암호모듈 시험 및 운영지침

제정 2021. 12. 23.

제1장 총칙

제1조(목적) 본 지침은 「전자정부법 시행령 제69조」 및 「암호모듈 시험 및 검증지침」에 따라 한국인터넷진흥원(이하 “진흥원” 이라 한다)이 객관적이고 공정한 업무를 수행을 위해 암호모듈 시험 수행에 필요한 사항과 암호모듈 검증 시험실 운영에 필요한 사항을 규정함을 목적으로 한다.

제2조(시험 원칙) 진흥원은 암호모듈 시험업무에 대한 신뢰성을 보장하기 위해 다음 각 호의 사항을 준수한다.

1. 시험업무의 객관성, 공정성, 반복성, 재생산성 및 정확성 보장
2. 시험연구원의 기술력 및 전문성 확보

제3조(용어 정의) 본 지침에서 사용하는 용어는 각 호와 같이 정의한다.

1. “검증”이라 함은 암호모듈 시험 결과를 확인하고 검증기준에 부합한지를 심의하여 의결하는 것을 말한다.
2. “검증기관”이라 함은 검증을 담당하는 기관을 말한다.
3. “검증기준”이라 함은 암호모듈이 충족해야 하는 보안요구사항 및 시험 방법과 제출물 요구사항을 명세한 시험요구사항을 말한다.
4. “검증필 암호모듈”이라 함은 시험기관에서 검증기준에 따라 시험한 암호모듈 시험결과를 검증기관이 검증한 암호모듈을 말한다.
5. “보안수준”이라 함은 암호모듈이 충족해야 하는 보안요구사항의 수준을 정의한 것으로 4단계로 분류한다.
6. “시험”이라 함은 암호모듈의 안전성이 검증기준에 부합되는지 여부를 확인하는 것을 말한다.
7. “시험기관”이라 함은 시험을 수행하는 기관을 말한다.
8. “시험도구”이라 함은 시험기관이 암호모듈 시험을 수행하기 위해 자체적으로 개발한 도구 또는 상용도구를 말한다.
9. “시험연구원”이라 함은 암호모듈 시험을 담당하며, 암호모듈 시험기술에 대한 연구·개발을 수행하는 자를 말한다.
10. “시험환경”이라 함은 시험기관이 시험도구 및 매뉴얼 등을 포함하여 암호모듈 시험을 수행하기 위한 장소, 장비 등을 말한다.
11. “신청기관”이라 함은 암호모듈 시험 및 검증을 의뢰하는 기관, 산업체·연구소 또는 개인을 말한다.

12. “암호모듈”이라 함은 암호알고리즘을 하드웨어·소프트웨어·펌웨어 등의 형태로 구현한 것으로 단독으로 사용되거나 정보보호시스템, 암호장치, 보안기능이 있는 정보통신기기에 적용되는 장치나 수단을 말한다.
13. “암호알고리즘”이라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 기밀성·무결성·인증·부인방지 등의 기능을 제공하는 수학적 논리를 말한다.
14. “재검증”이라 함은 검증필 암호모듈의 형상이 변경 또는 개선된 경우 해당 부분이 검증기준에 부합되는지 여부를 다시 시험 및 검증하는 것을 말한다.

제4조(적용 범위) 이 지침은 암호모듈에 대해 수행하는 다음 각 호에 적용된다.
1. 암호모듈 시험 및 검증 업무
2. 암호모듈 시험을 수행하는 시험연구원
3. 암호모듈검증 시험실

제5조(시험연구원의 자격) 암호모듈 시험연구원은 다음 각 호의 업무적인 지식을 보유한 자로 한다.
1. 암호모듈 검증·시험 기준에 대한 이해
2. 검증대상 암호알고리즘 및 구현에 대한 이해
3. 소프트웨어 시험절차 및 방법에 대한 이해
4. 기타 취약점 분석 등 정보보호에 관한 사항

제2장 암호모듈 시험 절차

제6조(시험준비 지원) ① 진흥원은 시험 신청기관의 암호모듈 시험 신청 전, 제출물 완성도 향상을 위해 제출물에 대해서 예비검토를 진행할 수 있다.
② 진흥원은 특이사항을 발견하거나 추가설명 요청이 필요한 경우, 신청기관에게 별도의 설명회나 업무협의를 요청할 수 있다.

