암호모듈 구현 안내서

2013. 1.

암호모듈 검증기관

암호모듈 시험기관

목 차

Ⅰ. 개요

Ⅰ-1. 서론

「암호모듈 구현 안내서」는 암호모듈 개발자에게 암호모듈 요구사항에 대한 이해를 향상시키고, 개발 시 반드시 준수해야 할 주의사항과 개발과정에서 발생한 개발자의 궁금증을 해소하고자 제공하는 문서이다.

- 본 안내서는 '암호모듈 시험요구사항(KS X ISO/IEC 24759)'과 '소프트웨어 암호모듈 검증기준'의 보안요구사항, 기타 시험 관련 일반사항을 명확히 하는 내용을 포함하고 있으며, 현재까지의 암호모듈 시험 시 개발업체가 주로 질의했던 사항 및 제출물 보완사항을 기반으로 작성되었다.
- 본 안내서의 내용은 검증기관 및 시험기관에 의해 예고 없이 변경될 수 있다.

Ⅰ-2. 법적근거

- 「전자정부법 시행령」제69조 (전자문서의 보관·유통 관련 보안조치)
- 「암호모듈 시험 및 검증안내서」(2004.12.31.)

Ⅰ-3. 적용기준

- KS X ISO/IEC 19790: 암호모듈 보안요구사항
- KS X ISO/IEC 24759: 암호모듈 시험요구사항
- 소프트웨어 암호모듈 검증기준 (2011.5.)
- 암호알고리즘 검증기준 Ver 2.0 (2012.3.)

Ⅰ-4. 문서의 구성

- 본 안내서는 암호모듈 검증제도 운영에 대한 요구사항을 다루는 일반사항, 11개 보안영역별 요구사항과 암호알고리즘에 대한 요구사항으로 구성되어 있다.

- 본 안내서는 질의 및 답변의 형식을 따르고 있으며, 각 질의별로 해당하는 '암호모듈 시험요구사항(KS X ISO/IEC 24759)', '소프트웨어 암호모듈 검증기준'을 참조할 수 있도록 연관관계를 명시하였다.

Ⅱ. 일반사항

질의	암호모듈 검증 신청
Ⅱ-1	암호모듈 검증 신청을 위해 구현해야 할 검증대상 암호알고리즘은 무엇인가? 또한 신청인이 작성해야 하는 제출물은 무엇인가?
요구사항	-

【 개념 정리 】

○ 검증대상 암호알고리즘 : 블록암호, 해시함수, 메시지 인증코드, 난수발생기, 키 설정, 공개키 암호, 전자서명 암호알고리즘에 대해 암호모듈 검증기관이 안전성과 신뢰성, 그리고 상호운용성 등을 고려하여 선정한 암호알고리즘

【 답변 】

○ 암호모듈 검증을 신청하는 암호모듈에는 <검증대상 암호알고리즘 목록>에 명시된 알고리즘 중 사용하고자 하는 검증대상 암호알고리즘과 파라미터를 포함해야 한다.

○ 암호모듈 검증을 신청하는 신청인은 아래의 제출물을 시험기관에 제출해야 한다.
※ 제출물은 신청인이 자율 형식으로 작성한다.

구 분	내 용
기본 및 상세설계서	- 암호모듈이 보안요구사항을 만족하기 위해 구현된 내용
형상관리문서	- 암호모듈 형상을 관리하는 방법 (암호모듈 구성요소, 버전 부여방법, 형상변경 통제방법 등)
시험서	- 개발과정 각 단계별 수행해야 하는 시험항목 - 각 시험항목별 시험목적 - 시험절차 및 결과 **※ 다양한 운영환경에서 동작하는 암호모듈에 대해서는 모든 운영환경에서의 시험결과를 포함해야 함**
암호모듈, 소스코드 및 하드웨어 설계서	- 검증 신청하는 암호모듈(실행 파일, 라이브러리, 하드웨어 등) - 암호모듈 범위에 포함되는 소프트웨어와 펌웨어의 소스코드 - 하드웨어 설계서(하드웨어 암호모듈의 경우)

○ 시험기관은 위에 기술된 제출물 외에 암호모듈 시험을 위해 추가적인 제출물을 요구할 수 있다.
- 난수발생기 엔트로피 분석서
- 소스코드 취약성 분석서
- 기타 시험에 필요한 제출물 등

○ 시험기관은 신청인이 암호모듈 검증을 신청하더라도 다음과 같은 사유에 의해 신청을 반려할 수 있다.
- 제출물의 내용이 시험을 진행하기 위한 수준에 미치지 못하는 경우
- 요구한 제출물을 포함하지 않은 경우

질의	재검증 요구사항
II-2	검증된 암호모듈의 검증유효기간 중에 암호모듈의 형상이 변경된 경우, 어떤 절차로 검증을 유지할 수 있는가?
요구사항	-

【 개념 정리 】

○ 재검증 : 검증된 암호모듈의 검증유효기간 중에 암호기능이 변경 또는 개선되어 암호모듈을 수정한 경우, 변경된 부분에 대한 검증을 받는 것

【 답변 】

○ 암호모듈에 대한 검증은 신규 검증과 재검증으로 분류된다. 신규 검증은 신청인이 검증을 받고자 하는 암호모듈에 대해 최초로 검증을 신청하는 것이며, 재검증은 기존에 검증을 획득한 암호모듈에 대해 검증을 유지하기 위한 목적으로 신청하는 것이다.

○ 신청인은 검증을 획득한 암호모듈에 대해 형상변경이 발생하는 경우 재검증을 신청해야 한다.

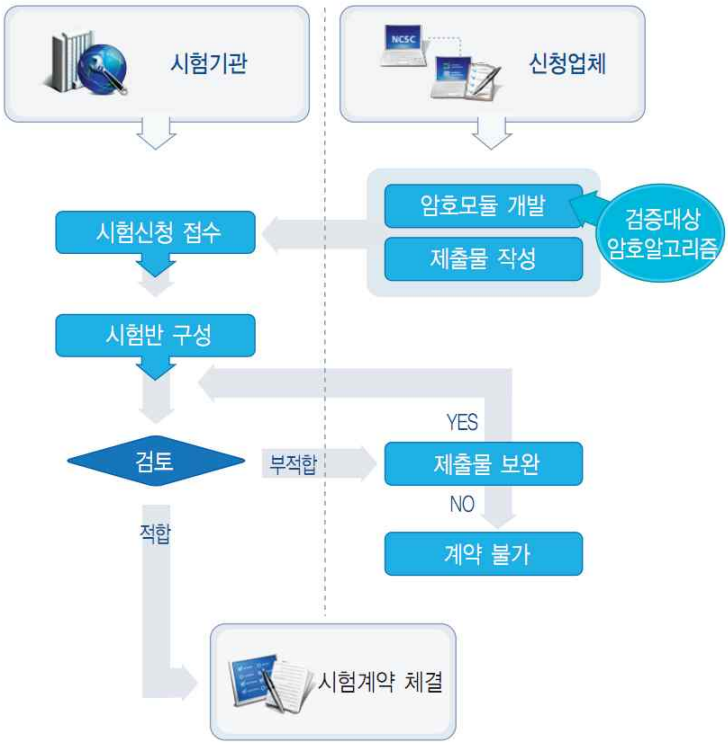
(Ex) 형상변경 사유
- 운영환경 변경
- 버그 발견
- 암호알고리즘 변경
- 암호모듈 이름/버전 변경
- 기타 사유로 인한 형상 변경

○ 또한 암호모듈 자체 및 소스코드 등의 형상은 변경되지 않았더라도 개발사의 이름 변경 등과 같이 암호모듈 정보가 변경되는 경우도 재검증을 신청해야 한다.

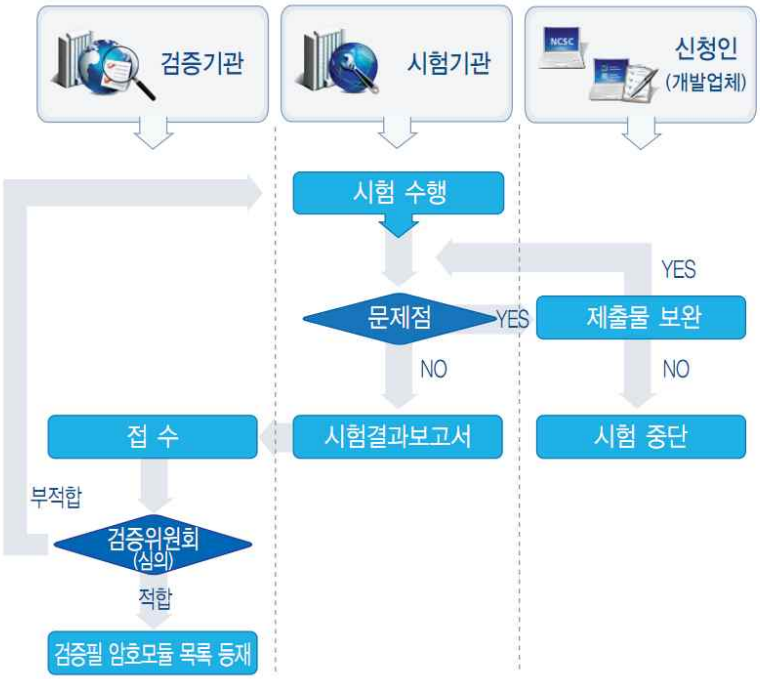
○ 암호모듈 재검증 제출물은 신규 검증 시의 제출물에 변경내역서가 추가된다. 변경내역서에는 검증을 획득한 암호모듈에서 형상이 변경된 부분과 변경된 부분이 영향을 미치는 보안요구사항에 대한 내용을 기술해야 한다. 기존 암호모듈 검증 시 제출했던 기본 및 상세설계서, 형상관리문서, 시험서, 암호모듈, 소스코드, 하드웨어 설계서도 변경된 형상을 반영하여 제출해야 한다.

【 참고사항 】

○ 암호모듈 시험신청 및 사전검토 절차



○ 암호모듈 시험 및 검증 절차



○ 검증유지 및 사후관리 절차

질의	보안요구사항 검증 범위
II-3	암호모듈 보안요구사항 영역에 대해 신청인 임의로 일부 영역만을 선택하여 검증받을 수 있는가?
요구사항	-

【 답변 】

○ 신청인이 암호모듈 보안요구사항 전체 영역 중 임의로 일부 영역만을 선택하여 검증받을 수는 없다.

○ 암호모듈은 각 영역에 대해 최소 보안등급 1의 보안요구사항을 만족해야 한다. 단, 암호모듈 형태에 따라 적용되지 않는 영역이 있다.

- 소프트웨어 암호모듈에는 물리적 보안 영역이 적용되지 않는다.

- 하드웨어나 펌웨어 암호모듈처럼 변경가능하지 않은 운영환경에서는 운영환경 영역이 적용되지 않는다.

○ 기타 공격에 대한 대응 영역은 암호모듈이 하나 또는 그 이상의 공격에 대한 대응이 의도적으로 설계 및 구현되었을 경우에만 적용된다. 단, 질의 III-11-1 답변에 명시된 공격에 대해서는 대응방법을 제공해야 한다.

○ 보안정책문서에는 암호모듈이 만족하는 전체 보안등급 및 영역별 보안등급을 표시한다. 영역별 보안등급에서 적용되지 않은 보안영역은 N/A(Not Applicable)로 표시한다.

