TTA Technical Report

기술보고서

TTAR-xx.xxxx 제정일: 2018년 12월 xx일

암호모듈 시험기술표준 사용지침(기술보고서)

Guideline for Using the Testing Standards of the Cryptographic Modules (Technical Report)

TTA 한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회	응용보안 및 평가인증 프로젝트그룹(PG504)				
기술보고서안 심의 위원회	정보보호 기술위원회(TC5)				
	성명	소 속	직위	위원회 및 직위	기술보고서번호
기술보고서(과제) 제안	최희봉	ETRI 부설연구소	책임	WG5041 의장	
기술보고서 초안 작성자	최희봉	ETRI 부설연구소	책임	WG5041 의장	
	양광직	ETRI 부설연구소	선임	WG5041 의원	
	염용진	국민대학교	교수	WG5041 부의장	
	김예원	국민대학교	연구원		
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임		

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 기술보고서의 목적

이 기술보고서의 목적은 암호모듈 시험기술 관련 KS, TTA, ISO/IEC 표준들의 목적, 개발배경, 사용분야, 사용방법, 사용시 참고사항, 표준들 사이의 연계성 등 사용지침을 제시한다. 또한 검증기관에 암호모듈 검증을 신청하는 경우 필수적으로 적용되어야 할 표준들을 설명한다. 이 기술보고서는 (1) 국내·외 암호모듈 검증기관에 시험평가를 신청하기 위해 관련 표준들을 준용하는 암호모듈을 개발하는 경우, (2) 암호모듈 시험평가시 암호모듈 시험기술 관련 표준들을 사용하고자 할 경우 혹은 (3) 암호모듈 사용기관이 암호모듈 도입시 유용하게 사용될 수 있다.

2 주요 내용 요약

이 기술보고서는 KS 암호모듈 보안요구사항, KS 암호모듈 시험요구사항, TTA 잡음원 수집방법 및 응용지침, TTA 암호모듈 인정절차, ISO/IEC 암호모듈 보안요구사항, ISO/IEC 암호모듈 시험요구사항, ISO/IEC 암호모듈에 대한 비침투 공격 대응기술 시험방법, ISO/IEC 암호알고리즘 구현 적합성 시험, ISO/IEC 난수발생기 시험방법, ISO/IEC 물리적 보안 공격 대응기술 및 보안요구사항, ISO/IEC 암호모듈 시험자 자격기준, ISO/IEC 암호모듈 현장시험 가이드 등 제정되었거나 개발되고 있는 많은 암호모듈 시험기술 표준들을 설명하고 사용지침을 제시한다. 한국 암호모듈 검증제도(KCMVP)에서 준용하고 하고 있는 검증기준 및 시험기준인 KS 암호모듈 보안요구사항 및 KS 암호모듈 시험요구사항이 있으며 KCMVP 수행시 참조할 수 있는 ISO/IEC 암호모듈에 대한 비침투 공격 대응기술 시험방법, ISO/IEC 암호알고리즘 구현 적합성 시험, ISO/IEC 난수발생기 시험방법 등이 있다. 국제 암호모듈 검증기준 및 시험기준은 ISO/IEC 암호모듈 보안요구사항 및 ISO/IEC 암호모듈 시험요구사항을 준용하고 있으며 미국, 캐나다, 일본 등은 자국의 암호모듈 검증을 위해 국제표준 도입을 준비하고 있다. 또한 미국, 캐나다, 일본 등은 하드웨어 암호모듈 검증시 ISO/IEC 암호모듈에 대한 비침투 공격 대응기술 시험방법을, 암호모듈에 구현된 암호알고리즘 검증시 ISO/IEC 암호알고리즘 구현 적합성 시험을, 암호모듈에 구현된 또는 사용되는 난수발생기 검증시 ISO/IEC 난수발생기 시험방법 등을 참조하고 있다.
이 기술보고서는 위의 표준들의 목적, 개발배경, 사용분야, 사용방법, 사용시 참고사항, 표준들 사이의 연계성 등 사용지침을 제시하여 관련 표준들의 이해를 돕고자 한다.

3 인용 기술보고서와의 비교

3.1 인용 기술보고서와의 관련성

- 해당사항 없음

3.2 인용 표준과 본 기술보고서의 비교표

- 해당사항 없음

Preface

1 Purpose

This technical report proposes the guideline which should be used to understand the testing standards related to the cryptographic modules. This standard describes their purpose, the background of their development, the area for their use, the method to use them, the notes on using them and the relation among them, etc.

This technical report is useful for the developers who develop a cryptographic module claimed them in order to apply for the validation to the validation authority from domestic or abroad, for the testers who use them on testing the cryptographic modules, for the users who procure the cryptographic modules.

2 Summary

A lot of standards related the cryptographic module testing technology have been published or developing. There are KS Security requirements for cryptographic modules, KS Test requirements for cryptographic modules, TTA Guideline for the collection and application of noise source on operating systems, TTA Accreditation process of cryptographic module to operate, ISO/IEC Security requirements for cryptographic modules, ISO/IEC Test requirements for cryptographic modules, ISO/IEC Cryptographic algorithms and security mechanisms conformance testing, ISO/IEC Testing methods for the mitigation of non-invasive attack classes against cryptographic modules, ISO/IEC Competence requirements for information security testers and evaluators-Part 2: Competence requirements for ISO/IEC 19790 testers, ISO/IEC Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408, ISO/IEC Guidelines for testing cryptographic modules in their operational environment. ISO/IEC Physical security attacks, mitigation techniques and security requirements in the cryptographic module testing family. The KCMVP claims KS Security requirements for cryptographic modules and KS Test requirements for cryptographic modules as the validation criteria and testing criteria.

ISO/IEC Security requirements for cryptographic modules and ISO/IEC Test requirements for cryptographic modules are claimed as the international validation criteria and testing criteria. The USA, Canada and Japan will adopt them as their national standards.

This technical report describes their purpose, the background of their development, the area for their use, the method to use them, the notes on using them and the relation among them, etc and help to understand them.

3 Relationship to Reference Standards

- None

목 차

암호모듈 시험기술표준 사용지침
(Guideline for Using the Testing Standards of the Cryptographic Modules)

1 적용 범위

이 기술보고서에서는 암호모듈 시험기술 관련 KS, TTA, ISO/IEC 표준들의 목적, 개발배경, 사용분야, 사용방법, 사용시 참고사항, 표준들 사이의 연계성 등 사용지침을 제시한다. 또한 검증기관에 암호모듈 검증을 신청하는 경우 필수적으로 적용되어야 할 표준들을 설명한다.

