우*, 정 성 민*, 박 성 근*, 김 일 준**

*한세대학교 정보통신학과, **국가보안기술연구소

Abstract

CMVP(Cryptographic Module Validation Program) validates cryptographic modules to FIPS 140-1, 2, and other FIPS cryptography based standards.

This paper gives an overview of the CMVP, cryptographic modules, cryptographic algorithms, and the applicable standards. This provides a brief overview of the security requirements that must be met by each cryptographic module that is submitted to a CMT laboratory for conformance testing and describes the Cryptographic Algorithm Testing.

I. 서 론

인터넷의 발달은 과거 대면사회에서 사이버 사회로의 전환을 가져왔다. 우리는 현재 이러한 전환의 과도기에 있으며, 대면사회에서 행하던 일을 사이버 사회에도 똑같이 하기를 원한다. 전자상거래가 바로 이러한 것이며, 가상공간의 비대면 특성으로 인해 사이버 사회의 구현은 많은 문제점과 기술적 어려움을 가지고 있다. 이러한 문제를 해결하기 위한 가장 핵심적인 기술이 바로 암호기술이다. 정보보호에 대한 인식이 확산되면서 정보보호 제품 수요가 증가되고 있으며 이에 따라 국외에서는 CC, CMVP(Cryptographic Module Validation Program) 등 정보보호 제품에 대한 평가가 활발히 진행중에 있다. 국내에선 정보호호 제품에 대한 평가제도는 한국 정보보호진흥원의 K1~K7E 평가에서 시작되어 최종적으로 암호알고리즘에 대한 평가를 병행하고 있다. 반면에 국내에선 암호모듈 평가 프로그램인 CMVP가 국내에 정착되지 않은 상태이며, 본 특집에서 정보보호 제품에 탑재된 암호모듈의 안정성 평가체계인 CMVP에 대해 소개하려고 한다. 2장에서 CMVP에 현황과 소개를 하며 3장에선 암호 모듈 안정성 평가항목중 가장 기본적이고 중요한 암호 알고리즘 구현 적합성 테스트 방법에 대해 자세히 소개하며 4장에선 다른 평가제도에 대해 설명한다.

II. CMVP

1. CMVP 역사

북미에서 현재 활발히 진행하고 있는 정보보호 암호모듈 평가 체계인 CMVP는 1995년 7월 미국 NIST(National Institute of Standards and Technology)와 캐나다 주정부의 CSE (Communications Security Establishment)가 공동으로 개발한 암호 모듈의 안전성 검증을 위한 프로그램으로 1994년 미국의 NIST가 제정한 'Security Requirement for Cryptographic Modules'(FIPS 140-1)[2]와 2001년 개정된 FIPS 140-2, 암호알고리즘 관련 FIPS

표준문서를 근간으로 만들어졌다. CMVP는 시험평가 후 Level 1~4를 부여하고, List of Validated FIPS 140-1(FIPS 140-2) Modules'에 등재되어 평가제품으로서 효력을 발휘할 수 있게 된다. 1994년도부터 시작된 암호모듈 평가가 2003년도 현재 280개 이상의 평가된 암호모듈을 보유하여, 평가제품 목록을 통하여 실수요자인 정부기관에게 판매되고 있다. 암호모듈의 평가제도 역시 6개의 민간 평가 기관을 지정하여, 실제 평가토록하고 있으며, 정부기관(NIST/CSE)은 이를 승인하는 FIPS 140-2 평가절차를 따르고 있다. 각 등급은 사용자가 제품을 선택할 수 있는 기준을 제시하며, 사용환경에 따라 적절한 제품을 선택하면 된다.

1994.1 : FIPS 140-1 공표
1995.6 : CMT labs(Infogard)승인
1995.7 : CMVP 개시
1998.10 : RFC for FIPS 140-2
2001.5 : FIPS 140-2 공표
2001.11 : FIPS 140-2 DTR 유효
2002.11.15 : FIPS 140-2 시험 개시

〈그림 1〉에서와 같이 CMVP는 암호 알고리즘을 기반으로한 암호 모듈평가에 기반을 둠으로서 암호 모듈 기반의 정보 보호 제품 평가의 보안적인 측면에서 폭넓은 신뢰성을 제공한다고 할 수 있다.

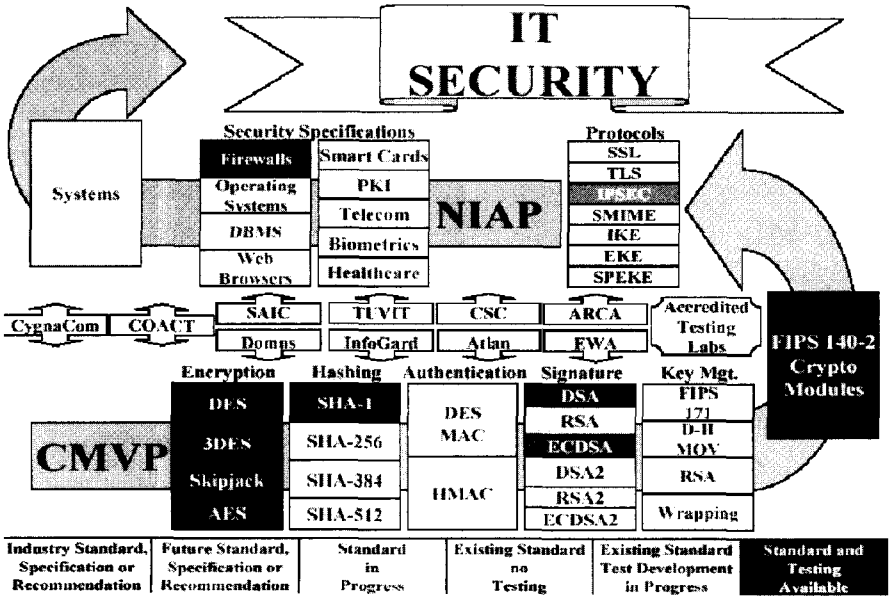
2. CMVP에서 요구하는 평가

CMVP에서 요구하는 암호 모듈의 안전성 평가는 크게 3가지로 구분할 수 있다.

