* 펌웨어 모듈은 제한되거나 변경이 불가능한 운영환경에서 실행하는 펌웨어 구성 요소들이며, 암호경계는 펌웨어 경계를 이용하여 구분될 수 있도록 명세화된 모듈이다. 펌웨어 구성 요소가 실행되는 연산 플랫폼 또는 운영체제는 정의된 펌웨어 모듈 경계 외부에 있지만 펌웨어 모듈과 항상 결합된 형태이어야 한다.

암호경계의 일반 요구사항

암호경계는 암호모듈의 모든 구성 요소의 경계에 의해서 설정되는 통합 경계(즉, 하드웨어 구성 요소, 소프트웨어 구성 요소 및 펌웨어 구성 요소의 집합)이어야 한다[02.07]. 해당 표준의 요구사항들은 암호모듈의 암호경계 내의 모든 알고리즘, 프로세스 및 구성 요소에 적용되어야 한다[02.08]. 암호경계는 암호모듈(즉, 이 표준의 범위 내에 있는 보안에 관련된)의 모든 알고리즘, 모든 프로세서 및 모든 구성 요소를 반드시 포함해야 한다[02.09]. 검증대상 동작모드에 사용되는 비보안 알고리즘, 비보안 프로세서 또는 비보안 구성 요소는 암호모듈의 검증대상 동작을 방해하거나 손상시키지 않는 방법으로 구현되어야 한다[02.10].

암호모듈의 명칭은 암호경계 내에 있는 구성 요소만의 조합을 의미하도록 정해져야 하며, 암호경계 내에 있는 구성 요소의 조합보다 더 큰 범위의 제품이나 구성 요소의 조합을 의미하는 명칭이 되지 않아야 한다[02.11]. 암호모듈은 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소 각각에 대하여 최소한 특정 버전 정보는 가져야 한다[02.12].

암호경계 외부에 있는 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 암호모듈의 검증대상 동작을 방해하거나 손상을 초래하지 않도록 구현되어야 한다. 암호경계 외부에 있는 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 해당 표준의 보안 요구사항을 적용받지 않는다[02.13]. 보안 요구사항에 해당하지 않는 하드웨어, 소프트웨어 또는 펌웨어는 **부속서** A의 요구사항을 충족하도록 명세되어야 한다[02.14].

7.2.4.2 정상 동작

정상 동작은 알고리즘의 집합, 서비스 또는 프로세스가 사용 가능하거나 구성 가능한 상태를 말한다.

CSP는 검증대상 서비스 및 동작모드와 비검증대상 서비스 및 동작모드에서 독립적으로 분리되어야 한다(예: 상호 공유되거나 접근할 수 없어야 한다)[02.22]. 검증대상 난수 발생기의 출력은 난수 발생기 씨드를 비검증대상 동작모드로 접근할 수 없는 한 그 씨드를 제로화하지 않고 비검증대상 알고리즘이나 프로세스에 제공될 수 있다.

모듈의 보안정책은 검증대상 동작모드와 비검증대상 동작모드에서 제공하는 모든 서비스의 집합을 정의해야 한다[02.23].

모든 서비스들은 검증대상 동작모드에서 검증대상 암호알고리즘이나 프로세스를 사용할 때 각 서비스에 대한 표시기를 제공해야 한다. 여기서 이들 서비스와 프로세스는 **7.4.3**에 명세되어 있다[02.24].

모듈이 오류 상태로 들어간다면 암호모듈은 제한 기능 동작을 지원하기 위해 설계될 수 있다. 암호모듈이 제한 기능 동작 상태로 동작하기 위해서는 다음이 적용되어야 한다[02.25].

• 오류 상태를 벗어난 후에만 제한 기능 동작으로 전환되어야 한다[02.26].

• 모듈이 재구성되고 제한 기능 동작 상태로 진입했을 때 상태 정보를 제공해야 한다[02.27].

• 오동작을 일으킨 메커니즘이나 기능은 분리되어야 한다[02.28].