다양한 형태의 암호 모듈이 정보통신시스템에서 중요한 정보를 보호하기 위해 정보보호 시스템 내부에 탑재되어 사용되고 있다. 암호 모듈은 넓은 범위의 데이터(낮은 가치의 기업, 수억 가치의 정보 통신, 개인정보, 생명보호정보 등)과 다양한 응용환경(생산 기업, 사무실, 이동 매체, 공개된 장소)에서 활용될 수 있다. 암호모듈 개발은 키관리, 자체 보호, 암호 함수 구현 등 전문적 기술들을 요구한다. KCMVP, CMVP, JCMVP와 같은 검증기관은 다양한 형태의 암호모듈을 검증하고 암호모듈의 안전성을 보증한다. 사용기관은 조직의 보안정책, 보호 자산의 가치, 위협, 취약성 등을 분석한 후 자산을 보호하기 위한 암호모듈의 보안요구사항을 설계하고 검증기관이 검증한 암호모듈을 선정하여 사용한다. 이러한 암호모듈 개발, 검증 및 도입/운용와 관련한 수많은 암호모듈 시험기술 표준들이 제정되었거나 개발되고 있다.

암호모듈 시험기술 표준들로는 KS 암호모듈 보안요구사항, KS 암호모듈 시험요구사항, TTA 잡음원 수집방법 및 응용지침, TTA 암호모듈 인정절차, ISO/IEC 암호모듈 보안요구사항, ISO/IEC 암호모듈 시험요구사항, ISO/IEC 암호모듈에 대한 비침투 공격 대응기술 시험방법, ISO/IEC 암호알고리즘 구현 적합성 시험, ISO/IEC 난수발생기 시험방법, ISO/IEC 물리적 보안 공격 대응기술 및 보안요구사항, ISO/IEC 암호모듈 시험자 자격기준, ISO/IEC 암호모듈 현장시험 가이드 등이 있다.

한국 암호모듈 검증제도(KCMVP)에서 준용하고 있는 검증기준 및 시험기준인 KS 암호모듈 보안요구사항 및 KS 암호모듈 시험요구사항이 있으며 KCMVP 수행시 참조할 수 있는 ISO/IEC 암호모듈에 대한 비침투 공격 대응기술 시험방법, ISO/IEC 암호알고리즘 구현 적합성 시험, ISO/IEC 난수발생기 시험방법 등이 있다. 국제 암호모듈 검증기준 및 시험기준은 ISO/IEC 암호모듈 보안요구사항 및 ISO/IEC 암호모듈 시험요구사항을 준용하고 있으며 미국, 캐나다, 일본 등은 자국의 암호모듈 검증을 위해 국제표준 도입을 준비하고 있다. 또한 미국, 캐나다, 일본 등은 하드웨어 암호모듈 검증시 ISO/IEC 암호모듈에 대한 비침투 공격 대응기술 시험방법을, 암호모듈에 구현된 암호알고리즘 검증시 ISO/IEC 암호알고리즘 구현 적합성 시험을, 암호모듈에 구현된 또는 사용되는 난수발생기 검증시 ISO/IEC 난수발생기 시험방법 등을 참조하고 있다.

이 기술보고서는 위 표준들의 목적, 개발배경, 사용분야, 사용방법, 사용시 참고사항, 표준들 사이의 연계성 등 사용지침을 제시하여 관련 표준들의 이해를 돕고자 한다. 본 표준은 암호모듈을 처음 개발하는 개발자나 또는 암호모듈 보안요구사항에 익숙하지 않은 사용자에게 특히 유용하다.
이 기술보고서는 암호모듈에 구현되는 암호알고리즘들에 대한 표준은 적용범위에서 제외한다.

2 인용 표준

- 해당사항 없음

3 용어 정의

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

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

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

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

3.5 한국 암호모듈 검증제도(KCMVP)
전자정부법 시행령 제 69조와 [암호모듈 시험 및 검증지침]에 의거, 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도

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

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

3.8 운영환경 (operational environment)

모듈이 안전하게 운영할 수 있는 운영체제 및 하드웨어 플랫폼으로 구성된 모든 소프트웨어와 하드웨어 집합

3.9 물리적 보호 (physical protection)
물리적 수단을 사용하여 암호모듈, CSP 및 PSP를 보호하는 것.

3.10 보안수준
모듈 자체(예: 내부 구성 요소와 동작에 대한 접근과 인식) 보호 수준 및 모듈 내에서 관리되는 SSP 보호 수준을 나타내며 보안수준1에서 보안수준4까지 있으며 단계적으로 증가함

4 약어

API Application Program Interface
KCMVP Korean Cryptographic Module Validation Program
CMVP Cryptographic Module Validation Program
JCMVP Japanese Cryptographic Module Validation Program
KAT Known Answer Test
NIST National Institute of Standards and Technology
FIPS Federal Information Processing Standard
IUT Implementation Under Test
CSP Critical Security Parameter
PSP Public Security Parameter
SSP Sensitive Security Parameter

5 암호모듈 시험기술 표준화 작업기구

5절에서는 암호모듈 시험기술 표준화가 수행되는 표준화 작업기구들을 소개한다.

5.1 TTA 표준화 작업기구

TTA에서 TTA 표준화를 주관하고 있으며 단체표준으로 준용되고 있다.
정보보호 기술위원회(TC5)는 국내 정보보호 표준개발, 국제 표준화 추진 및 대응을 위하여 정보보호기반(PG501), 개인정보 및 ID관리, 블록체인(PG502), 사이버보안(PG503), 응용보안/평가인증(PG504), 바이오인식(PG505) 등의 프로젝트그룹으로 구성되어 운영하고 있으며 암호모듈 시험기술 TTA 표준은 응용보안/평가인증 프로젝트그룹(PG504)에서 수행되고 있다.
다음 표는 PG504에서 제정 완료된 암호모듈 시험기술 TTA표준들을 나타내고 있다.

<표 5-1> 암호모듈 시험기술 TTA 표준

표준 번호	표준 명칭
TTAS.KO-12.0235/R1	운영체제별 잡음원 수집방법 및 사용지침
TTAK.KO-12.0293	암호모듈 현장시험 지침
TTAK.KO-12.0264	운영시 암호모듈 인정 프로세스

소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침 및 암호모듈 시험기술표준 사용지침은 2018년 9월 현재 PG504에서 제정 진행 중인 암호모듈 시험기술 TTA표준들이다다.

5.2 KS 표준화 작업기구

한국기술표준연구원 및 국립전파연구원에서 KS 표준화를 주관하고 있으며 대한민국 국가표준으로 준용되고 있다. KS는 한국산업표준(KS)으로서 기본 부문(A)부터 정보 부문(X)까지 21개 부분으로 구성되어 있으며, 크게 제품 표준, 방법 표준, 전달 표준으로 분류할 수 있다. 한국 산업 표준의 제개정 방법은 기술표준원장이 제안하거나 개인, 기업, 관련 기관 등 이해 관계인이 신청하면, 이해 관계인의 의견 수렴과 산업표준 심의회의 심의를 거쳐 기술표준원장이 관보에 고시함으로써 한국산업표준(KS)으로 확정된다.
한국산업표준(KS)은 제정일로부터 5년마다 적정성을 검토하여 개정, 확인, 폐지 등의 조치를 하게 되며, 필요한 경우 5년 이내라도 개정 또는 폐지할 수 있다.
암호모듈 시험기술 표준은 한국산업표준(KS)의 정보 분야(X)로 분류된다. 이에 따라 암호모듈 시험기술 표준은 KS X로 시작하고 있다.
다음 표는 KS 정보보호 기술심의 위원회에서 제정 완료된 암호모듈 시험기술 KS 표준들을 나타내고 있다.