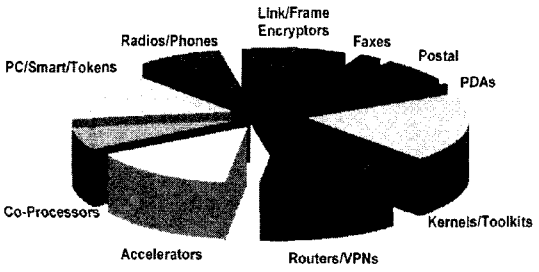
첫째로 구현 적합성 평가이다. 이 평가는 구현된 암호 기술이 표준에 따라 제대로 구현되었는지를 평가하며, 이는 각 표준에 따라 평가하는 방법이 다름을 의미한다.

둘째로 암호 키 운용 및 관리 평가이다. 이 평가는 암호 기술의 안전성에 직접적인 영향을 미치는 암호 키의 생성, 확립, 분배, 입/출력, 저장, 파기 등에 대한 방법 및 과정을 평가함으로서 잘못된 암호 키 운용 및 관리에 따른 암호 키의 유출 가능성을 평가함으로 암호 모듈 안전성 평가에 있어서 가장 중요한 부분이라고 할 수 있다.

셋째로 물리적 보안 평가이다. 이 평가는 암호 모듈의 사용 환경에 대한 평가로 암호 모듈의 운



〈그림 1〉 IT 보안과 평가



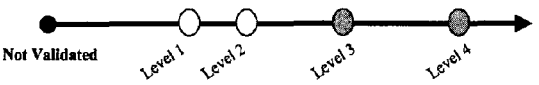
〈그림 2〉 평가 대상 모듈 유형

영 환경, EMI/EMC, Self-Testing 등에 대한 평가를 의미한다.

위와 같이 안전성 평가에 따라 최종적으로 보안 등급을 받은 승인된 제품은 정부기관에서 사용 가능한 제품군으로 등록된다. 승인된 제품은 〈그림 2〉에서 보듯이 하드웨어/소프트웨어/펌웨어 방식의 구현, 칩/Smartcard/USB의 단말 제품에서부터 VPN, CA등의 시스템레벨까지 포함한다. 2003년 현재 CMVP내 등록 리스트[12]에서 약 316개 정도의 H/W, S/W 등 다양한 암호 모듈 기반의 제품들이 안정성 평가를 받고 등록되어 있다. 등록 리스트에는 해당 제품의 모델명과 회사, 연락처, 제품의 형태와 기능적인 설명, 그리고 제품에 대한 최종적인 보안등급과 운영 환경에 대한 정보를 알 수 있다. CC 평가체계와 CC 기반의 보안성 검토의 국내 제도화 이전에, CMVP 제도가 선행되어야 한다고 판단되어, 적용성은 매우 광범위하다고 할 수 있다.

3. CMVP 보안 레벨

CMVP FIPS 140-2[1]에서 규정하고 있는 안전성 등급(Security Level)은 4단계로 나뉘어 있으며, 본 표준안에 담고 있는 각각의 안전성 요구사항이 Level의 등급에 따라 정의되고 규정되어 있다. Level 1부터 Level 4까지 증가되는 보안 등급은 이와 함께 안전성 요구조건도 증가됨을 의미한다. Level에 따른 요구사항을 간단하게 살펴보면 다음과 같다.



〈그림 3〉 보안 등급

보안 등급 1—레벨 1은 가장 기본 등급의 안전성을 보장한다. 적어도 하나 이상의 승인된(즉, 표준) 알고리즘 혹은 승인된 안전한 함수를 사용해야 한다. 특정한 물리적 보안 매커니즘은 필요가 없으며, 평가받지 않은 운영체제(즉, Window나 DOS와 같은 일반 PC상의 O/S)에서 사용되는 보통의 컴퓨팅 시스템 상의 암호 모듈 소프트웨어 부분의 보안 수준을 의미한다.

보안 등급 2—레벨 2는 레벨 1에 물리적 보안 매커니즘 부분을 보완시킨 등급이다. 물리적 보안 매커니즘은 tamper-evidence(eg. tamper-evident coating 혹은 seals 혹은 모듈의 제거될 수 있는 커버상의 pick-resistent locks)에 대한 안전성 요구사항을 다룬다. 레벨 2는 CC (Common Criteria) Protection Profile(PPs)과 CC 평가 등급 EAL2(혹은 그 이상)에서 요구하는 운영체제에서 운용되는 암호기술적 모듈의 소프트웨어 안전성 수준을 의미한다.

보안 등급 3—레벨 3는 레벨 2에 tamper-evident가 포함된 물리적 보안 매커니즘을 보완시킨 등급이다. 따라서 Level 3 등급에서는 암호기술적 모듈 안에 보관되어 있는 CSPs(Critical Security Parameter)에 대한 침입자의 접근을 막고자 하는 시도를 포함한다. 또한 Level 3에서는 신원기반 인증 매커니즘이 필요하며, CC 평가 등급 EAL3(혹은 그 이상)에서 요구하는 운영체제에서 운용되는 암호 모듈의 소프트웨어 안전성 수준을 의미한다.

보안 등급 4—레벨 4는 표준안에서 제정한 가장 높은 안전성을 제공하는 Level 이다. Level 4 등급에서는 물리적 보안 매커니즘이 해당 모듈에 대한 인가되지 않은 어떠한 물리적 접근에 대해서도 완벽한 방어, 봉쇄 기능을 제공해야 한다. 어떠한 방법으로라도 모듈의 enclosure에 침투할 때는 매우 높은 확률로 탐지가 가능해야 하며, 모든 평문 CSPs와 하드웨어 자체에 대한 삭제가

수행되어야 한다. Security Level 4 등급의 암호 모듈은 물리적으로 보호받지 못하는 환경에서의 작업에 효과적이다. 레벨 4는 레벨 3에서의 요구조건과 함께 CC 평가 등급 EAL4(혹은 그 이상)에서 요구하는 운영체제에서 운용되는 암호 모듈의 소프트웨어 안전성 수준을 의미한다.

4. FIPS 140-1 & 140-2

FIPS 140-1(Security Requirement for Cryptographic Modules)은 1994년 1월, 사용자와 개발자로 구성된 정부와 산업계의 Working group에 의해 개발되어지고 표준안으로 제정되었다. 2001년 개정된 FIPS 140- 2, 암호알고리즘 관련 FIPS 표준문서를 근간으로 만들어졌다. Working group은 데이터 민감성의 넓은 분포(e.g., Low value administrative data, million dollar funds transfers, life protecting data)와 적용 환경의 다양성(e.g., a guarded facility, an office, a completely unprotected location) 등을 규정하기 위한 암호 모듈의 4가지 보안 등급(Security Level)을 설정하고 이에 따른 요구 조건들을 제시하였다.

