情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

보안적합성 검증 및 암호검증 문서 작성법

김종길*, 나학연*, 정지훈*

요 약

최근의 국내 정보보호 인증체계는 암호검증제도의 시행과 CCRA 가입으로 큰 변화를 맞이하였다. 이런 변화는 국가기관의 정보보호제품 도입체계에도 많은 영향을 미치고 있다. 본 고에서는 정보보호제품 인증 체계 변화, 이 후의 개편된 보안적합성 검증제도에 대한 간략히 소개하고, 보안적합성 검증제도와 암호검증제도의 신청을 위한 제출 문서 작성법을 제시하여, 보안적합성 검증제도와 암호검증제도 신청 또는 연 도움을 주고자 한다.

Ⅰ. 서 론

최근의 암호검증제도의 시행과 CCRA 가입으로 인해 국내 정보보호 제품 인증 체계는 큰 변화를 맞이하였다. 또한 국가기관은 정보보호제품의 국가기관 도입을 위한 보안적합성 검증의 전제 조건으로 암호검증 또는 CC 평가인증을 요구하고 있어, 많은 정보보호업체의 관심은 어느 때보다 커지고 있다.

국내의 정보보호제품의 평가 체계는 CC 평가·인증 체계, 보안적합성 검증제도, 암호모듈 시험 및 검증 제도(이하 '암호검증제도')로 나누어 질 수 있다. 이 중 보안적합성 검증은 정보보호제품의 국가도입 시 적합성을 검증하는 제도로, 크게 CC 평가·인증을 획득한 제품과 암호검증제도에 의해 검증 받은 암호모듈을 탑재한 제품 그리고 소자 장비와 같이 CC평가나 암호검증제도 대상에서 벗어나는 제품을 그 대상으로 한다. 보안적합성 검증 신청을 위해서는 국가기관의 도입이 전제되어야하며, 신청주체도 국가기관이 된다.

CC 평가·인증은 CCRA에 의한 국제 상호 인증 체계로 국내에서 국가정보원을 인증기관으로 하고, 인증기관에서 인정한 KISA, KTL, KOSYAS가 평가기관으로서 평가를 수행하고 있다.

암호검증제도는 S/W, F/W, H/W 또는 그 조합의 형태로 이루어진 암호모듈에 대한 구현정확성을 시험 및 검증하는 제도로 암호검증기관은 국가정보원이며, 암호시험기관은 국가보안기술연구소로 한다. 암호검증제도에 의해 검증된 암호모듈을 탑재한 정보보호제품의 경우, 보안적합성 검증 대상 정보보호제품이 될 수 있다.

본 고에서는 보안적합성 검증 제도와 암호검증제도에 대해 설명하고, 각 제도의 제출문서 작성법을 제시하고자 한다.

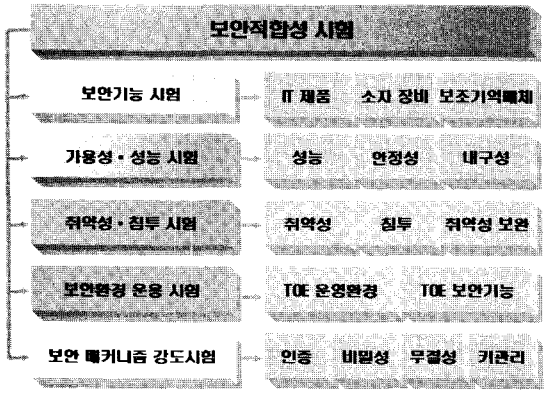
Ⅱ. 보안적합성 검증제도 개요

정보보호제품이 보안적합성 시험을 신청하기 전에 CC평가와 암호검증제도 중 어느 것을 먼저 받아야하는지는 신청자가 선택하는 것이 아니라 제품의 성격에 달려 있다. IT인증사무국에서는 네트워크/컴퓨팅 제품군은 CC 평가를, 암호기반제품은 암호검증을 받도록 규정하고 있다.

보안적합성 검증 제품 중 CC평가나 암호검증제도의 대상에서 벗어나는 보안 제품은 보안 USB 제품, 자료완전삭제 제품과 SI사업의 형태로 국가기관에 특화되어 도입되는 제품(이하 '비상용 제품')이 있으며, 이런 제품에 대해서는 적합성 시험뿐 아니라, 보안 기능에 대한 시험도 수행한다.

보안적합성 검증은 정보보호제품의 국가도입 시, 제품이 국가기관의 정보통신환경에 적합한지 여부를 판단하기 위한 제도로 크게 5가지 시험으로 나누어지며, 각각에 대한 시험은 [그림 1]과 같다. 각 시험 항목은 CC 기준이나 암호검증기준과 상당부분이 중복되나, 이는 비상용 또는 보안 USB 제품의 평가를 위한 것으로 CC

* 한국전자통신연구원 부설연구소 (lithium@ensec.re.kr)



〔그림 1〕 보안적합성 시험 개요

평가와 암호검증을 획득한 제품에 대한 중복된 보안기능 시험이나 보안 메커니즘 강도 시험 등의 시험은 수행하지 않는다. 하지만 제품이 획득한 보증등급이나 보안등급이 국가기관에서 요구하는 수준에 맞지 않을 경우, 추가 또는 재시험을 수행할 수 있으며, 개발자는 이를 위한 문서 또는 제품을 검증기관에 제출해야한다.

