암호모듈 재검증 가이드라인

2014. 2.

암호모듈 검증기관

암호모듈 시험기관

목 차

Ⅰ. 재검증 가이드라인 개요

1. 서론

「암호모듈 재검증 가이드라인」(이하 가이드라인)은 암호모듈 개발업체가 재검증을 신청하는 절차를 기술한 문서이다. 이 가이드라인에서는 검증필 암호모듈의 재검증 사유에 따라 재검증을 신청하기 위한 절차, 제출물 작성방법 등을 설명한다.

※ 이 가이드라인의 내용은 검증기관 및 시험기관에 의해 변경될 수 있다.

2. 법적근거

□「전자정부법」제56조(정보통신망 등의 보안대책 수립·시행)
□「전자정부법시행령」제69조(전자문서의 보관·유통 관련 보안 조치)
□「암호모듈 시험 및 검증지침」(안행부고시)

3. 적용기준

□ KS X ISO/IEC 19790 암호모듈 보안요구사항
□ KS X ISO/IEC 24759 암호모듈 시험요구사항
□ 소프트웨어 암호모듈 검증기준 Ver 1.0
□ 암호알고리즘 검증기준 Ver 2.0

4. 용어 정의

□ **(검증기관)** 시험기관의 시험결과를 검증 및 승인하고, 검증필 암호모듈 목록을 관리하는 기관
□ **(검증기준)** 암호모듈을 시험 및 검증하는 기준으로 KS X ISO/IEC 19790, KS X ISO/IEC 24759, 소프트웨어 암호모듈 검증기준 Ver 1.0, 암호알고리즘 검증기준 Ver 2.0을 준용
□ **(검증번호)** 검증기관이 검증하고 승인한 암호모듈을 식별하기 위하여 부여한 번호
□ **(검증유효기간)** 검증번호를 부여받은 암호모듈이 검증필 암호모듈 목록에 등재된 이후부터 목록에서 삭제될 때까지 검증 효력이 유지되는 기간으로 5년임
□ **(검증필 암호모듈)** 검증기관이 검증 및 승인하여 검증번호가 부여된 암호모듈
□ **(검증필 암호모듈 목록)** 암호모듈 검증절차에 따라 검증번호가 부여된 암호모듈 중 검증유효기간이 만료되지 않은 암호모듈을 검증순서에 따라 나열한 목록. 국가사이버안전센터 홈페이지에서 확인 가능함
□ **(긴급패치)** 검증필 암호모듈의 취약점에 대한 임시적인 보완조치
□ **(보안기능)** 검증기준에서 정의한 보안요구사항을 충족하기 위한 기능 중 암호경계 내·외부에서 보안성에 영향을 미치는 기능
□ **(보안요구사항)** 암호모듈이 준수하여야 하는 안전한 설계와 구현에 관한 요구사항

□ **(비보안기능)** 검증기준에서 정의한 보안요구사항을 충족하기 위한 기능 중 암호경계 내·외부에서 보안성에 영향을 미치지 않는 기능

□ **(시험기관)** 암호모듈 개발업체의 검증 신청을 접수하고 암호모듈 검증기준에 따라 시험평가를 수행하는 기관

□ **(신청인)** 암호모듈을 신규검증 또는 재검증을 신청하는 개인 또는 단체

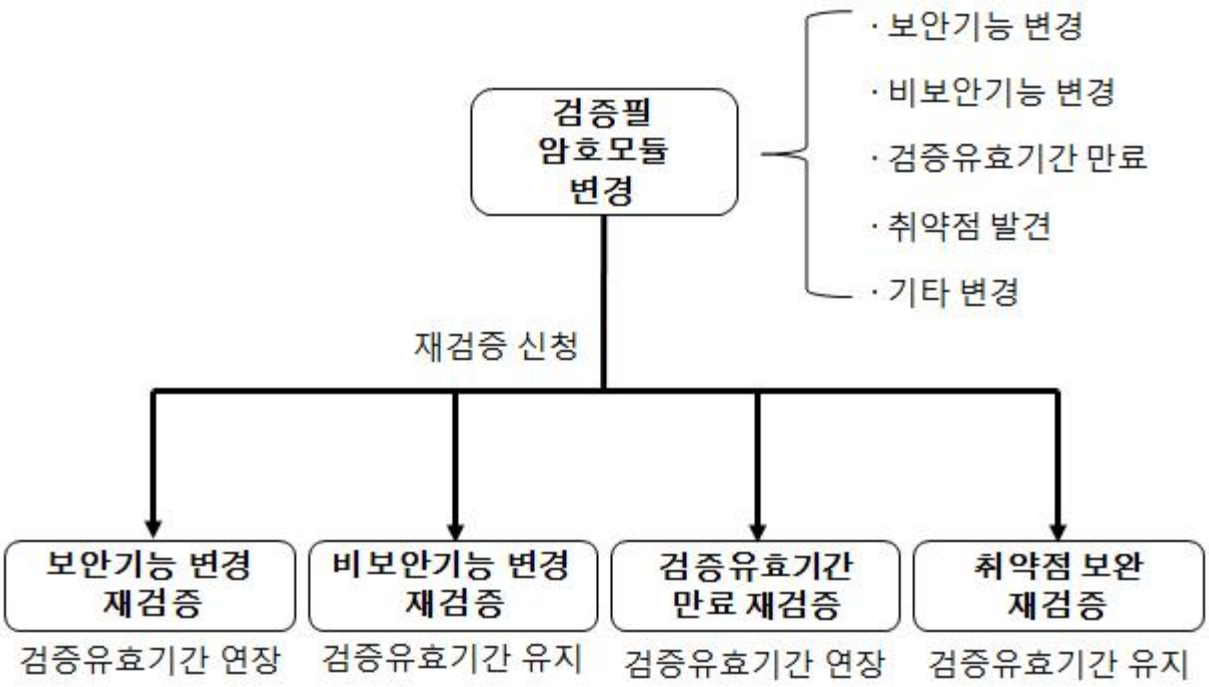
□ **(암호경계)** 암호모듈의 물리적 경계 또는 논리적 경계를 설정하여 명시적으로 정의된 연속 경계. 암호모듈의 모든 하드웨어, 소프트웨어 등 구성요소를 포함함

□ **(재검증)** 검증된 암호모듈을 검증유효기간 중에 형상 변경, 검증유효기간 만료, 취약점 보완 등의 이유로 다시 검증하는 것

Ⅱ. 재검증 개요

□ **(재검증 개요)** 재검증은 검증필 암호모듈 목록에 등재된 암호모듈을 다시 검증하는 것으로 이를 재검증 사유에 따라 구분하면, 보안기능이 일부 변경되어 재검증을 신청하는 재검증(이하 보안기능 변경 재검증), 비보안 기능이 변경되어 재검증을 신청하는 재검증(이하 비보안기능 변경 재검증), 암호모듈의 검증유효기간이 만료되어 기존 형상 그대로 검증유효기간을 연장하기 위한 재검증(이하 검증유효기간 만료 재검증), 취약점을 긴급하게 보완하기 위한 재검증(이하 취약점 보완 재검증)으로 나누어진다.