• 제한 기능 동작 진입 후 모든 조건부 알고리즘 자가시험은 암호알고리즘이 처음 동작하기 전에 수행되어야 한다[02.29].

• 비동작 알고리즘이나 프로세스를 사용하려는 경우 서비스는 표시기를 제공해야 한다[02.30].

암호모듈은 모든 동작 전 자가시험을 성공적으로 통과할 때까지 제한 기능 동작 상태로 남아 있어야 한다[02.31]. 암호모듈은 제한 기능 동작 상태를 벗어나기 위한 조건처럼 모든 동작 전 자가시험의 확실한 진단을 수행해야 한다. 암호모듈이 동작 전 자가시험을 실패한다면 모듈은 제한 기능 동작에 진입할 수 없다[02.32].

암호모듈은 모든 논리적 정보 흐름이 암호경계의 입출구로 식별되는 물리적 접근 지점과 논리적 인터페이스에 제한되도록 해야 한다[03.01]. 암호모듈 논리적 인터페이스들은 한 개의 물리적 포트를 공유하더라도 서로 구별되어야 하며(예: 입력 데이터와 출력 데이터가 동일한 포트를 통해 입출력될 수 있다), 하나 이상의 물리적 포트(예: 입력 데이터가 직렬 및 병렬 포트 모두를 통해 들어올 수 있다.)로 분산하여 사용될 수 있다. 암호모듈의 소프트웨어 구성 요소의 API는 하나 이상의 논리적 인터페이스로 정의될 수 있다[03.02].

**A.2.3**의 요구사항을 충족하는 개발 문서를 제출해야 한다[03.03].

1. **데이터 입력 인터페이스** 암호모듈에 입력되고 모듈에 의해 처리되는(평문 데이터, 암호문 데이터, SSP, 다른 모듈로부터의 상태 정보를 포함한) 모든 데이터(제어 입력 인터페이스를 통해 들어오는 제어 데이터는 제외)는 데이터 입력 인터페이스를 통해 입력되어야 한다[03.05]. 데이터는 모듈이 자가시험(**7.10**)을 수행하는 동안 데이터 입력 인터페이스를 통해 그 모듈로 입력할 수 있다.

2. **데이터 출력 인터페이스** (평문 데이터, 암호문 데이터, SSP를 포함한) 암호모듈에서 출력되는 모든 데이터(상태 출력 인터페이스를 통해 출력되는 상태 데이터와 제어 출력 인터페이스를 통해 출력되는 제어 데이터 제외)는 데이터 출력 인터페이스를 통해 출력되어야 한다[03.06]. 수동 키를 주입하는 상태, 동작 전 자가시험 상태, 소프트웨어/펌웨어를 로드하는 상태 및 제로화하는 상태 또는 암호모듈이 오류 상태에 있을 때는 ‘데이터 출력’ 인터페이스를 통과하는 모든 데이터 출력은 금지되어야 한다[03.07].

3. **제어 입력 인터페이스** 암호모듈의 동작을 제어하는 데 사용되는 모든 입력 명령, 신호(예: 클럭 입력) 및 제어 데이터(함수 호출과 스위치, 버튼 및 키보드 같은 수동 제어 장치를 포함하는)는 ‘제어 입력’ 인터페이스를 통해 입력되어야 한다[03.08].

4. **제어 출력 인터페이스** 암호모듈의 동작 상태를 제어하거나 표시하는 모든 출력 명령, 신호 및 제어 데이터(예: 다른 모듈에 입력시키는 제어 명령)는 ‘제어 출력’ 인터페이스를 통해 출력되어야 한다[03.09]. 개발 문서의 보안정책에 서술된 예외 사항 이외의 오류 상태에 있을 때, ‘제어 출력’ 인터페이스를 통한 암호모듈의 모든 제어 출력은 금지되어야 한다[03.10].

