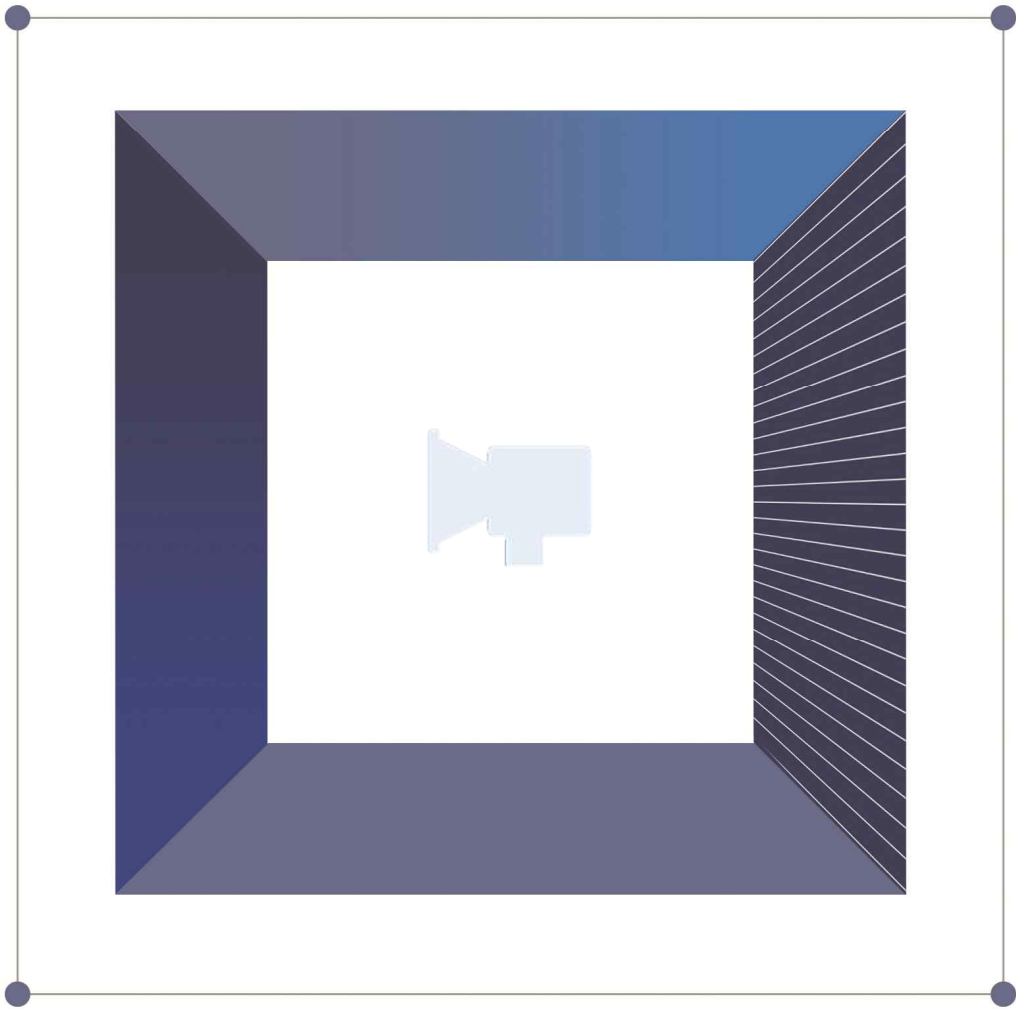


# 05

해외인증 실무 가이드북

CE-RED


사이버보안-무선통신기기



산업통상자원부  
해외인증지원단

KSA 한국표준협회

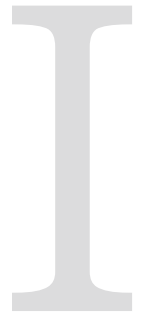
● 제품

품목명 (HS CODE)	무선통신기기 8517.62-10, 8517.62-90	지역/국가 인증명	유럽 CE-RED								
품목정의	<ul style="list-style-type: none"> <li>• 일반적 정의                             <ul style="list-style-type: none"> <li>- 사이버보안은 컴퓨터, 네트워크, 소프트웨어 애플리케이션, 중요 시스템 및 데이터를 잠재적 디지털 위협으로부터 보호하는 행위</li> <li>- 무선기기의 발전과 함께 인터넷과의 연결이 많아짐에 따라 사용자의 개인정보와 프라이버시가 무선기기를 통해 보호가 가능한지의 우려가 증가하고 있음</li> <li>- EU에 유통되는 무선기기에 대한 사이버보 확보를 위해 2025년 8월1일부터 RED(Radio Equipment Directive) 지침(2014/53/EU)의 필수적 요구사항 제3조(3),(d),(e),(f))의 EU 집행위원회가 공포한 사이버보안 조화 표준을 준수하도록 규정함</li> </ul> </li> <li>• 기술적 정의                             <ul style="list-style-type: none"> <li>- RED의 사이버보안 조항을 충족하기 위해 제조사는 Secure Communication(보안 통신), Access Control(접근 통제), Data Protection(데이터 보호), Software and Firmware Integrity(소프트웨어 무결성), Resilience to Attacks(공격 저항성), Provisioning of Security Updates(보안 업데이트 제공) 등의 기술적 요소를 구현해야 함</li> </ul> </li> </ul>										
적용대상품목	무선기능이 있는 블루투스 사용제품, Wi-Fi 사용제품, 무선 송/수신기 원격 제어장치 등 <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th>적용대상</th> <th>예시</th> </tr> </thead> <tbody> <tr> <td>인터넷을 통해 통신 할 수 있는 기기</td> <td>스마트폰, 태블릿, 디지털카메라 등</td> </tr> <tr> <td>장난감 및 육아 장비</td> <td>장난감, 베이비 모니터 등</td> </tr> <tr> <td>웨어러블 기기</td> <td>스마트워치, 피트니스 트랙커 등</td> </tr> </tbody> </table> <p>※ 의료기기는 RED 대상이 아님. 단, 자동차, 도로교통시스템, 무인항공기를 원격으로 제어하는 장비, 항공기에 설치 될 수 있는 비공중 특성의 장비는 3.3(d) 항만 적용</p>			적용대상	예시	인터넷을 통해 통신 할 수 있는 기기	스마트폰, 태블릿, 디지털카메라 등	장난감 및 육아 장비	장난감, 베이비 모니터 등	웨어러블 기기	스마트워치, 피트니스 트랙커 등
적용대상	예시										
인터넷을 통해 통신 할 수 있는 기기	스마트폰, 태블릿, 디지털카메라 등										
장난감 및 육아 장비	장난감, 베이비 모니터 등										
웨어러블 기기	스마트워치, 피트니스 트랙커 등										
유사품목 키워드	유무선 통신기기										
마크											