【 참고사항 】

○ 암호모듈에 대한 보안요구사항은 암호모듈의 설계 및 구현에 관련된 영역으로 구성된다.

질의	검증필 암호모듈을 탑재한 신규 암호모듈 개발 시 검증
II-4	검증필 암호모듈을 탑재한 새로운 암호모듈을 구현하는 경우, 제출물의 종류와 만족해야 할 보안요구사항은 어떤 것이 있는가?
요구사항	-

【 답변 】

○ 검증필 암호모듈이 암호서비스를 제공하는 정보보호제품에 탑재되어 제품 형태의 암호모듈로 검증을 신청하는 경우는 암호모듈 신규 검증에 해당한다.

(Ex) 제품 형태의 암호모듈 : 메일 암호화, 구간 암호화, PKI, SSO, 디스크·파일 암호화, 키보드 암호화, 하드웨어 보안 토큰, DB 암호화, 기타 암호화 제품 등

○ 검증필 암호모듈은 신규 검증 신청하는 제품 형태 암호모듈의 구성요소 중 일부에 해당한다. 따라서 검증필 암호모듈을 탑재한 신규 암호모듈은 신청하는 보안등급의 보안요구사항을 만족할 수 있도록 구현해야 한다. 또한 질의 II-1 답변에 명시된 신규 검증에 해당하는 모든 제출물을 작성하여 제출해야 한다.

○ 제출물에는 탑재한 검증필 암호모듈에 대한 정확한 형상을 명세해야 한다.
또한 검증필 암호모듈에서 제공하는 암호 서비스를 신규 암호모듈에서 사용하고 있는 방식도 포함해야 한다.

(Ex) 라이브러리 형태의 검증필 암호모듈에서 제공하는 API 형태의 암호서비스를 사용하는 경우, 다음과 같은 사항을 포함해야 한다.
- 사용 암호알고리즘
- 동작모드 전환 여부
- 신규 암호모듈에서 암호 서비스를 사용하고 있는 위치
- API 호출 방식 및 파라미터 설정 방식 등

○ 검증필 암호모듈에서 제공하는 기능을 이용하여 신규 암호모듈의 보안요구사항을 만족하는 경우에는 해당 내용을 제출물에 명시하고 근거를 제시해야 한다.

(Ex) 암호알고리즘에 대한 KAT(Known Answer Test) 보안요구사항을 검증필 라이브러리 암호모듈에서 제공하는 KAT 기능으로 대체하는 경우

○ 시험기관은 신규 암호모듈에서 검증필 암호모듈을 적절히 사용하였는지 여부를 확인하기 위해 기존 검증필 암호모듈 검증 시의 제출물을 요구할 수 있다.

【 참고사항 】

○ 라이브러리 형태의 검증필 암호모듈을 사용하지 않고 제품 형태의 암호모듈 자체로도 암호모듈 검증을 신청할 수 있다.

○ 이때, 암호모듈의 경계는 암호모듈 전체로 설정되며, 질의 II-1 답변에 명시된 신규 검증에 해당하는 모든 제출물을 작성하여 제출해야 한다.

Ⅲ. 항목별 요구사항

Ⅲ-1. 암호모듈 명세

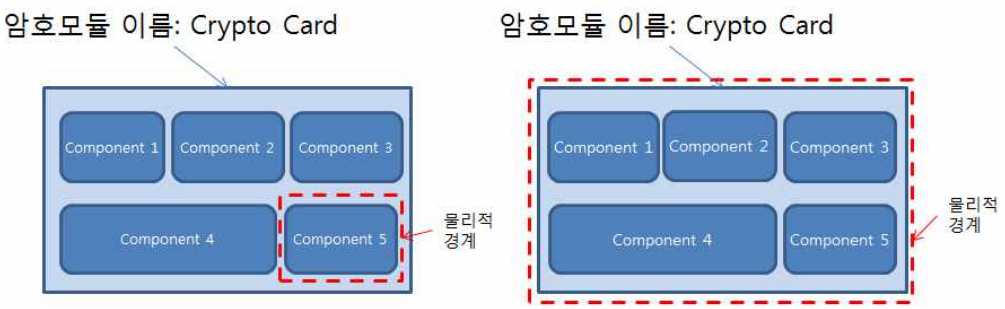
질의	암호모듈의 이름	
Ⅲ-1-1	정의된 암호경계와 암호모듈 이름은 어떠한 관계를 가져야 하는가?	
요구사항	KS X ISO/IEC 24759	AS01.06
	소프트웨어 암호모듈 검증기준	AS01.03

【 답변 】

○ 암호모듈은 암호경계 안에 암호모듈 관련 모든 구성요소가 포함되도록 해야 한다.

○ 제출물에 명시한 암호모듈 이름과 정의된 암호경계는 반드시 일치해야 한다. 암호모듈 이름이 정의된 암호경계보다 더 많은 컴포넌트를 포함하는 모듈을 지칭하는 것이라면 적합하지 않다.

(Ex) 암호모듈 이름은 Crypto Card로 되어 있고 암호경계는 카드 내부의 여러 컴포넌트 중 하나로 정의된다면 이 암호모듈 이름은 잘못된 것이다. 암호모듈 이름을 반드시 Crypto Card로 할 경우 암호경계는 카드 전체로 해야 한다.



[잘못된 암호모듈 이름] [올바른 암호모듈 이름]

질의	동작모드 전환 시 요구사항	
Ⅲ-1-2	검증대상 동작모드에서 비검증대상 동작모드로의 전환 또는 그 반대로의 동작모드 전환 시 요구사항은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS01.12, AS01.15
	소프트웨어 암호모듈 검증기준	AS01.05, AS01.07

【 개념 정리 】

○ 검증대상 동작모드 : 암호모듈에서 검증대상 암호알고리즘만으로 운영되는 모드

○ 비검증대상 동작모드 : 비검증대상 암호알고리즘을 운영할 수 있는 모드이며, 검증대상 암호알고리즘을 사용할 수도 있음

【 답변 】

○ 검증대상 동작모드에서 정의된 핵심보안매개변수는 비검증대상 동작모드에서 접근되거나 공유되지 않도록 해야 한다.

○ 검증대상 암호알고리즘이 비검증대상 동작모드에서 사용될 수 있으나 비검증대상 동작모드에서 생성된 키 혹은 사용된 암호알고리즘의 무결성이나 안전성을 보장하지는 않는다.

○ 검증대상 난수발생기는 비검증대상 동작모드에서 사용될 수 있으나 검증대상 동작모드에서 생성된 난수발생기의 내부 상태가 비검증대상 동작모드에서 접근되거나 공유되면 안 된다.

질의	다중 검증대상 동작모드	
Ⅲ-1-3	암호모듈이 다중 검증대상 동작모드를 구현할 수 있는가? 다중 검증대상 동작모드 운영 시 요구사항은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS01.12
	소프트웨어 암호모듈 검증기준	AS01.05

【 답변 】

○ 암호모듈이 하나의 검증대상 동작모드만으로 구현되도록 제한하지는 않는다.

○ 하나의 암호모듈은 다수의 검증대상 동작모드를 지원할 수 있다. 다수의 검증대상 동작모드를 지원할 경우, 아래 사항을 명세해야 한다.
- 각 검증대상 동작모드의 정의
- 각 검증대상 동작모드가 어떻게 구성되는지에 대한 설명
- 각 검증대상 동작모드가 지원하는 서비스들
- 각 검증대상 동작모드에서 사용할 수 있는 암호알고리즘들
- 각 검증대상 동작모드에서 사용하는 핵심보안매개변수
- 각 검증대상 동작모드에서 수행하는 자가시험

○ 하나의 검증대상 동작모드에서 다른 검증대상 동작모드로 전환하는 경우, 암호모듈은 반드시 초기화를 수행하고 새로운 동작모드와 관련된 전원인가 자가시험을 수행해야 한다.
- 선택한 검증대상 동작모드에서 사용되는 암호알고리즘들에 대한 전원인가 자가시험이 반드시 수행되어야 한다.
- 이전에 전원인가 자가시험을 수행했더라도 새로 선택한 검증대상 동작모드에 대한 전원인가 자가시험은 반드시 수행되어야 한다.

질의	암호모듈의 정의	
Ⅲ-1-4	소프트웨어 암호모듈, 펌웨어 암호모듈, 하이브리드 암호모듈은 어떻게 정의되는가?	
요구사항	KS X ISO/IEC 24759	AS01.01
	소프트웨어 암호모듈 검증기준	AS01.02

【 개념 정리 】

○ 암호모듈: 정의된 암호경계 내에 포함된 암호알고리즘과 키 생성을 포함하는 암호 함수와 프로세스를 동작시키는 하드웨어와 소프트웨어 및 펌웨어의 집합 형태

○ 운영환경: 암호모듈을 동작시키기 위해 필요한 소프트웨어, 펌웨어 및 하드웨어의 구성요소의 관리를 말하며, 변경 가능한 운영환경, 제한된 운영환경, 변경 불가능한 운영환경으로 분류됨

【 답변 】

○ 소프트웨어, 펌웨어 및 하이브리드 암호모듈의 다음과 같이 정의할 수 있다.

구 분	정의
소프트웨어 암호모듈	- 암호경계 내에 하나 또는 그 이상의 소프트웨어 컴포넌트로 구성 - 운영환경: 변경가능 형태
펌웨어 암호모듈	- 암호경계 내에 하나 또는 그 이상의 펌웨어 컴포넌트로 구성 - 운영환경: 제한된 운영환경 혹은 변경 불가능한 형태
하이브리드 암호모듈	- 특별한 목적의 분리된 암호 하드웨어(예: 하드웨어 가속카드, 하드웨어 칩 등)와 이를 활용하는 소프트웨어 혹은 펌웨어 암호모듈로 구성 • 하드웨어 + 소프트웨어 = 하이브리드 소프트웨어 모듈 - 소프트웨어 운영환경: 변경가능 형태 • 하드웨어 + 펌웨어 = 하이브리드 펌웨어 모듈 - 펌웨어 운영환경: 제한된 운영환경 혹은 변경 불가능한 형태

○ 하이브리드 암호모듈은 보안등급 1이며, 보안등급 1의 요구사항만을 만족하면 된다.

○ 소프트웨어 혹은 펌웨어 암호모듈에 적용되는 요구사항에 추가하여, 다음의 요구사항이 하이브리드 암호모듈에 적용되어야 한다.