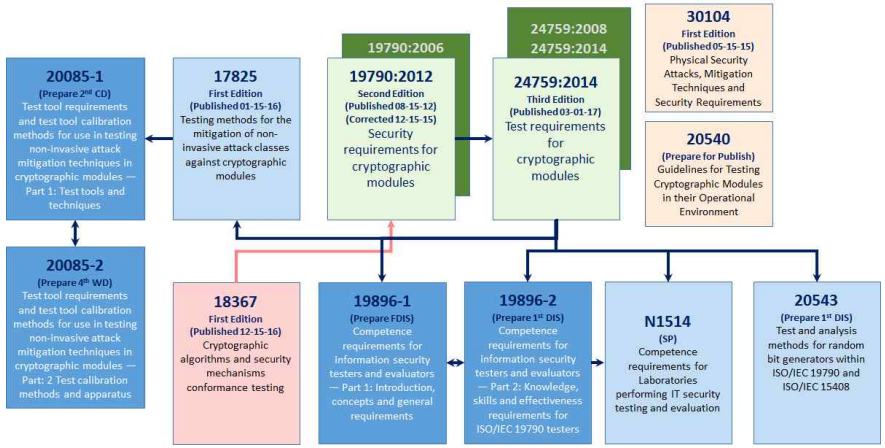
<표 5-2> 암호모듈 시험기술 KS 표준

표준 번호	표준 명칭
KS X ISO/IEC 19790	암호모듈 보안요구사항
KS X ISO/IEC 24759	암호모듈 시험요구사항

암호 알고리즘 및 보안 메커니즘 적합성 시험 및 물리적 보안 공격, 완화방법 및 보안요구사항은 2018년 9월 현재 KS 정보보호 기술심의 위원회에서 제정 진행 중인 암호모듈 시험기술 KS표준들이다.

5.3 ISO/IEC 표준화 작업기구

ISO/IEC JTC1 SC27에서 IT보안기술에 대하여 국제표준화를 주관하고 있다. SC27 산하에 5개의 작업그룹에서 정보 보안 관리시스템(WG1), 암호 및 보안 메커니즘(WG2), 보안 평가기준(WG3), 보안통제 및 서비스(WG4), 신원관리 및 개인정보 기술(WG5) 등의 보안기술 분야에서 국제표준화를 수행하고 있다. 암호모듈 시험기술 ISO/IEC 표준은 보안 평가기준(WG3)의 작업그룹에서 수행되고 있다. 다음 그림은 ISO/IEC JTC1 SC27 WG3에서 제정되었거나 제정 중인 암호모듈 시험기술 국제표준들을 나타내고 있다. ISO/IEC 핵심표준으로서 ISO/IEC 19790 및 ISO/IEC 24759와 이들 핵심표준을 지원하는 표준들로 구성되어 있다.



(그림 5-1) ISO/IEC 암호모듈 시험기술 관련 국제표준

6 암호모듈 시험기술 표준 및 사용지침

6.1 암호모듈 시험기술 TTA 표준

6.1.1 TTAS.KO-12.0235/R1 운영체제별 잡음원 수집방법 및 사용지침

6.1.1.1 적용 범위 및 목적

(목적) TTAS.KO-12.0235/R1 운영체제별 잡음원 수집방법 및 사용지침 표준은 윈도즈 운영체제, 리눅스 운영체제, 안드로이드 운영체제, iOS 등 운영체제에 따라 잡음원을 수집하는 방법 및 전산기의 CPU 칩에서 제공하는 하드웨어 잡음원 생성기로부터 잡음원을

수집하는 방법과 수집된 잡음원을 응용하는 방법에 대한 지침을 제시한다.

(잡음원 종류 및 적용) 운영체제에서 수집할 수 있는 잡음원은 운영체제가 제공하는 함수들을 이용할 수 있으며, 운영체제에서 수집한 잡음원의 엔트로피가 제한적인 경우 운영체제와 별도로 CPU칩에서 제공하는 하드웨어 잡음원 생성기 등 하드웨어로 구현된 잡음원 생성기를 통하여 잡음원을 추가로 수집할 수 있다. 수집된 잡음원은 기밀성, 인증, 접근통제, 부인봉쇄 등 암호의 안전한 사용에 필수적인 난수발생기의 씨드 등에 응용될 수 있다.

(표준 사용자) 본 표준은 암호제품을 개발하는 개발자가 운영체제에서 잡음원을 수집하는 경우와 수집된 잡음원을 응용하는 경우에 적용될 수 있다.

6.1.1.2 개발배경

(제도적 배경) 암호모듈 검증제도를 운영하고 있는 국가는 한국, 미국, 캐나다, 일본 등이 있다. 사용기관(예: 정부기관, 금융기관, 산업체, 학교 등)이 정보보호를 위해 암호모듈을 도입할 때 검증기관에서 검증받은 암호모듈을 요구하는 경우가 있다. 한국 정부에서 암호모듈을 도입할 때는 KCMVP 검증필 암호모듈을 요구하며, 미국 정부에서 암호모듈을 도입할 때는 CMVP 검증필 암호모듈을 요구하고 있다. 즉 암호모듈에 포함된 난수발생기(RBG)는 KCMVP는 검증기준 KS X ISO/IEC 19790를 만족해야 하고, CMVP는 검증기준 FIPS 140-2를 만족해야 하고, JCMVP는 검증기준 JS X ISO/IEC 19790을 만족해야 한다. 변경 가능한 운영환경에서 동작하는 소프트웨어 암호모듈 또는 제한된 운영환경에서 동작하는 펌웨어 암호모듈에 포함된 결정론적 난수발생기의 입력인 씨드는 검증기준을 만족하는 엔트로피를 갖는 잡음원으로 구성되어야 한다. 본 표준에서 제공하는 운영체제별 잡음원 수집 API로 구성하면 엔트로피 검증기준을 만족할 수 있다.

(중요성) 암호 서비스에서 키의 중요성은 매우 높다. 키가 노출되거나 해독되면 암호 서비스는 취약하게 된다. 이렇게 중요한 키를 생성하는데 난수발생기가 사용되며 난수발생기의 입력인 씨드의 엔트로피가 안전한 키의 중요한 요소가 된다. 따라서 씨드로 사용될 충분한 엔트로피를 갖는 잡음원의 수집이 매우 중요하다.

(표준 내용) 변경 가능한 운영환경 또는 제한된 운영환경을 구성하는 윈도즈 운영체제, 리눅스 운영체제, 안드로이드 운영체제, iOS 운영체제 등에서는 잡음원을 제공하는 API 함수들을 제공하고 있다. TTAS.KO-12.0235/R1에서 이들 API 함수들을 명시하고 API 함수를 잡음원으로 사용할 시 주의사항을 제시하고 있다.

(표준 사용 목적) 운영체제에서 잡음원 수집하는 암호모듈을 구현하는 암호모듈 개발자를 지원하기 위해 작성된 표준이다. 암호모듈을 처음 개발하는 개발자인 경우 엔트로피에 친숙하지 않아 엔트로피를 갖는 잡음원 생성 운영체제 API를 찾기가 쉽지 않다. 본 표준

을 참고하면 이들 잡음원 생성 운영체제 API 함수들 쉽게 찾아 암호모듈 구현에 사용할 수 있다.