Part. 01  
무선통신기기



해외인증  
실무  
가이드북



사이버보안 : CE-RED  
인증소개

## 인증개요

품목명 (HS CODE)	무선통신기기		지역/국가	유럽
	8517.62			
인증마크			인증명 (제도명)	CE-RED
인증유형	(유형1)	<input checked="" type="checkbox"/> 제품인증 <input type="checkbox"/> 시스템	(유형2)	( <input checked="" type="checkbox"/> 강제 <input type="checkbox"/> 임의 <input type="checkbox"/> 기타)
인증 종류	<input checked="" type="checkbox"/> DoC <input checked="" type="checkbox"/> CoC ※ DoC(자기적합성 선언) / CoC(적합성 인증)			

## 인증소개

### □ 개요

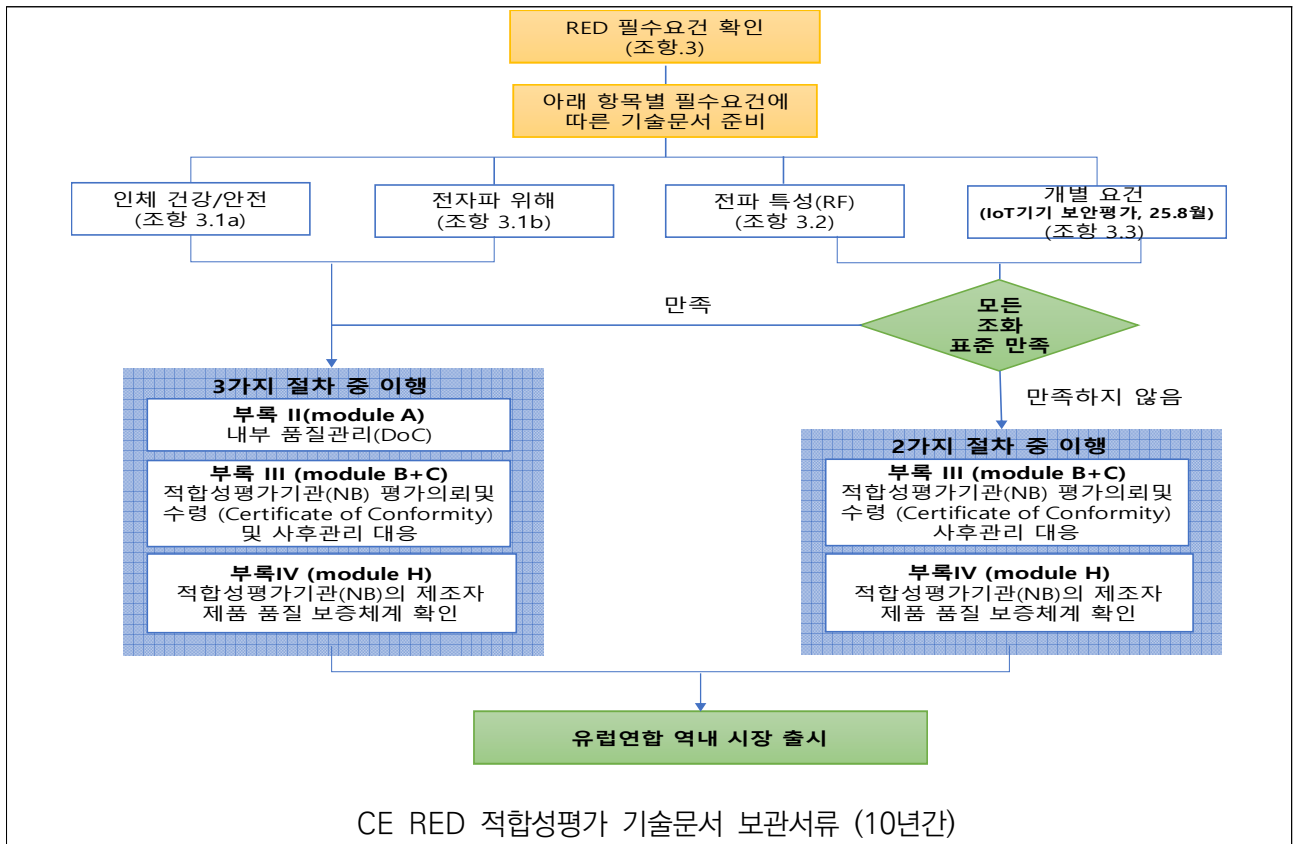
- EU는 디지털 시대 변화에 대응하여, 유럽적 가치에 기초한 기술 주도권을 확보하고 디지털 역량을 강화하기 위해 다양한 디지털 정책과 입법을 추진
- 2016년 10만개의 IoT 제품을 이용한 대규모 DDoS 공격으로 무선·스마트 장비 보안취약점이 RED 사이버보안 관련 필수적 요구사항(Art. 3(3))을 활성화하는 정책적 촉매가 됨

[표-1] EU 사이버 보안 관련 주요 개정 사항

연도	주요개정사항	주요 내용
2020.12	사이버 보안전략 발표	디지털 시대의 핵심요소로 '신뢰(trust)'와 '보안(security)'을 강조하고, 사이버위협에 대한 EU의 대응역량 강화
2022.1	Delegated Reg. 2022/30 채택	RED 보안조항 공식 발효(6 개월 후) - 제조사 30개월 전환시작
2022.9	사이버복원력법	디지털 요소가 있는 제품에 대한 공통의 사이버보안 기준 마련 및 EU 역내 시장에 공급되는 제품에 대한 적합성 평가·인증체계 마련
2023.1	사이버 보안 관련 NIS2 지침, CER 지침 개정	철도, 의료, 에너지 등 필수·중요조직의 사이버보안 및 사고 대응력을 강화하고 자연재해, 테러, 사이버위협 등 다양한 위협으로부터 주요 조직(critical entities)의 복원력을 확보하기 위한 지침 개정
2023-7	적용시점 1년 연기 결정(C(2023) 4823)	산업계 요청으로 2025-08-01까지 연기
2024-06~2025-01	CE-RED 대상 IoT 제품 사이버 보안 EN 18031 시리즈 확정	IoT 무선 제품등 의 일반적 보안 준수사항 등 규정
2025.8	CE-RED 사이버 보안 평가 기준 시행	이 시점 이후 출시되는 IoT 무선제품은 보안성 평가 성적서 보유