검증필 암호모듈의 변경 또는 검증유효기간 만료 시점 도래 등이 발생하면, 신청인은 이 가이드라인의 기준에 따라 해당하는 재검증을 신청하여야 한다.



□ (보안기능과 비보안기능 구분)

보안요구사항	보안기능 변경	비보안기능 변경
암호모듈 명세	암호경계 내부의 변경	암호경계 외부의 변경
암호모듈 포트 및 인터페이스	○	X
역할, 서비스 및 인증	○	X
유한상태모델	○	X
물리적 보안	○	X
운영환경	운영체제 추가 등 운영환경 변경이 암호모듈의 기능에 영향을 미치는 변경	암호모듈의 보안성 및 보안기능에 영향을 미치지 않는 범위 내에서 운영체제 추가 등 운영환경의 변경
암호키 관리	○	X
전자파 적합성	X	○
자가 시험	○	X
설계 보증	보안성 및 보안기능에 영향을 미치는 암호모듈의 배포 및 관리방법의 변경	보안성 및 보안기능에 영향을 미치지 않는 범위 내에서 설계보증 변경

□ (일반사항)

○ **(검증결과 재활용)** 검증받을 당시의 기준과 현재의 기준이 동일한 검증항목은, 검증 당시 검증한 결과를 재사용할 수 있다.

○ **(명시되지 않은 사항 판단)** 보안기능 변경 대상, 신규검증 대상, 비보안기능 변경 대상, 검증유효기간 만료 재검증 대상 등을 명확하게 판단하기 어려울 경우, 검증기관과 시험기관이 결정할 수 있다.

Ⅲ. 보안기능 변경 재검증

1. 재검증 개요

□ **(재검증 목적)** 보안기능 변경 재검증은 검증필 암호모듈 목록에 등재된 암호모듈의 보안기능을 변경할 경우 최신 검증 기준에 따라 재검증을 받기위하여 신청한다. 이 재검증을 완료하면 재검증 완료시점에서 검증유효기간을 5년 연장할 수 있다.

□ **(재검증 대상)**

○ **(보안기능 변경)** 보안요구사항 중 보안기능을 변경하는 경우 보안기능 변경 재검증 대상이다.

○ **(성능개선)** 보안기능을 성능개선하기 위하여 변경하는 경우 보안기능 변경 재검증 대상이다.

○ **(간소화 버전)** 기존 검증필 암호모듈의 간소화 버전을 개발한 경우에도 보안기능 변경 재검증을 신청하여야 한다.

※ (신규검증 대상) 보안기능 변경 재검증은 암호모듈의 개발자 요구사항(VE: VEndor requirements)을 30% 미만으로 변경한 경우만 신청할 수 있다. VE를 30% 이상 변경한 경우는 신규검증으로 신청하여야 한다.

□ **(적용 검증기준)**

○ **(현재 검증기준 적용)** 보안기능 변경 재검증은 검증필 암호모듈을 검증받을 당시의 기준이 아닌, 현재의 검증기준으로 재검증을 수행한다.