5. **상태 출력 인터페이스**  암호모듈의 상태를 표시하기 위해 사용되는 모든 출력 신호, 표시기(예: 오류 표시기) 및 상태 데이터[응답 코드 및 (디스플레이, 표시기 램프 같은) 시각 신호, (버저, 톤, 벨소리 같은) 소리, (진동 같은) 기계적 신호와 같은 물리적 표시기]는 “상태 출력” 인터페이스를 통해서 출력되어야 한다. 상태 출력은 암시적이거나 명시적일 수 있다[03.11].

암호모듈은 운영자에게 인가된 역할을 지원하고 각 역할에 상응하는 서비스를 제공해야 한다[04.01]. 한 명의 운영자가 복수 역할을 맡을 수도 있다. 암호모듈이 복수 운영자가 모듈을 동시에 이용하는 것을 지원하는 경우, 암호모듈은 내부적으로 각 운영자의 역할과 이에 상응하는 서비스를 분리하여 유지할 수 있어야 한다[04.02]. 운영자는 CSP와 PSP가 변경 또는 공개, 대체되지 않는 경우, 서비스를 수행하도록 인가된 역할을 맡을 필요가 없다(예: 상태 표시, 자가시험 및 모듈의 보안에 영향을 주지 않는 기타 서비스).

인증 메커니즘은 모듈에 접근하는 운영자를 인증하기 위해, 운영자가 요청된 역할을 맡고 그 역할 내 서비스를 수행하도록 권한을 위임받았음을 검증하기 위해 암호모듈 내부에서 요구될 수 있다.

**A.2.4**를 만족하는 개발 문서가 제출되어야 한다[04.03].

암호모듈은 적어도 하나의 암호관리자 역할을 지원해야 한다[04.04]. 암호관리자 역할은 암호 초기화나 관리 기능 및 일반 보안 서비스를 수행하는 역할이어야 한다(예: 암호모듈의 초기화, PSP와 CSP의 관리, 감사 기능)[04.05].

역할

암호모듈은 사용자 역할을 지원할 수도 있다. 암호모듈이 사용자 역할을 지원하면, 사용자 역할은 암호 기능과 검증대상 암호알고리즘을 포함한 일반 보안 서비스를 수행하는 것이다[04.06].

암호모듈은 유지보수 역할을 지원할 수도 있다. 유지보수 역할은 물리적 또는 논리적 유지보수 서비스[예: 서비스 덮개 열기, 빌트인 자가시험(BIST) 등과 같은 진단 수행] 동안 담당하는 역할이다. 모든 보호되지 않은 SSP는 암호모듈이 유지보수 역할로 들어가거나 혹은 벗어날 때 제로화되어야 한다[04.07]

암호모듈은 위에서 명시한 역할 외 다른 역할을 지원할 수도 있다.

### 서비스

#### 서비스 일반 요구사항

서비스는 모듈에서 수행되는 모든 동작, 서비스, 기능으로 정의된다[04.08]. 서비스 입력은 특정 서비스, 동작 또는 기능을 시작하거나 동작하기 위해 암호모듈로 입력되는 데이터 입력과 제어 입력으로 구성된다[04.09]. 서비스 출력은 서비스 입력에 의해 시작 또는 수행되는 서비스, 동작 및 기능으로부터 얻어지는 데이터 출력, 제어 출력과 상태 출력으로 구성된다[04.10]. 각 서비스 입력의 결과로 서비스 출력이 생성된다[04.11].

암호모듈은 운영자에게 다음 서비스를 제공해야 한다[04.12].

1. 모듈의 버전 정보 표시. 암호모듈은 검증 기록과 관련된 명칭 또는 모듈 식별자 그리고 버전 정보(예: 하드웨어, 소프트웨어 또는 펌웨어 버전 정보)를 출력해야 한다[04.13].

2. 상태 표시. 암호모듈은 현재 상태 정보를 출력해야 한다[04.14]. 이것은 서비스 요청에 대응한 상태 표시가 포함될 수 있다.