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with *split knowledge procedures.*	
EMI/EMC	47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15, Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

〈그림 4〉 FIPS 140-2의 항목별 요구사항

또한 4가지 보안 등급은 각각 11가지 상세한 요구조건에 따라 분류되며, Level 1부터 Level 4까지 증가되는 보안 등급은 이와 함께 안전성 요구조건도 증가됨을 의미한다. FIPS 140-2는 FIPS 140-1의 개정판으로 개발자와 연구소, 사용자 모임으로부터 지적된 사항들을 바탕으로 적용할 만한 표준과 기술의 변화를 포함하고 있다.

이 표준안에서 제시되는 보안 요구사항들이 암호 모듈의 안전성을 포함하는 경향이 있으나, 요구 사항을 모두 만족한다고 해서 테스트 모듈의 안전성을 보장하는 것은 아니다.

다음은 FIPS 140-2의 11가지 상세한 요구조건 항목에 대해서 간략히 나타낸다.

가) 암호모듈 규격
- 암호알고리즘, 암호적용범위, 동작모드, 제품 설명, HW/SW/FW 등 구성요소, 보안 정책 등

나) 암호모듈 포트와 인터페이스
- 보안 포트와 비 보안포트, 포트에 입력되는 보안 파라메터

다) 역할, 서비스, 인증
- 제품의 사용자들의 역할과 해당 서비스, ID/역할 기반 인증

라) 동작모델(Finite State Model)
- 제품의 모든 동작 상태(state), 해당 전이 상태(state transform)

마) 물리적 보안
- 물리적 접근에 대한 레벨별 요구사항

바) 운영환경
- 독립된 운영환경, CC 평가 EAL 4 레벨 단위별 운영환경

사) 암호키 관리
- 키의 생존주기(생성, 설정, 주입, 분배, 파괴) 동안 관리. 운영

아) EMI/EMC
- FCC Part 15의 Class A, B 에 대한 규격

자) 자가 테스트
- Power-up 테스트, 조건 테스트

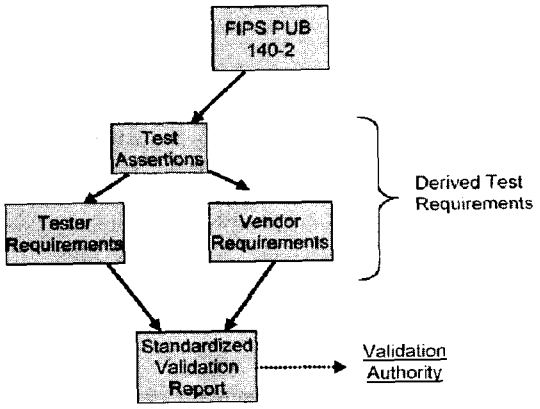
차) 설계 보증
- 설계 시, 개발 환경 툴 및 구성관리(configuration management), CC 기반의 평가 항목(정책 대 구현 일치성, 설치/운영, 상위레벨 기능규격, 모델 등)

카) 공격에 대한 완화
- 공격에 대한 파워 분석, 타이밍 분석, 결함 제시

5. FIPS 140-2 DTR

이 문서는, 암호 모듈이 FIPS 140-2의 요구사항을 따르는가 하는 점을 테스트하기 위해 연구소에서 사용하는 방법을 설명하고 있다. 문서에는 상세한 절차, 조사방법들, 평가자가 반드시 따라야 하는 테스트들, 그리고 암호 모듈이 FIPS 140-2 요구조건을 만족시키기 위해 얻어져야만 하는 기대 결과값 등, 많은 내용이 담겨져 있다. 이처럼 상세한 방법들을 설명함으로서 테스트가 진행되는 동안 높은 객관성을 제공하고 검정을 진행하는 인가된 연구소들 사이의 결과에 관한 일관성을 꾀할 수 있다.

또한 DTR 문서[3]에서는 암호 모듈 탑재 제품을 생산하는 개발자의 입장에서도 그들의 제품이 FIPS 140-2의 요구조건을 만족한다는 충분한



〈그림 5〉 DTR 발전단계

증거를 제공하기 위해 취해야 할 상세한 조건들을 찾을 수 있다. 따라서 연구소에 자신들의 제품 테스트를 의뢰하기 전 표준문서의 안전성 요구조건에 부합하는지를 자체적으로 알아보기 위해 이 문서를 사용하면 효과적일 것이다.

6. CMT Lab.

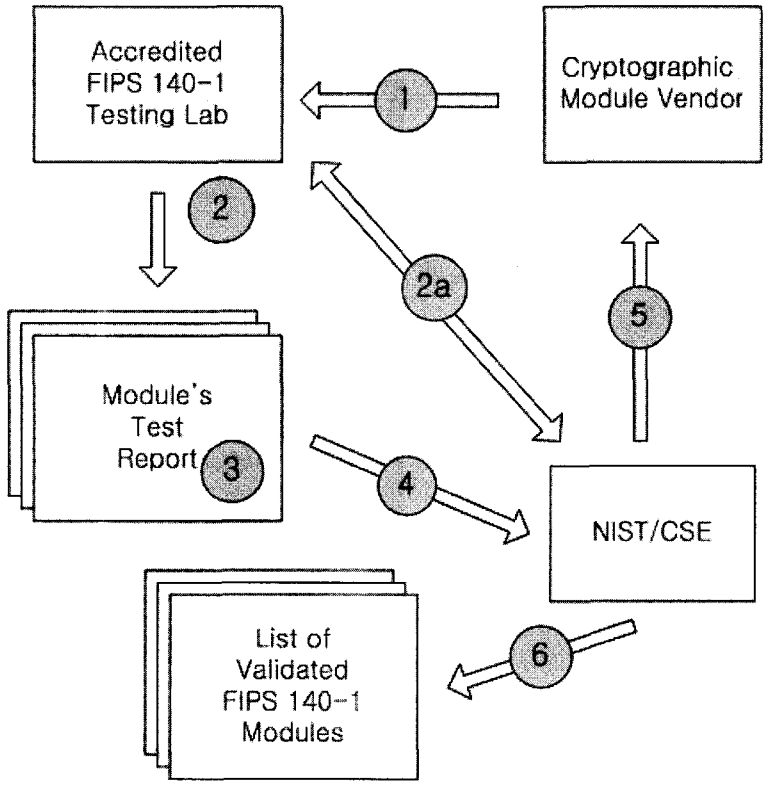
표준암호알고리즘이 결정된 후, 민간 기관에 의한 적합성 평가는 ISO 인정기관인 NIST가 2002년 6개의 민간 평가 기관을 인증기관으로 선정하되 NIST의 HANDBOOK 150 시리즈에 의한 기관 평가, 시험 평가, 인증 평가를 시행하고 있으며, 현재 7개 기관이 NVLAP에 등록되어 CMVP테스트를 진행중에 있다.