제7조(시험 신청) 진흥원은 시험 신청기관에서 암호모듈 시험을 신청받는 경우, 다음 각 호의 문서를 제출받는다.
1. 신청기관의 암호모듈 시험신청 공문
2. 별지 제1호 서식에 따른 암호모듈 검증신청서 또는 별지 제2호 서식에 따른 재검증신청서
3. 시험을 위한 제출물
4. 별지 제3호 서식에 따른 시험협조 동의서

제8조(시험 접수) 진흥원은 시험 신청을 접수한 경우에는 관련 사항을 별지 제4호 서식에 따른 암호모듈 관리기록부에 기록하고 신청인에게 별지 제5호 서식에 따른 시험신청 접수증을 발급한다.

제9조(사전 검토) ① 진흥원은 신청기관이 제출한 제출물에 대해서 검토하여, 미비한 경우 신청기관에게 보완요청할 수 있다.

② 진흥원은 암호알고리즘 구현 적합성, 엔트로피 평가, 소스코드 취약점 점검을 수행하며, 문제점이 발견된 경우 신청기관에게 보완을 요청할 수 있다.

③ 진흥원은 다음 각 호의 사유로 인해 시험신청을 취소할 수 있으며, 시험신청을 취소할 경우에는 별지 제6호 서식에 따른 시험신청 취소 사유서를 작성하여 신청기관에게 취소사유를 통보하여야 한다.

1. 신청기관으로부터 시험신청 취소 요청을 받는 경우
2. 신청기관이 제출물 보완을 정해진 기간 내에 반복적으로 이행하지 않는 경우
3. 제출물의 내용에 미비점이 발견되어 신청기관에 보완을 요청하였으나 신청기관이 이를 이행하지 않은 경우
4. 기타 신청기관의 폐업, 연락두절 등의 귀책사유가 있는 경우

제10조(시험계약) 진흥원은 시험 접수 후, 기본적인 시험 준비가 완료된 경우 신청기관과 협의하여 별지 제7호 서식에 따른 암호모듈 시험 및 검증 계약을 체결한다.

제11조(시험연구원 할당) 진흥원은 시험계약 체결 후, 해당 암호모듈에 적합한 시험연구원을 배정한다. 단 해당 시험연구원이 신청기관과 이해관계가 있는 자는 배제한다.

제12조(시험 진행) ① 진흥원은 원활한 시험수행을 위해 신청기관에게 시험에 필요한 제반 시설, 개발 환경 등의 지원을 요청할 수 있으며, 이 때 별지 제8호 서식에 따른 장비 인수/인계증을 작성한다.

② 진흥원은 암호모듈의 특성에 따라 보안수준에 맞게 보안요구사항이 구현되어 만족되었는지 다음 각 호의 기준에 따라 암호모듈을 시험한다.

1. KS X ISO/IEC 19790:2015
2. KS X ISO/IEC 24759:2015
3. 기타 암호모듈 시험 수행에 필요한 운영 및 시험매뉴얼 등

③ 진흥원은 별표 제1호에 따른 보안점검 항목에 대해 신청기관의 암호모듈 개발 환경 보안관리 실태를 점검할 수 있다.

④ 진흥원은 시험과정에서 제출물이 미비하여 시험수행이 불가능할 경우 신청기관과 제출물 보완사항에 대해 협의를 실시하고, 협의한 내용을 별지 제9호 서식에 따른 보완요청서에 작성하여 신청기관에게 보완조치를 요청한다.

⑤ 진흥원은 시험과정에서 외부 전문가 참여나 시험을 외부기관에 의뢰할 필요가 있다고 판단할 경우 신청기관 및 검증기관과 사전 협의하여 진행할 수 있다.

제13조(시험 중단) ① 진흥원은 다음 각 호의 사유가 발생한 경우에는 시험을 중단할 수 있다.

1. 제출물 보완을 요청받은 신청기관이 특별한 사유 없이 이에 응하지 아니하는 경우
2. 신청기관의 귀책사유로 인하여 시험을 계속 진행하기가 곤란하다고 인정되는 경우

② 진흥원은 시험을 중단하고자 하는 경우 별지 제10호 서식에 따른 시험중단 사유서를 신청기관에게 통보하고 일정기한을 정하여 시험을 계속 진행시키기 위한 조치를 요청할 수 있다.

③ 진흥원은 신청기관이 제2항에 의한 조치를 취하지 아니하는 경우 별지 제11호 서식에 따른 시험계약 해지 사유서를 신청기관에게 통보한다.