3. 자가시험 수행. 암호모듈은 **7.10.2**에 명세된 대로 동작 전 자가시험을 수행해야 한다[04.15].

4. 검증대상 암호알고리즘 수행. **7.2.4**에 명시된 대로 검증대상 동작모드에서 사용되는 검증대상 암호알고리즘을 적어도 한 개 이상 수행해야 한다[04.16]

5. 제로화 수행. 암호모듈은 **7.9.7**에 명시된 대로 파라미터의 제로화를 수행해야 한다[04.17].

암호모듈은 위에서 명시한 서비스 외에 검증대상 및 비검증대상 동작모드에서의 서비스, 운영 또는 기능을 제공할 수 있다. 특정 서비스는 한 개 이상의 역할에서 제공할 수 있다(예: 키 주입 서비스는 사용자 역할과 암호관리자 역할에서 제공할 수 있다).

#### 우회 기능

우회 기능은 암호 기능 또는 프로세스를 부분적 또는 전체적으로 피하는 서비스 기능이다. 암호모듈이 특정 데이터나 상태값을 암호로 보호된 형태(예: 암호문)로 출력할 수 있고, 또한 이들을 (모듈의 설정이나 운영자 개입의 결과로) 보호되지 않은 형태(예: 평문)로도 출력할 수 있다면 우회 기능이 정의되어 있어야 한다[04.18].

암호모듈이 우회 기능이 구현된 경우

• 암호모듈에 우회 기능이 구현된 경우, 인가된 역할의 사용자만이 우회 기능을 설정할 수 있다[04.19].

• 단순한 오류로 인한 평문 데이터의 의도하지 않은 유출을 방지하기 위해, 우회 기능을 활성화하는 두 개의 독립된 내부 조치가 요구되어야 한다[04.20]. 두 개의 독립된 내부 조치가 우회 기능만을 수행하는 전용 소프트웨어 혹은 하드웨어를 동작할 수 있어야 한다(예: 두 개의 다른 소프트웨어 또는 하드웨어 플래그를 설정하고 그중 하나는 사용자가 시작시키도록 한다)[04.21].

• 그 모듈은 다음과 같이 우회 기능의 상태를 표시해야 한다[04.22].

1. 우회 기능이 비활성화 상태이고 모듈은 암호 처리만을 제공한다(예: 평문의 암호화).

2. 우회 기능이 활성화 상태이고 모듈은 암호 처리를 제외한 서비스만 제공한다(평문을 암호화하지 않음).

3. 우회 기능이 선택적으로 활성화, 비활성화되며 일부 서비스는 암호 처리와 함께 또한 일부 서비스는 암호 처리 없이 제공한다(예: 복수 통신 채널을 가진 모듈의 경우, 평문 데이터는 각 채널 설정에 따라 암호화되거나 또는 암호화되지 않는다).

자가 초기화된 암호 출력 기능은 외부 운영자 요청 없이 암호 운영 및 기타 검증대상 보안기능 또는 SSP 관리 기술을 수행할 수 있는 모듈의 기능이다. 자가 초기화된 암호 출력 기능은 암호관리자에 의해 설정되고 이러한 설정은 모듈의 리셋, 재부팅 또는 전원 재인가 시 보존되어야 한다[04.23].

암호모듈에 자가 초기 암호 출력 기능이 구현된 경우

• 단순 오류로 인한 의도하지 않은 출력을 방지하기 위해 두 개의 독립된 내부 조치가 필요하다[04.24]. 두 개의 독립된 내부 조치를 통해서만 암호 출력 기능을 조정하는 전용 소프트웨어 혹은 하드웨어를 동작시킬 수 있어야 한다(예: 두 개의 서로 다른 소프트웨어 또는 하드웨어 플래그를 설정하고 그중 하나는 사용자가 시작시키도록 한다)[04.25].

• 모듈은 그 기능이 활성화되었는지 상태를 표시해야 한다[04.26].