6.1.1.3 사용방법 및 사용시 참고사항

(표준 사용방법) TTAS.KO-12.0235/R1는 윈도즈 운영체제, 리눅스 운영체제, 안드로이드 운영체제, iOS 운영체제 등에 대하여 잡음원을 제공하는 API 함수들을 제공하고 있다. 또한 CPU 칩에서 제공하는 하드웨어 잡음원을 수집하는 방법들도 제공하고 있다.

원칙적으로 엔트로피를 갖는 잡음원인 경우 한 개의 잡음원에서 엔트로피를 축적할수록 즉 많은 출력 비트를 생성하여 조합하면 엔트로피를 증가 시킬 수 있기 때문에 한 개의 잡음원을 사용하는 것은 가능하다. 그러나 운영체제에서 잡음원은 PRNG를 통해 생성되거나, 예측 가능한 시간정보를 이용하거나, 시스템별로 고정된 정보를 이용하거나 또는 충분한 엔트로피를 생성해도 신뢰성(Trust)이 보증되지 않을 수 있다. 따라서 잡음원의 안전성을 최대한 확보하기 위해 본 표준에서 제공하는 모든 잡음원 API 함수들을 조합하여 사용하는 것을 권고한다.

(참고사항) TTAS.KO-12.0235/R1에 명시한 운영체제에서 수집하는 잡음원 API 함수 중에서 중요 API 함수들에 대해서 엔트로피 특성을 서술하고 있으므로 엔트로피를 대략적으로 추정할 수 있으며 엔트로피가 높은 것으로 서술되어 있는 API 함수들은 필히 결정론적 난수발생기의 입력 씨드로 사용되어야 한다. 또한 2018년 8월 현재 암호학적 난수발생기의 잡음원에 대한 시험평가기준이 TTA 표준 추진 중이며 이 표준이 완료되면 잡음원에 대한 엔트로피를 확인할 수 있다.

6.1.1.4 사용분야

TTAS.KO-12.0235/R1는 변경 가능한 운영환경 또는 제한된 운영환경을 구성하는 윈도즈 운영체제, 리눅스 운영체제, 안드로이드 운영체제, iOS 운영체제 등에서 동작하는 소프트웨어 암호모듈 또는 펌웨어 암호모듈에 포함된 결정론적 난수발생기 입력을 구현할 경우 사용된다. 즉 안전한 난수생성이 필요한 암호분야에서 사용된다.

6.1.1.5 다른 암호모듈 시험기술 표준과 연계성

TTAS.KO-12.0235/R1는 KS X ISO/IEC 19790, KS X ISO/IEC 24759, ISO/IEC 19790, ISO/IEC 24759에서 암호모듈에 포함되는 난수발생기의 보안요구사항과 연계성을 가진다. 본 표준에서 수집된 잡음원은 TTA 표준 추진 중인 소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침 및 NIST SP 800-90B에 의해 엔트로피를 평가할 수 있다.

6.1.2 TTAK.KO-12.0293 암호모듈 현장시험 지침

6.1.2.1 적용 범위 및 목적

(적용범위) TTAK.KO-12.0293 암호모듈 현장시험 지침 표준은 사용자 응용환경에서 암호모듈의 현장시험을 위한 지침을 제시한다. 암호모듈 현장시험 지침은 KCMVP에서 검증받은 암호모듈을 사용자 응용환경에 적용하기 전에 사용자가 암호모듈 현장시험을 실시할 때 준수해야 하는 지침을 포함하고 있다.

(표준 내용) 본 표준은 KS X ISO/IEC 19790을 준용하고 KCMVP에서 검증받은 암호모듈에 대한 보안요구사항, 암호모듈 운영환경에 대한 보안요구사항, 암호모듈 현장시험 주요 개념 및 요구사항, 암호모듈 보고서 작성을 포함한다. 또한 암호모듈 현장시험 요구사항으로서 시험자 자격조건, 현장시험 참고문서, 시험활동, 시험절차, 시험지침, 시험 체크리스트를 포함한다.

(목적) 사용자가 검증받은 암호모듈을 사용자 응용환경에 정확하게 적용함으로써 정보통신시스템에서 발생할 수 있는 암호 취약점을 최대한 감소시켜 정보통신시스템의 안전성을 확보할 수 있다. 본 표준은 주로 사용자가 운영시 유용하게 사용될 수 있고 또한 개발자 또는 평가자가 암호모듈 개발, 평가시 유용하게 사용될 수 있다.

6.1.2.2 개발배경

암호모듈 검증제도를 운영하고 있는 국가는 한국, 미국, 캐나다, 일본 등이 있다. 사용기관(예: 정부기관, 금융기관, 산업체, 학교 등)이 정보보호를 위해 암호모듈을 도입할 때 검증기관에서 검증받은 암호모듈을 요구하는 경우가 있다. 특히 한국, 미국, 캐나다는 국가정부기관에 사용되는 암호모듈은 검증기준을 만족하도록 요구하고 있다. 그러나 사용기관의 사용자는 암호모듈의 보안요구사항을 정확히 인지하지 못하여 암호모듈 도입을 잘못하거나 암호모듈 운영을 정확히 인지하지 못하여 암호 취약점을 발생시키는 경우가 많다. 본 표준은 사용기관이 암호모듈를 도입할 경우 암호모듈 현장시험 필요성을 제시하고 정확한 암호모듈의 사용을 위한 지침을 제공하기 위해 개발되었다.

6.1.2.3 사용방법 및 사용시 참고사항

검증필 암호모듈이 개발될 때의 의도된 운영환경과 다른 운영환경에서 사용될 경우 암호모듈이 사용환경에 적합한지 판단하기 위해 본 표준에 명시된 현장시험 지침을 사용한다. 즉 사용기관이 정보통신시스템에서 정보를 보호하기 위해 암호모듈을 도입할 경우 본 표준을 적용한 현장시험을 실시하고 암호모듈의 적합성 여부를 판단해야 한다.
사용자는 현장시험시 별도의 요구사항을 본 표준에 추가하여 사용할 수 있다. 검증받은 암호모듈의 의도된 운영환경과 사용기관의 운용환경이 동일한 경우, 암호모듈 현장시험을 생략할 수 있다.

6.1.2.4 사용분야

정보통신망에서 중요 정보를 보호하는 암호 IT 산업 분야에서 KCMVP 검증필 암호모듈을 단독으로 도입하여 운영하는 경우 본 표준이 사용될 수 있다. 또한 검증필 암호모듈이 탑재될 수 있는 스마트카드, DB 암호제품, VPN, PKI 제품, 디스크 암호제품 등을 개발하거나 운영할 경우 본 표준이 사용될 수 있다.

6.1.2.5 다른 암호모듈 시험기술 표준과 연계성

TTAK.KO-12.0293는 KS X ISO/IEC 19790, KS X ISO/IEC 24759를 만족하는 암호모듈에 대하여 적용하고 있다. 따라서 TTAK.KO-12.0293는 KS X ISO/IEC 19790를 만족하고 있다.