보안적합성 시험의 사례별 제출물 구분은 다음과 같다. [표 1]은 CC 평가·인증필 제품과 암호검증필 제품이 보안적합성 시험 시, 제출하여야할 문서의 목록이다. 이 외에 필요 시, 검증기관 또는 시험기관의 요구에 따라 추가적인 문서 제출이 있을 수 있다.

[표 2]는 저장매체 완전삭제 제품, 보안 USB 및 비상용 제품이 보안적합성 시험 시 제출하여야할 문서의 목록이다. 이 외에 필요 시, 검증기관 또는 시험기관의 요구에 따라 추가적인 문서 제출이 있을 수 있다.

〔표 1〕 제품사례별 보안적합성 검증 제출문서-1

	CC 평가·인증필 제품	암호검증필 제품
신청자 제출문서	보안적합성 검증신청서 사용자 보안요구사항 정보통신망 구성도	
개발자 제출문서	CC인증서 사본	(암호모듈을 제외한 부분에 대한) 보안목표명세서 보안기능 설계서 형상관리문서 제품 설명서 취약성 분석서 시험결과서 암호검증서 사본

〔표 2〕 제품사례별 보안적합성 검증 제출문서-2

	저장매체완전삭제	보안 USB/ 비상용 제품
신청자 제출문서	보안적합성 검증신청서 사용자 보안요구사항	
개발자 제출문서	보안기능 설계서 제품 설명서 시험 결과서	
		보안목표명세서 형상관리문서 취약성 분석서

Ⅲ. 보안적합성 검증 제출물 작성법

보안적합성 검증을 위한 문서의 작성법을 위해 공개된 기준은 없지만, 작성 방식은 가능한 CC의 작성방식을 따르도록 권고하고 있다. 이는 신청 제품별로 그 구성이나 기능이 매우 다양하기 때문이며, 작성법 역시 이런 다양성 때문에 세부적으로 일반화하여 설명하기에는 어려움이 있다.

3.1. 보안목표명세서

보안목표명세서는 보안문제의 범위와 특정 제품이나 시스템에 적용할 수 있는 보안기능을 정의한다. 보안목표 명세서는 검증대상제품 평가의 근거로 사용되는 보안기능과 설계 명세서의 집합이 된다. 보안목표명세서의 목차 예시는 다음과 같다.

1. 보안목표명세서 소개
1.1 보안목표명세서 식별
1.2 보안목표명세서 개요
2. 검증대상제품 설명
3. 보안환경
3.1 가정사항
3.2 위협
3.3 조직의 보안정책
4. 보안목적
4.1 보안목적
4.2 환경에 대한 보안목적
5. 보안기능 대한 보안요구사항
6. 이론적 근거
6.1 보안목적의 이론적 근거
6.2 보안기능의 이론적 근거

3.2. 형상관리문서

형상관리문서는 제품 형상과 관련 정보를 분류 또는 변경하는 과정이 규칙적이고 체계적인 관리 하에 이루어지는 지 확인하기 위한 문서이다. 형상관리문서를 통해 제품의 무결성이 유지됨을 보장되어야 한다. 형상관리문서는 인가되지 않은 추가, 변경, 삭제를 방지하여 평가에 사용된 검증대상제품 및 문서가 배포될 것과 동일함을 보증하는 역할을 한다. 형상관리문서의 목차 예시는 다음과 같다.

1. 검증대상제품 식별
2. 형상목록
2.1 형상항목 식별자 부여방법
2.2 형상항목
3. 형상관리시스템
3.1 형상항목 관리절차
3.2 개인의 역할과 책임
3.3 변경 보증절차
3.4 일치성 보증절차
3.5 버전 관리 방법
3.6 형상항목 접근 통제 방법
3.7 형상관리 기록

3.3. 보안기능 설계서

보안기능 설계서는 크게 기능명세, 상위설계 그리고 하위설계로 나누어진다. 기능명세는 보안목표명세서에 기술된 보안기능을 좀 더 상세하게 기술하는 문서로 실제 사용자가 볼 수 있는 인터페이스와 동작에 대한 기본 설명을 포함해야한다. 상위설계는 보안기능을 주요 구성단위(Sub System)로 서술하고, 구성단위와 이 들이 제공하는 기능과의 관계를 설명한다. 상위설계에서는 앞에서 언급된 기능명세를 서브시스템단위로 상세화하여야 한다. 하위설계는 보안기능 내부 동작에 대한 모듈과 모듈간의 상호관계 및 종속관계를 설명하여야 한다. 이를 위해 서브시스템을 모듈로 상세화하고, 보안기능에 관여하는 각 모듈에 대하여 목적, 기능, 인터페이스, 종속관계, 보안기능 수행의 구현 등을 설명하여야 한다. 기본 및 상세설계서의 목차 예시는 다음과 같다.