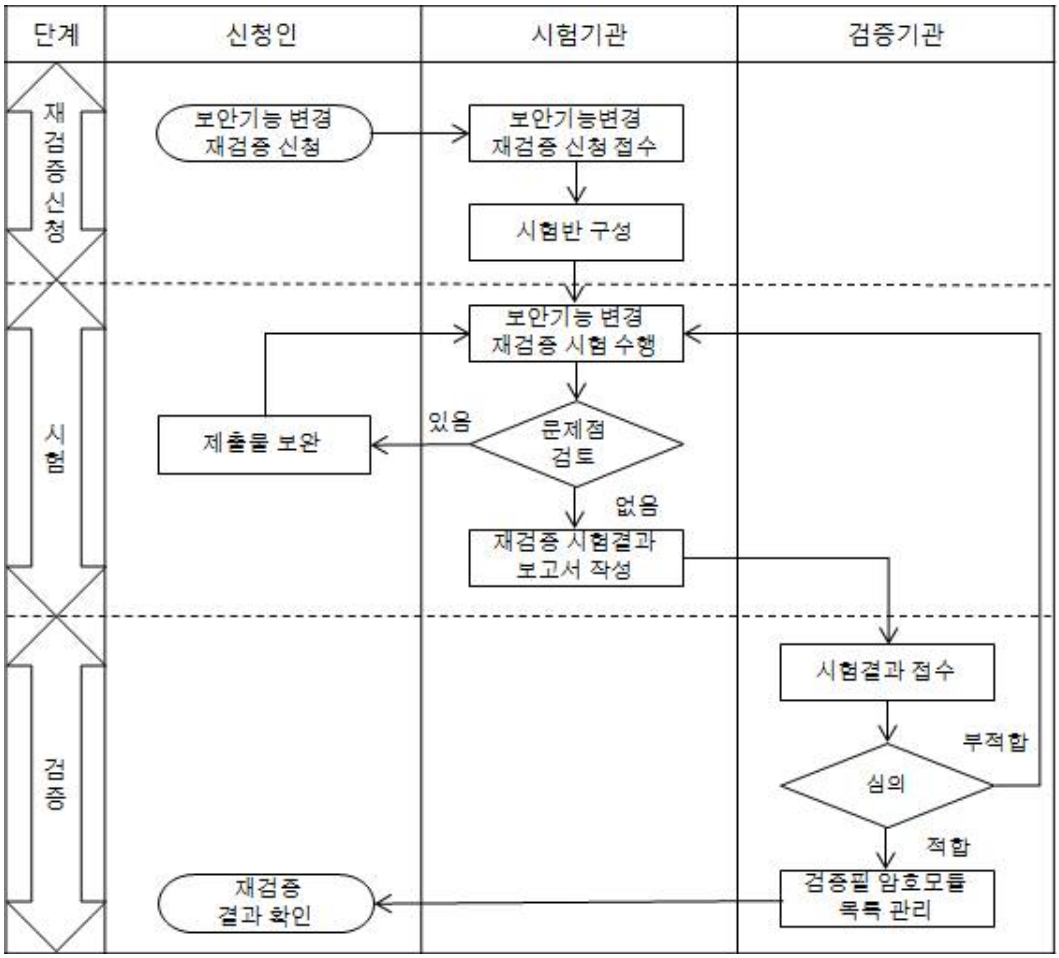
□ **(검증필 암호모듈 목록관리)**

○ **(신규 검증번호 부여)** 보안기능 변경 재검증을 완료하면, 새로운 검증번호를 부여하고, 검증필 암호모듈 목록에 등재한다.

○ **(기존 검증번호 유지)** 보안기능 변경 재검증을 완료하여 새로운 검증번호를 부여하였어도, 기존 검증번호는 검증필 암호모듈 목록에서 검증유효기간 동안 유지된다. 신청자가 요청하면, 기존 검증번호를 삭제할 수 있다.

□ **(재검증 신청 시기)** 보안기능 변경 재검증을 신청하려면 잔여 검증유효기간이 6개월 이상이어야 한다.

2. 재검증 절차



① 신청인은 공문, 재검증 신청서, 영향분석서, 제출물 등을 시험기관에 제출하고, 보안기능 변경 재검증을 신청한다. 이때 신청인은 검증필 암호모듈의 버전정보가 포함된 암호모듈명으로 재검증 신청을 한다.

② 시험기관은 공문과 보안기능 변경 재검증 관련 제출물을 접수한다. 시험기관은 신청인이 제출한 영향분석서를 검토하여, 개발자 요구사항을 30% 이상 변경하였다고 판단하거나, 비보안기능을 변경하였다고 판단하면 신규검증 또는 비보안기능 변경 재검증으로 다시 신청하도록 요청할 수 있다.

③ 시험기관은 시험반을 구성하고, 보안기능 변경 재검증 시험을 수행한다.

④ 시험기관은 보안기능 변경 재검증 시험과정에서 제출물의 보완이 필요하면 신청인에게 제출물의 보완을 요청할 수 있다.

⑤ 시험기관은 신청인이 제출물 보완을 이행하지 않을 경우, 시험을 중단할 수 있다. 시험을 중단하더라도, 기존의 검증필 암호모듈은 검증유효기간 동안 검증필 암호모듈 목록에서 유지된다.

⑥ 시험기관은 보안기능 변경 재검증 시험을 완료한 후, 재검증 시험결과보고서를 검증기관에게 제출하여야 한다.

⑦ 검증기관은 시험기관이 제출한 보안기능 변경 재검증 시험결과를 심의하고, 보완할 필요가 있다고 판단하면 시험기관에게 재시험을 요청할 수 있다.

⑧ 검증기관은 보안기능 변경 재검증 시험결과를 심의하여 적합하면 검증필 암호모듈 목록에 반영한다. 검증필 암호모듈 목록에는 신청한 암호모듈명과 부여한 검증번호를 등재하고, 검증유효기간은 새로 5년을 부여할 수 있다.

Ⅳ. 비보안기능 변경 재검증

1. 재검증 개요

□ **(재검증 목적)** 비보안기능 변경 재검증은 암호모듈의 보안기능을 제외한 부분을 변경하였을 때, 변경내역 및 보안기능에 미치는 영향 등을 간단히 재검증하기 위하여 수행한다. 비보안기능 변경 재검증을 완료하더라도 검증필 암호모듈 목록의 검증유효기간은 변동이 없다.

※ 간단한 성능개선을 하거나 배포방식을 변경하는 경우라도 재검증 절차에 따르지 않고 무단으로 암호모듈을 변경하여 배포하면 검증필 암호모듈 목록에서 삭제할 수 있다.

□ **(재검증 대상)**

○ **(비보안기능 변경)** 암호모듈의 보안기능에 영향을 미치지 않는 변경은 비보안기능 변경에 해당된다.

○ **(암호모듈 관련 정보의 변경)** 업체명, 암호모듈명 등 보안에 관련 없는 정보를 변경한 경우 비보안기능 변경 재검증 대상이다.

○ **(비검증대상 암호알고리즘 변경)** 암호경계 내부에 있더라도 비검증대상 암호알고리즘을 변경한 경우 비보안기능 변경 재검증 대상이다.

○ **(운영환경 변경)** 암호모듈의 보안성 및 보안기능에 영향을 미치지 않는 범위 내에서 호환 운영체제의 추가 등 운영환경을 변경한 경우 비보안기능 변경 재검증 대상이다.

ex) 리눅스 2.5 환경에서 검증받은 암호모듈을 리눅스 2.6 환경에서 인터페이스 등의 변경 없이 정상적으로 사용할 수 있다면 비보안기능 변경 재검증을 통하여 호환 운영체제를 추가할 수 있다.

○ **(설계보증 변경)** 보안성 및 보안기능에 영향을 미치지 않는 범위 내에서 설계보증 변경은 비보안기능 변경 재검증 대상이다.

○ **(전자파 적합성 시험 결과 변경)** 암호모듈의 전자부품 등을 변경하여 전자파 적합성 시험 결과가 달라지더라도 기준치 이하인 경우 비보안기능 변경 재검증 대상이다.

□ **(적용 검증기준)**

○ **(검증 당시 검증기준 적용)** 비보안기능 변경 재검증은 현재의 검증기준이 아닌 검증필 암호모듈이 검증받은 당시의 기준으로 재검증을 수행한다. 다만 암호모듈의 취약점 검증 등 기타공격에 대한 대응은 시험기관이 정한 방법과 기준에 따라 검증한다.