6.1.3 TTAK.KO-12.0264 운영시 암호모듈 인정 프로세스

6.1.3.1 적용 범위 및 목적

다양한 형태의 암호모듈이 정보통신시스템에서 중요한 정보를 보호하기 위해 정보보호시스템 내부에 탑재되어 사용되고 있다. 암호모듈은 넓은 범위의 데이터(낮은 가치의 행정정보, 수억 가치의 정보 통신, 개인정보, 생명보호정보 등)과 다양한 응용환경(생산기업, 사무실, 이동매체, 공개된 장소)에서 활용될 수 있다. 암호모듈 개발은 키관리, 자체보호, 암호함수 구현 등 전문적인 기술을 요구한다.
KCMVP, CMVP, JCMVP와 같은 검증기관은 다양한 형태의 암호모듈을 검증하고 암호모듈의 안전성을 보증한다. 사용기관은 예산, 조직의 보안정책, 운영인력, 자산의 가치, 위협, 취약성 등을 분석한 후 자산을 보호하기 위한 보안요구사항을 설계한다. 사용기관이 직접 암호모듈을 개발하여 사용하거나, 검증기관이 검증한 암호모듈들 중에서 선정해서 사용할 수 있다.

(적용범위) 암호모듈이 다양한 운영환경에서 사용될 때, 운영환경에 적합한 암호모듈을 선정하기 위하여 전문기술이 필요하다. 그러므로 사용기관은 정보통신시스템에서 정보보호를 위하여 암호모듈을 도입할 때, 체계적인 인정절차를 통하여 암호모듈을 인정하는 것이 필요하다.
TTA.KO-12.0264 운영시 암호모듈 인정 프로세스 표준은 사용기관이 검증기관에서 검증한 암호모듈을 도입할 경우 정보통신시스템에 적합한 암호모듈을 승인하는 인정프로세스를 제시한다.
(목적) TTA.KO-12.0264에서 적용하고 있는 암호모듈은 ISO/IEC 19790 검증기준을 따르고 있다. TTA.KO-12.0264에서 제시한 암호모듈 인정프로세스는 사용기관이 정보통신시스템의 암호모듈을 도입할 경우 유용하게 적용될 수 있다.

6.1.3.2 개발배경

암호모듈 검증제도를 운영하고 있는 국가는 한국, 미국, 캐나다, 일본 등이 있다. 사용기관(예: 정부기관, 금융기관, 산업체, 학교 등)이 정보보호를 위해 암호모듈을 도입할 때 검증기관에서 검증받은 암호모듈을 요구하는 경우가 있다. 한국 정부에서 암호모듈을 도입할 때는 KCMVP 검증필 암호모듈을 요구하며, 미국 정부에서 암호모듈을 도입할 때는 CMVP 검증필 암호모듈을 요구하고 있다. 그러나 사용기관의 사용자는 암호모듈의 보안 요구사항을 정확히 인지하지 못하여 암호모듈 도입을 잘못하거나 암호모듈 운영을 정확히 인지하지 못하여 암호 취약점을 발생시키는 경우가 많다. 본 표준은 사용기관이 암호모듈를 도입할 경우 암호모듈 인정 프로세스 필요성을 제시하고 안전한 암호모듈의 도입을 위한 지침을 제공하기 위해 개발되었다.

6.1.3.3 사용방법 및 사용시 참고사항

정보통신망에서 중요 정보를 보호하는 암호 IT 산업 분야에서 KCMVP 검증필 암호모듈을 도입한 경우, 사용기관의 예산, 조직의 보안정책, 운영 인력, 자산의 가치, 위협, 취약성 등을 분석하여 암호모듈의 사용 승인을 할 때 본 표준의 인정 프로세스를 적용한다. 본 표준의 인정 프로세스 중 인정평가 단계에서 TTAK.KO-12.0293 암호모듈 현장시험 지침을 활용할 수 있다.

6.1.3.4 사용분야

사용 기관들로서 정부 및 정부 산하기관, 공장, 병원, 은행, 통신회사, 인터넷 시비스 제공업체 등에서 정보통신망에서 정보를 보호하고자 하는 기술분야가 될 수 있다.

6.1.3.5 다른 암호모듈 시험기술 표준과 연계성

TTA.KO-12.0264는 KS X ISO/IEC 19790, KS X ISO/IEC 24759를 만족하는 암호모듈을 도입하는 경우 적용되며, 인정평가 수행 중에 TTAK.KO-12.0293를 활용한다.

6.1.4 (TTA표준 제정 중) 소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침

6.1.4.1 적용 범위 및 목적

소프트웨어 암호모듈의 난수발생기용 잡음원 엔트로피 평가기준 표준은 암호학적 난수발생기에 사용되는 잡음원에 대한 엔트로피 평가방법과 평가기준을 제시하고 있으며 암호모듈 검증제도(KCMVP)의 안전성 기준에 따른 난수발생기 잡음원 평가의 정량적인 기준 및 적용 가이드를 제공하고 있다. 난수발생기용 잡음원 엔트로피 평가기준은 현재 응용보안/평가인증(PG504) 작업그룹에서 TTA 표준제정 추진 중에 있다.

6.1.4.2 개발배경

암호모듈 검증제도를 운영하고 있는 국가는 한국, 미국, 캐나다, 일본 등이 있다. 사용기관(예: 정부기관, 금융기관, 산업체, 학교 등)이 정보보호를 위해 암호모듈을 도입할 때 검증기관에서 검증받은 암호모듈을 요구하는 경우가 있다. 한국 정부에서 암호모듈을 도입할 때는 KCMVP 검증필 암호모듈을 요구하며, 국내 검증필 암호모듈은 소프트웨어 암호모듈이 대부분이다. 소프트웨어 암호모듈에 탑재되는 난수발생기의 입력은 운영체제에서 수집된 잡음원을 사용하고 있다. 운영체제에서 수집된 잡음원의 엔트로피를 평가하는데 특화된 시험평가 기준이 필요하여 본 표준이 개발되고 있다.

6.1.4.3 사용방법 및 사용시 참고사항

본 표준이 개발되면 표준을 적용한 엔트로피 시험용 프로그램도 배포될 예정이다. 시험용 프로그램은 본 표준과 별도로 배포될 예정이다. 소프트웨어 암호모듈에 사용되는 운영체제에서 수집된 잡음원을 본 표준에 따라 수집하여 엔트로피 시험 프로그램으로 엔트로피를 평가할 수 있다. 평가된 엔트로피는 암호모듈 개발자의 개발문서로 작성되어 암호모듈에 사용되는 엔트로피의 근거로 사용될 수 있다.

6.1.4.4 사용분야

사용 기관들로서 정부 및 정부 산하기관, 공장, 병원, 은행, 통신회사, 인터넷 시비스 제공업체 등에서 정보통신망에서 정보를 보호하고자 하는 소프트웨어 암호모듈에 난수발생기가 탑재되는 경우, 난수발생기 입력의 엔트로피를 평가하는 분야가 될 수 있다.