1. 기능명세
1.1 구성 기능
1.2 서브 시스템간의 연관 관계
1.3 모듈 구성
2. 상위설계
2.1 기능요소
- 정의 및 기능
- 모듈의 연관 관계
2.2 가정사항
- 사전설치 S/W 기능
- 연관관계
3. 하위설계
3.1 식별 및 인증
3.2 기밀성
3.3 무결성
3.4 접근통제

3.4. 제품설명서

제품 설명서는 관리자 설명서, 사용자 설명서, 설치 지침서로 나누어진다. 관리자 설명서는 관리자의 시험대상제품에 의해 제공되는 보안기능에 대한 이해를 돕기 위한 문서이다. 사용자 설명서는 사용자가 사용할 수 있는 보안기능 및 안전하게 사용하기 위한 지시와 지침을 서술한 문성이다. 설치 지침서는 검증대상제품의 설치, 생성, 시동, 제거에 대한 지침을 제공한다. 제품설명서의 목차 예시는 다음과 같다.

1. 관리자 설명서
1.1 보안기능
- 목적, 행위, 인터페이스와의 상호관계, 보안 파라미터
1.2 인터페이스
- 목적, 보안기능성, 호출방법, 보안 파라미터
1.3 안전한 운영
- 기능과 특권에 대한 통제
- 관리자와 관련된 가정사항
- 관리자와 관련된 IT 환경에 대한 보안요구사항
- 보안관련 사건
2. 사용자 설명서
2.1 보안기능
- 목적, 행위, 인터페이스와의 상호관계, 보안 파라미터
2.2 인터페이스
- 목적, 보안기능성, 호출방법, 보안 파라미터
2.3 안전한 운영

- *기능과 특권에 대한 통제*
- *사용자와 관련된 가정사항*
- *사용자와 관련된 IT 환경에 대한 보안요구사항*

3. 설치 지침서

3.5. 취약성 분석서

취약성 분석서는 오용분석과 취약성 분석으로 나뉜다. 오용분석은 관리자 또는 사용자가 안전하지 않은 방식으로 검증대상제품을 구성 또는 설치할 가능성을 줄여준다. 또한, 운영 시, 사람 또는 기타 오류에 의해 보안기능을 비활성화 되거나, 무력화 될 위험을 최소화할 수 있다. 취약성 분석에서는 다음의 내용이 분석되어져야한다.

- 자원에 대한 사용자의 인가되지 않은 접근 허용
- 보안기능을 방해 또는 변경할 가능성
- 사용자간의 인가된 능력을 방해 여부

이를 통해 취약성 분석에서는 식별된 취약성들이 검증대상제품의 예상된 환경 내에서 악용될 수 없고, 시험대상제품이 명백한 침투 공격에 내성을 기술하여야한다. 취약성 분석서의 목차 예시는 다음과 같다.

1. 오용분석
1.1 관리자 설명서 분석
1.2 사용자 설명서 분석
1.3 설치, 생성, 시동절차 분석
2. 취약성 분석
2.1 정보보호방식 분석
- *식별 및 인증 방식*
- *비밀통신 방식*
- *데이터 보호 방식*

2.2 취약성 분석
- *취약성 식별*
- *식별된 취약성의 악용 여부 분석*
- *이론적 근거*

3.6. 시험결과서

시험결과서는 제품에 구현된 시험대상제품의 보안기능이 정확하게 동작하는 지 여부를 입증하기 위한 시험계획, 절차, 결과를 기술한다. 시험결과서를 통해 작성자는 기능이 명세대로 동작하고, 보안기능이 보안목표명세서의 기능요구사항을 만족함을 입증하여야 한다. 시험결과서의 목차예시는 다음과 같다.

1. 시험계획
1.1 시험구성 및 환경
1.2 시험항목
2. 시험절차
3. 시험결과
3.1 예상 시험 결과
3.2 실제 시험 결과

Ⅳ. 암호모듈 검증 제도 개요

암호모듈의 신청은 국가기관이 아니라, 개발업체가 하며, 신청접수는 시험기관이 진행한다. 시험기관은 시험 종료 후, 검증 기관에 시험 결과에 대한 검증을 요청하고, 검증기관은 검증 위원회를 통해 시험 결과를 검증하고, 검증필증을 발급한다.

암호모듈 검증제도의 대상 제품은 어떠한 형태로든 모듈화된 암호모듈을 대상으로 한다. 기준에서는 S/W, F/W, H/W 또는 그 조합이라고 명시되어 있는 것은 암호모듈의 구성형태에는 제한을 두지 않음을 의미한다. 하지만 암호모듈을 신청하기 위해서는 반드시 모듈화된 제품이어야 하며 이는 암호모듈이 뚜렷한 논리적 또는 물리적 경계를 가져야함을 의미한다.

암호검증 시에 제출하여야 할 문서는 총 6종으로 [표 3]과 같다.

