국제공인 시험기관, 국립전파연구원 지정시험기관, 산업통상자원부 시험기관

인증 · 시험평가 전문기관
엔트리연구원

www.ntree.or.kr

IoT 사이버보안 - ETSI EN 303 645

TÜVNORD

무선기기 사이버보안 - CE RED(ETSI EN 18031)

TÜVNORD

산업 보안 표준 - IEC 62443

소프트웨어 품질 평가: KOLAS 공인 인정 시험기관
- KS X ISO/IEC 25023
- KS X ISO/IEC 25051

KOREA LABORATORY ACCREDITATION SCHEME
KOLAS
TESTING NO. KT511

미국 FCC의 U.S. Cyber Trust Mark

국내 IoT 보안인증 자문/지원

사이버보안 평가 및 인증 문의
담당자: 김 한 주
E-mail: hjkim3@ntree.or.kr

㈜엔트리연구원
경기도 수원시 권선구 산업로
155번길 228-60(고색동)

엔트리연구원 적합성 평가 시험 서비스

◎ EMC/EMF - 전자파 분야

◎ RF - 무선 통신 분야

◎ SAR - 전자파흡수율 분야

◎ R&E - 신뢰성 및 환경 시험 분야

◎ Global Certification - 해외인증

◎ Noise - 소음 분야

◎ Safety - 제품 전기 안전 분야

◎ Photometry - 광학 분야

◎ MAS - 영상감시장치 화질 성능 평가

◎ MS Certification - 경영시스템 인증 서비스

유럽연합(EU) & 영국(UK) 사이버보안 법규

- **CE RED(Radio Equipment Directive) 사이버보안 요구사항**

(d) 무선기기는 서비스의 부적절한 성능 저하를 일으키지 않도록 네트워크 또는 그 기능에 해를 끼치지 않으며, 네트워크 자원을 남용하지 않아야 함

(e) 무선기기는 사용자 및 가입자의 개인 데이터와 개인정보를 보장하기 위한 안전 장치를 내장해야 함

(f) 무선기기는 사기 방지를 보장하는 특정 기능을 지원해야 함

RED article 3.3 d)	Protection of Network	EN 18031-1
RED article 3.3 e)	Privacy	EN 18031-2
RED article 3.3 f)	Protection of monetary transactions	EN 18031-3

- 적용대상: **유럽시장에 출시되는 모든 무선기기에 의무적용**
- 시행시기: **2025. 08. 01.부터**

- **Cyber Resilience Act(CRA)**

유럽 사이버 복원력 법은 유럽 연합 시장에 출시되는 디지털 요소가 포함된 하드웨어 및 소프트웨어 제품에 대한 사이버보안 요구 사항을 설명하는 법적 규정입니다.
이제 제조업체는 제품 수명 주기 전반에 걸쳐 보안을 중요하게 고려해야 할 의무가 있습니다.

- 적용대상: **유럽시장에 출시되는 디지털 요소가 포함된 하드웨어 및 소프트웨어 제품에 의무적용**
- 시행시기: **2027년 말부터**

- **영국 PSTI법**

소비자 IoT 보안 강화를 위한 최초의 법률 중 하나

- 주요 내용
  - 기본 패스워드 금지
  - 보안 업데이트 및 지원 기간
  - 취약점 신고 체계 구축

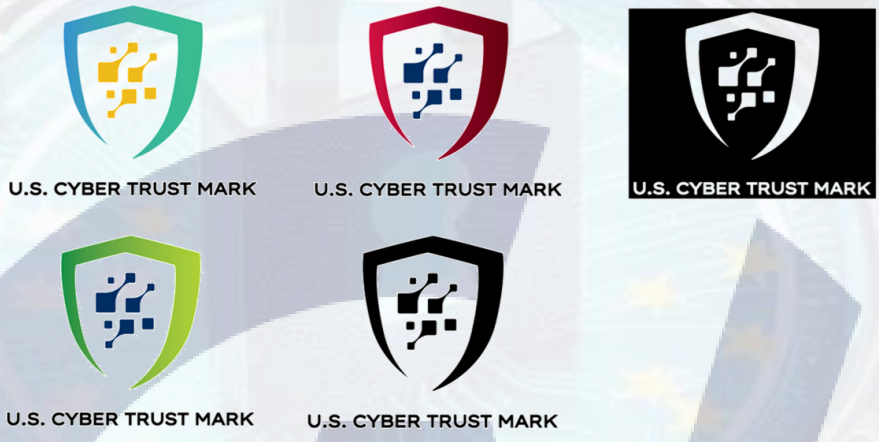
- 적용대상: **영국시장에 출시되는 소비자 커넥티드 제품(IoT 제품)**
- 시행시기: **시행 중(2024.4.29~)**

엔트리연구원은 TUV NORD와의 업무협약으로 TUV NORD 인증서 발급이 가능합니다.

미국(US) 사이버보안 법규

- **U.S. Cyber Trust Mark**

FCC의 자발적 사이버 보안 라벨링 프로그램



프로그램 특징

- 자발적 참여: 소비자 스마트 제품이 강력한 사이버보안 기준을 충족하면 "**U.S Cyber Trust Mark**" 라벨 부착 승인
- 소비자 정보 제공: 라벨(QR cord)을 통해 소비자는 제품의 보안성을 쉽게 확인 (미국 소비자가 구매 제품의 보안을 확인할 수 있는 유일한 수단)
- 제조업체 인센티브: 제조업체는 더 높은 사이버보안 기준을 충족하기 위해 노력

- **적용대상: 미국시장에 출시되는 무선 소비자 IoT 제품에 자율적용**
- **시행시기: 곧 시행 예정**

▪ **기반표준**

✓ **NIST IR 8259**
- IoT 디바이스 제조업체를 위한 기본 사이버 보안 활동

✓ **NIST IR 8259A**
- IoT 디바이스 사이버 보안 기능 핵심 기준

✓ **NIST IR 8259B**
- IoT 비기술 지원 기능 핵심 기준

✓ **NIST IR 8425**
- 소비자 IoT 제품을 위한 IoT 핵심 기준 개요

국내 사이버보안 법규

- **IoT 보안인증**

- IoT 보안인증·시험 서비스는 IoT 제품 및 연동 모바일 앱에 대해 일정 수준의 보안을 갖추었는지 시험하여 기준 충족 시 인증서를 발급해주는 서비스로, 인증 대상은 IoT 제품 및 연동 모바일 앱을 포함(유효기간 3년, 2년 연장 가능)

- 시험•인증기관: 한국인터넷진흥원(KISA)
- 시험대행기관: 한국기계전기전자시험연구원(KTC), 한국정보통신기술협회(TTA)

- **적용대상: 국내 IoT제품 및 제품과 연동되는 모바일 앱**
  - **네트워크에 연결되어 감지, 제어, 중계, 촬영, 관리, 운행 등의 기능을 수행하는 기기를 총칭(모듈 포함)**
- **시행시기: 시행 중**

- **소프트웨어 품질 평가**

정부과제 (R&D) 프로젝트의 경우 사업 최종 결과 전에 제3자 전문기관으로 시험을 의뢰해서 시험을 의뢰합니다.
공신력 있는 품질 평가가 필요한 모든 곳에 활용이 가능합니다.

- 의뢰자가 제시한 조건에 따라 소프트웨어에 대한 기능과 성능을 시험
- 소프트웨어를 대상으로 한 정부과제의 정략적 목표 달성 여부를 확인하는 시험

엔트리연구원은 KOLAS 인정 시험기관으로 소프트웨어 정부 과제 품질 시험 및 IoT보안인증 시험 자문/지원이 가능합니다.