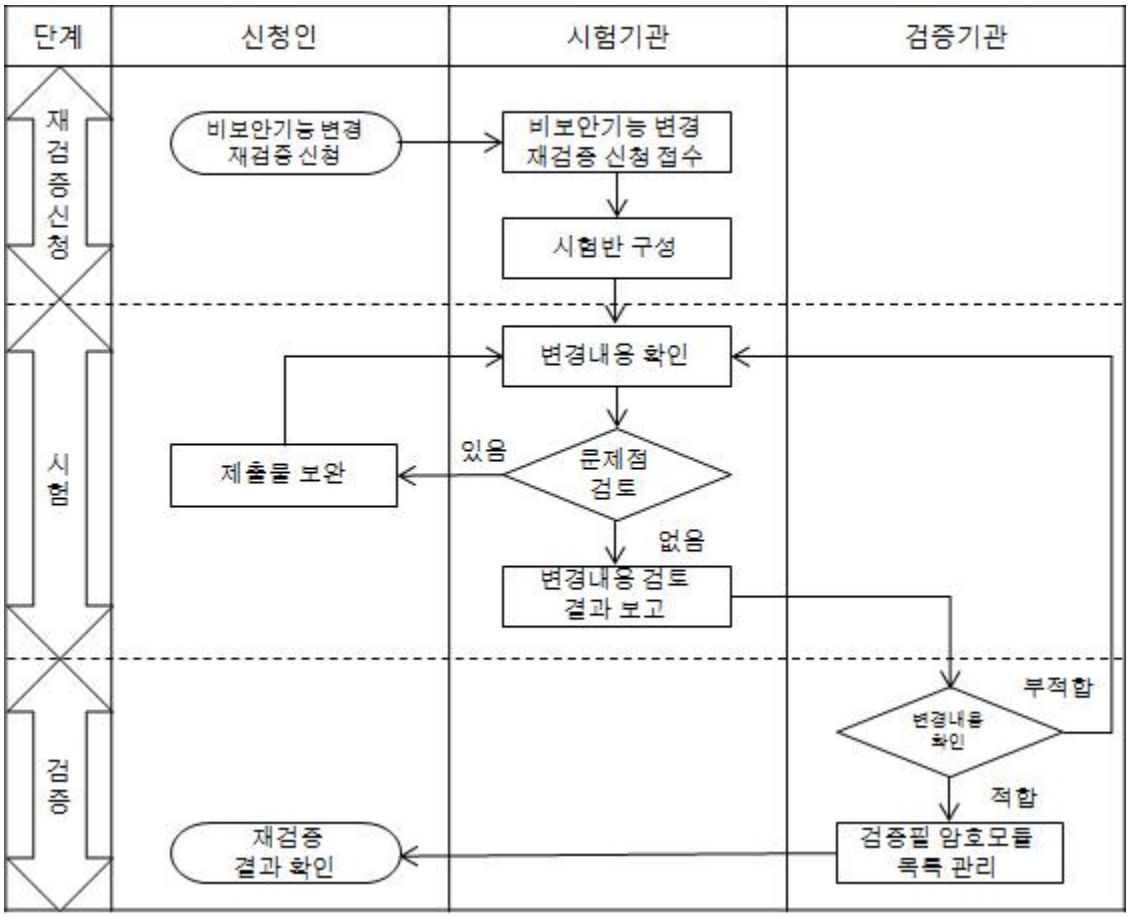
□ **(검증필 암호모듈 목록관리)**

○ **(검증번호 유지)** 비보안기능 변경 재검증을 완료하더라도, 검증필 암호모듈 목록에서 검증번호를 변경하지 않는다. 변경이력은 검증필 암호모듈 목록에 기재할 수 있다.

○ **(암호모듈명 변경)** 신청인의 요청에 따라 기존 암호모듈명이나 새로운 암호모듈명으로 검증필 암호모듈 목록에 반영할 수 있다.

□ **(재검증 신청 시기)** 비보안기능 변경 재검증을 신청하려면 잔여 검증유효기간이 6개월 이상이어야 한다.

2. 재검증 절차



① 신청인은 공문, 재검증 신청서, 영향분석서, 제출물 등을 시험기관에 제출하고, 비보안기능 변경 재검증을 신청한다. 이때 신청인은 암호모듈명을 유지하거나 새로운 암호모듈명으로 검증유지신청을 할 수 있다.

② 시험기관은 공문과 재검증 관련 제출물을 접수한다. 시험기관은 신청인이 제출한 영향분석서를 검토하여, 보안기능이 변경되었다고 판단하면 변경정도에 따라 신규검증 또는 보안기능 변경 재검증으로 다시 신청하도록 요청할 수 있다.

③ 시험기관은 암호모듈의 변경내용 중 보안기능 변경에 해당되는 사항이 있는지 검토하고 필요하면 기능시험을 실시할 수 있다. 이때 보안기능 변경이 없더라도 시험기관이 정한 방법에 따라 암호모듈의 취약점이 존재하는가를 확인할 수 있다.

④ 시험기관은 변경내용을 검토한 후, 변경정도에 따라 검증기관에 재검증 검토 결과 또는 시험결과서를 제출하여야 한다.

⑤ 검증기관은 시험기관이 제출한 재검증 검토 결과(또는 시험결과서)를 심의하고, 보완할 필요가 있다고 판단하면 시험기관에게 재검토를 요청할 수 있다.

⑥ 검증기관은 비보안기능 변경 재검증에 적합하다고 판단하면 검증필 암호모듈 목록에 반영하여야 한다. 검증필 암호모듈 목록에서 해당 암호모듈은 기존 암호모듈명 또는 새로운 암호모듈명으로 교체되고, 검증유효기간 변동은 없다. 검증필 암호모듈 목록에 기존의 암호모듈명이 새로운 암호모듈명으로 교체된 이력을 표시할 수 있다.

Ⅴ. 검증유효기간 만료 재검증

1. 재검증 개요

□ **(재검증 목적)** 검증필 암호모듈 목록에 등재된 암호모듈의 검증유효기간이 만료되기 전에 기존 형상 그대로 검증유효기간을 연장하고자 할 때 검증유효기간 만료 재검증을 신청한다.