〔표 3〕 암호검증 제출문서 목록

암호검증 제출문서
기본 및 상세설계서
형상관리문서
제품 사용 설명서
취약성에 대한 분석과 대응 방법 기술문서
암호모듈 보안정책
시험 결과서

Ⅴ. 암호모듈 검증 제출물 작성법

암호검증 기준의 문서화 요구사항을 요약한 것이다. 암호모듈 제작자는 다음의 내용을 명세해야 한다.

5.1. 기본 및 상세설계서

5.1.1. 암호모듈 명세

- 암호모듈의 H/W, S/W 및 F/W 구성요소의 명세해야 한다. 각 구성요소의 암호경계 및 암호모듈의 물리적인 환경에 대해 명세해야 한다.
- 본 기준의 보안 요구사항에서 제외된 암호모듈의 H/W, S/W 및 F/W 구성요소와 제외된 이유에 대해 명세해야 한다.
- 암호모듈의 물리적 포트와 논리적 인터페이스에 대해 명세해야 한다.
- 암호모듈의 수동 또는 논리적 제어, 물리적 또는 논리적 상태 표시기, 물리적/논리적/전기적 특성을 명세해야 한다.
- 암호모듈에 사용된 검증대상 및 비검증대상 동작 모드의 명세 및 이에 채택된 검증대상 및 비검증대상 보호함수의 목록이 있어야한다.
- 암호모듈의 주요 H/W 구성요소와 구성요소 연결부를 설명하는 블록 다이어그램이 있어야 한다.
- 암호모듈의 H/W, S/W 및 F/W 설계를 명세해야 한다.
- 개인키 및 비밀키(키 값은 평문과 암호문 모두를 말함), 인증 데이터(패스워드, PIN 등), 핵심 보안 매개변수 및 보안감사 사건 및 보안감사 데이터와 같이 노출 시에 암호모듈의 안전성을 침해할 수 있는 정보에 대해 명세해야 한다.
- 암호모듈의 보안정책에 대해 명세해야 한다. 보안정책은 본 기준의 요구사항으로부터 도출된 규칙 및 제조업체가 제시한 추가적인 요구사항으로부터 도출된 규칙을 포함해야 한다.

5.1.2. 암호모듈 포트와 인터페이스

- 암호모듈의 물리적 포트, 논리적 인터페이스, 모든 입·출력 데이터 경로에 대해 명세해야 한다.

5.1.3. 역할, 서비스 및 인증

- 암호모듈이 제공하는 인가된 역할(role)에 대해 명세해야 한다.
- 암호모듈이 제공하는 인가된 그리고 비인가 된 서비스, 운영, 기능에 대해 명세해야 한다. 각 서비스에 대해, 서비스 입력과 이에 대응되는 서비스 출력 및 서비스가 수행되는 역할에 대해 명세해야 한다.
- 암호모듈이 제공하는 인가된 역할을 요구하지 않는 서비스에 대해 명세해야 한다. 또한, 이러한 서비스가 암호키나 핵심 보안 매개변수 등을 수정/노출/대체하지 않는 방법, 수정/노출/대체되었을 경우 암호모듈의 안전성에 미치는 영향을 명세해야 한다.
- 암호모듈이 제공하는 인증 메커니즘, 인증 메커니즘을 수행하는데 필요한 인증 데이터, 암호모듈로의 최초 접근에 대한 통제 방법, 인증 메커니즘 초기화, 인증 메커니즘의 강도 등에 대해 명세해야 한다.

5.1.4. 유한상태모델

- 유한상태모델은 상태 천이도와 상태 천이표로 표현되며, 이 표현 매체는 동작상태, 오류상태, 상태천이, 상태천이를 일으키는 입력 사건(데이터 입력, 제어 입력 포함) 및 상태천이에서 야기된 출력 사건(내부 암호모듈 상태, 데이터 출력, 상태 출력 포함)을 명세해야 한다.

5.1.5. 물리적 보안

- 암호모듈의 물리적 보안 메커니즘이 구현하고자 하는 보안등급 및 물리적 구현형태에 대해 명세해야 한다. 암호모듈이 사용하는 물리적 보안 메커니즘에 대해 명세해야 한다.
- 암호모듈의 내용물에 대해 물리적으로 접근할 수 있는 유지관리 역할이 암호모듈에 포함되거나 물리적인 접근을 허용하도록 설계된 경우, 유지관리에 대한 접근 인터페이스를 명세해야 한다. 또한 유지관리 인터페이스 접근 시 평문으로 된 비밀키 및 핵심 보안 매개변수가 어떻게 제로화 되는 지 명세해야 한다.
- 암호모듈의 정상동작 범위를 명세해야 한다. 암호모듈에 채택된 환경장애보호 또는 환경장애시험을 명세해야 한다.

5.1.6. 운영환경

- 암호모듈의 운영환경을 명세해야 한다.
- 암호모듈 운영체제의 보호 프로파일 준수여부 및 CC 보증 등급을 확인해야 한다.