6.1.4.5 다른 암호모듈 시험기술 표준과 연계성

본 표준은 KS X ISO/IEC 19790, KS X ISO/IEC 24759를 만족하는 소프트웨어 암호모듈에 난수발생기를 탑재하는 경우 난수발생기가 운영체제에서 잡음원을 수집하는 경우 적용된다. TTAS.KO-12.0235/R1에서 권고하는 잡음원에 대하여 엔트로피를 평가 할 수도 있다.

6.2 암호모듈 시험기술 KS 표준

6.2.1 KS X ISO/IEC 19790 암호모듈 보안요구사항

6.2.1.1 적용 범위 및 목적

KS X ISO/IEC 19790 암호모듈 보안요구사항 표준은 컴퓨터와 통신 시스템 내 중요 정보를 보호하는 보안 시스템에서 사용하는 암호모듈을 위한 보안요구사항을 명시한다. KS X ISO/IEC 19790은 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. KS X ISO/IEC 19790은 11개 요구사항 영역별 4개의 보안수준을 명시한다 (보안수준 1: 가장 낮은 수준, 보안수준 4: 최고 높은 수준). 높은 보안수준의 보안요구사항은 낮은 보안수준의 보안요구사항을 포함한다.
KS X ISO/IEC 19790은 보안을 제공하는 암호모듈이 충족해야 하는 보안 요구사항을 명시하며, 암호모듈이 KS X ISO/IEC 19790에 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.

6.2.2 KS X ISO/IEC 24759 암호모듈 시험요구사항

6.2.2.1 적용 범위 및 목적

KS X ISO/IEC 24759 암호모듈 시험요구사항 표준은 암호모듈이 KS X ISO/IEC 19790에 명세된 요구사항에 적합한지 여부를 시험하기 위해서 시험기관이 사용하는 시험방법을 명세하고 있다. 이 방법은 시험을 수행하는 동안 객관성과 일관성을 보증하기 위하여 개발되었다. 또한 KS X ISO/IEC 24759는 벤더가 시험기관에 제출해야 하는 정보의 요구사항을 명세하고 있다. 이 정보의 요구사항은 암호모듈이 KS X ISO/IEC 19790에 명세된 요구사항에 적합함을 설명하는 증거들이다.
벤더는 시험기관에 암호모듈 시험을 신청하기 전에 암호모듈이 KS X ISO/IEC 19790에 명세된 요구사항을 충족하는지 여부를 검증할 때 KS X ISO/IEC 24759를 사용할 수 있다.

6.2.3 KS X ISO/IEC 18367 암호 알고리즘 및 보안 메커니즘 적합성 시험
6.2.3.1 적용 범위 및 목적

본 표준의 목적은 암호모듈에 구현된 암호 알고리즘 및 보안 메커니즘의 적합성 시험 방법을 명시하는데 있다. 구현된 암호 알고리즘 및 보안 메커니즘 보안 평가시 암호모듈과 분리해서는 안된다.

본 표준은 KS X ISO/IEC 19790과 KS X ISO/IEC 24759와 관련이 있다. KS X ISO/IEC 19790은 암호모듈 보안요구사항을 명시하고 있다. 암호모듈은 적어도 한 개 이상의 검증 대상 보호함수(예, 암호알고리즘 또는 보안 메커니즘)를 탑재하고 있다. KS X ISO/IEC 24759는 KS X ISO/IEC 19790의 보안요구사항에 대하여 시험요구사항을 명시하고 있다. 여기서, KS X ISO/IEC 24759는 암호 알고리즘 및 보안 메커니즘 적합성 시험을 수행하는 시험방법을 명시하고 있지 않다.

적합성 시험은 암호 알고리즘 또는 보안 메커니즘이 하드웨어, 소프트웨어 또는 펌웨어에 정확하게 구현되었는지를 보증한다. 적합성 시험은 특정 운영환경에서 정확하게 동작됨을 보증한다. 시험은 KAT, 몬테카를로 시험 또는 이들 시험의 조합으로 구성될 수 있다. 시험은 실제 구현물에서 수행되거나 시뮬레이션 환경에서 모델화되어 수행될 수 있다.

6.2.4 KS X ISO/IEC 30104 암호모듈 물리적 공격 및 완화방법
6.2.4.1 적용 범위 및 목적

모듈의 중요 보안 파라메터 보호가 필요한 경우, 물리적 보안 메커니즘이 암호모듈에 적용된다. 본 표준은 보안 환경의 위험을 줄이기 위해 물리적 보안 메커니즘 지원이 필요한 제품에 대하여 보안성이 어떻게 명시될 수 있는지 설명한다.

본 표준은 다음 주제를 설명한다.:

- 최소 기술 또는 자원이 요구되는 단순 공격에서부터 훈련되고 기술력을 갖춘 전문가 및 고비용 자원이 요구되는 고수준 공격까지 포함하는 알려진 물리적 공격에 대한 명세를 포함하는 서로 다른 하드웨어 형상에 대한 보안 공격에 대한 조사 결과 설명함
- 탬퍼 보호 메커니즘 및 이들 공격 완화 방법 설계에 대한 원리, 최선의 업무 수행 및 기술을 가이드 함
- 하드웨어 탬퍼 보호 메커니즘의 평가 또는 시험 및 하드웨어 탬퍼 평가 및 시험을 설명하는 현재 표준 및 시험 프로그램에 대한 참조를 가이드 함.

본 표준은 하드웨어 보안 구현물을 설계하고 최종 제품을 시험하거나 평가하는 제품 개발자에게 유용하다. 보호되어야 할 자산에 대한 복잡성, 비용, 위험을 통한 보호방법, 공격방법을 식별하고 있다. 비용 대비 효율적인 높은 수준의 보호방법이 고려될 수 있다.

6.3 암호모듈 시험기술 ISO/IEC 표준

6.3.1 ISO/IEC 19790 Security requirements for cryptographic modules

6.3.1.1 적용 범위 및 목적

ISO/IEC 19790 암호모듈 보안요구사항 표준은 컴퓨터와 통신 시스템 내 중요 정보를 보호하는 보안 시스템에서 사용하는 암호모듈을 위한 보안요구사항을 명시한다. ISO/IEC 19790은 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. ISO/IEC 19790은 11개 요구사항 영역별 4개의 보안수준을 명시

한다(보안수준 1: 가장 낮은 수준, 보안수준 4: 최고 높은 수준). 높은 보안수준의 보안요구사항은 낮은 보안수준의 보안요구사항을 포함한다.

ISO/IEC 19790은 보안을 제공하는 암호모듈이 충족해야 하는 보안 요구사항을 명시하며, 암호모듈이 ISO/IEC 19790에 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.