- Altan Laboratories
- CEAL : a CrynaCom Solutions Laboratory
- COACT Inc. CAFE Laboratory
- DOMUS IT Security Laboratory
- EWA Canada LTD, IT Security Evaluation Facility
- InfoGard Laboratories, Inc
- Logica IT Security Laboratory

7. 평가 절차

CMVP에서 진행하는 평가 절차는 〈그림 6〉과 같다.

① NIST로부터 제품 인증을 받고자 하는 업체는 업체가 임의로 선정한 CMT Lab.에 신청서를 제출한다. 이때 신청서에는 다음과 같은 정보를 담고있는 화일을 첨부하게 되는데 담겨있는 정보는 다음과 같다.
- 구현물 이름 및 버전



〈그림 6〉 평가절차

- 업체명 및 담당자
- 테스트 대상 제품이 소프트웨어인 경우, 운영체제, 운용환경
- 제품 설명 등

② Lab에 의해 신청 접수가 처리되면 NIST에 보고하게 되며 업체에서 제출한 정보를 기반으로 테스트 대상 제품에 해당하는 필요사항을 작성하여 업체에 보낸다. 테스트에 관한 사항을 NIST/CSE에 보내며 필요사항을 체크한다.

③ Lab에서는 해당제품에 대한 평가를 하며 평가에 관한 리포트를 작성한다.

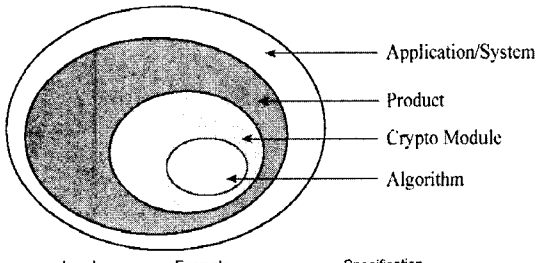
④ Lab은 테스트 결과를 NIST/CSE에 제출한다.

⑤ NIST는 해당 내용의 인증을 실시하며 테스트를 마친 구현물을 "Validation List"에 등재한다.

⑥ NIST/CSE에서는 인증서를 발급하고 해당제품에 대해 평가를 마친다.

Ⅲ. 암호 알고리즘 구현 적합성 평가

CMVP에서 암호 모듈 안정성 평가는 암호 기술의 구현 적합성 평가, 암호키 운용 및 관리, 물리적 보안 등 크게 3부분으로 나뉠 수 있다. 그중 가장 기본적이고 중요한 암호 알고리즘에 대한



Level	Example	Specification
Application	Air Traffic Control	?
Product	Firewall	Common Criteria
Security Module	Crypto Module	FIPS 140-2
Algorithm	AES	FIPS 197

〈그림 7〉 정보 보호제품과 평가 체계의 관계

〈표 1〉 NIST FIPS 승인 알고리즘

구 분	표준 번호	제 목
대칭키	FIPS PUB 46-3	Triple-DES
	FIPS PUB 185	SkipJack
	FIPS PUB 197	AES
	FIPS PUB 81	DES Mode of operation
공개키	FIPS PUB 186-2	DSS
	ANSI X9.31	rDSA
	ANSI X9.62	ECDSA
해쉬함수	FIPS PUB 180-1	Secure Hash Standard
MAC	ANSI X9.19	Enhanced Security DES MAC
	FIPS PUB 113	DES MAC and Triple-DES MAC
keyed Hash	FIPS 198	The keyed-HASH MAC
RNG	FIPS PUB 186-2	DSS Appendix 3.1-2
	ANSI X9.31	rDSA Appendix A
	ANSI X9.62	ECDSA A.4

구현 적합성 평가는 구현된 암호 기술이 표준에 따라 제대로 구현되었는지를 평가하며, 이는 각 표준에 따라 평가하는 방법이 다르다.

다음의 〈그림 7〉에서 같이 CMVP 내에서 수행하는 평가의 범위는 정보 보호 제품에서 가장 근간이 되는 암호 알고리즘을 기반으로한 암호 모듈의 평가에 있다고 할 수 있다.

위의 〈표 1〉은 FIPS 승인 알고리즘을 표로 간략히 나타낸 것이다. CMVP는 FIPS 승인 표준 알고리즘을 기반으로 블록암호 알고리즘, 공개키 암호 알고리즘, 메시지 인증 코드, 난수 생성, 키 관리 등에 대한 구현 적합성 검증방식을 표준하시키고 이에 대한 구현 적합성 검증을 수행하고 있다.

미국의 NIST에서는 미연방 정부의 관용 알고리즘 표준인 DES(Data Encryption Stand-

ard, FIPS 46-3), 전자서명 알고리즘 표준인 DSS(Digital Signature Standard, FIPS 186), 해쉬 알고리즘 표준인 SHS(Secure Hash Standard, FIPS 180-1), 그리고 Skipjack, 3-DES 등의 암호 알고리즘의 구현물이 표준을 준수하고 있는지 여부를 테스트하고 있다. 이 테스트는 NIST의 암호모듈 검증 프로그램(CMVP)의 일환으로 진행되고 있으며, CMT(Cryptographic Modules Testing) 연구소에서 주관하고 있다.

이 가운데, DES와 Skipjack에 대한 검증은 "NIST Special Publication 800-17 Modes of Operation Validation System(MOVS) : Requirements and Procedures"[5]에 기반해서 이루어지고 있으며, 3-DES에 대한 검증은 "NIST Special Publication 800-20 Mode of Operation Validation System for the Triple Data Encryption Algorithm(TMOVS) : Requirements and Procedures"[6]에 기반해서 이루어지고 있다. 또한 전자서명 및 해쉬 알고리즘에 대한 검증은 CMT 연구소에서 개발한 전자서명 표준 검증 시스템(DSSVS : Digital Signature Standard Validation System)[7]을 통해 이루어지고 있다.