요구사항	내 용
암호모듈 명세	- 하이브리드 암호모듈의 모든 구성요소에 대한 명세 (부품번호, 버전번호, 운영체제 등)
암호모듈 포트와 인터페이스	- 하이브리드 암호모듈의 모든 상태와 제어 포트, 그리고 인터페이스에 대한 명세 • (소프트웨어 모듈일 경우) 소프트웨어 구성요소와의 인터페이스 • (펌웨어 모듈일 경우) 펌웨어 인터페이스와의 인터페이스
역할, 서비스와 인증	- 하이브리드 암호모듈의 구성요소가 제공하는 모든 서비스
물리적 보안	- 하드웨어 컴포넌트가 하이브리드 구성의 한 부분으로 정의되기 때문에 물리적 보안의 요구사항 적용
운영환경	- 하이브리드 소프트웨어 모듈인 경우에는 운영환경의 요구사항 적용
암호 키 관리	- 운영 플랫폼의 경계 내에서 교환되는 키 그리고 하이브리드 암호모듈의 컴포넌트들 간에 교환되는 키는 평문 형태로 이동될 수 있다.
자가시험	- 하이브리드 암호모듈의 모든 컴포넌트에 자가시험 요구사항 적용 • 소프트웨어 무결성 시험: 소프트웨어 컴포넌트 적용 • 펌웨어 무결성 시험: 적용 가능한 특별한 목적의 펌웨어 구성요소 적용 • 전원인가 혹은 조건부 시험: 적용 가능한 모든 컴포넌트 적용

질의	커널 암호모듈 요구사항	
Ⅲ-1-5	커널모드에서 동작하는 암호모듈의 경우, 유저모드와 다르게 적용되는 요구사항은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS01.15
	소프트웨어 암호모듈 검증기준	AS01.07

【 개념 정리 】

○ 유저모드 : 응용프로그램 각각에 독립적인 가상 주소 공간을 제공하며, 응용프로그램이 다른 응용프로그램의 데이터를 변경할 수 없음

○ 커널모드 : 커널모드에서 동작하는 모든 코드는 하나의 가상 주소 공간을 공유하며, 잘못된 가상 주소에 데이터를 쓰게 되면 다른 드라이버나 운영체제가 손상될 수 있음

【 답변 】

○ 소프트웨어 암호모듈은 실행 레벨에 따라 커널모드와 유저모드로 구분할 수 있다.

○ 암호모듈은 노출이나 변경 시 암호모듈의 안전을 손상시킬 수 있는 핵심보안매개변수(비밀키, 개인키 및 인증데이터 등)에 대한 보호 방법을 제공해야 한다.

○ 커널모드에서 동작하는 암호모듈은 핵심보안매개변수와 그 밖의 보안에 영향을 미치는 모든 데이터에 대한 보호 방법을 제시해야 한다.

(EX) 인가되지 않은 커널 모듈 혹은 커널 쓰레드가 해당 암호모듈의 핵심보안매개변수 및 주요 데이터에 접근하는 것을 막는 방법 등

Ⅲ-2. 암호모듈 포트와 인터페이스

질의	입력 인터페이스 구분	
Ⅲ-2-1	논리적 인터페이스에서 데이터 입력과 제어 입력이 어떻게 구분되는가?	
요구사항	KS X ISO/IEC 24759	AS02.02, AS02.03, AS02.04, AS02.07
	소프트웨어 암호모듈 검증기준	AS02.01, AS02.02

【 답변 】

○ 암호모듈의 정보흐름과 물리적 접근지점은 모든 입·출구를 명세하고 있는 물리적 포트와 논리적 인터페이스로 제한되어야 한다.

○ 논리적 인터페이스는 정보의 종류와 정보의 흐름에 따라 4개의 인터페이스(데이터 입력, 데이터 출력, 제어 입력, 상태 출력)로 정의될 수 있다.

○ 데이터 입력과 제어 입력은 대상이 되는 값에 따라 다음과 같이 구분할 수 있다.

구분	입력값의 정의
데이터 입력	- 암호모듈에서 처리하는 평문/암호문 데이터, 핵심보안 매개변수 등
제어 입력	- 암호모듈을 동작하기 위한 입력 명령, 신호 및 제어 데이터 (함수 호출 및 키보드와 같은 수동 제어 포함)

○ 제어 입력과 데이터 입력의 논리적 인터페이스는 물리적/논리적으로 공유될 수 있다. 하지만 제어 입력으로는 외부의 물리적인 수동 제어 장치(예: 버튼, 스위치 등)가 사용될 수 있으므로 논리적 인터페이스는 데이터 입력과 분리될 수 있다.

질의	단절된 상태의 정의	
Ⅲ-2-2	키 관리에서 키 생성, 키 주입 및 키 제로화의 수행은 암호모듈 출력 데이터 경로와 논리적으로 단절된 상태에서 진행되어야 한다고 하는데 단절된 상태 요구사항은 어떻게 정의될 수 있는가?	
요구사항	KS X ISO/IEC 24759	AS02.13
	소프트웨어 암호모듈 검증기준	-

【 답변 】

○ 암호모듈의 데이터를 출력하는 물리적, 논리적 경로는 키 생성, 키 주입, 키 제로화를 수행하는 프로세스로부터 논리적 또는 물리적으로 단절되어 있어야 한다.

○ 출력 데이터와 키 정보가 전달되는 물리적, 논리적 경로가 물리적으로 공유되는 경우, 암호모듈이 출력데이터와 키 정보를 논리적으로 분리해야 한다.

○ 암호모듈은 키 생성, 키 주입, 키 제로화 시 키 정보를 출력 데이터 경로로 전달하는 것을 허용하지 않아야 한다. 또한 암호모듈로부터의 출력 데이터가 키 생성, 키 주입, 키 제로화를 방해하는 것을 허용하지 않아야 한다.

질의	데이터 출력 금지에 대한 명세방법	
Ⅲ-2-3	암호모듈의 데이터 출력 금지를 수행하는 절차를 명세할 때 소스코드 혹은 의사코드를 포함해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS02.06
	소프트웨어 암호모듈 검증기준	AS02.02

【 답변 】

○ 암호모듈은 오류 상태, 자가시험 상태에서 데이터 출력이 금지되어야 한다.

○ 오류 상태 및 자가시험 상태에서 데이터가 출력되지 않음을 명시하고, 출력되지 않는 방법을 서술하기 위해 소스코드 또는 의사코드를 포함해야 한다.

○ 데이터 출력에 대한 요구사항은 자가시험 항목에서도 적용된다.

요구사항	KS X ISO/IEC 24759	소프트웨어 암호모듈 검증기준
오류 상태에서의 데이터 출력 금지	AS08.06	AS 07.03
자가시험 상태에서의 데이터 출력 금지	AS08.11	-

질의	신뢰된 경로의 명세방법	
Ⅲ-2-4	암호모듈이 직접 통제하지 않는 환경에서의 신뢰된 경로(trusted path)는 어떻게 명세하면 되는가?	
요구사항	KS X ISO/IEC 24759	AS02.16, AS02.17
	소프트웨어 암호모듈 검증기준	AS02.01, AS02.02

【 개념 정리 】

○ 신뢰된 경로 : 사용자가 신뢰를 가지고 통신할 수 있는 수단 또는 메커니즘

【 답변 】

○ 키 설정 등이 구현되어 있지 않은 암호모듈에서 출력되거나 입력되는 핵심보안매개변수들은 신뢰된 경로로 보호하여야 한다.

○ 보안등급 1과 2에서는 신뢰된 경로의 요구사항이 없으며, 보안등급 3과 4는 다음과 같은 요구사항을 명시하고 있다.
- 송수신 암호모듈 간 보호되지 않는 평문의 핵심보안매개변수, 키 구성요소, 인증데이터 등을 신뢰된 경로로 전송해야 한다.
- 신뢰된 경로는 통신 연결 상의 허용되지 않은 수정, 변조, 노출 등을 방지해야 한다.
- 물리적 포트는 다른 모든 물리적 포트로부터 분리되어야 하며, 논리적인 포트는 다른 암호모듈이 사용하는 모든 논리적 포트로부터 분리되어야 한다.
- 신뢰된 경로가 사용 중일 경우 사용 상태 여부를 알 수 있는 정보를 제공해야 한다.

○ 보안등급 3과 4의 암호모듈이 신뢰된 경로 메커니즘을 평문 핵심보안매개변수 입출력을 위해 이용할 경우, 제출물에는 다음과 같은 내용을 명시하여야 한다.
- 송수신 암호모듈간의 신뢰된 경로에 대한 명세
- 신뢰된 경로의 특성에 대한 명세
- 신뢰된 경로의 운영 및 설정을 위한 명령에 대한 명세
- 신뢰된 경로를 유지하기 위해 사용되는 제어에 대한 명세

Ⅲ-3. 역할, 서비스 및 인증

질의	역할구분	
Ⅲ-3-1	역할을 반드시 관리자와 사용자로 구분해야 하는가? 즉, 관리자 모드의 역할을 사용자 역할에서 수행하면 안 되는가?	
요구사항	KS X ISO/IEC 24759	AS03.03
	소프트웨어 암호모듈 검증기준	AS03.02

【 개념 정리 】

○ 역할 : 암호모듈에서 제공하는 서비스에 대한 사용자 접근권한 또는 접근통제를 정의한 것

○ 사용자 : 암호 기능과 검증대상 암호알고리즘을 포함한 일반적인 보안 서비스를 수행하는 역할

○ 관리자 : 암호 초기화를 수행하거나 암호모듈의 초기화, 암호키 및 핵심보안 매개변수 입출력 등과 같은 기능을 관리하는 역할

【 답변 】

○ 암호모듈은 운영자에게 인가된 역할과 각 역할에 상응하는 서비스를 제공해야 한다.

○ 암호모듈에서는 사용자 역할과 관리자 역할을 구분하여 정의해야 한다. 그러나 암호모듈의 형태, 설치방법 등에 의해 사용자 역할만 정의하는 것도 가능하며, 이때 사용자가 관리자 역할까지 수행하는 합당한 근거를 제시하여야 한다.

【 참고사항 】

○ 라이브러리 형태의 암호모듈의 경우 사용자가 관리자의 역할을 동시에 수행할 수 있으므로 역할을 구분할 필요가 없다.

질의	인증기능 제공 여부	
Ⅲ-3-2	암호모듈 자체적으로 인증 기능을 반드시 제공해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS03.28
	소프트웨어 암호모듈 검증기준	AS03.07, AS03.08

【 개념 정리 】

○ 역할기반 인증 : 운영자에 의해 선택된 역할에 대한 인증을 수행하는 것

○ 신원기반 인증 : 운영자의 개별적인 신원 식별을 통해 인증을 수행하는 것

【 답변 】

○ 보안등급 1에서는 암호모듈 접근통제를 위해 인증 기능을 사용하지 않아도 된다. 보안등급 2 이상의 암호모듈의 경우에는 필수적으로 인증 기능을 제공해야 한다.

○ 보안등급 1에서 운영체제에서 제공하는 인증 기능을 이용하는 경우, 운영체제를 이용하여 운영자 인증 기능을 제공하는 방식을 제출물에 명세하여야 한다.

질의	복수운영자	
Ⅲ-3-3	복수운영자는 단일운영자와 어떻게 구분되는가?	
요구사항	KS X ISO/IEC 24759	AS03.02
	소프트웨어 암호모듈 검증기준	AS03.01

【 개념 정리 】

○ 운영자 : 암호모듈에 접근하는 개인 또는 개인을 대신하여 작동하는 프로세스를 말하며, 맡겨진 역할과는 관계없음

【 답변 】

○ 단일운영자는 암호모듈에 접근하는 운영자가 유일한 경우를 지칭한다. 즉, 운영체제에 복수의 운영자가 존재하지 않고, 유지보수 등의 관리자 역할을 수행하기 위한 별도의 운영자도 존재하지 않는 경우를 말한다.

○ 복수운영자는 암호모듈에 접근하는 운영자가 다수인 경우를 지칭한다.

(Ex) 암호모듈에 사용자 역할의 운영자와 암호 관리자 역할의 운영자가 존재하는 경우를 복수운영자라고 볼 수 있다.

○ 복수운영자가 동시에 암호모듈을 이용하는 것이 지원되는 경우, 암호모듈은 내부적으로 각 운영자의 역할과 이에 상응하는 서비스를 분리하여 유지해야 한다.

【 참고사항 】

○ 암호모듈에서 복수의 운영자가 동시에 암호모듈 사용을 지원하는 경우, 신청인은 제출물에 각 운영자의 역할 및 제공 서비스를 구분하는 방법을 명세해야 한다.