□ **(재검증 대상)**

○ **(검증기준 일치)** 검증 당시의 검증기준과 현재의 검증기준이 동일한 경우, 신청인이 암호모듈 형상의 변경 없이 재검증을 신청하면, 시험기관이 암호모듈 형상 변경 및 검증기준 일치 여부 등을 간단한 확인하고 검증유효기간 연장을 할 수 있다. 다만 암호모듈의 취약점 검증 등 기타공격에 대한 대응은 검증기준 일치와 무관하게 시험기관이 정한 방법에 따라 검증하고, 취약점이 발견되면 신청인은 취약점을 보완하여야 한다.

○ **(암호모듈의 형상일치)** 검증필 암호모듈의 형상 변경이 없어야 한다.

※ 검증 당시와 현재의 검증기준이 일치하지 않거나, 보안기능 및 비보안기능의 변경이 있을 경우, 신청인은 해당 사유에 따른 재검증 또는 신규검증으로 신청하여야 한다.

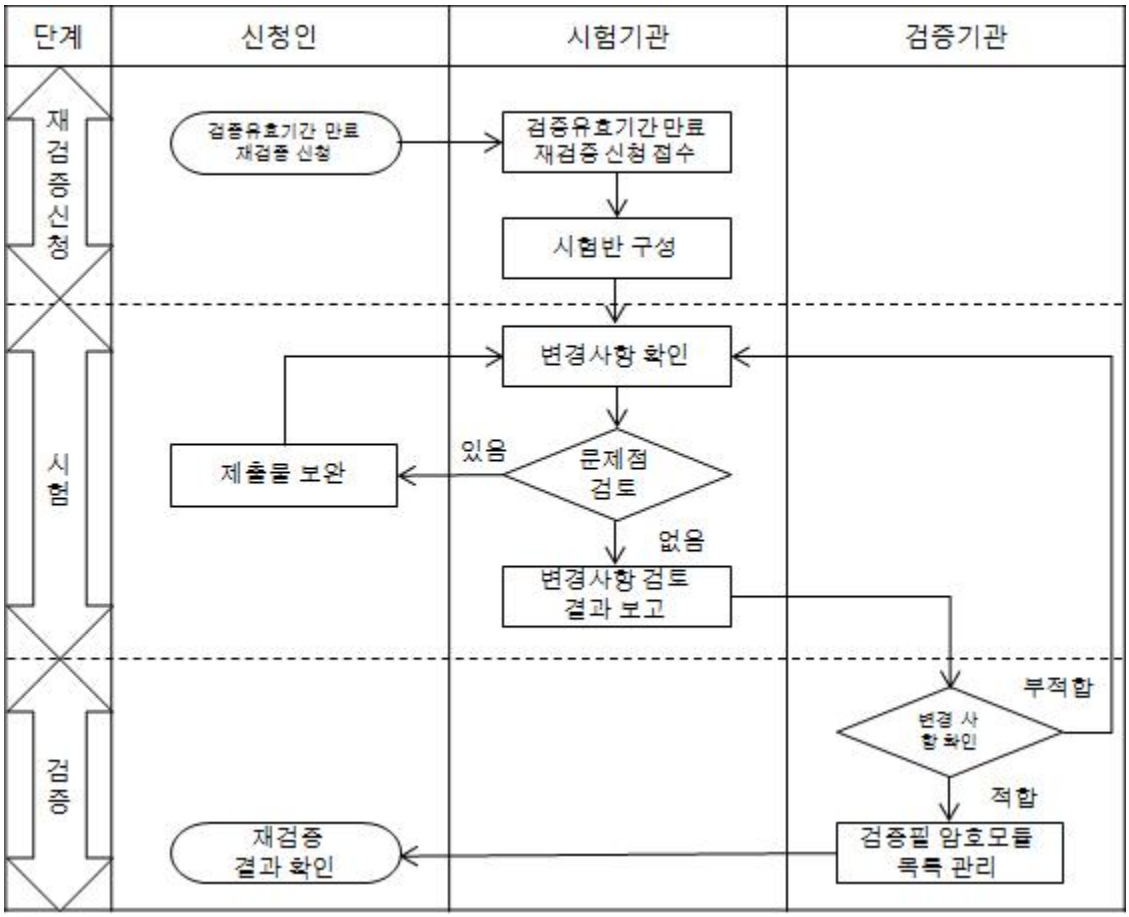
□ **(검증필 암호모듈 목록관리)**

○ **(신규 검증번호 부여)** 검증유효기간 만료 재검증을 완료하면, 검증유효기간이 연장된 새로운 검증번호를 부여하고, 검증필 암호모듈 목록에 등재한다.

○ **(기존 검증번호 삭제)** 검증유효기간 만료 재검증을 완료하여 새로운 검증번호를 부여하면, 기존 검증번호는 삭제한다.

□ **(재검증 신청 시기)** 검증유효기간 만료 재검증을 신청하려면 잔여 검증유효기간이 6개월 이상 12개월 미만이어야 한다.

2. 재검증 절차



① 검증필 암호모듈 목록에 등재된 암호모듈의 잔여 검증유효기간이 6개월 이상 12개월 미만일 때 신청인은 공문, 재검증 신청서, 영향분석서, 제출물 등을 시험기관에 제출하고, 검증유효기간 만료 재검증을 신청할 수 있다.

② 시험기관은 공문과 검증유효기간 만료 재검증 관련 제출물을 접수한다. 시험기관은 신청인이 제출한 영향분석서를 검토하여, 검증기준이 일치하지 않거나, 암호모듈의 변경사항이 있다고 판단하면 변경정도에 따라 신규검증, 보안기능 변경 재검증, 비보안기능 변경 재검증으로 다시 신청하도록 요청할 수 있다.

③ 시험기관은 제출물을 종합적으로 검토하여 변경여부를 확인한다. 이때 암호모듈의 변경사항이 없더라도 시험기관이 정한 방법에 따라 암호모듈의 취약점이 존재하는가를 확인할 수 있다. 시험기관은 검증유효기간 만료 재검증을 완료하면 검증기관에 재검증 검토 결과를 제출하여야 한다.

④ 검증기관은 시험기관이 제출한 재검증 검토 결과를 심의하고, 보완할 필요가 있다고 판단하면 시험기관에게 재검토를 요청할 수 있다.