〈표 2〉 해당 알고리즘 구현 적합성 검증 기반 방식

알고리즘	검 증 기 반	비 고
DES	NIST Special Publication 800-17, Modes of Operation Validation System (MOVS):	
Skipjack		
3-DES	NIST Special Publication 800-20 Mode of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)	
AES	The Advaned Encryption Standard Algoritm Validation Suite (AESAVS)	
SHS (SHA-1 Algorithm)	Digital Signature Standard Validation System (DSSVS)	해쉬 알고리즘 표준
DSS		전자서명 표준

다음의 〈표 2〉는 해당 알고리즘의 구현 적합성을 평가하는 검증 기반을 표로 나타낸것이다. 기존의 암호 알고리즘에 대한 검증 방식에 비해서 CMVP 내에서 수행하는 검증 방식은 테스트 벡터는 논리적 근거에 의해서 생성되고 테스트 벡터의 종류도 다양하다. 또한 검증 대상도 알고리즘의 요소함수에 근거하고 검증 실패시 실패 원인에 대한 분석이 용이하다는 장점이 있다.

1. MOVS

MOVS(Modes of Operation Validation System)는 DES와 SkipJack 암호 알고리즘의 구현 적합성을 검증하는 방식으로서 NIST SP 800-17로 표준화가 되었다. MOVS는 업체가 평가받기 원하는 구현물(IUT : Implementations Under Test)로부터 얻어진 데이터를 통해 자동으로 테스트를 수행하도록 설계되었다. MOVS의 검증 방식에 사용되는 테스팅 방식은 크게 Known Answer Test와 Modes Test 2가지로 볼 수 있다.

가. the Known Answer tests

KAT는 크게 3가지 타입으로 구분할 수 있다. 키의 값은 일정하게 두고 평문을 일정한 값으로 변화시키면서 테스팅하는 VP(Variable Plaintext) KAT, 평문 값은 일정하게 두고 키값을 일정한 값으로 변화시키면서 테스팅하는 VK (Variable Key) KAT, 그리고 마지막으로 해당 알고리즘의 요소별(AES의 GFSbox · KeySbox, DES[1]의 IP · IP^{-1} 등) 테스팅으로 구분한다.

KAT 검증 방식은 블록 암호 알고리즘의 4가지 운영모드(ECB, CBC, CFB, OFB)에 따라 암 · 복호화 테스팅을 수행한다.

MOVS: Initialize KEY: If DES, KEY=0101010101010101 (odd parity set)
If Skipjack, KEY=00000000000000000000
PT_1 = 8000000000000000
Send KEY, PT_1

IUT: FOR i = 1 to 64
{
$IB_i = PT_i$
Perform algorithm in encrypt state, resulting in CT_i
Send i, KEY, PT_i, CT_i
PT_{i+1} = basis vector where single "1" bit is in position i+1
}

MOVS: Compare results from each loop with known answers
If DES, use Appendix B, Table 1. If Skipjack, use Appendix B, Table 5.

〈그림 8〉 ECB 모드상에서 VP KAT

위의 〈그림 8〉은 DES 암호 알고리즘의 검증 방식인 MOVS에서 ECB 모드상에서 VP KAT 테스팅 알고리즘을 간략하게 의사 코드로 표현한 그림이다. 초기값으로 DES의 키값은 010101…, 즉 8의 배수번째 비트만 1의 값으로 초기화 시켰다는 것을 알수 있다. 이 키값을 토대로 평문을 일정하게 변화시켜 라운드당 출력되는 암호문인 CT를 검증방식에 준한 테이블값과 비교해서 해당 암호 알고리즘의 구현 적합성을 평가한다. 위 테스팅 방식에서 DES는 64개의 암호문 CT를 생성한다.

키의 길이 N비트에 비례해 암호문 CT는 N개 생성된다는 것을 알 수 있다.

나. The Modes tests

MCT는 KAT처럼 정형화된 키값이나 평문을 통한 테스팅이 아닌 키값, 평문, 초기 벡터값을 임의의 값으로 한다는데 차이가 있다. 또한 KAT는 테스팅 과정중에 암복호화가 수십내지 수백번 정도 일어나지만, MCT는 라운드당 수천에서 수만번의 암복호화 과정이 일어나므로 최종적으로는 수십만 내지 수백만번의 암복호화 과정을 통해서 테스팅을 수행한다는데 있다.

다음의 〈그림 9〉는 AES 암호 알고리즘 검증 방식인 AESAVS에서 ECB 모드 Encryption MCT 테스팅을 수행하는 알고리즘을 나타낸 그림이다. AES 알고리즘도 DES의 MOVS의 모드 테스트처럼 반복되는 횟수만 다를뿐 같은 방식으로 테스팅을 수행한다. 이는 Monte-Carlo test 수행 방식에 근간을 두기 때문에 DES의 MOVS와 AES의 구현 적합성을 검증하는 AESAVS의 검증 방식이 비슷한 면이 있다. 여기서 Key[0], PT[0]는 초기 값으로서 임의의 값이 입력되고 초기 평문인 PT[0]가 암호화되서 CT가 생성된다. 이 CT[0]가 다음에 평문값인 PT[1]으로 입력으로 들어가고 그에 해당하는 암호화된 값인 CT[1]이 생성된다. 이 과정이 CT[999]가 될 때까지 반복된다. 최종적으로 CT[999]가 해당 라운드의 암호문으로 생성되고 CT

```
Key[0] = Key
PT[0] = PT
For i = 0 to 99
  Output Key[i]
  Output PT[0]
For j = 0 to 999
  CT[j] = AES(Key[i], PT[j])
  PT[j+1] = CT[j]
  Output CT[j]
If ( keylen = 128 )
  Key[i+1] = Key[i] xor CT[j]
If ( keylen = 192 )
  Key[i+1] = Key[i] xor (last 64-bits of
  CT[j-1] || CT[j])
If ( keylen = 256 )
  Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
PT[0] = CT[j]
```

〈그림 9〉 ECB 모드상에서 AES MCT 테스팅

[999]가 다음 라운드의 평문으로 입력이 된다는 것을 알 수 있다.

이러한 Modes test의 또 다른 목적은, 구현상 혹은 구현물의 작동 중 에러로 인해 키나 평문이 노출되는 예상치 못한 현상이 IUT상에서 일어나는가를 확인해 보는 것이다.