5.1.7. 암호키의 관리

- 암호모듈에 사용된 모든 암호키, 암호키 구성요소 및 핵심 보안 매개변수를 명세해야 한다.
- 암호모듈에 사용된 난수발생기(검증대상/비검증대상 모두 포함)를 명세해야 한다.
- 암호모듈에 사용된 키 생성(검증대상/비검증대상 모두 포함) 방법을 명세해야 한다.
- 암호모듈에 사용된 키 합의 방법을 명세해야 한다.
- 암호모듈에 사용된 키 주입과 출력 방법을 명세해야 한다.
- 지식분산(split knowledge) 방법 사용 시 비밀 분산 방법을 명세해야 한다. 키를 복원하는데 n개의 정보가 필요하다면 (n-1)개의 정보로부터 키에 대한 어떤 정보도 노출되지 않는다는 증명을 포함해야 한다(보안등급 3, 4).
- 키 저장 방법에 대해 명세해야 한다.
- 키 제로화 방법에 대해 명세해야 한다.

5.1.8. 전자파 장해 및 전자파 적합성

- 전자파 장해 및 전자파 적합성 요구사항에 따른 증명서를 제출해야 한다.

5.1.9. 자기시험(Self-tests)

- 전원인가와 조건부 시험을 포함한 자가시험을 명세해야 한다.
- 자가시험 실패 시, 암호모듈에 생기는 오류 상태를 명세해야 한다. 오류 상태를 종료하고 정상 상태로 진입하기 위해 필요한 조건과 동작을 명세해야 한다.
- 암호모듈의 안전한 동작 위한 중요 보안 기능에 대해 명세 및 이에 적용 가능한 전원인가 시험과 조건부 시험에 대한 확인해야 한다.
- 암호모듈이 우회기능을 수행할 때, 절차를 전환하는 메커니즘이나 논리를 명세해야 한다.

5.2. 형상관리문서

5.2.1. 대상제품 식별

- 형상관리되는 검증대상제품이 다른 버전의 검증대상제품과 관련되지 않음을 보장해야 한다.
- 유일한 검증대상제품 버전과 명칭을 명세해야 한다.

5.2.2. 형상목록

- 형상관리하의 형상항목을 식별하고, 각 형상항목에 대한 식별번호 및 이를 부여하는 방법을 명세해야 한다.
- 형상항목(암호 검증 시 제출하는 모든 문서, 검증대상 소프트웨어, 구현물, 구현과 관련되어 보고된 보안결함들에 관한 사항들을 기록하기 위해 사용된 문서)

5.2.3. 형상관리시스템

- 개발 환경에서 형상관리시스템에 의해 수행되는 모든 활동을 명세해야 한다.
- 개별적인 형상항목을 운영(생성, 수정 및 삭제)하기 위해 요구되는 개인의 역할과 책임에 대해 명세해야 한다.
- 인가된 개인만이 형상항목에 대한 변경을 할 수 있다는 것을 보장하기 위해 사용된 절차를 명세해야 한다.
- 개발주기에서 하나의 형상항목에 대한 동시 등 같은 병해성 문제가 발생하지 않는다는 것을 보장하기 위해 사용된 절차를 명세해야 한다.
- 형상관리 되는 형상항목들을 유일하게 식별할 수 있게 형상 항목들의 버전을 제어하는 방법을 명세해야 한다.
- 형상항목에 대한 우회적인 접근을 방지하기 위한 접근통제 방법을 명세해야 한다.
- 형상관리시스템에서 사용된 절차를 적용함으로써 결과로 생성되는 증거물을 명세해야 한다.
- 형상항목 변경에 따른 설명, 책임, 영향을 받는 모든 형상항목 식별, 상태(진행중, 완료), 변경 날짜 및 시간 기록을 명세해야 한다.
- 형상목록 유지 및 버전관리를 지원하는 자동화 도구에 대해 명세해야 한다.

5.3. 제품 사용 설명서

5.3.1. 설계보증

- 암호모듈의 안전한 설치, 생성 및 시작에 대한 절차를 명세해야 한다.
- 암호모듈의 버전을 인가된 운영자에게 분배 및 배포하는 동안 보안을 유지하기 위해 필요한 절차를 명세해야 한다.
- 암호모듈의 H/W, S/W 및 F/W 구성요소의 설계와 암호모듈 보안정책의 대응관계를 명세해야 한다.
- 암호모듈이 S/W나 F/W 구성요소를 포함하고 있으면, S/W나 F/W 구성요소와 암호모듈 설계의 대응관계를 설명하는 주석이 첨부된 소스코드를 제출해야 한다.
- 암호모듈이 H/W 구성요소를 포함하고 있으면, H/W에 대한 구성도 또는 HDL를 제출해야 한다.
- 암호모듈, 암호모듈의 외부 포트/인터페이스 그리고 인터페이스의 목적에 대한 비정형적 기능을 명세해야 한다.(보안등급 2, 3, 4)
- 암호모듈 보안정책의 특성 및 규칙을 기술하는 정형 모델 명세, 정형모델은 집합론, 1차 논리 같은 수학에 기반을 둔 엄격한 표기로 이루어진 정형 명세 언어로 표현된다(보안등급 4).
- 정형 모델이 암호모듈 보안정책에 대하여 일관성과 완전성을 유지한다는 근거를 명세해야 한다.(보안등급 4)
- 정형모델과 기능 명세간의 대응관계에 대한 비정형적인 증명을 명세해야 한다.(보안등급 4)
- 각 H/W, S/W 및 F/W에 대하여 다음 두 가지를 명세하는 주석이 포함된 소스코드 첨부(보안등급 4)