⑤ 검증기관은 검증유효기간 만료 재검증에 적합하다고 판단하면 검증필 암호모듈 목록에 반영하여야 한다. 검증필 암호모듈 목록에서 암호모듈명은 변경하지 않고 검증유효기간이 연장된 새로운 검증번호를 부여한다. 검증필 암호모듈 목록에 기존의 검증번호가 새로운 검증번호로 교체된 이력을 표시할 수 있다.

Ⅵ. 취약점 보완 재검증

1. 재검증 개요

□ **(재검증 목적)** 취약점 보완은 암호모듈 및 암호모듈 적용환경의 취약점을 긴급하게 보완하기 위하여 수행하는 재검증으로 재검증을 완료하더라도 검증필 암호모듈 목록의 검증유효기간은 변동이 없다.

□ **(재검증 대상)**

○ **(검증필 암호모듈의 취약점 발견)** 검증필 암호모듈에서 취약점이 발견되어 긴급하게 보완을 해야 하는 경우 취약점 보완 재검증 대상이다.

○ **(암호모듈 적용환경의 취약점 발견)** 인증서 탈취 등 설계보증과 관련된 암호모듈 적용환경에서 취약점이 발견되어 긴급하게 보완을 해야 하는 경우 취약점 보완 재검증 대상이다.

○ **(암호알고리즘의 취약점 발견)** 암호알고리즘에 대한 새로운 공격방법 개발 등으로 운용중인 검증대상 암호알고리즘이 더 이상 안전하지 않다고 검증기관이 판단할 경우 취약점 보완 재검증 대상이다.

○ **(기타 취약점 발견)** 기타 취약점 보완이 필요하다고 검증기관이 판단할 경우 취약점 보완 재검증을 수행할 수 있다.

□ **(적용 검증기준)**

○ **(검증 당시 검증기준 적용)** 취약점을 보완하는 과정에서 불가피하게 취약점 보완 대상이 아닌 항목이 변경되면 검증필 암호모듈을 검증한 당시의 검증기준으로 취약점 보완 재검증을 수행할 수 있다.

○ **(취약점 검증 항목)** 취약점이 발견된 항목과 시험기관이 정한 추가적인 취약점 항목에 대하여 재검증을 실시할 수 있다.

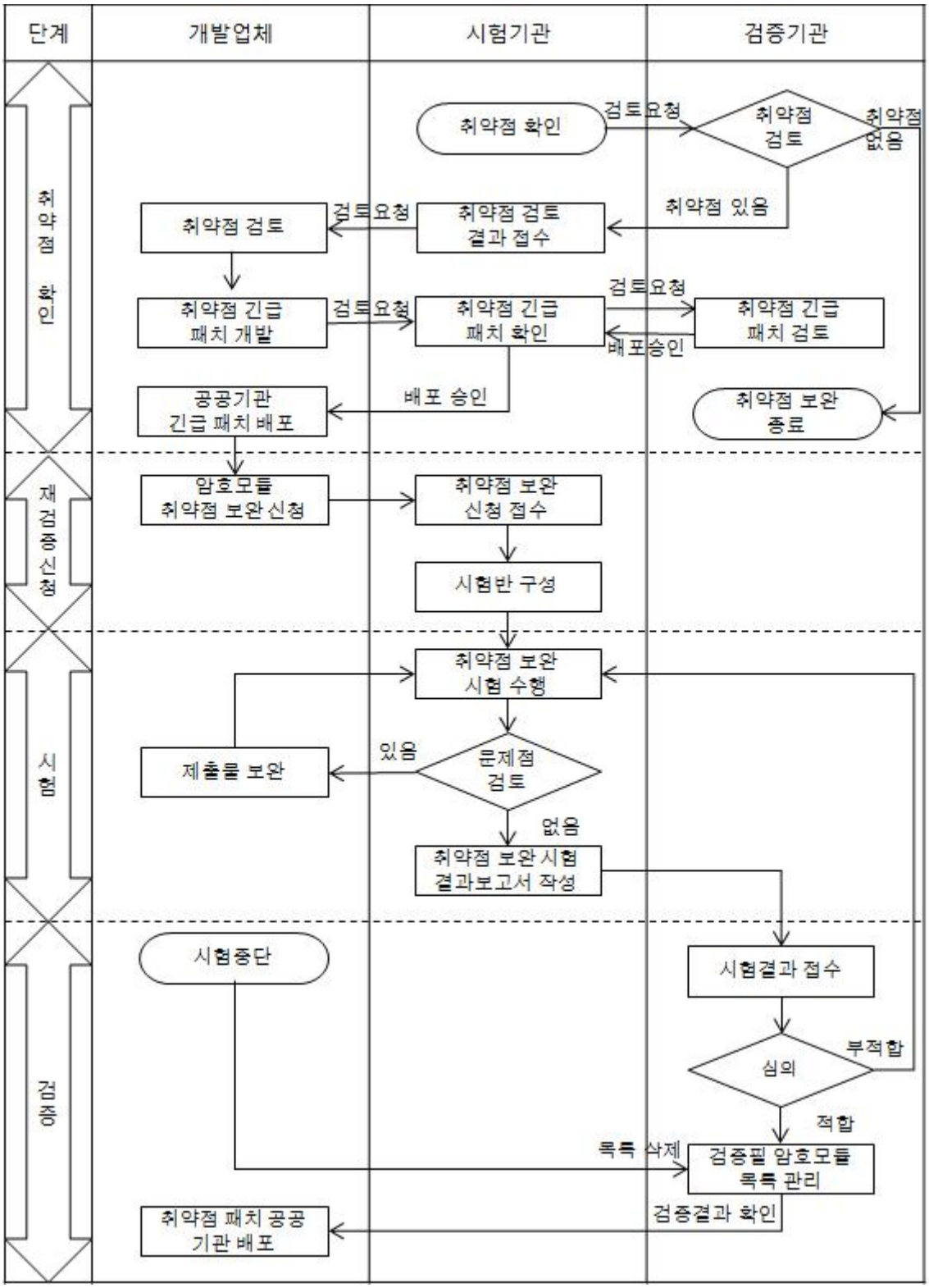
○ **(검증대상 암호알고리즘)** 암호알고리즘의 취약점 발견에 따른 재검증은 해당 암호알고리즘이 적용된 검증대상 암호알고리즘을 안전한 검증대상 암호알고리즘으로 변경하거나 비검증대상 암호알고리즘으로 전환하여 취약점 보완 재검증을 실시하여야 한다.