□ CE-RED(Radio Equipment Directive) 인증제도 개요

- CE-RED 인증 제도는 단순한 제품시험을 넘어, 제품의 기술적 완성도와 사용자 보호를 동시에 보장하는 제도로, 최근 무선 통신과 관련된 보안 위협이 증가함에 따라 사이버보안 항목이 제도에 포함되었으며, 해당 제도를 통해 제조사에게 제품 설계단계부터 보안과 안전을 고려할 것을 요구하며, EU 시장 진출을 위한 필수 요건으로 자리 잡고 있음
- CE-RED 제도는 유럽 시장 내 유통 전 반드시 취득해야 하는 의무가 있고 개인용, 산업용을 포함한 모든 무선통신기기를 적용 범위로 하고 있으며, 인증 완료 후에는 CE 마킹으로 제품에 표시를 하여 CE 마크를 부착하도록 하고 있음



- General description of the equipment(User Manual)
- Design and manufacturing drawings
- Schemes of components, circuits
- List of standards applicable and/or description of the technical solutions adopted
- List of components
- Test reports
- Declaration of Conformity based on radio test suites
- Sample label & Packaging Design
- Analysis and assessment of risk

[그림 1] CE-RED 적합성 평가 절차 및 기술문서 보관서류 예시

- CE-RED의 사이버보안은 요구사항은 제3조 제3항(d)(e)(f)에서 명시하고 있으며, 2022년 2월 1일부터 RED 지침 제3조 제3항(d)(e)(f)이 시행하여 42개월의 적용기간을 거쳐 2025년 8월 1일부터 의무화 적용될 예정
  - 1) 3.3(d) : 무선통신기기는 서비스의 부적절한 성능 저하를 일으키지 않도록 네트워크 또는 그 기능에 해를 끼치지 않으며, 네트워크 자원을 남용하지 않아야 함
  - 2) 3.3(e) : 무선통신기기는 사용자 및 가입자의 개인 데이터와 개인정보보호를 보장하기 위한 안전장치를 내장하여야 함
  - 3) 3.3(f) : 무선통신기기는 사기 방지를 보장하는 특정 기능을 지원해야 함
- CE-RED 제도에 대한 문의 시 아래의 공식 홈페이지 및 관련 이메일 등을 참고할 수 있음
  - 1) CE-RED 공식 홈페이지 : [https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red\\_en](https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en)
  - 2) CE-RED 문의 이메일 : GROW-RADIO-EQUIPMENT@ec.europa.eu

## ● 관련 법령/규정

- Directive 2014/53/EU : Radio Equipment Directive (RED) (제3조 제3항 (d), (e), (f))
- Commission Delegated Regulation (EU) 2022/30 supplements the Radio Equipment Directive (RED) by introducing cybersecurity, personal data privacy, and fraud protection requirements for certain radio equipment : 특정무선기기에 대한 사이버보안, 개인정보보호, 위변조 보호 기준
- Commission Delegated Regulation (EU) 2023/2444 : Commission Delegated Regulation (EU) 2022/30 규정에 따른 무선기기 필수요구사항 (사이버보안) 적용과 관련된 사항 개정 시행일 변경규정
- Guide to the Radio Equipment Directive 2014/53/EU

## ● 적용 표준

- EN 18031-1:2024, EN 18031-2:2024, EN 18031-3:2024 (25년 1월 유럽관보 공포)
- 이중 인터넷 연결이 가능한 무선기기에 일반적으로 적용되는 표준(EN 18031-1:2024)과 특히 무선 기기 중 개인정보 데이터를 다루는 기기에 적용되는 표준(EN 18031-2:2024)이 대부분의 무선 IoT 기기에 적용될 것으로 예상
- EN 18031-3의 경우 무선 인터넷을 통한 가상화폐 또는 신용카드 결제 데이터 등을 처리하는 단말 기기에 추가적으로 적용되는 표준임

표준번호	표준 명칭	적용 대상	주요 내용
EN 18031-1:2024	Cybersecurity for radio equipment – Part 1: Internet-connected radio equipment	인터넷 연결이 가능한 무선기기 (예: Wi-Fi, LTE, 5G 기반 IoT 제품 등)	- 무선 장비 전반에 적용되는 일반적인 사이버 보안 요구 사항을 정의 - 무선 장비의 사이버 보안 위험 관리, 보안 기능 구현, 보안 업데이트 등에 대한 내용 포함
EN 18031-2:2024	Common security requirements for radio equipment. – Part 2: Radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment	개인정보를 다루는 기기 (예: AI 스피커, IP카메라, 스마트워치 등 개인 데이터 처리 기기)	- 개인 데이터를 처리하는 무선 장비에 특화된 사이버 보안 요구 사항을 정의 - 데이터의 수집, 저장, 사용, 공유, 삭제 등 개인 데이터 처리 전반에 걸친 보안 요구 사항을 포함
EN 18031-3:2024	Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value	인터넷 연결로 가상통화 또는 화폐가치를 처리하는 무선기기 (예: 무인 결제 IoT 디바이스, POS 단말기 등)	- 가상 화폐 또는 금전적 가치와 관련된 무선 장비에 대한 사이버 보안 요구 사항을 정의 - 가상 화폐 거래, 자산 관리, 보안 업데이트 등에 대한 보안 요구 사항을 포함

- 3가지 사이버 보안 표준에 공통적으로 요구되는 사항은 액세스제어, 인증메커니즘, 보안업데이트 및 저장, 보안 통신 메커니즘 등이고 이외는 기기의 특성에 따라 다소 상이한 요구사항이 적용

요구 사항	3.3.(d)	3.3.(e)	3.3.(f)
[ACM] 액세스 제어 메커니즘	√	√	√
[AUM] 인증 메커니즘	√	√	√
[SUM] 보안 업데이트 메커니즘	√	√	√
[SSM] 보안 저장 메커니즘	√	√	√
[SCM] 보안 통신 메커니즘	√	√	√
[LGM] 로깅 메커니즘	-	√	√
[DLM] 삭제 메커니즘	-	√	-
[UNM] 사용자 알림 메커니즘	-	√	-
[RLM] 회복탄력성 메커니즘	√	-	-
[NMM] 네트워크 모니터링 메커니즘	√	-	-
[TCM] 트래픽 제어 메커니즘	√	-	-
[CCK] 기밀 암호화 키	√	√	√
[GEC] 일반 장비 기능	√	√	√
[CRY] 암호화	√	√	

## 규제기관

기관명	주소	홈페이지	이메일
DG GROW (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs) European Commission	Rue de la Loi / Wetstraat 200 B-1049 Brussels Belgium (사전예약 없이 방문은 불가)	<a href="https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en">https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en</a>	GROW-RADIO-EQUIPMENT@ec.europa.eu

## 적합성평가(인증)기관

- EU 역내 회원국이 지국내 적합한 기관을 적합성평가기관(Notified Body)으로 지정하여 운영 중이며 한국 지사를 통해 EU 역내 회원국 적합성평가기관의 서비스를 대행 받을 수 있음