○ 단일운영자 모드로 운영되는 암호모듈인 경우, 제출물에 운영환경별로 단일운영자 환경을 설정하는 방법을 명세해야 한다.

질의	우회기능	
Ⅲ-3-4	우회기능의 정확한 의미와 우회기능이 존재해도 문제가 없는 경우는 어떠한 경우인가?	
요구사항	KS X ISO/IEC 24759	AS03.11, AS03.12
	소프트웨어 암호모듈 검증기준	AS03.04

【 개념 정리 】

○ 우회기능 : 암호처리 없이 작동 가능한 서비스

(Ex) 암호모듈로부터 입·출력되는 데이터에 대해 암호화를 수행하지 않고 평문 형태로 전송하는 서비스

【 답변 】

○ 암호모듈에는 원칙적으로 우회기능 존재를 허용하지 않는다. 하지만 암호모듈에는 필요에 의해 우회기능을 탑재할 수 있으며, 이러한 경우 신청인은 제출물에 암호모듈에 대한 모든 우회기능을 명세해야 하고, 해당 기능이 필요한 근거와 상세한 기능 및 동작에 대해서 명세하여야 한다.

○ 백도어 같은 공식적으로 허용되지 않은 기능은 우회기능에 속하지 않는다.

【 참고사항 】

○ 허용 가능한 우회기능으로 라우터의 우회기능을 설명할 수 있다.

(Ex) 라우터와 같은 경우 우회기능이 존재하는 암호모듈에 해당한다. 라우터의 동작 중에서 목적지 주소(IP)가 없는 패킷이 수신되었을 경우 패킷을 처리하지 않고 default gateway로 패킷을 전달(re-direct)하는 기능이 있으며, 이러한 기능이 암호모듈의 암호화를 우회하는 기능에 포함될 수 있다.

질의	핵심보안매개변수 통제	
Ⅲ-3-5	라이브러리 암호모듈의 경우, 어떠한 방식으로 핵심보안매개변수에 대한 접근을 통제할 수 있는가?	
요구사항	KS X ISO/IEC 24759	AS03.14
	소프트웨어 암호모듈 검증기준	AS03.06

【 개념 정리 】

○ 핵심보안매개변수 : 노출되거나 변경되면 암호모듈의 보안을 손상시킬 수 있는 보안관련 정보

(Ex) 비밀키/개인키, 패스워드나 개인식별번호와 같은 인증 데이터

【 답변 】

○ 라이브러리 형태의 암호모듈의 경우 메모리상에 존재하는 핵심보안매개변수에 대해 다른 프로세스들이 접근하지 못하도록 운영체제에서 접근을 통제하고 관리하는 방법이 가능하다.

(Ex) 운영체제는 프로세스별로 가상 메모리 공간을 할당하여 프로세스 간 메모리 영역을 침범하지 못하도록 할 수 있다.

○ 암호모듈이 실행중이거나 운영되는 동안 다른 프로세스에서 핵심보안매개변수에 접근하지 못하도록 해야 하며, 운영체제가 제공하는 접근통제 방식에 대해서 제출물에 명세해야 한다.

Ⅲ-4. 유한상태모델

질의	유한상태 모델 요구사항	
Ⅲ-4-1	유한상태모델은 무엇을 의미하며, 유한상태모델에서 요구되는 최소 정보는 어떠한 것인가?	
요구사항	KS X ISO/IEC 24759	AS04.01, AS04.02
	소프트웨어 암호모듈 검증기준	AS04.01

【 개념 정리 】

○ 유한상태모델 : 순차적인 기계의 수학적 모델로서 구성요소는 다음과 같음
- 유한한 입력 사건의 집합
- 유한한 출력 사건의 집합
- 상태 집합과 입력 집합을 출력 집합으로 대응시키는 함수
- 상태 집합과 입력 집합을 상태 집합으로 대응시키는 함수
- 초기 상태를 설명하는 명세서

【 답변 】

○ 유한상태모델은 암호모듈의 기능과 동작에 대한 일반적인 명세로써 상태천이도 및 상태천이표로 표현해야 한다.

○ 유한상태모델은 최소한 다음과 같은 암호모듈의 동작상태와 오류상태를 포함해야 한다.
- 전원 켜짐/꺼짐 상태
- 암호관리자 상태
- 핵심보안매개변수 주입 상태
- 사용자 상태(역할 상태 등)
- 자가시험 상태
- 오류 상태
- 우회 상태(추가 정보)
- 유지보수 상태(추가 정보)

○ 소프트웨어 암호모듈의 경우, 메모리에 적재되는 순간부터 정상적인 동작을 완료하여 종료되는 시점까지 동작에 따른 상태를 모두 표현해야 한다.
(소프트웨어 암호모듈의 경우 메모리에 로드된 상태가 전원켜짐 상태임)

○ 오류 상태는 단순 오류와 심각한 오류 상태로 구분하여 정의하고 해당하는 오류에 따른 천이 동작을 표현하고 명세해야 한다.

【 참고사항 】

○ 암호모듈이 실제적으로 동작하는 상태천이에 근거하여 상태천이도를 작성해야 하며, 상태천이표에는 각각의 상태천이에 대해서 상세하게 명세하여야 한다. 또한 상태천이도와 상태천이표의 정보는 서로 일치하여야 한다.

○ 상태천이는 임의의 상태에서 동작 완료 후 자동으로 천이되는 경우와 그렇지 않은 경우로 구분하여 표시해야 한다.

질의	단순 오류의 종류	
Ⅲ-4-2	오류는 단순한 오류와 심각한 오류로 구분하며, 심각한 오류를 제외한 모든 오류는 복구 가능해야 한다고 명시되어 있다. 단순한 오류 상태가 어떠한 것들이 존재하는가?	
요구사항	KS X ISO/IEC 24759	AS04.03
	소프트웨어 암호모듈 검증기준	AS04.02

【 답변 】

○ 단순한 오류는 암호모듈의 수정 또는 재설치 등의 절차를 수행하지 않고 암호모듈 재시동 등의 동작에 의해 복구가 가능한 오류로 다음과 같은 경우가 해당한다.

- 응용프로그램 등에서 운용상의 잘못으로 외부 API로 잘못된 값을 전달하여 암호모듈에서 발생하는 오류
- 암호모듈의 현재 상태가 검증대상 동작모드라고 가정할 때 비검증대상 암호알고리즘에 대한 처리 요청이 입력될 경우 발생하는 오류

○ 심각한 오류는 암호모듈의 암호동작 실패 등과 같이 복구가 불가능한 심각한 문제가 발생한 상태로 다음과 같은 경우가 해당한다.

- 암호알고리즘 동작 실패
  (Ex) 블록암호 알고리즘의 동작이 수행되지 않는 오류발생 또는 암호알고리즘에서 잘못된 연산을 수행하는 경우 등
- 암호알고리즘 시험 실패
- 무결성 시험 실패
- 연속적인 난수발생기 시험 실패 등

질의	초기화 후 동작모드	
Ⅲ-4-3	유한상태모델에는 검증대상 동작모드와 비검증대상 동작모드가 있는데, 암호모듈이 초기화가 성공하면 어떤 동작모드로 시작해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS04.01
	소프트웨어 암호모듈 검증기준	AS04.01

【 개념 정리 】

○ 검증대상 동작모드 : 암호모듈에서 검증대상 암호알고리즘만으로 운영되는 모드

○ 비검증대상 동작모드 : 비검증대상 암호알고리즘을 운영할 수 있는 모드이며, 검증대상 암호알고리즘을 사용할 수도 있음

【 답변 】

○ 국가·공공기관 정보통신망에서 중요 정보의 보호를 위해 사용되는 암호모듈은 검증대상 동작모드로 시작되는 것을 기본 전제로 한다.

○ 검증대상 동작모드와 비검증대상 동작모드가 혼재하는 암호모듈의 경우 반드시 검증대상 동작모드로 초기 시동한 후 필요시 비검증대상 동작모드로 전환되어야 한다.

【 참고사항 】

○ 검증대상 동작모드와 비검증대상 동작모드가 혼재하는 암호모듈의 경우 검증대상 동작모드로 동작하고 있는 상태에서는 비검증대상 암호알고리즘이 수행되지 않도록 보호조치를 취해야 한다.

○ 검증대상 동작모드에서 비검증대상 동작모드로의 전환 시 모든 핵심보안매개변수에 대한 보호조치(예 : 핵심보안매개변수 초기화 등) 완료 후 동작모드가 전환되어야 한다.

질의	상태천이도와 상태천이표	
Ⅲ-4-4	암호모듈의 유한상태모델에서 상태천이도와 상태천이표가 반드시 필요한가?	
요구사항	KS X ISO/IEC 24759	AS04.01, AS04.02
	소프트웨어 암호모듈 검증기준	AS04.01

【 개념 정리 】

○ 상태천이도 : 암호모듈이 실제 동작함에 있어 변화가 발생하는 상태에 대해서 블록도 형태로 나타내는 것

○ 상태천이표 : 암호모듈이 실제 동작함에 있어 임의의 상태에서 다른 상태로 천이되는 과정 중에서 현재 상태, 입·출력동작, 그리고 입·출력에 따른 다음 상태로의 천이 동작에 대한 설명을 표 형태로 명세한 것

【 답변 】

○ 암호모듈의 동작은 상태천이도 및 상태천이표에 의해 표현되는 유한상태모델을 사용하여 명세해야 한다.

○ 상태천이도와 상태천이표는 다음과 같은 내용을 포함해야 한다.
- 암호모듈의 모든 동작상태(검증대상 및 비검증대상 동작모드 포함)와 오류 상태
- 임의의 상태에서 다른 상태로의 천이
- 임의의 상태에서 다른 상태로의 천이를 유발하는 입력
- 임의의 상태에서 다른 상태로의 천이에 따라 발생하는 출력

(Ex) 상태천이표 예시

현재상태	입력	출력	다음상태
전원꺼짐	전원 켬	출력없음	전원 켜짐

○ 상태천이도에서의 천이동작은 다음과 같이 두 가지로 구분한다

구분	내용
자동천이	임의의 상태에서의 동작 결과로 자동적으로 다른 상태로 천이 (Ex) 전원인가 상태에서 전원인가자가시험 상태로의 자동천이)
일반천이	운영자 등이 개입하여 임의로 변경되는 상태천이 (Ex) 검증대상 동작모드에서 비검증대상 동작모드로 천이)

【 참고사항 】

○ 상태천이도와 상태천이표의 정보는 반드시 서로 일치하여야 하며, 암호모듈의 동작과도 일치하도록 작성하여야 한다.

Ⅲ-5. 물리적 보안

질의	탐침 및 불투명	
Ⅲ-5-1	보안등급 2 수준의 불투명도는 어느 정도를 준수해야 하는가? 보안등급 2에서 탐침에 대한 요구사항이 필요한가?	
요구사항	KS X ISO/IEC 24759	AS05.48
	소프트웨어 암호모듈 검증기준	-

【 개념 정리 】

○ 불투명: 가시광선 영역의 인공적인 빛을 이용하여 가시적으로 관찰을 하여 제조 모델 넘버나 디자인 정보 등을 알아내지 못하는 것

○ 가시광선 파장 영역: 파장이 400nm에서 750nm에 해당함

【 답변 】

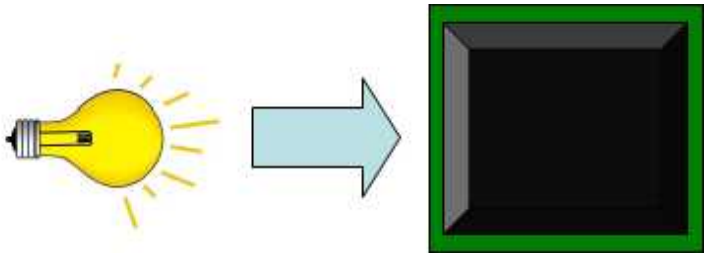
○ 하드웨어 암호모듈은 일반적으로 냉각을 위한 목적으로 팬, 환기, 구멍 등을 만든다. 이러한 것을 통해 암호모듈의 내부를 보기 위한 탐침이 가능한 공간이 생길 수 있다.