① 정확한 실행을 위한 암호모듈 구성요소, 기능 또는 절차의 입력에 요구되는 선행조건(precondition)
② 암호모듈 구성요소, 기능 또는 절차가 완전할 때 참(True)이 될 것을 기대하는 후위조건(postcondition)

- 암호모듈의 설계와 기능 명세 사이의 대응관계에 대한 비정형적인 증명에 대해 명세해야 한다.

5.3.2. 암호 관리자 지침서

- 암호 관리자가 사용할 수 있는 암호모듈의 관리기능, 보안사건, 보안 매개변수(적당한 매개변수 값), 물리적 포트 및 논리적 인터페이스를 명세해야 한다.
- 암호모듈을 안전한 방법으로 관리하기 위한 절차를 명세해야 한다.
- 암호모듈의 안전한 운영에 관련된 사용자 행위에 관한 가정사항을 명세해야 한다.

5.3.3. 암호 관리자 지침서

- 암호모듈 사용자가 사용할 수 있는 검증대상 보호함수, 물리적 포트, 논리적 인터페이스를 명세해야 한다.
- 암호모듈의 안전한 운영을 위해 필요한 모든 사용자 책임를 명세해야 한다.

5.3.4. 암호모듈화 된 설계

- 모듈화된 설계가 추천된다. 각 S/W 암호모듈은 잘 정의되고 쉽게 이해되는 논리적 인터페이스 가져야 한다.
- S/W 구성요소는 데이터 추상화 원칙을 사용하여 구조화되어야 한다. 가능하다면 객체 지향적이고 추상적인 데이터 형식을 지원하는 고급 언어가 사용되어야 한다.
- S/W는 계층화되어 설계되어야 한다.

5.3.5. 소프트웨어 암호모듈/프로시저 인터페이스

- S/W 암호모듈 또는 프로시저로의 입력은 명시적으로 정의된 인터페이스의 외부 호출 통해 이루어져야 한다.
- 각 프로시저는 1개의 진입지점과 최대 두개의 퇴장지점(정상적인 퇴장과 오류 시 퇴장)이 있어야 한다.
- 데이터는 S/W 암호모듈 사이에서 또는 프로시저 사이에서 인수 리스트 및 명시적인 반환 값을 사용을 통해 통신되어야 한다. 전역변수는 추상 데이터 형식을 구현할 때를 제외하고는 각 프로시저에서 사용되어서는 안 된다. 입력 값의 오류 범위가 확인되어야 한다.

5.3.6. 내부 구조

- 각 프로시저는 반드시 1개의 잘 정의된 함수를 수행해야 한다.

- 실행을 위한 단일 스레드 내에서 제어 흐름은 순차적으로 그리고 조건 분기문과 반복문 등을 사용하여 정의되어야 한다.
- 동시 수행이 가능할 경우, S/W 구성요소는 동시 실행수의 상계를 엄격하게 제한해야 하며 공유 데이터의 접근 통제를 위해 구조화된 동기화 구성을 사용해야 한다.
- 충돌되는 목적의 위한 복수의 메모리 사용을 허가하기 위해 동일 변수를 사용해서는 안 된다.
- 강한 명령어 파싱과 범위 체크 메커니즘은 범위 초과 파라미터와 입출력 버퍼 오버플로우 등을 방지하기 위해서 구현되어야 한다.

5.3.7. 소프트웨어 소스코드의 문서화

- 각 S/W 암호모듈, 절차 및 주요 프로그램 구조는 선/후조건 명세에 따른 기능을 명시하도록 문서화되어야 한다.
- 각 반복문은 종료가 보장할 수 있는 신뢰된 인수를 갖도록 한다.
- 변수명은 동일 프로시저 내에서 한번만 사용되어야 한다.
- 각 변수에는 변수의 목적에 맞는 주석이 붙어야 하며, 범위를 명시해야 한다.
- 동시 실행이 적용될 경우, 문서는 동시 실행수의 상계를 어떻게 제한하는지와 공유 데이터의 접근 동기화가 어떻게 이루어지는지 명세해야 한다.

5.3.8. 어셈블리 언어

어셈블리 언어가 사용될 경우 다음의 프로그래밍 방식이 추가 적용되어야 한다.