제14조(시험 종료) ① 진흥원은 시험이 종료된 경우 암호모듈 시험결과보고서를 작성하고, 검증기관에게 시험결과를 제출한다.

② 시험결과보고서에 포함되어야 하는 내용은 다음 각 호와 같다.

1. 시험결과 요약
2. 암호모듈 시험 개요
3. 암호모듈 시험결과
4. 암호알고리즘 구현적합성 검증 결과
5. 시험결과 결론 및 종합의견 등

③ 재검증 시험인 경우, 결과보고서에 포함되어야 하는 내용은 다음 각 호와 같다.

1. 시험결과 요약
2. 암호모듈 시험 개요, 변경내역 및 영향분석
3. 암호모듈 시험결과
4. 암호알고리즘 구현적합성 검증 결과
5. 시험결과 결론 및 종합의견

④ 진흥원은 검증기관의 시험결과에 대한 보완 요청에 대해 필요한 조치를 하여야 한다.

제3장 암호모듈검증 시험실 운영·관리

제15조(시험환경 및 보안관리) ① 진흥원은 암호모듈 시험을 진행할 수 있는 독립적인 시험환경을 구축하여 운영한다.

② 시험환경은 인가된 시험연구원만이 접근이 가능하다. 단, 시험수행을 위해 외부 인원 접근이 필요한 경우 시험연구원과 동행해야 한다.

③ 진흥원의 시험환경에 신청기관의 장비를 설치 또는 반출하고자 하는 경우에는 별지 제6호 서식에 따른 장비 인수/인계증을 작성한다.

제16조(시험도구 보안) ① 시험환경에는 암호모듈 시험을 위해 적절한 시험도구를 구비하며, 시험도구는 진흥원의 시험환경내에서 사용되어야 한다.

② 시험수행을 위해 시험도구를 진흥원이 아닌 타 기관 장비에서 사용해야 할 경우, 시험연구원은 타 기관의 장비에서 시험 수행 후 반드시 시험도구 및 관련 정보를 해당 장비에서 안전하게 삭제한다.

제4장 시험자료 관리

제17조(시험자료 분류) 시험자료는 암호모듈 시험 과정에서 생산된 결과물로 시험결과 입증 및 향후 암호모듈 관리를 위한 자료이며, 별표 제2호에 따른 제출물, 시험산출물, 결과보고서로 분류한다.

제18조(시험자료 보안관리) ① 시험자료는 다음 각 호와 같이 인가된 시험연구원만이 출입 가능한 설비 내에서 관리되어야 한다.

1. 전자파일 형태의 시험자료는 부대설비 내의 인가된 시험연구원만이 접근가능한 시험장비 상에서 관리되어야 한다.
2. 하드카피, CD 등의 시험자료는 인가된 시험연구원만이 개폐 가능한 안전한 장소에 보관한다.

② 진흥원은 진흥원장의 동의하에서만 시험자료의 외부 반출이 가능하다.

③ 시험자료를 인터넷 등 정보통신망으로 전송하는 경우, 암호화하여 송수신해야 한다.

제19조(시험자료의 접근) 진흥원의 시험자료는 인가된 시험연구원만이 접근 및 사용 가능하도록 관리되어야 한다.

제20조(정보자산의 반환 및 폐기) ① 진흥원은 신청기관에게 지원받은 시험도구 및 장비 등 시험환경을 반환할 경우, 해당 시험환경 내의 모든 고유 정보자산을 폐기하고 반환하여야 한다.

② 진흥원은 검증유지단계를 위한 자료를 제외하고 시험 완료 후에는 신청기관의 자료 일체를 폐기한다.

제5장 기타사항

제21조(보안의무) ① 진흥원에 소속된 자는 시험·검증 과정에서 지득한 사항을 업무와 무관한 사유로 외부에 유출하거나 공개하여서는 아니되며, 신청기관의 지적 재산권을 침해하여서는 아니된다.

② 진흥원은 시험연구원을 대상으로 정기적으로 보안교육을 실시하고, 시험관련 장비·기술 등에 대한 보안대책을 수립 시행하여야 한다.