○ 불투명에 관한 요구사항은 암호모듈 내부의 구성물과 설계 정보에 대해 직접 관찰하지 못하도록 하기 위함이다

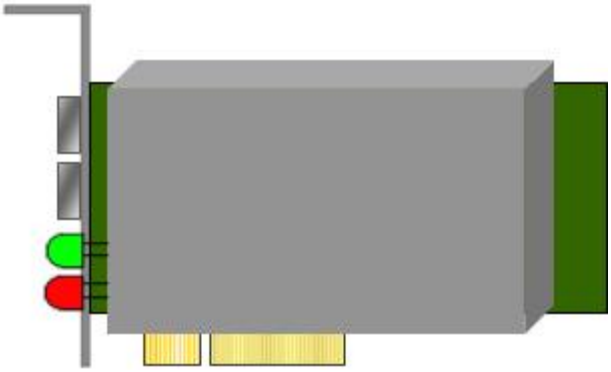
○ 탐침에 대한 요구사항은 보안등급 2에는 적용되지 않으며, 통풍구, 틈새 등을 통한 탐침에 대한 요구사항은 보안등급 3에 해당한다.

○ 다음은 보안등급 2 다중 칩 단독 암호모듈의 물리적 보안 요구사항이다.
- 암호모듈은 금속이나 견고한 플라스틱 재질의 외장 내에 전체가 포함되어야 한다.
- 외장에 탈착식 덮개나 문이 있을 수 있다.
- 외장은 가시광선 영역에서 불투명해야 한다.

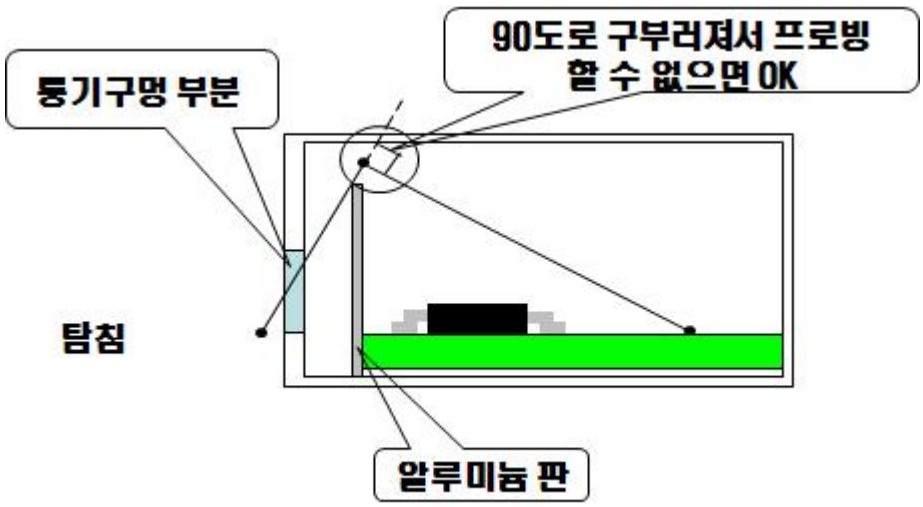
(Ex) 불투명 재료 사용: 에폭시 수지로 코팅되어 있어 불투명함



(Ex) 불투명한 외피: 암호모듈은 두께 2mm 알루미늄판으로 둘러싸여 있어 불투명함



(Ex) 물리적 탐침 방지 구조: 통풍구에 프로빙 방지 위한 알루미늄 판 설치



질의	탬퍼 증거 보호막	
Ⅲ-5-2	탬퍼(Tamper, 불법조작) 증거 보호막의 요구사항은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS05.37
	소프트웨어 암호모듈 검증기준	-

【 답변 】

○ 암호모듈이 탬퍼 증거 보호막을 이용할 경우에는 보호막이 불법 조작 증거 없이 제거되거나, 제거된 이후에 다시 부착이 불가능해야 한다.

○ 탬퍼 증거 없이 보호막 제거가 가능하고, 같은 보호막을 다시 적용할 수 있다면 탬퍼 증거 보호막 시험에 실패한 것이다.

○ 반대의 경우 임의의 조작으로 보호막을 제거하여 그 증거가 남거나, 다시 보호막을 적용할 때 증거를 남겼을 경우에는 탬퍼 증거 보호막 시험을 통과한 것이다.

(Ex) 탬퍼 증거 보호막 방법: 에폭시 수지로 코팅되어 있으며, 암호모듈에 대한 공격 시도는 긁힌 흔적이나 변형 등의 불법조작 증거를 생성함

질의	물리적 보안 가정사항	
Ⅲ-5-3	각 보안등급별 물리적 보안요구사항에서 정의하는 보호 방법, 공격 타입 그리고 운영자 역할 등에 대한 가정사항은 무엇인가?	
요구사항	KS X ISO/IEC 24759	-
	소프트웨어 암호모듈 검증기준	-

【 답변 】

○ 각 보안등급별 물리적 보안요구사항에는 공격 타입 및 운영자 역할 등이 가정되어 있다. 특히 보안등급이 높을수록 공격에 대한 강도가 높다고 가정한다.

○ <u>보안등급 1</u>

구 분	내 용
보호수준	- 핵심보안매개변수에 대한 물리적 보호 방법이 없음 (접근이 가능하다고 가정) □ 하드웨어: 각 구성요소의 탐침 및 관찰이 가능하다고 가정 □ 소프트웨어: 운영환경, 응용프로그램 그리고 데이터에 접근이 가능하다고 가정
사용자(운영자) 가정사항	- 검증대상 암호 서비스와 보안기능이 정상 동작한다고 가정 - 공격자는 암호모듈 내부에 있는 핵심보안매개변수와 데이터(평문, 암호문)에 접근한다고 가정 - 운영자가 모듈의 물리적 방어의 책임이 있다고 가정
공격 가능 형태	- 핵심보안매개변수와 데이터에 대한 직접적인 접근을 위한 수동적 공격
공격 특성 및 시험 가정사항	- 암호모듈에 대한 사전 접근은 없다고 가정 - 공격도구나 재료에 대해 필요가 없다고 가정
안전한 운영조건	- 암호모듈은 보안기능 및 서비스를 올바르게 제공해야 함 - 핵심보안매개변수 평문, 데이터의 방어는 암호모듈 운영자가 제공해야 함 - 암호모듈이 보호되지 않는 환경에서 사용되면, 그 암호모듈은 보호되지 않는 핵심보안매개변수, 평문 혹은 데이터를 가지고 있거나 유지해서는 안 됨

○ 보안등급 2

구 분	내 용
보호수준	- 불법 침입 증거 관찰이 가능해야 함 - 암호모듈의 물리적 경계는 직접적인 내부 보안 구성요소 관찰을 막기 위해 불투명해야 함 □ 하드웨어: 탐침이 가능하다고 가정 □ 소프트웨어: 보호되지 않은 핵심보안매개변수 그리고 데이터의 논리적 접근 보호가 EAL2에 따라 평가된 OS에 의해 제공
사용자(운영자) 가정사항	- 검증대상 암호 서비스와 보안기능은 정확히 동작하고 있다고 가정 - 공격자는 암호모듈 내부에 있는 핵심보안매개변수와 데이터(평문, 암호문)에 접근한다고 가정 - 운영자가 모듈의 물리적 방어의 책임이 있다고 가정
공격 가능 형태	- 핵심보안매개변수와 데이터에 대한 즉각적인 접근을 위한 능동적 공격
공격 특성 및 시험 가정사항	- 암호모듈에 대한 사전 접근은 없다고 가정 - 저가의 도구나 재료는 공격할 시점에 준비되어 있다고 가정 - 공격시간은 짧다고 가정
안전한 운영조건	- 암호모듈은 보안기능 및 서비스를 올바르게 제공해야 함 - 핵심보안매개변수 평문, 데이터 방어는 암호모듈 운영자가 제공해야 함 - 운영자는 불법 침입 증거로 내부 정보가 노출된 것에 대해서 인지해야 함 - 암호모듈이 무방비 환경에서 사용되어지면, 그 암호모듈은 보통 또는 높은 수준의 중요도를 갖는 핵심보안매개변수, 평문 혹은 데이터를 가지고 있거나 유지해서는 안됨

○ 보안등급 3

구 분	내 용
보호수준	- 불법 침입 증거 관찰 가능 - 암호모듈의 물리적 경계는 직접적인 내부 보안 구성요소 관찰을 막기 위해 불투명해야함 - 직접적인 침입, 탐침 공격 예방 - 불법 조작에 강한 견고한 뚜껑 혹은 외피 방벽 재료 사용 - 가능하다면 문이나 뚜껑이 열렸을 경우 능동적인 제로화 기능 □ 소프트웨어: 보호되지 않은 핵심보안 매개변수 그리고 데이터의 논리적 접근 보호가 EAL3에 따라 평가된 OS에 의해 제공

사용자(운영자) 가정사항	- 검증대상 암호 서비스와 보안기능은 정확히 동작하고 있다고 가정 - 핵심보안매개변수와 데이터(평문, 암호문)에 접근하는 직접적이지 않은 공격이 암호모듈에 시도되고 있다고 가정
공격 가능 형태	- 핵심보안매개변수와 데이터에 대한 즉각적인 접근을 위한 중간 수준의 강력한 공격
공격 특성 및 시험 가정사항	- 암호모듈에 대한 사전의 접근과 기본 지식이 있다고 가정 - 공격을 위한 도구와 재료가 미리 준비되어 있다고 가정 - 실제 공격 시간은 보통으로 가정함 (우선적인 접근 및 모듈의 기본적인 지식을 획득하기 위한 시간은 포함되지 않음)
안전한 운영조건	- 암호모듈은 보안기능 및 서비스를 올바르게 제공해야 함 - 핵심보안 매개변수 평문, 데이터 방어는 암호모듈 운영자(예, 모듈이 사용되는 환경) 그리고 암호모듈의 물리적 보호 메카니즘(예, 견고한 외장, 불법 침입 반응 커버와 문, 탐침 방지)에 의해 제공되어야 함 - 운영자는 불법 침입 증거로 내부 정보가 노출된 것에 대해서 인지해야함 - 공격은 사전에 계획되었지만 보통의 난이도를 가짐 - 암호모듈이 무방비 환경에 사용되는 경우 암호모듈은 높은 수준의 중요도를 갖는 핵심보안매개변수, 평문 혹은 데이터를 가지고 있거나 유지해서는 안 됨