운영 환경

|  |  |
| --- | --- |
| **형상 예** | **운영환경** |
| 코드 로딩을 허용하지 않는 컴퓨팅 플랫폼 운영자에 의한 컴퓨팅 플랫폼, 운영체제 또는 암호모듈의 형상 변경을 허용하지 않는 컴퓨팅 플랫폼 | 변경 불가 |
| 표준에서 요구하는 적용 가능한 모든 요구사항을 만족하고, 인증된 추가 코드의 로딩을 허용하는 운영체제를 포함한 컴퓨팅 플랫폼 | 제한적 |
| 표준의 소프트웨어 또는 펌웨어 로딩 요구사항을 만족하지 않고, 코드의 로딩을 허용하는 컴퓨팅 플랫폼 | 변경 가능 |
| 보안 보호 기법 제거를 허용한 운영자가 운영체제를 다시 설정할 수 있는 코드가 있는 컴퓨팅 플랫폼 | 변경 가능 |

암호모듈의 각 인스턴스는 암호모듈 자신의 SSP를 제어해야 한다[06.05].

• 운영환경은 응용 프로그램의 데이터가 운영환경 내의 프로세스 메모리에 있거나 영구 저장소에 저장되는 것과 상관없이 인가되지 않은 CSP에 대한 접근과, 제어되지 않는 보안매개변수의 변경을 방지함으로써 각각의 응용 프로세스가 독립적으로 동작할 수 있도록 하는 기능을 제공해야 한다[06.06]. 이는 암호모듈과 운영체제의 신뢰되는 부분에 의해서 CSP와 SSP로의 직접 접근이 제한된다는 것을 말한다. 운영환경 설정에 대한 제한 사항은 암호모듈의 보안정책 문서에 서술되어야 한다[06.07].

• 암호모듈에 인해 생성된 프로세스는 해당 암호모듈에 의해서만 소유되어야 하며, 외부 프로세스/운영자는 소유할 수 없다[06.08].

1. 이 요구사항은 관리자 설명서 및 절차에 의해 시행될 수 없으며, 암호모듈 자체에 의해 수행되어야 한다.

평문 CSP와 키 구성 요소, 인증 데이터는 암호모듈의 다른 물리적 포트와 논리적 인터페이스를 공유하는 물리적 포트와 논리적 인터페이스를 거쳐 주입 및 출력할 수 있다.

### 중요 보안매개변수의 주입 및 출력

중요 보안매개변수는 수동으로 모듈에 주입되거나 외부로 출력되는 경우 직접적으로(예: 키보드, 숫자 패드, 화면 출력) 또는 전자식으로(예: 스마트카드, 토큰, PC 카드, 전자식 키 저장 장치, 모듈의 운영체제) 수행된다. SSP가 수동으로 모듈에 주입되거나 외부로 출력되는 경우, 주입 또는 출력은 HMI, SFMI, HFMI 또는 HSMI(**7.3.2**) 인터페이스를 사용해야 한다[09.12].

**보안수준 1, 2**

평문 CSP와 키 구성 요소, 인증 데이터는 암호모듈의 다른 물리적 포트와 논리적 인터페이스를 공유하는 물리적 포트와 논리적 인터페이스를 거쳐 주입 및 출력할 수 있다.

소프트웨어 암호모듈 또는 하이브리드 소프트웨어 모듈의 소프트웨어 구성 요소의 경우, CSP, 키 요소 및 인증 데이터가 운영환경 내에서 관리되고 **7.6.3**의 요구사항을 충족한다면, 평문이거나 암호화된 형식으로 입출력될 수 있다[09.19].

### 중요 보안매개변수 저장

모듈 내 저장된 SSP는 평문이나 암호화된 형태로 저장할 수 있다. 암호모듈 내부에 저장되는 모든 SSP는 SSP를 지정한 개체(예: 운영자, 역할, 프로세스)와 연계되어야 한다[09.25].