No.	기관명	주소	홈페이지	전화번호
1	APPLUS+	Calle Campezo nº1, Edificio 3, Parque Empresarial Las Mercedes, 28022 Madrid, Spain	<a href="http://www.appluslaboratories.com">www.appluslaboratories.com</a>	+34-912-080-800(본사) +82-2-897-0970(한국)
2	UL	333 Pfingsten Road, Northbrook, Illinois 60062, USA	<a href="http://www.ul.com">www.ul.com</a>	+1-847-272-8800(본사) +82-2-2009-9000(한국)
3	TUV SUD	Westendstraße 199, 80686 München, Germany	<a href="http://www.tuvsud.com">www.tuvsud.com</a>	+49-89-5791-0(본사) +82-2-3215-1100(한국)
4	NEMKO	Philip Pedersens vei 11, 1366 Lysaker, Norway	<a href="http://www.nemko.com">www.nemko.com</a>	+47-22-96-03-30(본사) +82-31-330-1700(한국)
5	intertek	33 Cavendish Square, London, W1G 0PS, United Kingdom	<a href="http://www.intertek.com">www.intertek.com</a>	+44-116-296-1620(본사) 02-6090-9551(한국)
6	SGS	1 Place des Alpes, P.O. Box 2152, 1211 Geneva 1, Switzerland	<a href="http://www.sgs.com">www.sgs.com</a>	+41-22-739-91-11(본사) +82-2-749-1674(한국)

\* 전체 리스트는 아래 링크(NANDO 웹사이트)에서 확인 가능

☞ <https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies>

## 적합성평가(국내시험)기관

- EU RED 사이버 보안 시험은 해외 적합성평가기관(인증) 이외에 국내 시험기관을 통해서 진행 가능

No.	기관명	주소	홈페이지	전화번호
1	한국기계전기전자시험연구원(KTC)	경기도 군포시 흥안대로27번길 22	<a href="http://www.ktc.re.kr">www.ktc.re.kr</a>	031-428-3773
2	한국산업기술시험원(KTL)	서울특별시 구로구 디지털로26길 87(구로동)	<a href="http://www.ktl.re.kr">www.ktl.re.kr</a>	02-860-1243~4

No.	기관명	주소	홈페이지	전화번호
3	한국화학융합시험연구원 (KTR)	경기도 과천시 교육원로 98 (중앙동)	www.ktr.or.kr	02-2164-0011
4	디티앤씨 (DT&C)	경기도 용인시 처인구 유림로 154번길 42	www.dtnc.co.kr	031-321-2664
5	한국시험인증원 (KOTCA)	서울시 강서구 마곡중앙로 161-8 B동 1216호	www.kotca.co.kr	02-6929-1033

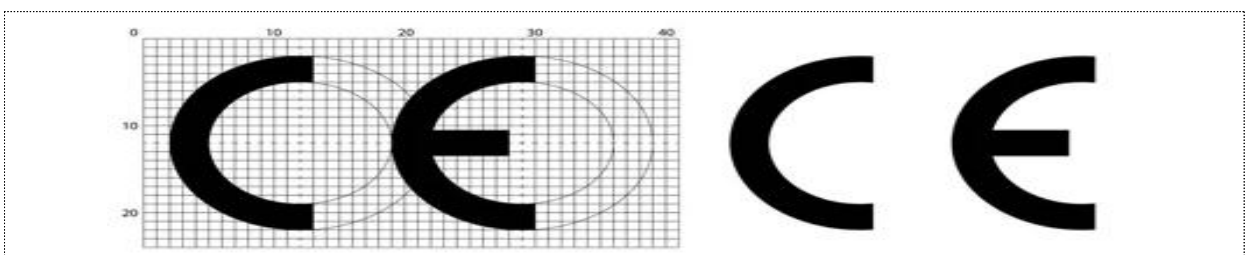
## 대응 및 정보제공기관

- 이외 전반적인 사이버 보안 대응과 정보제공 등 자문은 다음의 기관을 통해 가능

No.	기관명	주소	홈페이지	전화번호
1	한국인터넷진흥원 (KISA)	경기도 성남시 수정구 대왕판교로 815 기업지원허브 4층 정보보호클러스터 484호	www.kisa.or.kr	02-405-6625
2	해외인증지원단 (서울)	서울 강남구 테헤란로 69길 5 한국표준협회 3층	www.globalcerti.kr	02-6240-4770

## 표시사항

- CE 마킹에 대해서는 아래의 링크에 자세히 안내되어 있음  
[https://single-market-economy.ec.europa.eu/single-market/ce-marking\\_en](https://single-market-economy.ec.europa.eu/single-market/ce-marking_en)
- 유럽의 CE 마크는 1993년부터 현재의 마크로 존재해 왔으며, CE의 의미는 유럽 지침을 준수한다는 의미
- 제품의 CE 마킹 서비스는 EEA 내에서 제품에 부과된 법적 요구사항을 준수하므로 EEA 내에서 판매할 수 있음을 의미함
- 제조업체 또는 권한을 부여받은 대리인은 제품에 CE 마크를 부여하고 제품이 지침의 요구사항을 확인할 책임이 있음
- 유럽의 CE 마크는 EU 내에서 상품의 자유 무역을 촉진하며, EU 내에서 안전, 보건 및 환경에 관한 법률을 조화시키는 것임



- 표시 방법으로는 높이 5mm 이상의 'CE' 글자를 사용 및 지워지지 않고 잘 보이고, 식별 가능해야 함
- 1) Declaration of Conformity (DoC) : EU 공식 서식에 따라 작성, 10년간 보관

## ● 규제대상 품목

- RED는 무선통신장비 기능이 있는 장비에 대한 규제 지침으로 단순 전자기기 또는 유선기기는 포함되지 않음

분류	예
휴대용 통신기기	스마트폰, 태블릿, 무전기, 위성전화 등
무선 네트워크 장비	Wi-Fi 공유기, 무선 LAN 모듈, Bluetooth 모듈, ZigBee 제품
웨어러블 디바이스	스마트워치, 무선 이어폰, 피트니스 트래커 등
무선 센서/IoT 디바이스	홈 IoT 기기, 원격 제어 장치, RF 센서, Zigbee/Z-Wave 기기
차량 내 무선장비	원격 도어락, 타이어 공기압 모니터링 시스템 (TPMS), 차량 Wi-Fi
Drones/무인 항공기	2.4GHz/5GHz 통신이 탑재된 드론류
RFID/NFC 장비	근거리 무선통신 기능 탑재 장비 (e.g. POS 단말기)

## ● 시험 인증비용

- 시험비용 : 보안성 평가
- 시험비용(약 2~3천만원) + 컨설팅 비용(약 1~2천만, 선택)
- 인증비용 : NB(인증기관) 심사수수료 등 인증비용(약 1~2천만원)