○ <u>보안등급 4</u>

구 분	내 용
보호수준	- 불법 침입 증거 관찰 가능 - 암호모듈의 물리적 경계는 직접적인 내부 보안 구성요소 관찰을 막기 위해 불투명해야함 - 직접적인 침입, 탐침 공격 예방 - 불법 조작에 강한 견고한 뚜껑 혹은 외피 방벽 재료 사용 - 가능하다면, 문이나 뚜껑이 열렸을 경우 능동적인 제로화 기능 - 허가되지 않은 암호모듈에 대한 물리적 접근을 방어하기 위한 완전한 외장 필요 - 암호모듈의 외장 보안이 뚫리는 경우 즉각적인 핵심보안매개변수 평문의 제로화 또는 암호모듈의 동작이 불가능하도록 조치 - 직접적이지 않은 공격 방어 □ 소프트웨어: 보호되지 않은 핵심보안매개변수 그리고 데이터의 논리적 접근 보호가 EAL4에 따라 평가된 OS에 의해 제공

사용자(운영자) 가정사항	- 검증대상 암호 서비스와 보안기능은 정확히 동작하고 있다고 가정 - 암호모듈은 검증기준에 정의된 모든 물리적 공격의 불법 침입에 대해서 보호되어야 함
공격 가능 형태	- 핵심보안매개변수와 데이터에 대한 즉각적인 접근을 위한 강력한 공격
공격 특성 및 시험 가정사항	- 암호모듈에 대한 사전 접근과 기본 지식이 있다고 가정 - 공격을 위한 전문 도구와 재료가 준비되어 있다고 가정 - 온도 및 전압 공격이 가능하다고 가정 - 공격에 대한 시간제한이 없다고 가정
안전한 운영조건	- 암호모듈은 보안기능 및 서비스를 올바르게 제공해야 함 - 핵심보안매개변수 평문, 데이터 방어는 암호모듈 운영자(예: 모듈이 사용되는 환경) 그리고 암호모듈의 물리적 보호 메커니즘(예: 견고한 외장, 불법 침입 반응 커버와 문, 완전한 보호 외장, 즉각적인 핵심 보안매개변수 평문의 제로화 또는 암호모듈을 동작불능에 빠트리는 침투 탐지 방법)에 의해 제공되어야 함 - 운영자는 불법 침입 증거로 내부 정보가 노출된 것에 대해서 인지해야함 - 암호모듈은 공격자가 암호모듈을 위태롭게 하기 전에 모든 보호되지 않은 핵심보안매개변수는 제로화되어야 함

질의	견고한 코팅	
Ⅲ-5-4	보안등급 3에서 암호모듈의 코팅 또는 전기회로를 덮는 물질의 견고성을 확인하기 위해 어떤 시험이 시행되는가?	
요구사항	KS X ISO/IEC 24759	AS05.28, AS05.39, AS05.52
	소프트웨어 암호모듈 검증기준	-

【 개념 정리 】

○ 견고한(Hard)/견고함(Hardness): 덴팅(denting), 스크래칭(scratching) 혹은 벤딩(bending)에 대해 비교적 저항이 있는 재료로 물리적으로 강화되어 튼튼하고 내구성이 강함. 뚫는 것에 대해 비교적 저항이 있는 재료임

【 답변 】

○ 단일 칩/다중 칩 내장/다중 칩 단독 암호모듈이 보안등급 3과 4에 해당하면 암호모듈 전체가 견고한 코팅 등으로 덮여있어야 한다.

○ 시험방법은 에폭시(epoxy) 혹은 포팅(potting) 재료의 견고함에 대한 시험으로 최소한 아래의 시험을 수행한다.
- 중간수준의 강력한 정도의 힘으로(예: 송곳, 핸들용 툴) 회로망을 뚫으려는 시도
  ※ 드릴(drilling)이나 연마(grinding motion)는 범위에 벗어남
- 재료를 회로망에서 떼어내기 위해 중간수준의 강력한 위협 정도의 힘으로 기구를 이용
- 중간수준의 강력한 위협 정도로 재료를 떼어내거나 혹은 회로를 노출시키기 위해 재료를 부수거나 깨뜨리기 위한 플렉싱(flexing) 혹은 벤딩을 이용함

○ 시험 도중 해당 암호모듈은 지속적으로 심각한 손상이 생겼는지를 알아내기 위해 확인되어야 한다.

○ 에폭시 혹은 포팅 재료를 적용하는 제조방법은 노출이나 취약점을 만드는 포켓(pockets)이나 빈 공간(voids)이 존재하지 않아야 한다.

○ 암호모듈 견고성 시험은 제작사에서 명시하는 일반적인 동작환경에서 수행해야 하며, 제작사는 암호모듈이 손상되지 않는 범위의 최저/최고 온도 정보에 대해서 명시해야 한다. 개발업체가 정보를 제공하지 않는다면, 상온 환경에서 시험을 수행해야 한다.

○ 제출물에는 암호모듈의 견고성 시험의 최저/최고 온도 범위를 명시해야 한다. 암호모듈 견고성 시험이 일정 온도에서만 수행된다면, 암호모듈의 견고성 시험이 일정 온도에서만 시행되어졌다는 것을 분명히 명시해야 한다. 그리고 시험되지

않은 온도에서의 보안등급 3에 해당하는 견고성에 대해서는 보장하지 않음을 명시해야 한다.

○ 보안등급 3에서 모든 물리적 구현형태(단일 칩, 다중 칩 내장, 다중 칩 단독)에서 시험방법은 회로망에 접근을 하기 위한 드릴링, 분쇄, 절단, 연소, 용융, 연마, 포팅 물질/용기 분해를 포함하고 있지 않다. 이러한 타입의 공격은 보안등급 4 물리적 보안에 기술되어 있다.

Ⅲ-6. 운영환경

질의	암호모듈 운영환경 항목	
Ⅲ-6-1	암호모듈 운영환경에서 명세해야 할 항목들은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS06.02
	소프트웨어 암호모듈 검증기준	AS05.01

【 답변 】

○ 암호모듈의 제출물에는 암호모듈이 작동되는 운영체제 등 암호모듈의 운영환경을 명세해야 한다.

○ 암호모듈은 제출물에 명세한 운영환경에서만 시험하며, 해당 시험환경만을 검증필 운영환경으로 제한된다. 따라서 신청인은 운영환경의 정보를 제출물에 정확히 명세해야 한다.

○ 제출물에는 다음과 같은 사항을 명세해야 한다.
- 운영체제 종류
- 운영체제 버전
- 비트 정보
- CPU 모델
- 암호모듈이 개발된 환경(컴파일러, 통합개발환경, JDK 등에 대한 버전)
- 자바에서 운영되는 모듈은 자바가 실행될 수 있는 JRE와 같은 환경
- 각각의 운영환경에 대해 해당하는 암호모듈 이름

○ 특정 운영체제에 대해 버전 X.X 이하, X.X 이상과 같이 명확하지 않는 표현으로 작성해서는 안 된다.

○ 다양한 운영환경에서 검증을 받고자 하는 신청인은 반드시 신청하는 모든 운영환경에서 암호모듈이 정상 동작함에 대한 증거 자료(시험서 등)를 제출해야 한다.

질의	운영환경 변경/추가 요구사항	
Ⅲ-6-2	운영환경 변경/추가 시 요구되는 제출물에는 어떤 것들이 있는가?	
요구사항	KS X ISO/IEC 24759	AS06.02
	소프트웨어 암호모듈 검증기준	AS05.01

【 답변 】

○ 검증필 암호모듈에 대한 운영환경 변경/추가 시에 신청인은 변경내역서를 작성하여 재검증을 신청해야 한다.

○ 변경내역서에는 다음과 같은 사항을 명세해야 한다.
- 변경/추가된 운영환경 종류
- 운영환경 변경/추가를 통해 영향을 받는 보안요구사항
- 변경/추가된 운영환경을 반영한 업데이트된 모든 제출물

○ 운영환경 추가 시 신청인은 반드시 추가된 운영환경에서 암호모듈이 정상 동작함에 대한 증거 자료(시험서 등)를 제출해야 한다.

질의	서버에서의 단일운영자 동작모드	
Ⅲ-6-3	서버를 구현하는 경우, 보안등급 1의 암호모듈이 단일운영자의 요구사항을 어떻게 만족할 수 있는가?	
요구사항	KS X ISO/IEC 24759	AS06.04
	소프트웨어 암호모듈 검증기준	AS05.02

【 개념 정리 】

○ 단일운영자: 암호모듈에 접근하는 운영자가 유일한 경우를 지칭하며 운영체제에 복수의 운영자가 존재하지 않고, 유지보수 등의 관리자 역할을 수행하기 위한 별도의 운영자도 존재하지 않는 경우를 의미함

【 답변 】

○ 보안등급 1에서 운영환경은 단일운영자 동작모드로 한정되어야 하므로 서버에서 단일운영자 요구사항을 만족하기 위해서는, 동시에 단 한명의 운영자만 접근할 수 있도록 서버가 설정되어야 한다.

○ 서버에서 동작하는 응용프로그램에게 암호 기능을 제공하기 위해 컴포넌트 형태로 사용되는 암호모듈의 경우, 서버에서 동작하는 응용프로그램이 암호모듈을 단일 호출하므로 서버 응용프로그램 자체가 암호모듈의 단일운영자에 해당된다.

Ⅲ-7. 암호 키 관리

질의	전원인가 자가시험의 키 제로화	
Ⅲ-7-1	KAT 암호알고리즘 시험, 소프트웨어/펌웨어 무결성 시험 등의 전원인가 자가시험 과정에서만 암호모듈에서 사용되는 암호키는 핵심보안매개변수인가? 이러한 경우 제로화가 수행되어야 하는가?	
요구사항	KS X ISO/IEC 24759	AS07.35
	소프트웨어 암호모듈 검증기준	AS06.26

【 개념 정리 】

○ 제로화 요구사항: 암호모듈 내에 있는 평문으로 된 모든 비밀키, 개인키 및 핵심보안매개변수를 제로화하는 방법을 제공해야 함

【 답변 】

○ 전원인가 자가시험에서만 사용되는 암호모듈의 암호키(무결성 검증키, KAT 암호알고리즘 시험에 사용되는 키 등)는 핵심보안매개변수가 아니므로 제로화 요구사항을 충족할 필요가 없다.

【 참고사항 】

○ 제로화가 수행되지 않는 핵심보안매개변수에 대해서는 안전한 저장에 대한 방법을 제공해야 한다.

※ 라이브러리 형태의 암호모듈에서 모든 핵심보안매개변수는 제로화를 수행해야 한다.

질의	키 설정, 키 주입 및 출력	
Ⅲ-7-2	암호모듈의 키 설정, 키 주입·출력의 의미는 무엇인가? 암호모듈 포트와 인터페이스의 보안요구사항과는 어떤 연관관계가 있는가?	
요구사항	KS X ISO/IEC 24759	AS07.15 ~ AS07.30
	소프트웨어 암호모듈 검증기준	AS06.15 ~ AS06.23

【 개념 정리 】

○ 키 설정: 두 개 이상의 암호모듈이 암호 사용을 위해서 비밀정보를 공유하는 프로세스나 프로토콜을 의미하며, 방법으로는 키 전송(Key Transport)과 키 동의(Key Agreement)가 있음.