부 칙<2021. 12. 23>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

[별표 제1호] 보안점검 항목

보안점검 항목

점검항목		착안사항
보안정책	보안정책의 문서화	· 인적, 물리적, 절차적, 제품관리 측면에 대한 내용 (관련 규정이나 지침)
인적 보안	보안관리 조직	· 정기 및 수시 보안점검 내역
	내부인력 관리	· 개발인력 조직, 이력 및 현황 · 퇴사 및 직무변경 시 비밀유지 (자원 회수, 비밀유지 서약서)
물리적 보안	개발참여 외부 인력 관리	· 개발인력 현황, 업무일지, 보안서약서 · 보안제품 운영, 보안설정
	개발환경 출입통제	· 보안 관리 규정, 실험실 관리 지침(시설 안내서) · 출입통제 설비
절차적 보안	개발환경 및 네트워크 관리	· 사내 네트워크 구성, 정보보호시스템 운영, 설정 · 감사기록, 백업자료
	개발자료 보안	· 접근통제 방법 확인 및 기능 시연 · 배포에 따른 무결성, 비밀성 확보수단 등 확인
	개발환경 운영 통제	· 자산관리 현황·이력 · 장비 반출·입 내역
	개발·형상관리 운영 통제	· 개발·형상관리 정책 및 체계 · 개발·형상관리시스템, 개발·형상관리도구 · 소스코드, 바이너리, 제품, 문서 차별화된 관리
	개발·형상도구 관리	· 개발정보 보안대책(접근권한 및 암호화) · 형상도구에 대한 감사기록, 백업자료

[별표 제2호] 시험자료 분류

시험자료 분류

분류	내 용
제출물 (신청기관의 자산)	1. 기본 및 상세설계서 2. 시험서 3. 형상관리문서 4. 원시코드(소스코드, 하드웨어 설계서 등) 5. 기타 문서(안내서, 보안정책서 등)
시험산출물 (시험중 생산된 자료)	1. 소스코드 2. 암호모듈 3. 개발문서 4. VS 결과 5. IUT(테스트프로그램 포함) 6. 개발업체 보안점검 결과 7. 기술분석 문서(소스코드 구조도, 내부함수 및 내부메커니즘 상세정보 등) 8. 소스코드 캡쳐 자료 9. 동작시험 수행결과 10. 기타(환경 설정방법, 개발환경 정보 등)
결과보고서	1. 시험결과 기반으로 작성된 시험결과보고서

[별지 제1호 서식] 암호모듈 검증신청서

<table>
<tr><td>접 수 번 호
제 호</td><td colspan="4">검 증 신 청 서</td></tr>
<tr><td rowspan="4">신청인</td><td>①상 호</td><td></td><td>②사업자번호</td><td></td></tr>
<tr><td colspan="3">③주 소 □□□-□□□</td><td>(전화:)
(FAX :)</td></tr>
<tr><td>④대표 성명</td><td colspan="3"></td></tr>
<tr><td colspan="3">⑤담당자 성명 :
⑥부 서 :</td><td>(전화:)
(FAX :)
(E-mail:)</td></tr>
<tr><td rowspan="6">검증대상</td><td>⑦암호모듈명</td><td colspan="3"></td></tr>
<tr><td>⑧암호알고리즘</td><td colspan="3">■ 블록암호 (□ ARIA □ SEED □ LEA □ HIGHT)
■ 운영모드 (□ ECB □ CBC □ CFB □ OFB □ CTR □ GCM □ CCM)
■ 해시함수 (□ LSH □ SHA2 □ SHA3)
■ 메시지 인증코드 (□ HMAC □ GMAC □ CMAC)
■ 난수발생기 (□ Hash_DRBG □ HMAC_DRBG □ CTR_DRBG)
■ 공개키 암호 (□ RSAES)
■ 전자서명 (□ RSA-PSS □ KCDSA □ ECDSA □ EC-KCDSA)
■ 키 교환 (□ DH □ ECDH)
■ 키 유도 (□ KBKDF □ PBKDF)
■ 비검증대상 ( )</td></tr>
<tr><td>⑨제품구분</td><td colspan="3">□ 하드웨어 □ 소프트웨어 □ 펌웨어 □ 기타</td></tr>
<tr><td>⑩보안수준</td><td colspan="3">□ Level 1 □ Level 2 □ Level 3 □ Level 4</td></tr>
<tr><td>⑪운영체제
(해당되는 경우)</td><td colspan="3">□ Windows □ Linux □ Unix계열 □ Android □ iOS □ 기타</td></tr>
<tr><td>⑫모듈특징</td><td colspan="3"></td></tr>
<tr><td colspan="5">전자정부법 시행령 제69조 및 「암호모듈 시험 및 검증지침」에 의하여 상기와 같이 검증을 신청하며, 기재사항에 허위가 없음을 서약합니다.