6.3.2 ISO/IEC 24759 Test requirements for cryptographic modules

6.3.2.1 적용 범위 및 목적

ISO/IEC 24759 암호모듈 시험요구사항 표준은 암호모듈이 ISO/IEC 19790에 명세된 요구사항에 적합한지 여부를 시험하기 위해서 시험기관이 사용하는 시험방법을 명세하고 있다. 이 방법은 시험을 수행하는 동안 객관성과 일관성을 보증하기 위하여 개발되었다. 또한 ISO/IEC 24759는 벤더가 시험기관에 제출해야 하는 정보의 요구사항을 명세하고 있다. 이 정보의 요구사항은 암호모듈이 ISO/IEC 19790에 명세된 요구사항에 적합함을 설명하는 증거들이다.
벤더는 시험기관에 암호모듈 시험을 신청하기 전에 암호모듈이 ISO/IEC 19790에 명세된 요구사항을 충족하는지 여부를 검증할 때 ISO/IEC 24759를 사용할 수 있다.

6.3.3 ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing

6.3.3.1 적용 범위 및 목적

본 표준의 목적은 암호모듈에 구현된 암호 알고리즘 및 보안 메커니즘의 적합성 시험 방법을 명시하는데 있다. 구현된 암호 알고리즘 및 보안 메커니즘 보안 평가시 암호모듈과 분리해서는 안된다.

본 표준은 ISO/IEC 19790과 ISO/IEC 24759와 관련이 있다. ISO/IEC 19790은 암호모듈 보안요구사항을 명시하고 있다. 암호모듈은 적어도 한 개 이상의 검증대상 보호함수(예, 암호알고리즘 또는 보안 메커니즘)를 탑재하고 있다. ISO/IEC 24759는 ISO/IEC 19790의 보안요구사항에 대하여 시험요구사항을 명시하고 있다. 여기서, ISO/IEC 24759는 암호 알고리즘 및 보안 메커니즘 적합성 시험을 수행하는 시험방법을 명시하고 있지 않다.

적합성 시험은 암호 알고리즘 또는 보안 메커니즘이 하드웨어, 소프트웨어 또는 펌웨어에 정확하게 구현되었는지를 보증한다. 적합성 시험은 특정 운영환경에서 정확하게 동작됨을 보증한다. 시험은 KAT, 몬테카를로 시험 또는 이들 시험의 조합으로 구성될 수 있

다. 시험은 실제 구현물에서 수행되거나 시뮬레이션 환경에서 모델화되어 수행될 수 있다.

6.3.4 ISO/IEC 17825 Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

6.3.4.1 적용 범위 및 목적

본 표준은 보안수준 3 또는 4에 해당되는 ISO/IEC 19790의 보안요구사항에 대한 적합성을 결정하기 위한 비침투 공격 완화 시험방법을 명시하고 있다. 이 시험방법들은 ISO/IEC 19790에서 명시하고 있는 보호함수와 연계되어 있다. 이 방법은 암호모듈의 정의된 암호경계 및 정의된 경계에서 사용 가능한 I/O에서 수행될 수 있다.
암호모듈이 ISO/IEC 19790의 보안요구사항을 수행하는지 그리고 ISO/IEC 19790의 관련 보호함수에 대한 본 표준의 시험방법을 수행하는지를 시험하기 위해 시험기관에서 수행하는 시험방법은 ISO/IEC 24759에 명시되어 있다.
본 표준에 적용된 시험 접근법은 "push-button" 접근법으로서 시험은 객관적이고 재시험 가능하고 비용 대비 효율적이다.

6.3.5 ISO/IEC 20085-1 Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 1: Test tools and techniques

6.3.5.1 적용 범위 및 목적

본 표준의 목적은 비침투 공격 시험 도구를 명시하고 그 도구를 동작시키는 방법을 명시한다. 또한 목적은 시험 중인 암호모듈(구현물) (IUT)의 보안성을 증명하기 위한 비침투 신호를 수집하는 것이다.

6.3.6 ISO/IEC 20085-2 Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 2: Test calibration methods and apparatus

6.3.6.1 적용 범위 및 목적

본 ISO/IEC 20085는 시험 측정 방법 및 장치를 설명한다. 비침투 공격 완화방법의 보안요구사항을 명시한 ISO/IEC 17825에 정의된 시험방법들에 대하여 ISO/IEC 19790 및 ISO/IEC 24759 적용 암호모듈 시험도구를 측정할 때 본 표준을 사용한다.

6.3.7 ISO/IEC 19896-1 Competence requirements for information security testers

and evaluators - Part 1: Introduction, concepts and general requirements

6.3.7.1 적용 범위 및 목적

ISO/IEC 19896-1은 암호모듈 시험자 및 CC 평가자들이 가져야 하는 자격 요구사항을 이해하기 위한 개념 및 관련 용어들을 정의한다. 본 표준 사용자를 통하여 ISO/IEC 19896의 핵심 원리 및 개념을 공유할 수 있도록 한다. ISO/IEC 19896의 다른 파트 사용자에 대한 기본 정보를 제공한다.

6.3.8 ISO/IEC 19896-2 Competence requirements for information security testers and evaluators - Part 2: Competence requirements for ISO/IEC 19790 testers

6.3.8.1 적용 범위 및 목적

본 표준의 범위는 ISO/IEC 19790 및 ISO/IEC 24759를 사용한 적합성 스킴(scheme)에 필요한 시험 활동 및 평가 활동를 수행하는 암호모듈 시험자들의 자격에 대한 최소 요구사항을 제공한다.

6.3.9 ISO/IEC 20543 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

6.3.9.1 적용 범위 및 목적

본 표준은 비결정론적 난수발생기가 암호 응용에서 사용되기 위해 충분한 엔트로피를 갖는지를 결정하기 위해 사용되는 방법을 명시한다. 검증기관에 의해 수행되는 독립 검증 및 검정을 수행하기 위한 비결정론적 난수발생기의 통계적 시험 및 평가에 대한 가이드를 제시한다. 비결정론적 난수발생기의 설계 및 구현은 본 표준의 범위에 속하지 않는다.

6.3.10 ISO/IEC 20540 Testing cryptographic modules in their operational environment

6.3.10.1 적용 범위 및 목적

본 표준은 사용자 보안 시스템 상에서 암호모듈의 현장시험에 적용될 수 있다. ISO/IEC 19790 검증필 암호모듈 중에서 운영환경에 적합한 암호모듈을 선정하고 현장시험을 통해 확인할 수 있도록 가이드하고 있는 표준이다.

6.3.11 ISO/IEC 30104 Physical Security Attacks, Mitigation Techniques and Security Requirements

6.3.11.1 적용 범위 및 목적

모듈의 중요 보안 파라메터 보호가 필요한 경우, 물리적 보안 메커니즘이 암호모듈에 적용된다. 본 표준은 보안 환경의 위험을 줄이기 위해 물리적 보안 메커니즘 지원이 필요한 제품에 대하여 보안성이 어떻게 명시될 수 있는지 설명한다.

본 표준은 다음 주제를 설명한다.:

- 최소 기술 또는 자원이 요구되는 단순 공격에서부터 훈련되고 기술력을 갖춘 전문가 및 고비용 자원이 요구되는 고수준 공격까지 포함하는 알려진 물리적 공격에 대한 명세를 포함하는 서로 다른 하드웨어 형상에 대한 보안 공격에 대한 조사 결과 설명함
- 탬퍼 보호 메커니즘 및 이들 공격 완화 방법 설계에 대한 원리, 최선의 업무 수행 및 기술을 가이드 함
- 하드웨어 탬퍼 보호 메커니즘의 평가 또는 시험 및 하드웨어 탬퍼 평가 및 시험을 설명하는 현재 표준 및 시험 프로그램에 대한 참조를 가이드 함.