○ 키 주입: 암호모듈 경계 안으로 키가 들어오는 것

○ 키 출력: 암호모듈 경계 밖으로 키가 나가는 것

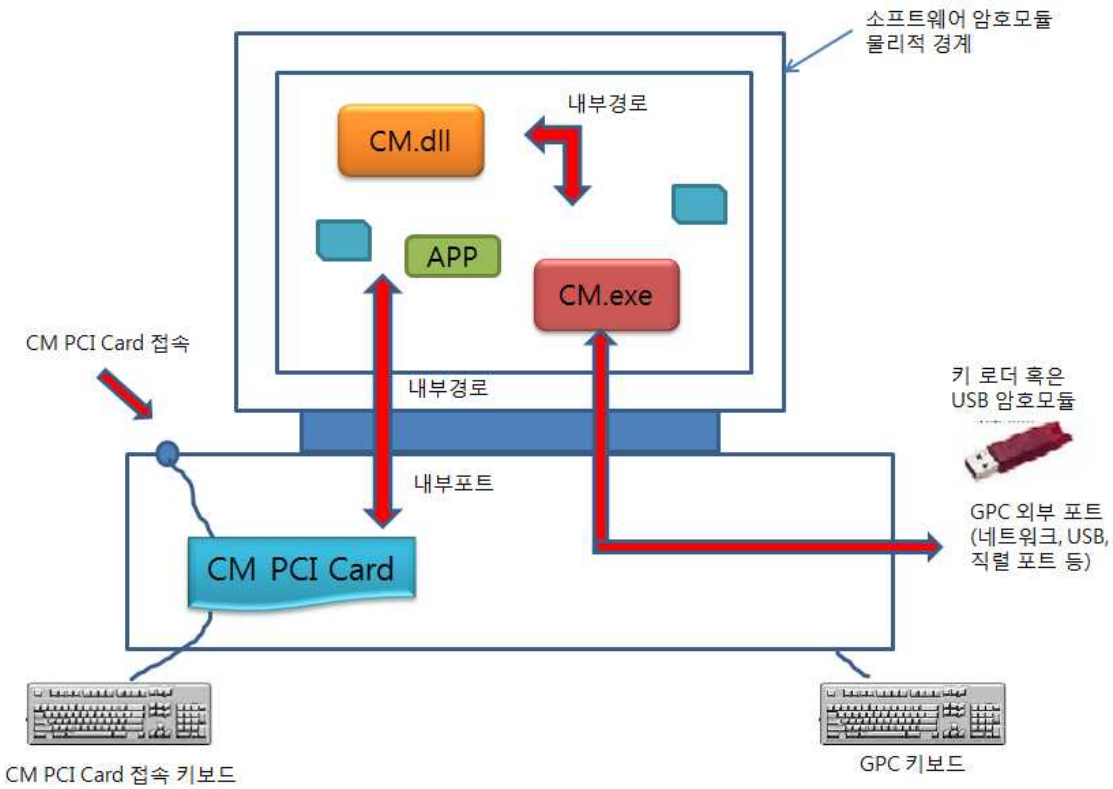
【 답변 】

○ 키 설정 및 키 주입/출력은 다음의 포트와 인터페이스로 통해 수행될 수 있다.

<table>
<tr><td colspan="2"></td><td colspan="8">분배 (설정)</td></tr>
<tr><td colspan="2"></td><td colspan="4">수동적인 분배방법</td><td colspan="4">전자적인 분배방법</td></tr>
<tr><td rowspan="5">주입/
출력</td><td rowspan="3">수동</td><td colspan="4">키보드, 스위치, 다이얼</td><td colspan="4" rowspan="3"></td></tr>
<tr><td>등급1</td><td>등급1</td><td>등급3</td><td>등급4</td></tr>
<tr><td>P/KT</td><td>P/KT</td><td>KT/SK</td><td>KT/SK</td></tr>
<tr><td rowspan="3">전자</td><td colspan="4">스마트카드, USB토큰, 키 로더</td><td colspan="4">키 설정
(키 전송/키 동의)</td></tr>
<tr><td>등급1</td><td>등급2</td><td>등급3</td><td>등급4</td><td>등급1</td><td>등급2</td><td>등급3</td><td>등급4</td></tr>
<tr><td>P/KT</td><td>P/KT</td><td>KT/SK</td><td>KT/SK</td><td>KE</td><td>KE</td><td>KE</td><td>KE</td></tr>
</table>

※ 약어

- P/KT: 평문(Plaintext)이나 키 전송(Key Transport)
- KE: 키 설정(Key Establishment)
- KT/SK: 분리된 물리적 포트나 신뢰된 경로(trusted path)를 이용한 키 전송(Key Transport)나 평문 지식 분산(Plaintext Split Knowledge)



설정 내용	설정방법
컴퓨터의 키보드로부터 소프트웨어 암호모듈 설정	MD/ME
컴퓨터 키 로더(예: CD, USB 등)와 소프트웨어 암호모듈 사이 설정	MD/EE
컴퓨터 외부 포트(예: 네트워크 포트)와 소프트웨어 암호모듈 사이 설정	ED/EE
컴퓨터 내부 경로를 통한 소프트웨어 암호모듈과 소프트웨어 암호모듈 사이의 설정	NA
컴퓨터 내부 경로를 통한 소프트웨어 암호모듈과 응용프로그램 사이의 설정	NA
컴퓨터 내부 경로를 통한 소프트웨어 암호모듈과 내부의 하드웨어 암호모듈 사이의 설정	NA
네트워크에 연결되지 않은 컴퓨터에서 소프트웨어 암호모듈과 외부의 하드웨어 암호모듈(키 로더) 사이의 설정	MD/EE
네트워크에 연결된 컴퓨터에서 소프트웨어 암호모듈과 외부의 하드웨어 암호모듈 사이의 설정	ED/EE
컴퓨터 내부 경로를 통한 내부의 하드웨어 암호모듈과 응용프로그램 사이의 설정	ED/EE
컴퓨터 내부 경로를 통한 내부의 하드웨어 암호모듈과 컴퓨터 외부 포트 사이의 설정	ED/EE
컴퓨터 내부 경로를 통한 컴퓨터 키보드부터 내부의 하드웨어 암호모듈로의 설정	ED/EE

직접 붙어 있는 키 로더와 내부의 하드웨어 암호모듈 사이의 설정	MD/EE
직접 붙어 있는 키보드로부터 내부 하드웨어 암호모듈로의 설정	MD/ME
네트워크에 연결된 컴퓨터와 외부의 하드웨어 암호모듈 사이의 설정	ED/EE
직접 붙어 있는 키 로더와 외부의 하드웨어 암호모듈 사이의 설정	MD/EE
직접 붙어 있는 키보드와 외부 하드웨어 암호모듈 사이의 설정	MD/ME

※ 약어

- MD/ME: 수동적 분배(Manual Distribution) / 수동적 주입(Manual Entry)
  (Ex) 키보드, 스위치, 다이얼
- MD/EE: 수동적 분배(Manual Distribution) / 전자적 주입(Electronic Entry)
  (Ex) 스마트카드, USB토큰, 키 로더
- ED/EE: 전자적 분배(Electronic Distribution) / 전자적 주입(Electronic Entry)
  (Ex) 키 설정 (키 전송/키 동의)

질의	난수발생기 엔트로피	
Ⅲ-7-3	난수발생기 엔트로피 리소스 선택 시 주의사항은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS07.12
	소프트웨어 암호모듈 검증기준	AS06.12

【 답변 】

○ 검증대상 난수발생기는 결정론적 난수발생기(DRBG, Deterministic Random Bit Generator)인 Hash_DRBG, HMAC_DRBG, CTR_DRBG이다.

○ 결정론적 난수발생기의 안전성은 입력되는 엔트로피 리소스의 안전성에 의존한다.

○ 암호모듈의 운영환경에서 사용되어지는 엔트로피 리소스에 대해 안전성 분석이 필요하며, 해당 엔트로피가 암호모듈 검증기준에서 제시하는 안전성 기준을 만족해야 한다.

【 참고사항 】

○ 암호모듈이 제공하는 모든 운영환경에서의 엔트로피 리소스에 대한 “난수발생기 엔트로피 분석”자료를 요구한다.

질의	전자서명의 키 생성	
Ⅲ-7-4	전자서명 알고리즘 구현 시 키 생성을 지원하지 않고, 서명 생성/검증만을 제공할 수 있는가?	
요구사항	KS X ISO/IEC 24759	AS07.10
	소프트웨어 암호모듈 검증기준	AS06.10

【 답변 】

○ 전자서명을 지원하는 암호모듈이 키 생성을 제공하지 않고, 외부에서로부터 받은 키를 이용하여 서명을 생성하고 검증할 수 있다.

○ 서명 검증만을 제공하는 암호모듈의 경우, 암호모듈은 서명키를 보관하거나 생성할 필요가 없으며, 필요시 서명 검증키가 암호모듈로 입력되면 된다.

○ 암호모듈에서 키를 생성할 경우, 검증대상 키 생성방법을 통해서 생성해야 한다.

【 참고사항 】

○ 전자서명에 대한 암호알고리즘 시험은 키 생성 검사, 서명 생성 검사, 서명 검증 검사로 구분하여 진행하며, 키 생성기능이 없는 경우는 키 생성 검사를 생략한다.

Ⅲ-8. 전자기 간섭/전자기 적합성

질의	전자기 간섭/전자기 적합성 인증	
Ⅲ-8-1	암호모듈 검증 신청 전에 전자기 간섭/적합성을 인증을 받고 신청해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS13.01 ~ AS13.05
	소프트웨어 암호모듈 검증기준	-

【 답변 】

○ 하드웨어 암호모듈은 전자기 간섭/적합성 인증서 사본이 필요하다.

○ 하드웨어 암호모듈의 최종 형상에 대한 전자기 간섭/적합성 인증서가 필요하므로, 신청 전에 인증을 받을 필요는 없다.

○ 전자기 간섭/적합성 인증서의 제품 이름과 시험 중인 암호모듈의 이름은 일치해야 한다.

【 참고사항 】

○ 전자기 간섭/적합성 인증 시험은 국립전파연구원에서 수행하고 있다.

○ 전자기 간섭/전자기 적합성 인증의 요구사항은 소프트웨어/펌웨어 암호모듈일 경우 제외된다.

Ⅲ-9. 자가시험

질의	암호알고리즘 시험	
Ⅲ-9-1	전원인가 시험의 암호알고리즘 KAT 수행시, 비검증대상 암호알고리즘에 대한 KAT도 수행해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS08.14
	소프트웨어 암호모듈 검증기준	AS07.08

【 개념 정리 】

○ 검증대상 동작모드 : 암호모듈에서 검증대상 암호알고리즘만으로 운영되는 모드

○ 비검증대상 동작모드 : 비검증대상 암호알고리즘을 운영할 수 있는 모드이며, 검증대상 암호알고리즘을 사용할 수도 있음

○ 전원인가 시험: 암호모듈에 전원이 인가(초기화, 재시동 등의 작동 후)될 때, 암호모듈의 암호알고리즘 시험, 난수발생기 엔트로피 시험, 소프트웨어 무결성 시험, 보안기능 시험 등이 운영환경에서의 정상 동작함을 확인하는 시험

○ KAT(Known Answer Test): 고정된 입력값에 대한 출력값이 올바른지 확인하는 기지 답안 검사

【 답변 】

○ 전원인가 시험에서의 KAT 방법을 이용한 암호알고리즘 시험은 구현한 암호모듈의 모든 검증대상 알고리즘에 대해서 수행되어야 하며, 비검증대상 암호알고리즘에 대한 KAT를 수행할 필요는 없다.

○ 비검증대상 암호알고리즘에 대한 KAT는 암호모듈 개발업체의 판단에 따라 포함할 수 있으나, 주기적인 전원인가시험을 수행해야 하고 검증대상 운영모드에서는 비검증대상 암호알고리즘을 사용할 수 없으므로 비검증대상 암호알고리즘을 이용 시 이를 고려해야 한다.