□ **(검증필 암호모듈 목록관리)**

○ (검증번호 유지) 취약점 보완 재검증을 완료하면, 버전 정보가 포함된 암호모듈명이 검증필 암호모듈 목록에 등재된다. 검증번호는 변경하지 않는다.

○ (검증유효기간 유지) 검증유효기간은 변동이 없다.

2. 취약점 보완 절차


단계
개발업체
시험기관
검증기관
취약점 확인
재검증신청
시험
검증
취약점 확인
검토요청
취약점 검토
취약점 없음
취약점 있음
취약점 검토 결과 접수
검토요청
취약점 검토
취약점 긴급 패치 개발
검토요청
취약점 긴급 패치 확인
검토요청
취약점 긴급 패치 검토
배포승인
배포 승인
공공기관 긴급 패치 배포
취약점 보완 종료
암호모듈 취약점 보완신청
취약점 보완 신청 접수
시험반 구성
취약점 보완 시험 수행
있음
문제점 검토
제출물 보완
없음
취약점 보완 시험 결과보고서 작성
시험중단
시험결과 접수
부적합
심의
적합
목록 삭제
검증필 암호모듈 목록 관리
검증결과 확인
취약점 패치 공공 기관 배포

① 공공기관, 개발업체 등이 검증필 암호모듈의 취약점을 발견하면, 즉시 시험기관에 이 사실을 알려야 한다. 시험기관은 개발업체 및 관련 전문가와 다각적으로 검토하고 검증필 암호모듈의 취약점 여부를 확인하여야 한다.

② 시험기관은 취약점이 있다고 판단하면 검증기관에게 취약점 검토를 요청하여야 하고, 검증기관이 검증필 암호모듈에 취약점이 없다고 판단하면, 시험기관은 취약점 보완을 종료할 수 있다.

③ 검증기관에서 취약점이 있다고 판단하면, 시험기관은 개발업체에게 취약점 검토를 요청할 수 있다. 개발업체는 발견된 취약점을 우회하거나 중지시키는 등 임시로 취약점을 보완할 수 있는 긴급 패치를 개발하고 시험기관에 제출하여야 한다.

④ 시험기관은 개발업체가 제출한 긴급패치를 확인하고, 검증기관에 검토를 요청하여야 한다. 검증기관이 긴급패치를 검토하고 승인하면, 시험기관은 개발업체가 암호모듈을 배포한 공공기관에 긴급패치를 배포하도록 승인할 수 있다.

⑤ 개발업체는 시험기관이 배포를 승인하면, 공공기관에 긴급패치를 배포한 후, 암호모듈의 취약점을 완전하게 보완한 제출물을 준비하여야 한다.

⑥ 개발업체는 공문, 취약점 보완신청서, 취약점분석서, 영향분석서, 암호모듈 배포기관, 취약점이 보완된 제출물을 제출하고 취약점 보완 신청을 해야 한다. 시험기관은 해당 취약점을 수정한 암호모듈을 시험하기 위한 시험반을 구성하고, 시험을 수행할 수 있다.

⑦ 시험기관은 취약점 보완 시험 과정에서 제출물의 보완을 요청할 수 있다.

⑧ 시험기관은 취약점 보완 시험을 완료하면, 시험결과보고서를 검증기관에 제출하여야 한다.

⑨ 검증기관은 시험결과보고서를 심의하고, 보완할 필요가 있다고 판단하면, 시험기관에게 재시험을 요청할 수 있다. 검증기관은 취약점 보완 결과를 심의하여 적합하다고 판단하면, 검증필 암호모듈 목록에 새로운 암호모듈명으로 등록하고, 검증번호와 검증유효기간은 변경하지 않는다.

⑩ 개발업체는 보완한 암호모듈이 검증필 암호모듈 목록에 등재되면, 패치 계획을 수립하여 취약점이 완전하게 해결된 암호모듈을 배포기관에 배포하고, 배포 결과를 시험기관에 통보하여야 한다.

Ⅶ. 재검증 요약

항목	보안기능 변경 재검증	비보안기능 변경 재검증	검증유효기간 만료 재검증	취약점 보완 재검증
재검증 목적	- 보안기능 변경사항 반영	- 비보안기능 변경 반영	- 검증유효기간 만료에 따른 연장	- 취약점 발견에 따른 긴급 대응
재검증 대상	- 보안기능 변경	- 비보안기능 변경	- 검증 당시와 현재 검증기준이 동일 - 검증유효기간 만료	- 취약점 발견
제출물	- 설계서(신버전) - 형상관리(신버전) - 시험서(신버전) - 영향분석서 - 소스코드 및 하드웨어 설계서 (구버전, 신버전) - 암호모듈 (구버전, 신버전)	- 설계서(신구대조표) - 형상관리(신구대조표) - 시험서(신구대조표) - 영향분석서 - 소스코드 및 하드웨어 설계서 (구버전, 신버전) - 암호모듈 (구버전, 신버전)	- 영향분석서 - 암호모듈(신버전)	- 설계서(신구대조표) - 형상관리(신구대조표) - 시험서(신구대조표) - 영향분석서 - 소스코드 및 하드웨어 설계서 (구버전, 신버전) - 암호모듈 (구버전, 신버전)
검증기준	- 현재 검증기준	- 당시 검증기준	- 현재 검증기준	- 당시 검증기준
검증 유효기간	- 5년 연장	- 변동 없음	- 5년 연장	- 변동 없음
의무사항	- 없음	- 없음	- 없음	- 취약점 확인하면 즉시 배포기관에 고지
재검증 신청시기	- 변경사항 발생시	- 변경사항 발생시	- 잔여 검증유효기간 (6개월 이상, 12개월 미만)	- 시험기관의 요청이 있으면 즉시 재검증 신청
재검증 중단시 처리	- 변동 없음	- 변동 없음	- 변동 없음	- 검증필 암호모듈 목록에서 삭제
검증번호	- 새로 부여	- 변동 없음	- 새로 부여	- 변동 없음
암호모듈명	- 변경 가능	- 변경 가능	- 변경 불가	- 변경 가능

Ⅷ. 검증필 암호모듈 관리

1. 검증필 암호모듈 관리

□ (검증필 암호모듈 목록 관리)

○ **(잔여 검증유효기간 목록 유지)** 보안기능 변경 재검증은 기존의 암호모듈은 잔여 검증유효기간 동안 검증필 암호모듈 목록에 유지되며, 개발업체의 요청에 따라 삭제할 수 있다.