MOVS는 IUT에 키, 평문(혹은 암호문)에 대한 초기 값(initial input)을 제공하며, Modes test가 수행될 때 암호문(혹은 평문) 결과값들은 모두 저장되며 미리 알고 있는 값과 비교하게 된다. 만약 에러가 발견되면 해당 결과를 저장하고 테스트는 비정상적으로 끝나게 되며, 이러한 상황이 벌어지지 않으면 테스트는 계속된다. 만약 IUT의 결과값들이 알고 있는 값과 모두 일치한다면 Modes test는 성공적으로 끝나게 된다.

2. TMOVS

(Modes of Operation Validation System for the Triple Data Encryption Algorithm)

TMOVS는 Triple DES algorithm(TDEA)이 ANSI X9.52, "Triple Data Encryption Algorithm Modes of Operation"과 일치하는지에 대한 Implementations Under Test(IUT)를 확인하기에 필요한 테스트를 나타낸다. TDEA를 IUT에 적용할 때, 이 문서(TMOVS)는 알고리즘 구현이 올바른지를 결정하는 테스트를 제공한다.

TMOVS는 Known Answer Test와 Monte Carlo Test의 두 가지 종류의 확인 테스트로 구성되어 있다. Known Answer Test는 IUT에서 DES 알고리즘의 구성요소들을 확인하기 위해 설계되었다. 이 테스트는 알고리즘의 모든 구성요소들의 각각의 비트를 시험한다. Known Answer Test를 시행하기 위해서, TMOVS는 알려진 값들을 제공한다. 그래서, IUT 결과로 나온 값과 기대값을 비교하도록 한다. Monte Carlo Test는 TDEA의 전체적인 구현을 시험하기 위해 설계되었다. Monte Carlo Test의 목적은 Known Answer Test의 입력을 조정함으로 찾아낼 수 없는 IUT의 단점을 발견하기 위함이다. 그러나, Monte Carlo Test는 TDEA를 구현하는 IUT의 근본적인 신뢰를 보장하지는 못한다. Monte Carlo Test를 시행하기 위해서, TMOVS는 초기평문, 키, (필요하다면) 초기벡터의 수도랜덤 값의 IUT를 제공한다. 이 값들을 이용하여서, IUT는 4백만 번의 DES 암/복호화 과정을 테스트하고, 그 결과 값을 기대값과 비교한다.

가. The Known Answer Tests

① The Variable Plaintext Known Answer Test : 이 테스트는 64개의 기본 벡터를 입력으로 사용하여서 테스트를 64번 반복한다. IUT로부터 얻어진 결과값이 정확하다면, 이는 IP와 E를 검증한다. 복호화 연산을 이용하면, IP-1도 검증할 수 있다.

② The Inverse Permutaion Known Answer Test : 이 테스트는 "The variable Plaintext Known Answer Test"와 동일한 연산과정을 거친다. 그러나, 위의 테스트와의 차이는 "The variable Plaintext Known Answer Test"에서 얻어진 암호문을 평문으로 사용하는 것이다. 키는 모두 0으로 초기화된다. 이 키는 "Self-dual Key"이다. IUT로부터 얻어진 결과 값이 정확하다면, 이는 IP-1를 검증한다. 복호화 연산을 이용하면, IP를 검증할 수 있다.

③ The Variable Key Known Answer Test

초기화 과정에서, 평문과 초기 벡터는 모두 0으로 초기화된다. 3개의 키는 모두 56비트의 기본 벡터로 초기화된다. 이 키를 사용하여서, 테스트를 56번 반복한다.

IUT로 얻어진 결과값이 정확하다면, 이는 키 스케줄의 PC1과 PC2를 검증한다.

④ The Permutation Operation Known Answer Test : 초기화 과정에서, 평문과 초기 벡터는 모두 0으로 초기화된다. 반면에, 키는 TMOVS에서 제공하는 32개의 키 중 하나로 3개의 키 값이 동일하게 초기

화된다. 32번의 테스트는 순열 P를 검증하는데 사용된다.

⑤ The Substitution Table Known Answer Test : 초기화 과정에서, 평문과 초기벡터는 모두 0으로 초기화된다. 반면에, 키는 TMOVS에서 제공하는 19개의 키 중 하나로 키 값이 초기화된다. 19번의 테스트는 8개의 S-box를 검증하는데 사용된다.

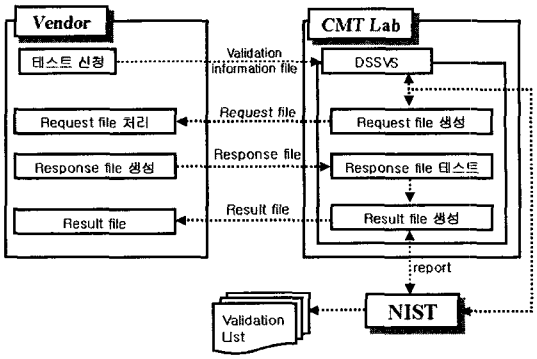
나. Monte Carlo Test

Monte Carlo Test는 TDEA의 전체적인 구현을 시험하기 위해 설계되었다. Monte Carlo Test의 목적은 Known Answer Test의 입력을 조정함으로 찾아낼 수 없는 IUT의 단점을 발견하기 위함이다. 그러나, Monte Carlo Test는 TDEA를 구현하는 IUT의 근본적인 신뢰를 보장하지는 못한다. Monte Carlo Test를 시행하기 위해서, TMOVS는 초기평문, 키, (필요하다면) 초기벡터의 수도랜덤 값의 IUT를 제공한다. 이 값들을 이용하여서, IUT는 4백만 번의 DES 암/복호화 과정을 테스트하고, 그 결과 값을 기대값과 비교한다.

각각의 Monte Carlo Test는 4백만번 IUT를 시행한다. 이 테스트는 1만번의 반복으로 구성된 4백개의 그룹으로 나뉘어진다. 각 그룹은 IUT를 거쳐 결과를 나타내고, 이는 TMOVS의 결과와 비교하게 된다.

3. DSSVS

DSSVS(Digital Signature Standard Validation System)는 DSS와 SHA-1을 구현한 하드웨어 및 소프트웨어에 대한 원격 테스트를 수행할 수 있도록 설계되었으며, 제품의 보안 강도를 측정하는 것이 아닌 표준의 준수 여부를 검증하는 프로그램이다. 즉, 이 프로그램은 DSS와 SHA-1을 구현하는 과정에서 발생할 수 있는 오류를 발견하도록 도와주는 역할을 한다고 할 수 있다. 따라서 NIST의 인증은 제품의 보안 강도에 대한 평가로 해석할 수 없다. 또한 DSSVS의 테스트는 구현물에서 생성한 모든 결과물에 대해서 테스트를 수행하지 않고, 결과물의 일부 sample을 선택해서 테스트하는 통계적인 방법으로 이루어진다. DSSVS에 의한 테스트 절차는 다음과 같다.



