암호화 모듈 평가 프로그램(CMVP) 표준인 Derived Test Requirement(DTR) of FIPS 140-2 분석

이병석*, 정성민*, 박성근*, 김석우*, 박일환**

*한세대학교 정보통신학과, **국가보안기술 연구소

Analysis FIPS 140-2 DTR(Derived Test Requirement of FIPS 140-2) of CMVP(Cryptographic Module Validation Program)

Byung-Seok Lee*, Sung-Min Jung*, Sung-Keun Park*, Seok-Woo Kim*, Il-Hwan Park**

*Department of Information and Communication Hansei Univ. , **National Security Research Institute

요 약

정보통신기술의 발달로 대부분 사회의 기반구조가 사이버 사회로 전환되었고 다양한 형태의 경제사회 활동을 수행키 위해 정보보호제품의 활용이 극대화되었으며 더욱 중요시되었다. 이러한 사회흐름에 기반하여 정보보호제품의 안전한 선택 및 사용을 위한 기본적 선택기준은 검증받은 암호화 모듈을 바탕으로 하는 정보보호제품에 대한 신뢰 기관의 안전성 평가 결과일 것이다. 암호화 모듈에 대한 안전성 평가로 가장 널리 참조되는 것은 미국의 NIST(National Institute of Standards and Technology)가 수행하는 CMVP(Cryptographic Module Validation Program)이며, 세계적으로 인정받고 있다. 본 논문에서는 암호 모듈의 평가체계에 대해 설명하였으며 그 기준인 FIPS 140-2 DTR을 분석하여 향후 개발 가능한 CMVP의 안전성 평가 툴 기준에 대해 제시하였다.

I. 서론

정보통신분야의 발전으로 인해 익명성의 사이버 사회가 도달하였고 해킹과 같은 역기능이 많이 발생함에 따라 이를 방지하기 위한 정보보호 제품 및 서비스에 대해 그 수요가 급증하고 있다. 하지만 정보보호 제품에 대한 그 평가의 기준이 제대로 정립되어 있지 않아 수요자로 하여금 제품 선택 시의 혼란, 제품 상호간의 운용 및 호환성 확보에 많은 어려움을 갖게 된다. 이 때문에 정보보호 제품에 대한 표준 지원여부가 객관성을 유지하고 공정하게 검증할 수 있는 표준 적합 시험이나 상호 운용성 시험 평가가 필수적으로 요구되는 것이다. 이에 국외에서는 CC, CMVP등 정보보호 제품 및 암호화 알고리즘, 암호화 모듈에 대한 평가가 활발히 진행중에 있는 반면에 국내 정보보호제품 평가 체계는 정보화 촉진 기본법에 의거하여 '침입차단시스템'과 '침입탐지시스템'에 대하여 한국정보보호진흥원에서 실시하고 있고, 각 제품에 대한 평가 등급은 K1~K7까지의 등급 체계로 운영되며 비밀성 기능을 제공하는 경우 각 평가등급에 'E'를 붙여 등급을 표기하고 있으나, 암호모듈 평가 프로그램인 CMVP(Cryptographic Module Validation Program)는 국내에 정착되지 않은 상태이다.

CMVP에서는 평가기준인 FIPS 140-2와 평가자, 벤더에게 필요한 평가 요구사항인 FIPS 140-2 DTR(Derived Test Requirements) 표준 문서가 있는데 본 논문에서는 정보보호 제품에 탑재된 암호모듈의 안전성 평가체계인 CMVP에 대해 소개하며 FIPS 140-2 DTR을 분석하였다.

II. CMVP

1. CMVP 역사

북미에서 현재 활발히 진행하고 있는 정보보호 암호모듈 평가 체계인 CMVP(Cryptographic Module Validation Programm)는 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 만들어 졌다. 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 350개 이상의 평가된 암호모듈을 보유하여, 평가제품 목록을 통하여 실수요자인 정부기관에게 판매되고 있다. 암호모듈의 평가제도 역시 7개의 민간 평가기관(Altan Lab., CEAL, EWA, Cnada LTD, InfoGard Lab., Logica IT Security Lab., COACT Inc., DOMUS)을 지정하여, 실제 평가토록 하고 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.

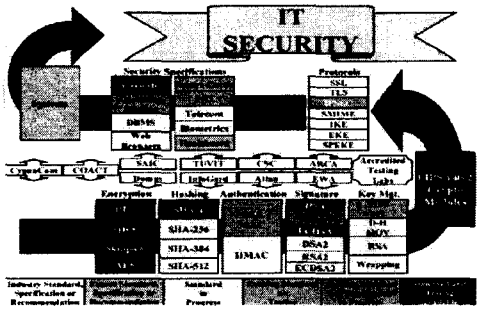

그림 1 : IT 보안과 평가

<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 암호기술이 표준에 따라 제대로 구현이 되었는가를 평가하며, 이는 각 표준에 따라 평가하는 방법이 다름을 의미한다.