질의	연속적 난수발생기 시험	
Ⅲ-9-2	연속적 난수발생기 시험에서 잡음원으로 입력되는 엔트로피에 대한 시험도 지원해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS08.34
	소프트웨어 암호모듈 검증기준	AS07.18

【 개념 정리 】

○ 연속적인 난수발생기 시험: 난수발생기를 사용 시 연속 n비트 출력을 비교하여 동일한 출력을 생성하지 않는지 확인함으로써, 난수발생기 내부상태가 계속적으로 변경되고 있음을 확인하는 시험

○ 난수발생기 엔트로피 시험: 전원인가 시 암호모듈의 운영환경에서의 엔트로피 리소스의 안전성을 분석하는 시험

【 답변 】

○ 연속적 난수발생기 시험에서 엔트로피 시험을 수행할 필요는 없다.

○ 조건부 시험인 연속적 난수발생기 시험은 난수발생기의 정상동작 여부를 확인하기 위한 시험이며, 통계적 난수성을 확인하지 않는다.

○ 난수발생기 엔트로피에 대한 시험은 전원인가 시험에 포함되며, 난수발생기 엔트로피 소스의 정상동작 여부를 시험한다.

질의	소프트웨어 무결성 시험	
Ⅲ-9-3	소프트웨어 무결성 시험에서 적용 가능한 암호알고리즘은 무엇인가?	
요구사항	KS X ISO/IEC 24759	AS08.21
	소프트웨어 암호모듈 검증기준	AS07.13

【 개념 정리 】

○ 소프트웨어 무결성 시험: 전원인가 시 검증대상 인증기술을 사용하여 암호경계 내부에 있는 모든 소프트웨어 구성요소에 대한 무결성을 확인하는 시험

【 답변 】

○ 소프트웨어 무결성 시험은 전원인가 시험 시 수행하며, 암호모듈 내 구성요소의 변조를 방지하기 위한 최소한의 요구사항이다.

○ 무결성 시험에 사용되는 기술은 검증대상 인증기술을 요구하고 있으므로, 다음과 같은 검증대상 암호알고리즘을 사용할 수 있다. 또한 검증대상 암호알고리즘 파라미터를 적용해야 한다.

구분		암호알고리즘
메시지 인증코드	해시함수 기반	HMAC
	블록암호 기반	GCM(GMAC) CCM, CMAC
전자서명		RSA-PSS, KCDSA ECDSA, EC-KCDSA

질의	소프트웨어/펌웨어 로드 시험	
Ⅲ-9-4	소프트웨어/펌웨어 로드 시험은 소프트웨어 무결성 시험과 무슨 차이가 있는가?	
요구사항	KS X ISO/IEC 24759	AS08.21, AS08.43
	소프트웨어 암호모듈 검증기준	AS07.21

【 개념 정리 】

○ 소프트웨어 무결성 시험: 전원인가 시 검증대상 인증기술을 사용하여 암호경계 내부에 있는 모든 소프트웨어 구성요소에 대한 무결성을 확인하는 시험

○ 소프트웨어/펌웨어 로드시험: 암호모듈이 암호경계 외부에 있는 소프트웨어나 펌웨어를 로드할 때, 검증대상 인증기술을 사용하여 해당 구성요소의 무결성을 확인하는 시험

【 답변 】

○ 소프트웨어 무결성 시험과 소프트웨어/펌웨어 로드 시험은 다음과 같이 구분된다.

구분	소프트웨어 무결성 시험	소프트웨어/펌웨어 로드시험
소프트웨어 위치	암호모듈 내부	암호모듈 외부
시험 수행 시점	전원인가 시점	소프트웨어 로드 시점
점검 내용	무결성 확인	무결성 확인

III-10. 설계보증

질의	형상관리 도구	
III-10-1	형상관리 도구를 반드시 사용해야 하는가?	
요구사항	KS X ISO/IEC 24759	AS09.01
	소프트웨어 암호모듈 검증기준	AS08.01

【 답변 】

○ 형상관리는 암호경계 내에 있는 모든 암호모듈 구성요소, 암호모듈, 암호모듈 관련 개발문서에 대해 적용되어야 한다.

○ 형상관리 도구는 암호모듈, 관련 문서들, 소스코드 등 제출물의 형상 및 이력 관리, 버전 관리 등에 필요하다. 이러한 형상관리 도구는 일반적으로 수동으로 처리하기에는 많은 어려움이 따르기 때문에 도구를 사용해야 한다.

【 참고사항 】

○ 형상관리 도구는 상용 혹은 자체 개발한 도구를 사용할 수 있으며 개발업체 보안점검 시에 형상관리 도구를 통해 암호모듈, 관련 문서들, 소스코드 등이 체계적으로 관리되고 있는지 확인하게 된다.

질의	배포	
Ⅲ-10-2	형상관리 중 암호모듈의 배포과정에 대한 보증이 필요한가?	
요구사항	KS X ISO/IEC 24759	AS09.04
	소프트웨어 암호모듈 검증기준	AS08.03

【 답변 】

○ 암호모듈의 안전한 배포, 설치 및 시작에 대한 보안요구사항을 명세해야 한다.

○ 암호모듈이 배포되는 방법, 절차, 그리고 배포 목록 관리가 반드시 이루어져야 한다. 또한 암호모듈 분배 및 배포 시 보안 유지 방법도 명세해야 한다.

○ 자체 배포(개발업체 내에서 다른 제품을 통한 배포)도 암호모듈 배포에 포함되며 암호모듈 배포와 동일하게 관리가 이루어져야 한다.

【 참고사항 】

○ 배포 절차나 계획 등은 개발업체 보안점검 시에 확인하게 된다.

○ 배포의 대상은 검증필 암호모듈이므로 검증을 받은 이후에도 배포의 연혁, 운용 등에 대해서 수시로 확인한다.

질의	형상관리 시점	
Ⅲ-10-3	암호모듈 시험과정 중 문서에 대한 형상관리는 최종단계에서 수행하는 것이 가능한가?	
요구사항	KS X ISO/IEC 24759	AS09.01
	소프트웨어 암호모듈 검증기준	AS08.01

【 답변 】

○ 형상관리는 검증된 암호모듈의 생명주기 동안 각 형상요소의 식별번호와 버전의 변경, 갱신을 관리 혹은 유지할 수 있어야 한다.

○ 암호모듈을 시험하는 과정에서 시험 항목들을 만족시키기 위해서 관련 개발 문서와 소스코드에 수정이 이루어 질 수 있다. 그러나 시험 중에 소스코드와 문서에 대한 변경이 이루어졌더라도 검증이 완료된 완성본에 대한 관리가 더욱 중요하므로 완성본을 중심으로 형상 관리가 이루어지면 된다.

【 참고사항 】

○ 형상관리는 버전 부여 방법, 형상변경 통제방법 등을 포함해야 하며 개발업체 보안점검 시에 확인하게 된다.

III-11. 기타 공격에 대한 대응

질의	기타 공격에 대한 대응	
III-11-1	반드시 포함되어야 할 공격에 대한 대응방법으로는 어떤 것들이 있는가?	
요구사항	KS X ISO/IEC 24759	AS10.01
	소프트웨어 암호모듈 검증기준	AS09.01

【 답변 】

○ 암호모듈 검증제도는 국가·공공기관으로의 도입을 목적으로 하고 있다. 따라서 최소한 다음의 공격에 대해서는 완화방법을 반드시 제공해야 한다.

- 소프트웨어 암호모듈의 경우 버퍼오버플로우 공격에 대한 대응
- RSA를 구현한 경우 타이밍 공격에 대한 대응
- 자바 운영환경 상에서 동작하는 암호모듈의 경우 코드 난독화 기술 적용

○ 개발업체는 해당 공격에 대한 대응방법에 대한 증거자료(시험서 등)를 제시해야 한다.

Ⅳ. 암호알고리즘 요구사항

질의	암호모듈 신청
Ⅳ-1	암호모듈에는 검증대상 암호알고리즘 목록에 명세된 모든 검증대상 암호알고리즘, 모든 운영모드 및 모든 파라미터가 반드시 구현되어야 하는가?
요구사항	-

【 답변 】

○ 검증대상 암호알고리즘은 블록암호, 해시함수, 메시지 인증코드, 난수발생기, 공개키 암호, 전자서명, 키 설정 방식 등으로 분류된다.

○ 모든 검증대상 암호알고리즘을 구현·탑재할 필요는 없으며, 개발업체에서 암호모듈에 구현한 암호알고리즘 중에서 검증대상 동작모드로 운영되는 암호알고리즘만이 검증대상이 된다.

【 참고사항 】

○ “소프트웨어 암호모듈 검증기준(2011.5), 부속서 C", “암호알고리즘 검증기준 Ver 2.0(2012.3)"에 검증대상 암호알고리즘 목록 및 파라미터가 명세되어 있다.

○ <검증대상 암호알고리즘 목록>에서는 검증대상 암호알고리즘 목록 및 검증대상 암호알고리즘 파라미터를 제공하고 있다.

질의	암호알고리즘의 선택적 요소에 대한 시험방법
Ⅳ-2	암호알고리즘의 선택적인 요소(예: 난수발생기의 예측내성 여부, 공개키 암호의 Salt 등)에 대해서는 어떻게 시험을 수행하는가?
요구사항	-

【 답변 】

○ 암호알고리즘 검증기준은 검증대상 암호알고리즘이 관련 표준에 따라 정확하게 구현되었는지를 검증하는 것을 목적으로 한다.

○ 공개키 암호, 전자서명, 키 설정, 난수발생기 등의 암호알고리즘은 해시함수의 선택, 예측내성 여부, Salt의 크기 등에서의 다양한 조합이 가능하다.

○ 신청인은 제출물에 검증대상 암호알고리즘의 선택적인 요소에 대한 정보를 포함하여 정확한 구현방법을 명세해야 한다.

○ 시험기관은 검증대상 알고리즘의 검증절차와 개발자가 구현한 선택적인 요소에 부합되는 요청파일(REQUEST)을 신청인에게 제공한다.

○ 신청인은 요청파일에 대한 응답파일(RESPONSE)을 제공해야 한다.

【 참고사항 】

○ 각각의 암호알고리즘에 대한 검증절차와 참고데이터는 “암호알고리즘 검증기준 Ver 2.0 (2012.03)"를 참조한다.

질의	검증대상 암호알고리즘 추가
Ⅳ-3	새로운 암호알고리즘을 검증대상 암호알고리즘에 포함시킬 수 있는가?
요구사항	-

【 답변 】

○ 암호모듈 검증제도는 국가·공공기관 도입 암호모듈에 대한 안전성과 신뢰성, 그리고 상호운용성을 보장하기 위해 충분히 성숙된 암호알고리즘을 검증대상 암호알고리즘으로 지정하고 있다.

○ “암호모듈 시험 및 검증안내서(2004.12.31, 행안부 고시 제2004-45호) 제14조(검증위원회)”에 의거하여, 검증위원회에서 검증대상 암호알고리즘에 대한 추가, 변경 등에 대한 심의·의결을 진행할 수 있다.

○ 검증대상 암호알고리즘의 선정은 다음과 같은 사항을 고려하여 선정한다.
- 현재의 암호 알고리즘 분석 기술
- 표준화 여부
- 산업체나 업계의 사용빈도
- 국내·외 암호사용 정책 등