- 모든 코드는 독립적으로 위치해야 한다. 단 안전성, 효율성, 하드웨어 제약이 위치 의존성을 요구할 때에는 제외한다.
- 모든 레지스터 참조는 상징적인(symbolic) 레지스터 명을 사용해야 한다.
- 자가 수정(self-modifying) 코드는 사용하면 안 된다.
- 모든 프로시저는 각 프로시저 내에서 사용된 레지스터의 내용을 저장하고 복구할 책임이 있다.
- 제어 흐름 명령어는 숫자를 사용하면 안 된다.
- 각 유닛은 유닛에 레지스터 사용을 기술하는 주석을 포함해야 한다.

5.4. 취약성에 대한 분석과 대응 방법 기술문서

5.4.1. 기타 공격에 대한 대응

- 암호모듈이 1개 이상의 공격을 완화하도록 설계된 경우, 해당 공격을 완화하기 위한 보안정책과 메커니즘을 명세해야 한다.

5.5. 암호모듈 보안정책

암호모듈 보안정책은 개발자에 의해 문서에 포함되어야 한다. 다음은 보안정책의 내용을 기술한 것이다.

5.5.1. 암호모듈 보안정책의 정의

암호모듈 보안정책은 다음의 사항으로 이루어져 있다.

- 암호모듈이 동작되는 보안규칙의 명세로 보안규칙은 본 기준의 요구사항과 개발자 또는 판매자가 추가적으로 부과하는 보안규칙을 포함한다.

다음의 질의에 대해 자세하게 명세해야 한다.

- 역할 Z에서 서비스 Y를 수행하는 운영자 X는 암호모듈에 포함되는 모든 역할, 서비스, 보안관련 데이터 항목에 접근하기 위한 보안 관련 데이터 항목 W에 접근하기 위해 무엇을 해야 하는가?
- 암호모듈을 보호하기 위해서 어떤 물리적인 보안 메커니즘을 구현하였고, 물리적인 안전성을 유지하기 위해서 요구되는 조치는 무엇인가?
- 본 기준에서 정의되지 않은 시험 가능한 요구사항이 적용된 공격을 완화하기 위해 암호모듈에 어떤 보안 메커니즘이 구현되었는가?

5.5.2. 암호모듈 보안정책의 목적

암호모듈 보안정책을 개발하고 이행하는 이유는 크게 두 가지로 요약된다.

- 암호모듈이 국가기관의 보안정책을 만족시키는지 판단할 수 있는 암호학적 안전성을 명세해야 한다.

- 암호모듈이 제공하는 성능, 보호 및 접근권한을 국가기관에게 설명함으로써, 암호모듈이 국가기관의 안전성 요구사항을 적절하게 지원하는 지 평가할 수 있도록 한다.

5.5.3. 암호모듈 보안정책의 명세

암호모듈 보안정책은 역할, 서비스, 암호키 및 핵심 보안 매개변수의 관점에서 표현되어야 한다. 보안정책은 최소한 다음의 사항을 명세해야 한다.

- 식별 및 인증(identification and authentication : I&A) 정책
- 접근통제 정책
- 물리적 보안 정책
- 기타 공격에 대한 완화 정책

5.5.4. 식별 및 인증 정책

암호모듈 보안정책은 다음을 포함하여 식별 및 인증 정책을 명시해야 한다.

- 모든 역할(사용자, 보안관리자, 유지관리 등)과 이것과 결합된 인증 방식(신원 기반, 역할 기반 등)
- 각 역할과 운영자에 요구되는 인증 데이터(패스워드, 생체 데이터 등)와 이에 해당하는 인증 메커니즘의 강도

5.5.5. 접근통제 정책

암호모듈 보안정책은 접근통제 정책을 명시해야 한다. 서비스를 수행되는 동안 운영자가 접근하는 암호키, 핵심 보안 매개변수 그리고 이 변수에 접근하기위해 운영자가 가지는 접근 형태를 판정할 수 있도록 자세히 기술어야 한다. 접근통제 보안정책은 다음을 명세해야 한다.

- 암호모듈이 제공하는 모든 역할
- 암호모듈이 제공하는 모든 서비스
- 다음 사항을 포함하여 암호모듈에서 사용되는 모든 암호키 및 핵심 보안 매개변수
  - 평문과 암호문으로 된 비밀키, 개인키 및 공개키
  - 패스워드 또는 개인식별번호(PIN)와 같은 인증 데이터
  - 기타 보안 관련 정보(예: 감사 사건과 감사 데이터)
- 각 역할에 따라, 운영자가 역할 내에서 수행하도록 인가된 서비스
- 각 역할 내의 각 서비스에 따라, 암호키와 핵심 보안 매개변수로의 접근 형태

5.5.6. 물리적 보안 정책

암호모듈 보안정책은 다음을 포함하여 물리적 보안 정책을 명세해야 한다.

- 암호모듈에 구현된 물리적 보안 메커니즘(예: 불법조작 증거 봉인, 잠금장치, 불법조작 대응 및 제로화 스위치, 경보 등)
- 물리적 보안의 유지를 보장하기 위해 운영자가 취해야 할 조치(예: 불법조작 증거 봉인의 주기적인 관찰, 불법조작 대응과 제로화 스위치의 시험)

5.5.7. 기타 공격에 대한 완화 정책

암호모듈 보안정책은 공격을 완화하기 위해 구현된 보안 메커니즘을 포함하여 기타 공격의 완화에 대한 보안정책을 명시해야 한다.