둘째로 암호키 운용 및 관리 평가이다. 이 평가는 암호기술의 안전성에 직접적인 영향을 미치는 암호키의 생성, 확립, 분배, 입/출력, 저장, 파기 등에 대한 방법 및 과정을 평가함으로서 잘못된 암호키 운용 및 관리에 따른 암호키의 유출 가능성을 평가하는 것이며, 암호모듈의 안전성 평가 항목 중 가장 중요한 부분이다.

셋째로 물리적 보안 평가이다. 이 평가는 암호모듈의 사용환경에 대한 평가로 암호모듈의 운영환경, EMI/EMC (electromagnetic interference / electromagnetic compatibility), Self-Testing등에 대한 평가를 의미한다.

위와 같이 안전성 평가에 따라 최종적으로 보안등급을 받은 승인된 제품은 정부기관에서 사용 가능한 제품군으로 등록된다. 승인된 제품은 아래 그림2 에서 보듯이 하드웨어/소프트웨어/펌웨어 방식의 구현, 칩/Smartcard/USB 단말 제품에서부터 VPN, CA 등의 시스템 레벨까지 포함한다.

2003년 현재 CMVP내 등록리스트[5]에서 약 350개 정도의 H/W, S/W등 다양한 암호 모듈 기반의 제품들이 안전성 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, Level에 따른 요구사항을 간단하게 살펴보면 다음과 같다.

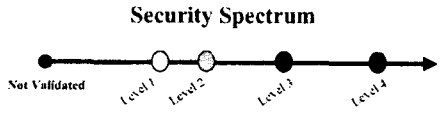

그림 2 : 보안등급

보안등급1 - 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 운영체제에서 사용되는 보통의 컴퓨팅 시스템 상의 암호 모듈 소프트웨어 부분의 보안 수준을 의미한다.

보안등급2 - 레벨 2는 레벨 1에 물리적 보안 매커니즘 부분을 보완시킨 등급으로 tamper-evidence에 대한 안전성 요구사항을 다룬다. 레벨 2는 CC(Common Criteria) Protection Profile (PPs)과 CC 평가 등급 EAL2 이상에서 요구하는 운영체제에서 운용되는 암호기술적 모듈의 소프트웨어 안전성 수준을 의미한다.

보안등급3 - 레벨 3는 레벨 2에 tamper-evident가 포함된 물리적 보안 매커니즘을 보완시킨 등급이다. 따라서 Level 3 등급에서는 암호기술적 모듈 안에 보관 되어있는 CSPs(Critical Security Parameter)에 대한 침입자의 접근을 막고자 하는 시도를 포함하며 신원기반 인증 매커니즘이 필요하다. CC 평가 등급 EAL3 이상에서 요구하는 운영체제에서 운용되는 암호 모듈의 소프트웨어 안전성 수준을 의미한다.

보안등급 4 - 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. 레벨 4는 레벨 3에서의 요구조건과 함께 CC 평가 등급 EAL4 이상에서 요구하는 운영체제에서 운용되는 암호 모듈의 소프트웨어 안전성 수준을 의미한다.

4. FIPS 140-1 & 140-2

FIPS 140-1은 1994년 1월, 사용자와 개발자로 구성된 정부와 산업계의 Working group에 의해 개발되어 지고 표준안으로 제정되었다. 2001년 개정된 FIPS 140- 2는 암호알고리즘 관련 FIPS 표준문서를 근간으로 만들어 졌다. Working group은 데이터 민감성의 넓은 분포와 적용 환경의 다양성 등을 규정하기 위한 암호 모듈의 4가지 보안 등급을 설정하고 이에 따른 요구 조건들을 제시하였다. 또한 4가지 보안 등급은 각각 11가지 상세한 요구조건에 따라 분류되며, Level 1부터 Level 4 까지 증가되는 보안 등급은 이와 함께 안전성 요구조건도 증가됨을 의미한다. FIPS 140-2 는 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.

III. FIPS 140-2 DTR

1. 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 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.