## ● 적합성평가(시험) 소요기간

- 약 4~8주 소요(기관별 상이, 다만, 제품의 종류, 복잡성, 적용 표준 범위(18031-1~3), 시험기관 대기 기간 등에 따라 추가 소요될 수 있음)

## ● 인증서 유효기간

- 영구 유효(Permanent Validity, 단, EN 표준 변경, HW 등 제품 주요사양 변경 등이 일어날 경우 재시험이 필요할 수 있음)

Part. 02  
무선기기  
(CE RED  
Cybersecurity)

해외인증  
실무  
가이드북



# CE RED

## 사이버보안 시험 실무

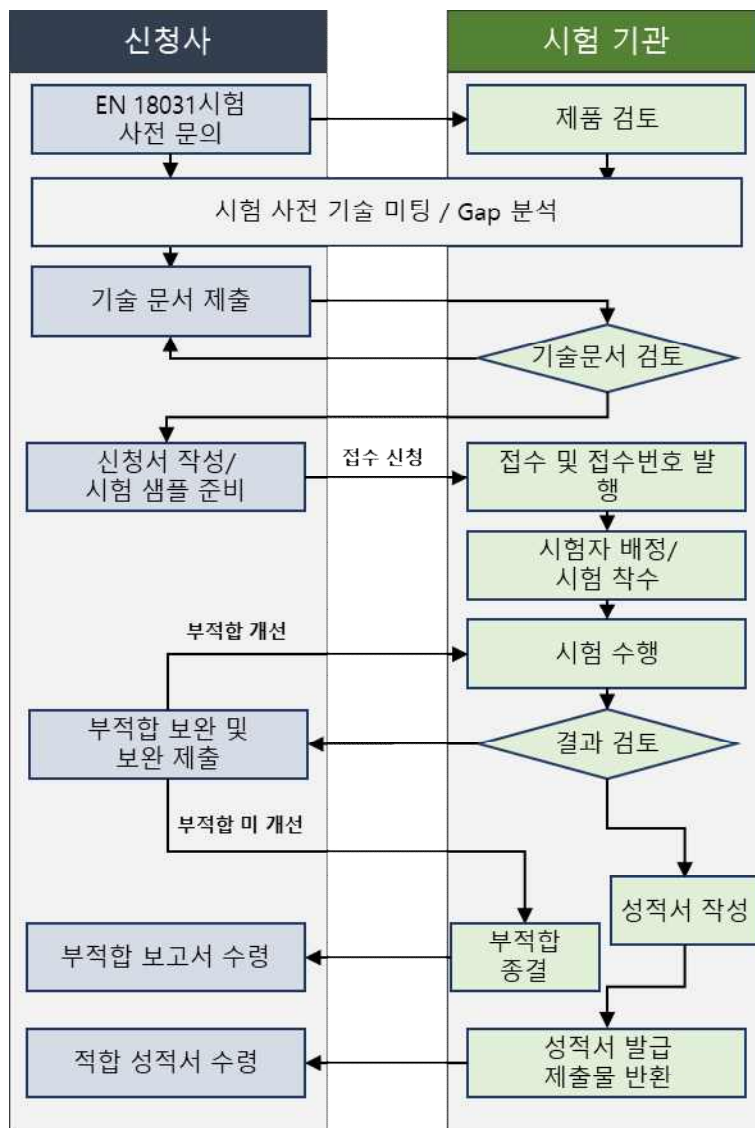
02 사이버보안 시험 실무

12

## 시험 절차

- 시험 기준 및 신청제품 기술 상담 → 시험 신청서 및 시험용 샘플 제출 → 시험 → 성적서 발행(개별제품, 시험검증 : Test certification) : 해당 무선기기에 대해 시험한 모델에 대해서만 인증하는 제도로 그 인증의 효력은 인증서에 기재된 단일 모델에 대해서만 발생

(모델별 시험검증(Type certification)) : 동일한 설계를 바탕으로 같은 제조공정에 따라 생산되는 제품 중에 한 시료로 형식시험(Type Test)을 함으로써 그 무선기기에 대해 모델 시험 완료



[그림 2-1] 보안시험평가 절차

## 시험 신청

- 시험 신청 시 필요 서류

- ① 신청서
- ② 제품설명서
- ③ 제품시험 샘플 제품
- ③ 사이버보안 체크리스트
- ④ 사업자등록증 사본

NO.	제출서류	필수 여부
1	시험 신청서(Application form)	필수
2	사용자(제품) 설명서	필수
3	사이버보안 체크리스트(미적용 사유 및 요구사항 검증 데이터 포함)	필수
4	제품 사양 및 세부시험 절차서	필수
5	하드웨어 설계도	필수
6	시험 대상 샘플 (시험 착수 시 제출)	필수

① 신청서 양식(한국기계전기전자시험연구원(KTC)의 시험 신청을 예시로 함)

시험·검사 신청서		결 계	승 인																		
<p>※신청용자는 <input type="checkbox"/> 바탕 해당란만 기재하시기 바랍니다.</p> <p>접수번호: _____ 한국기계전기전자시험연구원</p>																					
신청인	<p>회사명: _____ 성명: _____</p> <p>대표자: _____ 연락처: _____ 핸드폰: _____</p> <p>사업자등록번호: _____ 당 전화: _____</p> <p>주소: _____ 팩스: _____</p> <p>E-mail: _____</p>																				
세금계산서	<p><input type="checkbox"/> 계산서 정보와 신청인 정보가 동일 (아래 작성 선택)</p> <p>회사명: _____ 사업자등록번호: _____</p> <p>담당자 성명: _____ 휴대폰: _____ E-mail: _____</p>																				
신제품	<p>제품명: _____ 정격: _____</p> <p>모델명: _____ 시료수: _____</p> <p>제조사: _____ 시험방법: _____</p>																				
성격서	<p>성격서 유형: <input type="checkbox"/> 일반(비KOLAS) <input type="checkbox"/> KOLAS <input type="checkbox"/> 국문(부분 부) <input type="checkbox"/> 영문(부분 부)</p> <p>수령 방법: <input type="checkbox"/> 온라인(신청인 출력) <input type="checkbox"/> 방문수령 <input type="checkbox"/> 우편 (□상동 □별도주소: _____ /받는분: _____)</p> <p>사용 용도 (용도의 사용규격): <input type="checkbox"/> 품질관리용 <input type="checkbox"/> 계측용 (제출기관명: _____) <input type="checkbox"/> 기타( _____ )</p>																				
시험 후 시료처리	<p><input type="checkbox"/> 매기 <input type="checkbox"/> 방문수령 <input type="checkbox"/> 택배(착불) (□상동 □별도주소: _____ /받는분: _____)</p> <p>시험·검사 장소: <input type="checkbox"/> 원내 <input type="checkbox"/> 출장 (주소: _____)</p>																				
팩 서비스(별지1)	<p><input type="checkbox"/> 고속 <input type="checkbox"/> 객 <input type="checkbox"/> 신청안함</p>																				
적합성 진술(별지2)	<p><input type="checkbox"/> 요청 <input type="checkbox"/> 미요청</p>																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>시험검사항목</th> <th>수량</th> <th>수수료</th> <th>시험검사항목</th> <th>수량</th> <th>수수료</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <p>전처리: 원 출장비(액): 원 합계: (VAT별도)</p> <p>위와 같이 귀 원에 시험·검사를 의뢰합니다. 20 년 월 일</p> <p style="text-align: right;">신청인: (서명 또는 인)</p>		시험검사항목	수량	수수료	시험검사항목	수량	수수료														
시험검사항목	수량	수수료	시험검사항목	수량	수수료																
접수자	담당부서	성격서 발급 예정일	년 월 일																		
서식 P701-01(Rev.10)		Page 1 / 2																			