5.5.8. 보안 정책 체크리스트 표

다음의 체크 리스트는 보안정책이 완성되었음을 보장하는 지침서로 활용될 수 있으며, 적절한 세부사항을 포함해야 한다.

〔표 4〕 역할 및 요구되는 식별과 인증

역할(role)	인증 형태	인증 데이터
…	…	…
…	…	…

〔표 5〕 인증 메커니즘 강도

인증 메커니즘	메커니즘 강도
…	…
…	…

〔표 6〕 역할에 인가된 서비스

역할	인증된 서비스
…	…
…	…

〔표 7〕 서비스 내의 접근권한

서비스	암호키 및 핵심 보안 매개변수	접근 형태
…	…	…
…	…	…

〔표 8〕 물리적 보안 메커니즘의 관찰/시험

물리적 보안 메커니즘	추천되는 관찰/시험 빈도	관찰/시험 지침 세부사항
…	…	…
…	…	…

〔표 9〕 기타 공격의 완화

기타 공격	완화 메커니즘	특정 제한
…	…	…
…	…	…

5.6. 시험절차 및 결과서

- 기본 및 상세설계서와 일치되는 시험항목에 대한 시험계획, 시험절차 설명, 예상 시험결과, 실제 시험결과를 명세해야 한다.
- 시험계획은 시험대상 보안기능과 시험목적을 명세해야 한다.
- 시험절차는 기능 시험을 위한 계획 및 순서를 명세해야 한다.
- 시험대상 보안기능을 시험하기 위한 시험도구 및 시험 시나리오를 포함하는 시험환경에 대해 명세해야 한다.
- 시험해야 할 보안기능, 식별된 보안기능별 시험항목, 시험이 무엇을 하는지 나타내는 시험항목에 대해 명세해야 한다.
- 각각의 기능을 시험하기 위한 항목별 시험절차를 명세해야 한다.
- 시험이 성공적으로 수행될 경우의 예상 결과를 명세해야 한다.
- 실제 시험결과를 획득하기 위한 모든 절차를 명세해야 한다.

※만약 예상 시험결과와 실제 시험결과가 차이가 발생한다면 차이에 대한 정당한 이론을 제시해야 함

Ⅵ. 결 론

최근의 국내 평가 제도의 변화는 국가기관의 정보보호제품 도입체계에도 많은 영향을 미치고 있다. 특히, 국가기관 도입을 위한 보안적합성 검증제도도 이러한 흐름에 발 맞추어 다양화 되었고, 검증 제품의 범위도 확대되어 가고 있다.

암호검증제도 역시 최근 암호검증필 암호모듈을 탑재한 제품에 보안적합성 검증제도를 신청할 수 있는 자격을 부여함으로써, 그 관심이 커지고 있는 실정이다.

본 고에서는 이러한 변화 속에서 보안적합성 검증제도와 암호검증제도에 대한 이해를 높이고, 제출문서 작성에 대한 부담을 줄이고자 간략한 제도 소개와 신청 시 필요한 제출문서 작성법을 제시하였다. 아무쪼록 제시한 작성법이 국내 정보보호관련 업체들의 제출문서 작성의 부담을 줄이기 위해 널리 사용되었으면 하는 바람이다.

참고문헌

[1] 한국전자통신연구원 부설연구소, "국가용 IT 제품 보안적합성 시험 기준 V1.0", 2007

[2] 한국전자통신연구원 부설연구소, "암호시험기준 V1.0", March 2007.

[3] 국가정보원, "암호검증기준 V1.2", Dec 2006. 12.

〈著者紹介〉

김 종 길 (Jongkil Kim)

2002년 2월 : 한국과학기술원 산업공학과 졸업
2004년 2월 : 한국과학기술원 산업공학과 석사
2004년 3월~현재 : 한국전자통신연구원 부설연구소
<관심분야> 정보보호제품 시험 및 평가

나 학 연 (Hacyun Na)

1999년 2월 : 숭실대학교 컴퓨터학부 학사 졸업
2001년 2월 : 숭실대학교 소프트웨어공학과 석사 졸업
2006년 3월 ~ 현재 : 충남대학교 컴퓨터공학과 박사과정 재학 중
2000년 11월~현재 : 한국전자통신연구원 부설연구소
<관심분야> 정보보호제품 시험 및 평가

정 지 훈 (Jihoon Jeong)

1991년 2월 : 전북대학교 컴퓨터공학과 졸업
1993년 2월 : 전북대학교 대학원 컴퓨터공학과 석사 졸업
1993년 2월 ~ 2001년 12월 : 한국전자통신연구원 선임연구원
2002년 1월~현재 : 한국전자통신연구원 부설연구소 선임 연구원/팀장
2005년 3월 ~ 2006년 12월 : 충남대학교 컴퓨터공학과 박사과정 수료
<관심분야> 정보보호제품 시험 및 평가, 시스템 평가