인가되지 않은 운영자가 평문 CSP에 접근하는 것은 금지되어야 한다[09.26]. 인가되지 않은 운영자에 의한 PSP 변경은 금지되어야 한다[09.27].

### 7.9.7 중요 보안매개변수의 제로화

암호모듈 내부에서 보호되지 않은 모든 SSP와 키 구성 요소를 제로화하는 방법을 제공해야 한다[09.28]. 임시로 저장된 SSP와 모듈에 의해 소유된 다른 저장된 값은 미래 용도로 더 이상 필요 없을 때 제로화하여야 한다.

제로화된 SSP는 복구되거나 재사용될 수 없어야 한다[09.29].

보안수준 4를 제외하고 보호된 PSP의 제로화, 암호화된 CSP의 제로화, (이 표준의 요구사항을 만족하는) 추가 내장형 검증필 암호모듈 내에서 물리적으로 또는 논리적으로 보호된 CSP의 제로화는 요구하지 않는다.

인증 프록시(예: 모듈 초기화 키인 CSP) 과정에 어쩔 수 없이 평문 데이터로 보여지는 경우 SSP는 제로화 요구사항을 만족시킬 필요가 없다.

단지 **7.10**의 자가시험에만 사용하는 매개변수는 제로화 요구사항을 만족할 필요가 없다.

**보안수준 1**

보호하지 않은 SSP의 제로화는 모듈 운영자와 모듈의 독립적인 컨트롤(예: 하드 드라이브의 포맷, 재진입 중 모듈의 파괴)에 의해서 절차적으로 수행된다.

7.10.2 동작 전 자가시험

7.10.2.1 동작 전 자가시험 일반 요구사항

동작 전 자가시험

동작 전 자가시험 일반 요구사항

암호모듈에 전원이 인가되는 시점 또는 (전원 꺼짐, 리셋, 리부팅, 콜드스타트, 전원 인터럽트 등이 발생한 후) 인스턴스화되는 시점과 암호모듈이 동작 상태로 천이되기 직전 시점 사이에 암호모듈에 의해 동작 전 시험이 수행되고 성공적으로 통과되어야 한다[10.15].

암호모듈은 해당하는 경우 다음과 같은 동작 전 자가시험을 수행해야 한다[10.16].

• 동작 전 소프트웨어/펌웨어 무결성 시험

• 동작 전 우회 기능시험

• 동작 전 핵심 기능시험

동작 전 소프트웨어/펌웨어 무결성 시험

암호경계 내부의 모든 소프트웨어와 펌웨어 구성 요소는 7.5에 정의된 요구사항을 만족하는 검증대상 무결성 검증 기술을 이용하여 검증되어야 한다[10.17]. 검증이 실패하면 동작 전 소프트웨어/펌웨어 무결성 시험이 실패한다[10.18]. 이 표준의 보안 요구사항에서 제외된 소프트웨어나 펌웨어, 재구성이 불가능한 메모리에 저장된 실행 가능 코드는 동작 전 소프트웨어/펌웨어 무결성 시험을 실시할 필요가 없다.

하드웨어 암호모듈이 소프트웨어 또는 펌웨어를 포함하지 않는 경우, 모듈에는 동작 전 자가시험으로 7.10.3.2에 따라 적어도 하나의 암호알고리즘 자가시험이 구현되어야 한다[10.19].

동작 전 소프트웨어/펌웨어 무결성 시험을 위해 사용되는 검증대상 무결성 검증 기술에 사용되는 암호알고리즘은 우선 7.10.3.2에 따른 암호알고리즘 자가시험을 통과해야 한다[10.20].

동작 전 우회 기능시험

암호모듈에 우회 기능이 구현되는 경우, 우회 기능을 활성화하기 위해 필요한 통제 로직이 정확히 동작하는지 보증해야 한다[10.21].

암호모듈은 다음과 같은 방법에 의해 데이터 경로를 검증해야 한다[10.22].