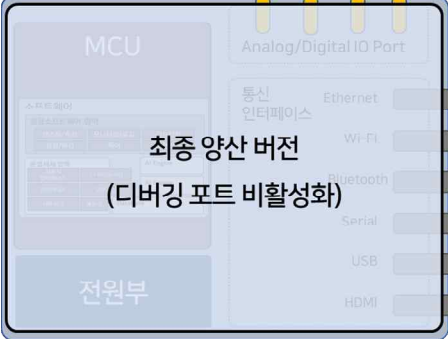
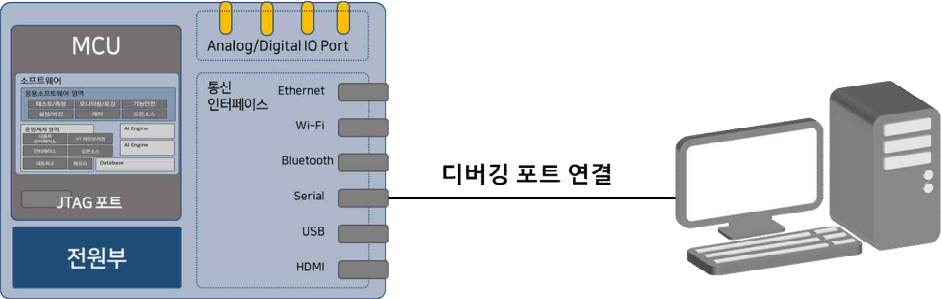
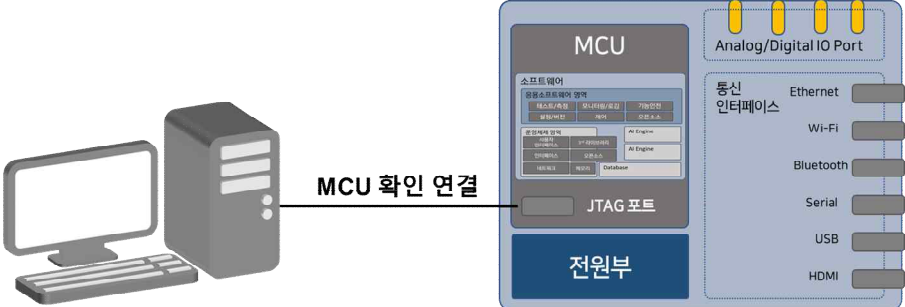
개인정보 수집·이용 및 제3자 제공 동의서	
<p>(재)한국기계전기전자시험연구원(이하 "연구원"이라 한다)은 접수, 상담, 안내, 성격서 및 인증서 발급 등을 위하여 아래와 같이 개인정보를 수집·이용 및 제3자에게 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주시기 바랍니다.</p>	
<p>■ 개인정보 수집 및 이용 내역</p> <p>① 개인정보 항목</p> <ul style="list-style-type: none"> <li>- 성명, E-mail, 전화번호, 핸드폰번호, FAX, 주소, 사업자등록(회사명, 연락처, 주소)</li> <li>* 본 동의 이전에 발생한 개인정보뿐만 아니라, 향후 발생하는 개인정보를 포함합니다.</li> </ul> <p>② 수집이용 및 목적</p> <ul style="list-style-type: none"> <li>- 시험, 검사, 검정, 인증에 대한 접수 및 성격서·인증서 발급, 세금계산서 발급, 고객 관리, 연구개발 등 연구원에서 수행하는 사업과 관련한 각종 서비스 제공.</li> </ul> <p>③ 보유기간: 5년</p> <p>④ 동의를 거부할 권리 및 불이익</p> <ul style="list-style-type: none"> <li>- 위의 개인정보 수집 및 이용에 대하여 동의를 거부할 권리가 있으며, 동의 후에도 언제든지 철회 가능합니다. 다만, 동의를 거부할 경우 연구원이 제공하는 각종 서비스에 제한을 받을 수 있으며, 철회 후에는 위의 기재된 수집이용 및 목적과 관련된 분쟁해결, 민원처리, 발령상 의무이행 등을 위하여 필요한 범위 내에서만 제한적으로 보유·이용됩니다.</li> </ul>	
<p>위와 같이 개인정보를 수집 및 이용하는데 동의하십니까? <input type="checkbox"/> 예 <input type="checkbox"/> 아니오</p>	
<p>■ 개인정보 제3자 제공 내역</p> <p>① 개인정보 항목</p> <ul style="list-style-type: none"> <li>- 성명, E-mail, 전화번호, 핸드폰번호, FAX, 주소, 사업자등록(회사명, 연락처, 주소)</li> <li>* 본 동의 이전에 발생한 개인정보뿐만 아니라, 향후 발생하는 개인정보를 포함합니다.</li> </ul> <p>② 수집이용 및 목적</p> <ul style="list-style-type: none"> <li>- 고객성문조사, 우편 업무, 연구원 업무 안내 및 관련 법령에 따른 자료 제공 등을 위하여 제3자 제공</li> </ul> <p>③ 보유기간: 1년</p> <p>④ 동의를 거부할 권리 및 불이익</p> <ul style="list-style-type: none"> <li>- 위의 개인정보 제3자 제공에 대하여 동의를 거부할 권리가 있으며, 동의 후에도 언제든지 철회 가능합니다. 다만, 동의를 거부할 경우 연구원이 제공하는 각종 서비스에 제한을 받을 수 있습니다.</li> </ul>	
<p>위와 같이 개인정보를 제3자에게 제공하는데 동의하십니까? <input type="checkbox"/> 예 <input type="checkbox"/> 아니오</p>	
<p>■ (해당 시) 고유식별정보 처리 내역</p> <p>연구원은 원칙적으로 고유식별정보를 수집·이용하지 않습니다. 다만 시험·인증 등 연구원 서비스를 공급받는 자가 사업자가 아닌 경우, 세금계산서 발급을 목적으로 부가가치세법 제32조에 따라 주민등록번호를 수집·이용 할 수 있습니다.</p>	
<p>20 년 월 일 성명 _____ (서명 또는 인)</p>	
<p>■ 기타 안내사항</p> <ol style="list-style-type: none"> <li>1. 신청 시 필요한 구비서류 및 시험 시료, 인증에 필요한 관련 정보를 제공하지 않을 시에는 검수를 거부할 수 있으며, 추가료 시료와 서류, 수수료도 요구 될 수 있습니다.</li> <li>2. 시험 진행 과정에 시료의 분해 또는 파손되는 시험 항목이 포함되므로 한국기계전기전자시험연구원에 이에 대한 책임을 요구 할 수 없으며, 시험이 끝난 시료는 파손되거나 정상 동작이 불가능할 수 있음을 알려 드립니다.</li> <li>3. 본 제품에 대하여 시료처리에 인수를 후 7일 이내 제품 인수가 없을 경우 시험·검사 완료 시료에 대한 소유권을 포기하고, 연구원이 폐기처분 등의 시료처리를 할에 동의하고 이에 대하여 향후, 어떠한 민형사 및 행정상의 조치를 취하지 않을 것을 신청서 문서로 확인 합니다.</li> <li>4. 성격서 부분은 발행일로부터 4년 이내에만 신청 가능함을 알려 드립니다.</li> <li>5. 일반서(비KOLAS)성격서로 접수할 경우, 발행 된 성격서는 KOLAS 인정효력을 직접적으로 수해할 수 없음을 알려 드립니다.</li> <li>6. 신청 후 진행현황 및 성격서 진위여부는 KTC 온라인접수시스템(cs.ktc.kr)에서 확인하실 수 있습니다.</li> </ol>	
<p>20 년 월 일 성명 _____ (서명 또는 인)</p>	
<p>(재)한국기계전기전자시험연구원 귀중</p>	
서식 P701-01(Rev.10)	
Page 2 / 2	