본 표준은 하드웨어 보안 구현물을 설계하고 최종 제품을 시험하거나 평가하는 제품 개발자에게 유용하다. 보호되어야 할 자산에 대한 복잡성, 비용, 위험을 통한 보호방법, 공격방법을 식별하고 있다. 가성비가 높은 보호방법이 고려될 수 있다.

6.3.12 Competence requirements for evaluation and testing laboratories

6.3.12.1 적용 범위 및 목적

본 표준의 범위는 ISO/IEC 19790 및 ISO/IEC 24759를 사용한 적합성 스킴(scheme)에 필요한 시험 활동 및 평가 활동를 수행하는 암호모듈 시험기관들의 자격에 대한 최소 요구사항을 제공한다. 암호모듈 시험기관의 자격요건을 제시하는 표준으로서 현재 ISO/IEC JTC1 SC27 WG3에서 표준화를 위해 NP 투표 단계에 있다.

부 록 Ⅰ

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

암호모듈 검증 신청 시 준수해야 할 표준

Ⅰ.1 국내 검증 시 준수해야 할 표준

벤더가 암호모듈을 KCMVP 검증기관에 검증 신청할 경우 검증대상 암호모듈이 준수해야 하거나 참조할 수 있는 표준들을 설명한다.

암호모듈 구현 시 암호모듈의 보안요구사항으로서 준수하거나 참조 할 수 있는 표준은 다음 표와 같다. 여기서 암호모듈이 탑재해야 승인된 암호알고리즘 및 보호메커니즘의 표준은 제외한다.

<표 Ⅰ-1> 암호모듈 구현시 적용될 표준

표준 번호	표준 명칭
KS X ISO/IEC 19790	암호모듈 보안요구사항
TTAS.KO-12.0235/R1	운영체제별 잡음원 수집방법 및 사용지침
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

암호모듈 구현 시 암호모듈의 보안요구사항으로서 참조 할 수 있는 표준인 물리적 보안 공격, 완화방법 및 보안요구사항는 2018년 9월 현재 KS표준으로 제정 진행 중에 있다.

개발자가 암호모듈 구현 후 개발문서 작성시 준수하거나 참조할 수 있는 표준은 다음 표와 같다.

<표 Ⅰ-2> 암호모듈 구현 후 개발문서 작성시 적용될 표준

표준 번호	표준 명칭
KS X ISO/IEC 19790	암호모듈 보안요구사항
KS X ISO/IEC 24759	암호모듈 시험요구사항
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

암호모듈 구현 후 개발문서 작성시 준수하거나 참조 할 수 있는 표준인 소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침은 2018년 9월 현재 TTA표준으로 제정 진행 중에 있다.

개발자가 암호모듈 구현 후 개발자 자체 시험시 참고할 표준은 다음 표와 같다.

<표 Ⅰ-3> 암호모듈 구현 후 개발자 자체 시험시 적용될 표준

표준 번호	표준 명칭
KS X ISO/IEC 19790	암호모듈 보안요구사항
KS X ISO/IEC 24759	암호모듈 시험요구사항
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
ISO/IEC 20085-1	Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 1: Test tools and techniques
ISO/IEC 20085-2	Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 2: Test calibration methods and apparatus

암호모듈 구현 후 개발자 자체 시험시 참조 할 수 있는 표준인 암호 알고리즘 및 보안 메커니즘 적합성 시험은 2018년 9월 중 KS표준으로 제정 진행 중에 있고, 소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침은 TTA표준으로 제정 진행 중에 있다.

Ⅰ.2 국내 검증 신청 시 표준 준수한 제출물

벤더가 KCMVP 검증기관에 암호모듈 검증 신청 시 제출해야 제출물은 다음과 같다.

- 검증 신청서
- 기본 및 상세 설계서
- 시험문서
- 구현물(소스코드 등)
- 암호모듈

기본 및 상세 설계서는 개발문서로서 KS X ISO/IEC 19790 암호모듈 보안요구사항, KS X ISO/IEC 24759 암호모듈 시험요구사항을 만족하도록 작성되어야 하고, ISO/IEC 17825 Testing methods for the mitigation of non-invasive attack classes against cryptographic modules를 참조할 수 있다.

시험문서는 KS X ISO/IEC 19790 암호모듈 보안요구사항, KS X ISO/IEC 24759 암호모듈 시험요구사항, SO/IEC 17825 Testing methods for the mitigation of

non-invasive attack classes against cryptographic modules, ISO/IEC 20085 Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 1: Test tools and techniques, Part 2: Test calibration methods and apparatus를 참조하여 시험을 수행하고 시험항목, 시험목적, 시험절차 및 시험결과를 작성된 문서이다.

암호모듈 및 구현물(소스코드 등)은 KS X ISO/IEC 19790 암호모듈 보안요구사항을 만족하도록 구현되어야 하고 TTAS.KO-12.0235/R1 운영체제별 잡음원 수집방법 및 사용지침, ISO/IEC 17825 Testing methods for the mitigation of non-invasive attack classes against cryptographic modules를 참조할 수 있다.

부 록 II-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님

지식재산권 확약서 정보

- 해당사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 기술보고서가 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 II-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

II-2.1 시험인증 대상 여부

- 해당사항 없음

II-2.2 시험표준 제정 현황

- 해당사항 없음

부 록 II-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

- 해당사항 없음

부 록 II-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] ISO, “Information technology — Security techniques - Security requirements for cryptographic modules”, ISO/IEC 19790, 2015.

[2] ISO, “Information technology — Security techniques - Test requirements for cryptographic modules”, ISO/IEC 24759, 2017.

[3] ISO, “Information technology — Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules”, ISO/IEC 17825, 2016.

[4] ISO, “Information technology — Security techniques - Cryptographic algorithms and security mechanisms conformance testing”, ISO/IEC 18367, 2016.

[5] ISO, “Information technology — Security techniques - Physical security attacks , mitigation techniques and security requirements”, ISO/IEC 30104, 2016.

[6] ISO, “Information technology — Security techniques - Testing cryptographic modules in their operational environment”, ISO/IEC 20540, 2018.

[7] ISO, “Information technology — Security techniques - Competence requirements for information security testers and evaluators - Part 1 : Introduction, concepts and general requirements - Part 2 : Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers”, ISO/IEC 19896, 2018.

[8] M.S Turan, et al., “Recommendation for the Entropy Sources Used for Random Bit Generation”, NIST Special Publication 800-90B, 2018.

[9] ISO, “Information technology — Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408”, ISO/IEC DIS 20543, 2018.

[10] ISO, “Information technology — Security techniques - Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 1 : Test tools and techniques, - Part 2 : Test calibration methods and apparatus”, ISO/IEC CD 20085, 2018.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 II-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

해당사항 없음

부 록 II-6

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2018.12.XX		암호모듈 시험기술표준 사용 지침	PG504