• 우회 기능 스위치가 암호 프로세스를 지원하도록 설정되는 경우, 암호모듈이 우회 기능을 통하여 전달되는 데이터가 암호에 의해 처리되는지 검증을 수행함.

• 우회 기능 스위치가 암호 프로세스를 지원하지 않도록 설정되는 경우, 암호모듈이 우회 기능을 통하여 전달되는 데이터가 암호에 의해 처리되지 않는지 검증을 수행함.

동작 전 핵심 기능시험

암호모듈의 안전한 운영을 위해 동작 전 시험에서 시험해야 하는 핵심적인 보안기능이 있을 수 있다[10.23]. 동작 전 시험에 포함되는 핵심 기능에 대하여 개발 문서에 명세해야 한다[10.24].

조건부 자가시험

조건부 자가시험 일반 요구사항

다음 시험에 대하여 개발 문서에 명세된 조건이 발생하면 암호모듈에 의해 조건부 자가시험이 수행되어야 한다[10.25].

암호알고리즘 자가시험, 암호키 쌍 일치 시험, 소프트웨어/펌웨어 로드 시험, 수동 주입 시험, 조건부 우회 기능시험 및 조건부 핵심 기능시험

조건부 암호알고리즘 시험

암호알고리즘 시험은 부속서 C∼E에 명세된 목록 중 모듈에 구현된 검증대상 암호알고리즘에 대하여 모든 암호 기능(예: 암호알고리즘, SSP 설정 방법, 인증)이 수행되어야 한다[10.26]. 암호알고리즘이 최초로 사용되기 이전에 조건부 자가시험이 수행되어야 한다[10.27].

암호알고리즘 자가시험에는 기지 답안 시험(known-answer test), 비교 시험(comparison test), 오류탐지 시험(fault-detection test)이 있다.

기지 답안 시험은 결과를 생성하기 위해 암호알고리즘이 동작에서 알고 있는 입력 벡터(예: 데이터, 키 정보, 임의 길이의 상수)로 구성한다. 결과는 알고 있는 예상 출력 결과값과 비교한다.

시험의 수행으로 계산된 출력값이 이미 알고 있는 정답과 일치하지 않으면 암호알고리즘의 기지 답안 자가시험은 실패로 판정된다[10.28].

알고리즘의 자가시험은 암호모듈에서 지원하는 검증대상 키 길이, 모듈의 크기, DSA용 소수 또는 타원 곡선의 각각에 대하여 최소한 가장 작은 것을 사용해야 한다[10.29].

알고리즘이 다중 운영 모드(예: ECB, CBC)를 지원하는 경우, 자가시험에서 암호모듈이 지원하거나 검증기관이 지정하는 최소한의 한 개 이상의 운영 모드가 선택되어야 한다[10.30].

기지 답안 검사의 예:

• 일방향 함수: 입력 테스트 벡터가 예상되는 값과 일치하는 출력을 생성해야 한다[10.31].

(예: 해시, 키를 사용한 해시, 메시지 인증, 엔트로피 벡터가 고정된 난수 발생기, SSP 합의)

• 가역 함수: 전방향 또는 역방향 기능이 모두 자가시험을 통과해야 한다[10.32].

(예: 대칭키 암호화 및 복호화, SSP 전송용 암호화 및 복호화, 전자서명의 생성과 검증)

비교 시험은 암호알고리즘을 두 번 이상 독립적으로 구현한 후 두 개 이상 구현물의 출력값을 비교한다. 출력값이 일치하지 않으면 암호알고리즘의 비교 자가시험은 실패로 판정된다[10.33].

오류 탐지 시험은 암호알고리즘 구현 범위 내에서 오류 탐지 메커니즘들의 통합된 구현을 포함한다. 만약 오류가 탐지되면 암호알고리즘에 대한 오류 탐지 자가시험은 실패로 판정된다[10.34].