⑥ 샘플제출

- (시료 제출 시 유의 사항) 시료는 2대 이상 필요하며 데이터 보호, 암호화 알고리즘 확인을 위하여 개발용 샘플 (디버깅 용) 1대, 최종 배포 샘플 1대를 필요 시험 소프트웨어와 함께 제공해야 함

구분	설명
<p>양산 샘플 (생산 완제품)</p>	 <p>최종 양산 버전 (디버깅 포트 비활성화)</p>
<p>디버깅 샘플 예시 1</p>	 <p>디버깅 포트 연결</p>
<p>디버깅 샘플 예시 2</p>	 <p>MCU 확인 연결</p>

[그림 2-2] 무선 IP CCTV 카메라 사례

## EN 18031 요구사항

- EN 18031:2024 Common security requirements for radio equipment

구분	표준명
EN 18031-1:2024	1부: 인터넷 연결 무선 장비 Part 1:Internet connected radio equipment
EN 18031-2:2024	2부: 데이터 처리 무선 장비, 즉 인터넷 연결 무선 장비, 보육용 무선 장비, 장난감용 무선 장비, 웨어러블 무선 장비 Part 2:radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
EN 18031-3:2024	3부: 가상 화폐 또는 금전적 가치를 처리하는 인터넷 연결 무선 장비 Part 3:Internet connected radio equipment processing virtual money or monetary value

- EN 18031:2024 요구사항 체크리스트

EN 18031:2024						
	구분		적용 요구사항			보안요구사항
			-1	-2	-3	
1	6.1 [ACM] 액세스 제어 메커니즘	액세스 제어 메커니즘의 적용성	6.1.1 [ACM-1]	6.1.1 [ACM-1]	6.1.1 [ACM-1]	장비는 액세스 제어 메커니즘을 사용하여 보안 자산 및 네트워크 자산에 대한 객체의 접근을 관리해야 해야 함
2		적절한 액세스 제어 메커니즘	6.1.2 [ACM-2]	6.1.2 [ACM-2]	6.1.2 [ACM-2]	ACM-1에 따라 요구되는 액세스 제어 메커니즘은 권한이 부여된 객체만 보호된 보안 자산 및 네트워크 자산에 액세스할 수 있도록 보장해야 함
3		장난감에 있는 어린이에 대한 기본 액세스 제어	-	6.1.3 [ACM-3]	-	장비가 장난감인 경우, 어린이가 외부 콘텐츠에 접근할 수 있는 각 개인정보 보호 기능과 어린이의 접근이 ACM-1에 따라 요구되는 접근 제어 메커니즘에 의해 관리된다면, 접근 제어 메커니즘은 기본적으로 개인정보 보호 기능을 통해 어린이가 외부 콘텐츠에 접근하는 것을 승인된 기관의 콘텐츠로 제한 해야 함

EN 18031:2024						
	구분	적용 요구사항			보안요구사항	
		-1	-2	-3		
4		장난감 및 보육 장비에 대한 어린이의 개인정보 자산에 대한 기본 액세스 제어	-	6.1.4 [ACM-4]	-	장비가 장난감이나 보육 장비인 경우, ACM-1에 따라 요구되는 모든 아동 개인정보 보호 기능 및 개인정보 접근 통제 메커니즘은 기본적으로 아동 본인 또는 부모/보호자 외에 장비에서 처리되는 아동 개인정보 및 개인정보에 대한 제3자의 접근을 제한해야 함
5		장난감을 가지고 있는 어린이를 위한 보호자 액세스 제어	-	6.1.5 [ACM-5]	-	장비가 장난감인 경우, 어린이가 접근할 수 있는 각 보안 및 개인정보 보호 자산에 대해 ACM-1에 따라 어린이의 접근을 관리하는데 필요한 모든 접근 제어 메커니즘은 승인된 기관에서 구성할 수 있어야 하며, 보호된 보안 및 개인정보 보호 자산에 대하여 어린이의 접근을 제한해야 함
6		장난감에 포함된 어린이의 개인정보 자산에 대한 다른 개체의 액세스를 위한 보호자 액세스 제어	-	6.1.6. [ACM-6]	-	장비가 장난감인 경우, 어린이 또는 부모나 보호자가 아닌 다른 기관이 접근할 수 있는 어린이의 개인 정보 자산이 다른 기관의 접근이 ACM-1에 따라 요구되는 접근 제어 메커니즘에 의해 관리되는 경우, 해당 접근 제어 메커니즘은 권한이 있는 기관이 구성하여 다른 기관이 관리되는 어린이의 개인정보 자산에 접근하는 것을 제한해야 함
7	6.2 [AUM] 인증 메커니즘	인증 메커니즘의 적용성 6.2.1.1[AUM-1-1]요구사항네트워크인터페이스	6.2.1 [AUM-1]	6.2.1 [AUM-1]	6.2.1 [AUM-1]	ACM-1에 따라 요구되는 액세스 제어 메커니즘은 다음을 허용하는 네트워크 인터페이스를 통해 객체의 액세스를 관리하기 위한 인증 메커니즘을 사용해야 함 : - 기밀 네트워크 기능 구성 또는 기밀 보안 매개변수 읽기, 또는 - 민감한 네트워크 기능 구성 또는 민감한 매개변수 수정, 또는 - 네트워크 기능 또는 보안 기능 사용
8		요구 사항 사용자 인터페이스	6.2.1.2 [AUM-1-2]	6.2.1.2 [AUM-1-2]	6.2.1.2 [AUM-1-2]	ACM-1에 따라 요구되는 액세스 제어 메커니즘은 다음을 허용하는 사용자 인터페이스를 통해 객체의 액세스를 관리하기 위한 인증 메커니즘을 사용해야 함 :