년 월 일 신청인 (서명 또는 인)</td></tr>
<tr><td colspan="5">제 출 물 (전자파일 1부)

1. 기본 및 상세설계
2. 형상관리
3. 개발과정 각 단계별 수행해야 하는 시험항목, 각 시험항목별 시험목적, 시험절차 및 결과
4. 제품 및 원시프로그램 또는 하드웨어 설계서</td></tr>
</table>

[별지 제2호 서식] 암호모듈 재검증신청서

<table>
<tr><td colspan="5">재검증 신청서</td></tr>
<tr><td>재검증 구분</td><td colspan="4">□ 보안기능 변경 □ 비보안기능 변경 □ 검증유효기간 만료 □ 취약점 보완</td></tr>
<tr><td rowspan="4">신청인</td><td>상 호</td><td></td><td>사업자번호</td><td></td></tr>
<tr><td>주 소 □□□-□□□</td><td colspan="3">(전화:)
(FAX :)</td></tr>
<tr><td>대표 성명</td><td colspan="3"></td></tr>
<tr><td colspan="2">담당자 성명 :
부 서 :</td><td colspan="2">(전화:)
(FAX :)
(E-mail:)</td></tr>
<tr><td rowspan="4">재검증대상</td><td>암호모듈명</td><td></td><td>검증서 번호</td><td></td></tr>
<tr><td>모듈특징</td><td colspan="3">예) - 검증대상 암호알고리즘만 제공하는 라이브러리형태 등 특징</td></tr>
<tr><td>제품구분</td><td colspan="3">□ 하드웨어 □ 소프트웨어 □ 펌웨어 □ 기타</td></tr>
<tr><td>제출물</td><td colspan="3"></td></tr>
<tr><td>변경항목</td><td colspan="4">※ 보안기능 변경, 비보안기능 변경이면 변경사항을 기술
검증유효기간 만료로 변경사항이 없으면 생략 가능
취약점 보완이면 취약점과 보완내역을 기술</td></tr>
<tr><td colspan="5">전자정부법 시행령 제69조 및 암호모듈 시험 및 검증지침에 의하여 상기와 같이 재검증을 신청하며, 기재사항에 허위가 없음을 서약합니다.
년 월 일 신청인 (서명 또는 인)</td></tr>
<tr><td colspan="5">제 출 물 (전자파일 1부)
1. 기본 및 상세설계
2. 형상관리
3. 개발과정 각 단계별 수행해야 하는 시험항목, 각 시험항목별 시험목적, 시험절차 및 결과
4. 제품 및 원시프로그램 또는 하드웨어 설계서</td></tr>
</table>

[별지 제3호 서식] 시험 협조 동의서

시험 협조 동의서

본 신청기관은 년 월 일부로 암호모듈 시험을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본 신청기관은 아래의 상황 발생 시, 시험기관이 시험중단을 요청할 수 있다는 사실을 인정하고, 이 요청을 따를 것임을 서약한다.
   가. 신청기관이 암호모듈 시험중단을 요청한 경우
   나. 신청기관이 제출물 보완을 정해진 기간내에 이행 못한 경우
   다. 시험기관이 제출물의 수준이 현격히 부적합하여 시험을 진행할 수 없다고 판단한 경우
   라. 아래의 시험이 특정 횟수 이상 실패한 경우
      - 암호알고리즘 구현적합성 검증시험을 5회 초과 실패한 경우
      - 엔트로피 평가를 5회 초과 실패한 경우
      - 취약점 보완을 5회 초과 완료하지 못한 경우

2. 본 신청기관은 시험이 원활히 진행될 수 있도록 시험기관의 요청에 적극 응할 것이며, 암호모듈 및 제출물 보완작업을 성실히 수행할 것을 서약한다.

년 월 일

서약자 소 속 :
직 급 (직 위) :
성 명 : (인)

한국인터넷진흥원장 귀하

[별지 제4호 서식] 암호모듈 관리기록부

암호모듈 관리기록부

관리번호	신청기관	모듈명칭	형상	보안수준	시험분류	상태	신청일	착수일	계약일	완료일	시험담당	신청인	신청인 연락처

[별지 제5호 서식] 시험신청 접수증

시험신청 접수증		
신청인	상호	
	주소	
	대표 성명	
	담당자 성명	
	연락처	
	E-mail	
암호모듈명		
제품구분	□ 하드웨어 □ 소프트웨어 □ 펌웨어 □ 기타	
보안수준	□ Level1 □ Level2 □ Level3 □ Level4	
비고		

위와 같이 접수하였음을 확인합니다.

