**[별지 제1호 서식]** 암호모듈 검증신청서

<table>
<tr><td>접 수 번 호<br>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: )<br>(FAX : )</td></tr>
<tr><td>④대표 성명</td><td colspan="3"></td></tr>
<tr><td colspan="3">⑤담당자 성명 :<br>⑥부 서 :</td><td>(전화: )<br>(FAX : )<br>(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)<br>■ 운영모드 (□ ECB □ CBC □ CFB □ OFB □ CTR □ GCM □ CCM)<br>■ 해시함수 (□ LSH □ SHA2 □ SHA3)<br>■ 메시지 인증코드 (□ HMAC □ GMAC □ CMAC)<br>■ 난수발생기 (□ Hash_DRBG □ HMAC_DRBG □ CTR_DRBG)<br>■ 공개키 암호 (□ RSAES)<br>■ 전자서명 (□ RSA-PSS □ KCDSA □ ECDSA □ EC-KCDSA)<br>■ 키 교환 (□ DH □ ECDH)<br>■ 키 유도 (□ KBKDF □ PBKDF)<br>■ 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<br>(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.<br><br>년 월 일 신청인 (서명 또는 인)</td></tr>
<tr><td colspan="5">제 출 물 (전자파일 1부)<br><br>1. 기본 및 상세설계<br>2. 형상관리<br>3. 개발과정 각 단계별 수행해야 하는 시험항목, 각 시험항목별 시험목적, 시험절차 및 결과<br>4. 제품 및 원시프로그램 또는 하드웨어 설계서</td></tr>
</table>