○ **(재검증 중 검증유효기간 만료)** 재검증을 완료하지 않은 상태에서 검증유효기간이 만료되면, 검증필 암호모듈 목록에서 삭제할 수 있다.

○ **(공개 매체)** 검증기관은 검증필 암호모듈에 대한 정보를 국가사이버안전센터 홈페이지 등 검증기관이 정한 매체에 공개하여야 한다.

○ **(검증필 암호모듈 공개정보)**

- **(암호모듈 개요)** 버전정보가 포함된 암호모듈명, 검증번호, 개발사, 보안수준, 모듈 형태, 검증일 등의 정보를 공개할 수 있다.
- **(검증 개요)** 암호모듈의 명칭, 적용기준, 세부 항목별 보안수준 정보를 공개할 수 있다.
- **(형상데이터)** 검증필 암호모듈의 불법 변경여부를 확인하기 위한 해쉬값을 pdf 파일 등 검증기관이 정한 형식으로 공개할 수 있다.
- **(보안정책문서)** 암호모듈 명세, 암호알고리즘 및 동작모드, 운영환경, 보안등급 등의 정보를 pdf 파일 등 검증기관이 정한 형식으로 공개할 수 있다.
- **(변경 이력)** 재검증 이력, 암호모듈명 변경 등의 이력을 공개할 수 있다.
- **(검증번호 구성)** 검증번호는 CM-XX-YYYY.M 형태로 구성한다. CM은 암호모듈임을 표시하고, XX는 순번, YYYY.M은 유효기간의 연도와 월을 나타낸다. 검증기관은 검증번호의 구성 방식을 변경할 수 있다.

□ (검증필 암호모듈 개발업체 의무)

○ **(소스코드 및 개발환경 관리)** 개발업체는 검증필 암호모듈의 소스코드 및 개발환경을 보안성 있게 관리하여야 한다.

ex) 비인가자가 형상관리시스템에 접근하거나, 보안관리가 부실하여 소스코드 등이 외부로 유출되는 경우, 검증필 암호모듈 목록에서 삭제할 수 있다.

○ **(검증기관/시험기관에 배포정보 제공)** 개발업체는 검증기관/시험기관의 요청이 있으면 암호모듈 배포기관 정보를 제공하여야 한다.

○ **(무단 변경 금지)** 개발업체는 검증필 암호모듈의 사소한 변경이더라도 재검증을 받아야한다. 절차에 따라 승인을 받지 않고 무단으로 암호모듈을 변경하여 배포하면 아니된다.

○ **(취약점 발견 고지)** 개발업체는 취약점이 발견될 경우, 검증기관/시험기관이 요청하면, 검증필 암호모듈을 배포한 국가·공공기관에 취약점을 발견했음을 알려야 한다.

○ **(인가된 관리 및 배포 방식)** 개발업체는 암호모듈 관리 및 배포에 대한 책임이 있으며, 인가되지 않은 배포방식을 사용하면 아니된다.

○ **(검증유효기간 고지)** 개발업체는 국가·공공기관 대상으로 검증필 암호모듈을 배포할 때 도입기관에 암호모듈의 검증유효기간을 고지하여야 한다.

※ 검증기관은 개발업체가 의무사항을 준수하지 않을 경우 해당 암호모듈을 검증필 암호모듈 목록에서 삭제할 수 있으며, 사안에 따라 해당 신청인의 암호모듈 검증신청 자격을 3년의 범위 내에서 제한할 수 있다.

2. 보안점검

□ **(보안점검 목적)** 시험기관(또는 검증기관 합동)이 암호모듈 검증 또는 재검증 신청업체의 개발환경에 대한 인적·물리적·절차적 측면의 보안점검을 확인하기 위하여 실시하며 시험기관이 실시 여부를 결정할 수 있다.

□ **(보안점검 절차)**

○ **(사전협의)** 시험기관은 신청업체와 협의하여 점검일정을 확정한다.

○ **(계획수립)** 시험기관은 신청업체가 보안점검을 위하여 필요한 제반 조치를 취할 수 있도록 점검 10일 전에 보안점검 계획을 통보한다.

○ **(보안점검 수행)** 시험기관은 보안점검 세부항목에 대해 측정하고, 수행결과에 대한 총평 및 정리된 결과를 설명하고 보안점검을 종료한다.

○ **(보안점검 결과)** 시험기관은 보안점검 결과를 시험결과보고서에 기재하며, 보안점검 결과는 암호모듈의 재검증 승인여부에 반영할 수 있다. 시험기관은 개발환경 보안유지를 위하여 보완이 필요하면 신청업체에 통보한다.

[부록] 재검증 신청서 양식

<table>
<tr><th colspan="5">재검증 신청서</th></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="2"></td><td>(전화:)
(FAX :)</td></tr>
<tr><td>대표 성명</td><td colspan="3"></td></tr>
<tr><td colspan="3">담당자 성명 :
부 서 :</td><td>(전화:)
(FAX :)
(E-mail:)</td></tr>
<tr><td rowspan="4">재검증대상</td><td>암호모듈명</td><td></td><td>⑧검증서 번호</td><td></td></tr>
<tr><td>모듈특징</td><td colspan="3">예) - 검증대상 암호알고리즘만 제공하는 라이브러리 형태의 암호모듈
- 암호제품에 대한 프레임워크 형태의 암호모듈</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)
- 기본 및 상세설계서(변경사항이 없으면 제출 면제)
- 형상관리문서(변경사항이 없으면 제출 면제)
- 시험서(변경사항이 없으면 제출 면제)
- 영향분석서
- 소스코드 및 하드웨어 설계서
- 암호모듈</td></tr>
</table>