년 월 일

한국인터넷진흥원

접수인

[별지 제6호 서식] 시험신청 취소 사유서

시험신청 취소 사유서

1. 신청기관 정보:

2. 암호모듈 정보:

3. 시험진행 현황:

4. 취소사유:

5. 취소일시:

6. 기타사항:

년 월 일

한국인터넷진흥원

[별지 제7호 서식] 암호모듈 시험 및 검증 계약서

암호모듈 시험 및 검증 계약서

신청 암호모듈명 :

계약 당사자
시험기관 : 한국인터넷진흥원장
신청인 :

위 신청인의 암호모듈 시험을 위하여 시험기관과 신청인은 다음과 같이 계약을 체결한다.

제1조(목적) 이 계약의 목적은 「국가정보보안 기본지침」(국정원, 2014. 4.)과 「암호모듈 시험 및 검증지침」(행정안전부 고시2004-45)에 따라 시험기관은 신청인의 신청에 의하여 암호모듈 시험(이하, '시험'이라 한다)을 수행함에 있어 시험기관과 신청인의 권리와 의무를 명확히 정하는데 있다.

제2조(계약의 이행) 시험기관과 신청인은 암호모듈의 시험이 원만히 진행될 수 있도록 국가정보원장이 규정한 「국가정보보안 기본지침」과 행정안전부장관이 규정한 「암호모듈 시험 및 검증지침」 및 본 계약서의 내용을 성실히 이행하여야 한다.

제3조(제출물 제출 및 반환) ① 신청인은 시험대상인 암호모듈의 안전성·구현적합성을 증명하기 위하여, 시험기관이 요청하는 원시프로그램 및 하드웨어 설계도 등 제반문서 및 구현된 암호모듈을 제출하여야 한다.

② 시험기관은 신청인이 제출한 제출물을 확인하고 이에 대해 검증접수증을 서면으로 신청인에게 통보한다.

③ 시험기관은 국가정보원(이하, '검증기관'이라 한다.)의 검증절차가 완료된 시점으로부터 3일 이내에, 암호모듈의 원시프로그램 및 하드웨어 설계서 등을 신청인에게 인계한다.

④ 신청인이 제출한 제출물 중, 제3항에 해당하지 않은 제출물은 해당 암호모듈의 검증유효기간 동안 시험기관이 보관한다. 다만, 신청인의 귀책사유로 인하여 시험이 중단되거나 검증필 암호모듈의 검증유효기간이 만료되는 경우, 시험기관은 모든 제출물을 신청인에게 인계한다.

제4조(제출물 보완) ① 시험기관이 시험 수행을 위해 신청인에게 제출물 보완을 요청한 경우 신청인은 제출물 보완을 요청한 날로부터 10일 이내에 제출물을 보완하여 시험기관에게 제출하여야 한다.

② 시험기관은 필요에 따라 신청인이 10일이 초과되는 보완 기간을 요청할 경우 보완에 의한 지체의 책임이 신청인에게 있음을 통보한다.

③ 시험기관은 신청인의 귀책으로 인하여 제출물의 보완이 불가능할 경우, 시험을 중단할 수 있다.

제5조(검증수수료) 「암호모듈 시험 및 검증지침」 제 10조 5항에 의거하여 신청인은 시험기관에게 검증계약 체결 시 검증수수료를 납부하여야 한다. 다만, 검증기관이 별도로 고시할 때 까지 검증수수료의 납부를 면제한다.

제6조(제출물 보안유지 및 관리) ① 시험기관은 신청인이 시험을 위해 제출한 모든 제출물을 안전하게 보관 및 관리할 책임을 진다. 다만, 다음 각 호에 해당되는 사항은 예외로 본다.

1. 전시·천재지변 또는 기타 불가항력에 의하여 제출물이 손상되거나 유실된 경우

2. 기능시험을 위해, 암호모듈의 전부 또는 일부를 훼손할 경우

② 시험기관은 신청인의 동의 없이 신청인이 제출한 제출물을 시험 이외의 목적으로 복제하거나, 외부에 유출 또는 공개하여서는 안 된다.