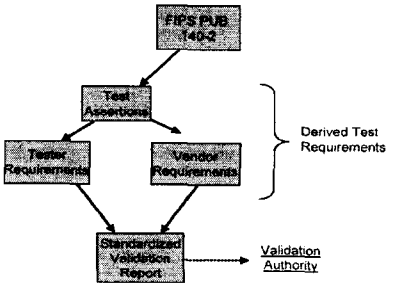

그림 3 : DTR 발전단계

문서는 FIPS 140-2에서 안전성 요구조건을 위해 구분한 다음과 같은 11개 section(암호 모듈 규격, 암호 모듈 포트와 인터페이스, 역할·서비스·인증, 동작모델, 물리적 보안, 운영환경, 암호키관리, EMI/EMC, 자가 테스트, 설계보증, 공격에 대한 완화)에 해당하는 내용을 담고 있다.

각각의 Section은 해당되는 안전성 요구조건들에 대한 평가항목들로 이루어져 있으며, 모든 평가항목들은 FIPS PUB 140-2로부터 직접적으로 인용된다.

평가항목들은 다음과 같은 형식으로 표시된다.

AS<Requirement_number>.<Assertion_Sequence_number>

"Requirement_number"는 FIPS 140-2 문서에 표시되어 있는 section을 뜻하며(따라서 "Requirement_number" 는 01부터 11까지의 숫자), "Sequence_number"는 각각의 Section에서 보고되는 평가항목의 순서를 뜻하는 숫자를 의미한다. 각각의 평가항목 뒤에는 해당되는 안전성 수준을 괄호로 묶어 표기한다.

이어지는 평가항목은 개발자에게 부과되는 요구조건에 관한 집합이다. 이들 요구조건들은 문서의 형식 또는 개발자가 주장하는 평가항목 내용을 확인시키기 위해 평가자에게 제공하는 명확한 정보 등을 설명하고 있다. 이들 요구조건들은 다음과 같은 형식으로 표기된다.

VE<Requirement_number>.<Assertion_sequence_number>.<Sequence_number>

"Requirement_number"와 "Assertion_Sequence_number"는 위의 평가항목과 같은 내용을 가지고 있으며, 마지막 "Sequence_number"는 개발자 요구조건에 관련된 내용들의 순서를 뜻한다.

또한 개발자에게 부과되는 각각의 평가항목과 요구조건들은 또한 암호 모듈 평가자 에게도 부과된다. 이들 요구조건들은 주어진 평가항목에 충실하게 암호 모듈을 검사하기 위해 해야 할 것들을 평가자에게 알려주고 있다. 이들 요구조건들은 다음과 같은 형태로 표기된다.

TE<Requirement_number>.<Assertion_Sequence_number>.<Sequence_number>

위의 표기된 형태는 개발자를 위한 평가항목 형태와 동일한 구조를 가지고 있다.

한 항목에 대해 예로 들겠다.

AS01.03(Level 1,2,3,4) 운용자(Operator)ms 승인된 동작 모드중 원하는 모드를 결정할 수 있다.

VE01.03.01 소유권이 없는 보안 정책을 제공하는 개발자는 승인된 동작 모드의 설명을 제공한다.

TE01.03.01 평가자는 소유권이 없는 보안 정책을 제공하는 개발자가 승인된 동작모드의 설명을 제공하는지를 확인한다.

2. 평가 절차

CMVP에서 진행하는 평가 절차는 아래 그림 6과 같다.

① NIST로부터 제품 인증을 받고자 하는 업체는 업체가 임의로 선정한 CMT Lab.에 신청서를 제출한다. 이때 신청서에는 다음과 같은 정보를 담고있는 파일을 첨부하게 되는데 담겨있는 정보는 다음과 같다.

- 구현물 이름 및 버전
- 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.

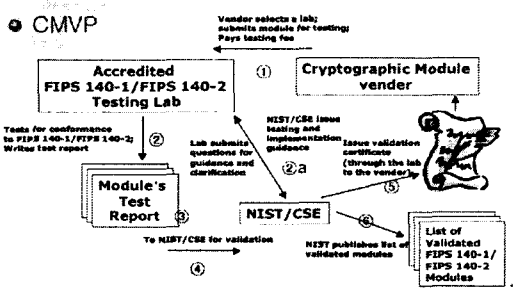

그림 4 : 평가절차

3. DTR 항목별 설명 및 레벨별 요구사항

다음은 FIPS 140-2 DTR 문서를 각 AS항목에 맞추어 레벨별로 구분해 놓은 것이다.