〈그림 10〉 DSSVS 테스트 절차

① NIST로부터 제품 인증을 받고자 하는 업체는 업체가 임의로 선정한 CMT Lab.에 신청서를 제출한다. 이때 validation information file(.inf)을 첨부하게 되는데 담겨있는 정보는 다음과 같다.
- 구현물 이름 및 버전
- 업체명 및 담당자
- 테스트 대상 제품이 소프트웨어인 경우, 운영 체제, 운용환경
- 제품 설명

② Lab에 의해 신청 접수가 처리되면 NIST에 보고하게 되며 validation information file을 기반으로 Request file(.req)을 생성하여 업체에 보낸다. 요청 파일에는 테스트를 위한 업체의 구현물 처리정보 생성을 요구하고 있다.

③ 업체는 요구된 파일에 대한 응답으로 Response file(.rsp)을 생성한다.

④ Lab은 응답파일을 테스트하게 되며 이에 대한 결과 파일인 Result file(.out)을 생성한다.

⑤ Lab은 생성된 결과 파일을 기반으로 NIST에 보고한다. NIST는 해당 내용의 인증을 실시하며 테스트를 마친 구현물을

"Validation List"에 등재한다.

⑥ Lab은 해당 평가, 인증결과를 Vendor에게 전달함으로 평가를 마친다.

가. SHS(Secure Hash Standard) tests

SHS 테스트는 다음의 3가지로 구성된다.

(1) 다양한 길이의 메시지(Messages of varying length)에 대한 테스트

- SHS의 구현물은 임의의 길이를 가진 메시지에 대한 정확한 요약(digest)을 할 수 있어야 한다. 이를 확인하기 위해서 DSSVS는 0비트부터 1,024비트의 길이를 가지는 1,025개의 메시지를 임의로 생성하여 테스트 대상에게 전달하고, 각각의 메시지에 대한 메시지 다이제스트를 생성하여 저장한다. 메시지를 전달받은 테스트 대상은 이 메시지 각각에 대해서 메시지 다이제스트를 생성하여 DSSVS에 전달한다. 테스트 대상으로부터 메시지 다이제스트를 전달받은 DSSVS는 자신이 생성하여 저장하고 있는 메시지 다이제스트와 비교하여 모든 메시지 다이제스트가 동일하면 테스트를 통과한 것으로 간주한다.

(2) 선택된 긴 메시지(Selected long message)에 대한 테스트

- SHS 구현물은 1,024비트 이상의 긴 메시지에 대해서 정확한 메시지 다이제스트를 생성할 수 있어야 한다. 테스트 절차는 다양한 길이의 메시지 테스트와 동일하며, 테스트에 사용하는 메시지는 1,024비트 이상의 다양한 길이를 갖는 100개의 메시지이다.

(3) 임의로 생성된 메시지(Pseudorandomly generated messages)에 대한 테스트

- SHS 구현물은 임의로 생성된 메시지에 대해서 정확하게 메시지 다이제스트를 생성할 수 있어야 한다. 테스트 절차는 다양한 길이의 메시지 테스트와 동일하며, 420비트의 길이를 갖는 초기값(seed)으로부터 생성된 100개의 메시지를 테스트에 사용한다.

나. DSS(Digital Signature Standard) tests

DSS 테스트는 다음의 6가지로 구성된다.

- 소수 테스트
- 파라미터 p, q, g 생성 테스트
- 공개키쌍 생성 테스트
- 서명 생성 테스트
- 서명 확인 테스트
- *p*, *q*, *g*의 정확성 확인 테스트

Ⅳ. 다른 평가 제도

1. TCSEC(Trusted Computer Security Evaluation Criteria)

TCSEC은 신뢰성 있고 상업적으로 유용한 자동화된 데이터 처리(Automated Data Processing, ADP) 시스템에 적용하기 위한 것으로 기존 시스템의 평가 및 ADP 시스템 결과물에 대한 보안 요구사항 명세에 이용할 수 있다.

국방부는 안전·신뢰성이 입증된 컴퓨터 시스템을 국방부 및 정부기관에 보급하기 위하여 TCSEC을 C1, C2, B1, B2, B3, A1의 6개 등급으로 분류하여 각 기관별 특성에 맞는 컴퓨터 시스템을 도입·운영하도록 권고하고 있다.

TCSEC은 비밀 처리를 위하여 정보노출을 방지하여야 한다는 보안 요구사항을 갖춘 상용 제품이 지녀야 할 보안 특성의 표준을 제작자에게 제공하기 위한 것이다. 또한 국방부 관련 부서에 중요 정보의 안전한 처리를 위한 컴퓨터 시스템이 가져야 할 신뢰 정도를 평가하는 척도를 제공하고 구매명세서에 보안 요구사항을 명시하는 근간을 제공하고자 개발되었다.

2. ITSEC

ITSEC은 영국, 독일, 프랑스 및 네덜란드 등 자국의 정보보호시스템 평가기준을 제정하여 시행하던 4개국이 평가제품의 상호 인정 및 평가기준이 상이함에 따라 정보보호 제품의 중복 평가에 허비되는 시간, 인력 및 소요 비용을 절감하기

위하여 개발한 공동의 기준이다. 4개국은 1989년 소위 "조화된 기준(Harmonized Criteria)"을 작성하기로 합의하고 1991년에 ITSEC v1.2를 제정하였다.

ITSEC은 TCSEC과는 달리 단일 기준으로 모든 정보보호제품을 평가하고자 하였다. 따라서 보안기능은 개발자가 제품이 사용될 환경을 고려하여 보안기능을 설정하거나 TCSEC 혹은 독일의 ZSIEC에서 미리 정의한 보안기능을 사용토록 하였으며 제품에 대한 평가는 보증부분만으로 수행이 된다.

ITSEC을 적용하고 있는 국가는 영국, 독일, 프랑스, 네덜란드, 이태리, 스웨덴, 호주 등 7개국이다.