제7조(협조) 시험기관은 효율적인 시험 진행을 위하여 필요한 경우 신청인에게 시험에 필요한 장비 등 시험환경 구축을 위한 기술적인 협조를 요청할 수 있고 신청인은 최대한 협조하여야 한다.

제8조(현장실사) ① 시험기관은 검증기관과 공동으로 시험대상 암호모듈의 개발환경 보안관리실태를 확인하기 위한 현장실사를 실시할 수 있다.

② 시험기관은 현장실사 기간 중, 시험대상 암호모듈의 인적·물리적·절차적 보안관리실태 확인을 위한 제반 문서 열람을 신청인에 요청할 수 있으며, 신청인은 특별한 사유가 없는 한 이에 응해야 한다.

제9조(계약의 해지) 시험기관은 다음 각 호의 사항이 발생한 때에는 계약을 해지할 수 있다.

1. 신청인이 시험 중단을 요청하는 경우
2. 신청인이 제출물의 보완을 협의된 기간 내에 이행하지 않을 경우
3. 기타 사유로 인해, 시험기관이 제출물에 대한 시험을 진행할 수 없다고 판단하고 이를 검증기관이 인정한 경우

제10조(계약의 양도·양수) ① 신청인은 다음 각 호에 해당되는 경우, 시험이 진행 중인 암호모듈에 대한 본 계약의 전부 또는 일부를 제3자에게 양도할 수 있다.

1. 신청인의 유고 또는 이와 동일한 불가항력적인 사정으로 인하여 시험을 지속할 수 없는 경우
2. 신청인의 사유로 인하여 시험 대상 암호모듈의 소유권을 제3자에게 이

전할 경우

② 제1항의 경우, 양수인은 본 계약서에 기재된 양도인의 권리와 의무를 동시에 승계한 것으로 본다.

제11조(계약의 효력) 본 계약은 쌍방이 서명날인한 날로부터 검증기관이 검증을 종료한 시점까지 유효하다.

제12조(기타사항) ① 본 계약서는 2부를 작성하여 시험기관과 신청인이 각기 기명날인하여 각각 1부씩 보관한다.

② 본 계약서의 사본은 작성하지 않는다.

년 월 일

시험기관 : 한국인터넷진흥원장 (인)

주 소 : 전라남도 나주시 진흥길 9

신 청 인 : (인)

주 소 :

[별지 제8호 서식] 장비 인수/인계증

장비 인수/인계증

1. 암호모듈명 :
2. 기관명 :
3. 장비 내역

   아래의 장비를 인수·인계 합니다.

순번	장비명	수량	비고

년 월 일

• 인 수 자

- 소속:
- 성명: (인)

• 인 계 자

- 소속:
- 성명: (인)

[별지 제9호 서식] 보완요청서

보 완 요 청 서

시험일자 :　　년　　월　　일

1. 귀사에서 암호모듈 시험을 의뢰한 ***모듈명***에 대하여 ***해당시험단계***를 수행하던 중 첨부와 같이 보완 사항이 발생하였습니다.

2. 이에 따라 귀사께서는 아래와 같이 제출문서를 보완하시기 바랍니다.

< 아　　래 >

o 시험신청기관명 :
o 평가모듈버전 :
o 보완요청 내용 :
o 보완요청 기간 : ~　　월　　일까지(약　　주)

첨부 : ***모듈명*** 보완요청 1부

년　　월　　일

한국인터넷진흥원

첨부 : <*모듈명*> 보완요청

1. 개발업체:

2. 보완대상: ***모듈명*** 제출물

3. 보완내용:

※ 소스코드 및 문서별 발생한 보완사항 기재

■ 기본 및 상세 설계서

■ 소스코드

■ 형상관리 문서

■ 시험서

■ 기타

[별지 제10호 서식] 시험중단 사유서

시험중단 사유서

1. 신청기관 정보:

2. 암호모듈 정보:

3. 시험진행 현황:

4. 중단사유:

5. 중단일시:

6. 기타사항:

년 월 일

한국인터넷진흥원

[별지 제11호 서식] 시험계약 해지 사유서

시험계약 해지 사유서

1. 신청기관 정보:

2. 암호모듈 정보:

3. 시험진행 현황:

4. 해지사유:

5. 해지일시:

6. 기타사항:

년 월 일

한국인터넷진흥원