1) 암호모듈 규격

- 암호 알고리즘, 암호적용범위, 동작모드, 제품설명, HW/SW/FW등 구성요소, 보안정책 등

표 1 : 암호모듈 규격의 레벨별 항목

레 벨	항 목
1,2,3,4	AS01.01, 02, 03, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16
3,4	AS01.04

2) 암호모듈 포트와 인터페이스

- 보안 포트와 비 보안포트, 포트에 입력되는 보안 파라미터

표 2 : 암호모듈 포트와 인터페이스 레벨별 항목

레 벨	항 목
1,2,3,4	AS02.01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15
3,4	AS02.16, 17, 18

3) 역할, 서비스, 인증

- 제품의 사용자들의 역할과 해당 서비스, ID/역할 기반 인증

표 3 : 역할, 서비스, 인증 레벨별 항목

레 벨	항 목
1,2,3,4	AS03.01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 21, 23, 29
1	AS03.30
2,3,4	AS03.16, 22, 24, 25, 26, 27
2	AS03.17, 18, 31
3,4	AS03.19, 20, 32

4) 동작모델(Finite State Model)

- 제품의 모든 동작 상태(state), 해당 전이상태(state transform)

표 4 : 동작모델 레벨별 항목

레 벨	항 목
1,2,3,4	AS04.01, 02, 03, 04, 05

5) 물리적 보안

- 물리적 접근에 대한 레벨별 요구사항

표 5 : 물리적 보안의 레벨별 항목

레 벨	항 목
1,2,3,4	AS05.01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 12, 13, 14, 33, 34, 46, 47
1	AS05.11
2,3,4	AS05.15, 16, 24, 25, 26, 35, 36, 37, 48, 49, 50
3,4	AS05.17, 18, 19, 20, 21, 27, 28, 29, 38, 39, 51, 52, 53
4	AS05.22, 23, 30, 31, 32, 40, 41, 42, 43, 44, 45, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69

6) 운영환경

- 독립된 운영환경, CC 평가 EAL 4 레벨 단위별 운영환경

표 6 : 운영환경 레벨별 항목

레 벨	항 목
1,2,3,4	AS06.01, 02, 03, 07, 08
1	AS06.04, 05, 06
2,3,4	AS06.11, 12, 13, 14, 15, 16, 17, 18, 19
2	AS06.09, 10
3,4	AS06.20, 21, 22, 23, 24, 25
4	AS06.26, 27

7) 암호키 관리

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

표 7 : 암호키 관리 레벨별 항목

레 벨	항 목
1,2,3,4	AS07.01, 02, 03, 04, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 37, 38, 39, 40, 41, 42
3,4	AS07.30, 31, 32, 33, 34, 35, 36

8)EMI/EMC

- FCC Part 15의 Class A, B에 대한 규격

표 8 : EMI/EMC 레벨별 항목

레 벨	항 목
1,2,3,4	AS08.01, 02, 03
1,2	AS08.04
3,4	AS08.05

9) 자가 테스트

- Power-up 테스트, 조건 테스트

표 9 : 자가테스트 레벨별 항목

레 벨	항 목
1,2,3,4	AS09.01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48

10) 설계 보증

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

표 10 : 설계보증 레벨별 항목

레 벨	항 목
1,2,3,4	AS10.01, 02, 03, 05, 06, 07, 08, 21, 22, 23, 24, 25
2,3,4	AS10.04, 09, 10
3,4	AS10.11, 12, 13
4	AS10.14, 15, 16, 17, 18, 19, 20

11) 공격에 대한 완화

- 공격에 대한 파워 분석, 타이밍 분석, 결함 제시

표 11 : 공격에 대한 완화 레벨별 항목

레 벨	항 목
1,2,3,4	AS11.01

IV. 결론

안전성과 신뢰성이 요구되는 사이버 사회에서 다양한 형태의 경제활동을 수행하기 위해서는 정보보호제품의 활용은 보편화 될 것이 분명하며 그 중요성은 더욱이 커져 갈 것이다. 본고에서 설명한 것과 같이 국외의 선진국들은 암호화 모듈에 대해 안정성 평가가 활발히 이루어지고 있어 정보보호제품에 대한 신뢰성과 개발자들에게는 제품 개발에 대한 가이드 라인을 제공하는 수준에까지 있다. 그러나 국내에서는 정보통신관련 일부 제품에 대한 시험평가가 진행되고 있으나 암호화 모듈에 대한 안정성 평가 국외의 CMVP처럼 전반적인 평가 체계가 없고 단지 암호화 알고리즘에 대한 안전성 평가만을 수행중이다. 게다가 국외 선진국들은 정보보호제품의 평가 기술에 대해 공개를 꺼리고 있기 때문에 국내의 독자적 기술 개발이 요구되어 진다. 따라서 본고에서 설명한 것과 같이 미국의 CMVP를 토대로 한국의 실정에 맞는 암호모듈에 대해 제도적이고 체계적인 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] "Cryptographic Modules Validation Program", NIST, http://csrc.nist.gov/cryptval/

[6] "암호 제품 평가 체계 분석", 한국정보보호진흥원, 2002