3. CC(Common Criteria)

정보를 처리하는 중에 우연 또는 고의적인 방법에 의해 정보가 훼손, 변조, 유출되는 것을 방지하기 위한 기술적 보호 수단의 핵심인 정보보호 시스템의 개발을 위하여 선진 각국은 시스템의 설계, 구현, 생산, 설치, 운영 시스템 생명 주기(life cycle)를 포함한 모든 과정에 대한 기준과 이에 따른 제품의 평가를 체계적으로 시행하여 왔다. 정보 보호 시스템을 효율적으로 개발하고, 평가하고, 사용하기 위해서는 각 사용자, 개발자, 평가자 사이에 서로 공통되는 기준이 필요한데, 이를 정보보호 시스템 평가기준이라고 하며, 1985년 미국의 TCSEC(Trusted Computer Security Evaluation Criteria)를 시작으로 2000년 10월 현재 국제 공통의 평가기준으로 CC 2.1이 ISO 15048 표준으로 발표되어 있다. 미국의 NIST와 NSA, 캐나다의 CSE, 프랑스의 SCSSI, 독일의 BSI, 네덜란드의 NL-NCSA, 영국의 CESG의 6개국이 주관이 되어 1993년부터 개발하여 왔고, 이제는 국제공통표준으로서 인정되어 세계 각국(현재는 13개 MRA 인증국 사이)에서 상호승인제품으로 사용 가능하다.

공통 평가 기준은 크게 1, 2, 3부로 구성된다. 제1부는 공통 평가 기준의 소개 및 일반 적용 모델을 기술하고 있고, 제2부는 정보 보호 시스템의 보안 기능을 명시할 수 있는 보안 기능 요구 사항을, 제3부는 평가시 요구되는 보증 요구 사항을 기술하고 있다.

보안 기능 요구 사항은 총 11개 클래스로 구성되어있다.

1) 보안 감사 클래스(FAU)
2) 통신 클래스(FCO)
3) 암호 지원 클래스(FCS)
4) 사용자 데이터 보호 클래스(FDP)
5) 식별 및 인증 클래스(FIA)
6) 보안 관리 클래스(FMT)
7) 프라이버시 클래스(FPR)
8) TSF 보호 클래스(FPT)
9) 자원 활용 클래스(FRU)
10) TOE 접근 클래스(FTA)
11) 안전한 경로/채널 클래스(FTP)

V. 결 론

본고에서는 현재 북미에서 활발히 진행중에 있는 암호모듈 평가 프로그램인 CMVP에 대해 전반적으로 알아보았다. 암호 모듈의 안전성 평가는 암호 모듈을 기반으로 한 정보 보호제품 평가에 있어서 가장 기본이 되는 평가일뿐만 아니라 검증된 암호 모듈을 채용한 제품들에 대해 어느 정도의 신뢰성을 보장해 준다고 할 수 있다. 그러나 이러한 암호 모듈을 기반으로 한 시스템의 전체적인 안정성 평가는 평가 기반 자체가 없을뿐더러 평가 자체가 어렵다고 할 수 있다.

암호 모듈에 대한 안정성 평가 체계 확립은 사용자의 입장에서는 제품에 대한 신뢰를 가질수 있고, 개발자에게 있어서는 제품 개발에 대한 가이드 라인으로 삼을 수 있을 뿐만 아니라, 제품의 보안 등급에 따라 타사 유사 제품과의 경쟁 우위를 확보할 수 있다.

국내의 경우 미국 CMVP처럼 암호 모듈에 대한 전반적인 평가 체제가 자체가 없을뿐더러 단

지 암호 알고리즘에 대한 안정성 평가만을 수행 중이고 구현물의 평가가 아닌 이론적 평가에 머무른 실정이다.

따라서 국내에서도 미국의 CMVP를 토대로 한국의 실정에 맞는 암호 모듈에 대한 제도적이고 기술적인 평가체계 확립이 필요하리라 본다.

참 고 문 헌

〔1〕 "Security Requirements for Cryptographic Modules", NIST, FIPS 140-2, 2001

〔2〕 "Security Requirements for Cryptographic Modules", NIST, FIPS 140-1, 1994

〔3〕 "Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules", NIST, 2001

〔4〕 "Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program", NIST, 2001

〔5〕 "NIST SP 800-17 : MOVS", NIST, 1998

〔6〕 "NIST SP 800-20 : TMOVS", NIST, 2000

〔7〕 "DSSVS User's Guide", NIST, 2001. 01

〔8〕 박성근외 5명, "CMVP 테스트를 적용한 SEED 암호 알고리즘 모듈 구현", 정보 처리 학회지 춘계 학술 발표 대회 논문집 제10권 제1호 하권, pp.1937-1940, 2003. 05

〔9〕 정성민외 4명, "블록 암호 알고리즘 정확성 테스트 모듈 구현", 한국정보보호학회지, 2002. 11

〔10〕 "암호 제품 평가 체계 분석", 한국정보보호진흥원, 2002

〔11〕 "Cryptographic Module Validation Program Conference", NIST, 2002. 03

〔12〕 "Cryptographic Module Validation Program", NIST, http://csrc.nist.gov/cryptval/

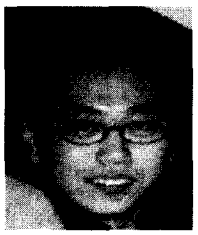
저 자 소 개

김 석 우

1979년 2월 한국항공대학(통신정보 학사학위), 1989년 10월 뉴저지 공대(전산학 석사 학위), 1995년 3월 아주대학교(컴퓨터공학 박사 학위), 1979년 1월~1980년 5월 : (주) 삼성전자 사원, 1987년 1월~1989년 1월 : (주) AT&T Bell Lab 초빙연구원, 1980년 8월~1997년 2월 : 한국전자통신연구원 실장(책임 연구원), 1997년 3월~현재 : 한세대학교 부교수, 〈주관심 분야 : 정보 보호〉

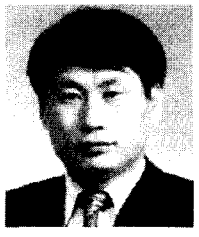
정 성 민

1997년 3월 한세 대학교(정보 보호 전공), 1997년 3월~현재 : 한세 대학교(정보 보호 연구소), 〈주관심 분야 : 정보 보호〉



박 성 근

1997년 3월 한세 대학교(정보 보호 전공), 1997년 3월~현재 : 한세 대학교(정보 보호 연구소), 〈주관심 분야 : 정보 보호〉



김 일 준

1983년 2월 동국대학교(전자공학 학사), 1998년 2월 요코하마 대학(전자공학 박사), 1984년 3월~2003년 현재 : 국가보안기술연구소, 〈주관심 분야 : 정보 보호〉