조건부 암호키 쌍 일치 시험

암호모듈이 공개키, 비밀키 쌍을 생성한다면, 부속서 C∼E의 암호알고리즘 명세에 따라 생성된 공개키, 비밀키 쌍에 대하여 암호키 쌍 일치 시험을 수행해야 한다[10.35].

조건부 소프트웨어/펌웨어 로드 시험

암호모듈이 외부에서 소프트웨어 또는 펌웨어를 로드하는 기능이 있을 때, 7.4.3.4에 추가하여 다음 요구사항이 충족되어야 한다[10.36].

• 암호모듈은 로드되는 소프트웨어 또는 펌웨어의 유효성 확인을 위해 검증대상 인증기술을 구현해야 한다[10.37].

• 참조될 인증키는 소프트웨어 또는 펌웨어가 로드되기 이전에 독립적으로 암호모듈에 로드되어야 한다[10.38].

• 적용된 검증대상 인증기술이 성공적으로 검증되어야 한다[10.39]. 그렇지 않으면 소프트웨어/펌웨어 로드 시험은 실패로 판정된다[10.40]. 소프트웨어/펌웨어 로드 시험의 실패 시 로드된 소프트웨어 또는 펌웨어는 사용될 수 없어야 한다[10.41].

조건부 수동 주입 시험

SSP 또는 키 구성 요소가 수동으로 암호모듈에 직접 주입되거나, 인간 운영자가 입력값을 잘못 주입하여 오류가 유발될 수 있는 경우, 다음과 같은 수동 주입 시험이 수행되어야 한다[10.42].

• SSP 또는 키 구성 요소에 오류탐지코드(EDC)가 적용되어야 한다[10.43]. 또는 중복 입력으로 주입되어야 한다[10.44].

EDC가 사용된다면 EDC는 적어도 16비트의 길이를 가져야 한다[10.45]. EDC 검증이 실패하거나 반복 입력된 값이 일치하지 않으면 해당 시험 항목은 실패로 판정된다[10.46].

7.10.3.8 조건부 우회 기능시험

암호모듈에 암호 처리 없이 서비스를 제공하는 우회 기능이 구현되어 있다면(예: 모듈을 통해 평문이 전송되는 경우), 다음과 같은 우회 기능시험이 수행되어 암호모듈의 구성 요소 가운데 단 하나라도 실패하는 경우 의도하지 않은 평문의 출력이 방지됨을 확인해야 한다[10.47].

암호모듈이 서로 배타적인 우회 서비스나 암호 서비스 중 하나만을 선택할 때, 암호 기능을 제공하는 서비스가 올바르게 동작하는지 시험해야 한다[10.48].

암호 처리를 지원하는 서비스와 암호 처리를 지원하지 않는 서비스를 제공하는 경우, 암호모듈이 우회 서비스와 암호 서비스를 자동적으로 선택할 수 있다면, 암호모듈은 전환 과정 통제 메커니즘이 변경될 때(예: IP 송신/수신 주소 테이블) 암호 처리를 지원하는 서비스의 정확한 동작을 시험해야 한다[10.49].

암호모듈이 우회 기능을 통제하는 내부 정보를 유지한다면, 암호모듈은 통제 정보의 변경이 진행되는 즉시 검증대상 인증기술로 통제 정보의 무결성을 검증해야 한다[10.50]. 그리고 통제 정보의 변경 직후 검증대상 인증기술을 이용하여 새로운 무결성 검증값을 생성해야 한다[10.51].

7.10.3.7 조건부 핵심 기능시험

암호모듈의 안전한 운영에 핵심적인 보안기능이 있으면 조건부 자가시험에 반영되어야 한다[10.52].

7.10.3.8 주기적인 자가시험

보안수준 1, 2

암호모듈에 대한 주기적 시험의 요청이 있으면 암호모듈은 동작 전 또는 조건부 자가시험을 실행해야 한다. 주기적 자가시험을 시작하기 위해 요청할 수 있는 수단은 제공되는 서비스 요청, 리셋, 리부팅 또는 반복적인 전원 인가 등이다[10.53].