		EN 18031:2024			
구분		적용 요구사항			보안요구사항
		-1	-2	-3	
					<ul style="list-style-type: none"> <li>- 기밀 네트워크 기능 구성 또는 기밀 보안 매개변수 읽기, 또는</li> <li>- 민감한 네트워크 기능 구성 또는 민감한 매개변수 수정, 또는</li> <li>- 네트워크 기능 또는 보안 기능 사용</li> </ul>
9	적절한 인증 메커니즘	6.2.2 [AUM-2]	6.2.2 [AUM-2]	6.2.2 [AUM-2]	AUM-1-1(네트워크 인터페이스) 또는 AUM-1-2(사용자 인터페이스)에 따라 요구되는 인증 메커니즘은 지식, 소유 및 내재 범주 중 최소 한 가지 요소의 증거를 검토하여 법인의 주장을 검증해야 함(단일 요소 인증)
10	인증자 검증	6.2.3 [AUM-3]	6.2.3 [AUM-3]	6.2.3 [AUM-3]	AUM-1-1(네트워크 인터페이스) 또는 AUM-1-2(사용자 인터페이스)에 따라 요구되는 인증 메커니즘은 사용 운영 환경의 사용 가능한 정보에 따라 사용된 인증자의 모든 관련 속성 검증해야 함
11	인증자 변경	6.2.4 [AUM-4]	6.2.4 [AUM-4]	6.2.4 [AUM-4]	AUM-1-1또는 AUM-1-2에 따라 요구되는 인증 메커니즘은 상충되는 보안 목표 때문에 변경이 불가능한 인증자를 제외하고, 인증자를 변경할 수 있도록 허용해야 함
12	비밀번호 강도 공장기본비밀번호요구 사항	6.2.5 [AUM-5] 6.2.5.1 [AUM-5-1]	6.2.5 [AUM-5] 6.2.5.1 [AUM-5-1]	6.2.5 [AUM-5] 6.2.5.1 [AUM-5-1]	AUM-1-1 또는 AUM-1-2에 따라 요구되는 인증 메커니즘에서 공장 초기 비밀번호를 사용하는 경우 : <ul style="list-style-type: none"> <li>- 장비마다 고유해야 함, 그리고</li> <li>- 강도에 대한 모범 사례를 따라야 함, 또는 사용자가 처음 사용하기 전 또는 처음 사용할 때 변경하도록 강제해야 함</li> </ul>
13	공장 기본값이 아닌 비밀번호에 대한 요구 사항	6.2.5.2 [AUM-5-2]	6.2.5.2 [AUM-5-2]	6.2.5.2 [AUM-5-2]	AUM-1-1 또는 AUM-1-2에 따라 요구되는 인증 메커니즘에서 공장 초기 비밀번호가 아닌 비밀번호를 사용하는 경우 : <ul style="list-style-type: none"> <li>- 처음 사용하기 전 또는 처음 사용할 때, 그리고 장비가 네트워크에 논리적으로 연결되기 전에 사용자가 설정하도록 강제해야 함, 그리고</li> <li>- 액세스가 권한 있는 엔터티로 제한되는 네트워크 내의 권한 있는 엔터티가 정의되어야 함, 또는</li> <li>- 강도에 대한 모범 사례를 사용하여 장비</li> </ul>

EN 18031:2024						
	구분		적용 요구사항			보안요구사항
			-1	-2	-3	
						에서 생성하고 액세스가 권한 있는 엔터티로제한되는 네트워크 내의 권한 있는 객체에게만 전달해야 함
14		무차별 대입 공격 보호	6.2.6 [AUM-6]	6.2.6 [AUM-6]	6.2.6 [AUM-6]	AUM-1-1 또는 AUM-1-2에 따라 요구되는 인증 메커니즘은 무차별 대입 공격에 대해 탄력적이어야 함
15	6.3 [SUM] 보안 업데이트 메커니즘	업데이트 메커니즘의 적용성	6.3.1 [SUM-1]	6.3.1 [SUM-1]	6.3.1 [SUM-1]	장비는 펌웨어를 포함하여 보안 자산 및/또는 네트워크 자산에 영향을 미치는 소프트웨어를 업데이트하기 위한 업데이트 메커니즘을 하나 이상 제공해야 함
16		보안 업데이트	6.3.2 [SUM-2]	6.3.2 [SUM-2]	6.3.2 [SUM-2]	SUM-1에 따라 요구되는 각 업데이트 메커니즘은 설치 시점에 무결성과 진본성이 유효한 소프트웨어만 설치해야 함
17		자동 업데이트	6.3.3 [SUM-3]	6.3.3 [SUM-3]	6.3.3 [SUM-3]	SUM-1에 따라 요구되는 각 업데이트 메커니즘은 다음과 같이 소프트웨어를 업데이트할 수 있어야 함
18	6.4 [SSM] 보안 저장 메커니즘	보안 저장 메커니즘의 적용성	6.4.1 [SSM-1]	6.4.1 [SSM-1]	6.4.1 [SSM-1]	장비는 장비에 영구적으로 저장된 보안 자산 및 네트워크 자산을 보호하기 위해 항상 안전한 저장 메커니즘을 사용해야 함
19		보안 저장 메커니즘에 대한 적절한 무결성 보호	6.4.2 [SSM-2]	6.4.2 [SSM-2]	6.4.2 [SSM-2]	SSM-1에 따라 요구되는 각 보안 저장 메커니즘은 저장하는 보안 자산과 네트워크 자산의 무결성을 지속적으로 보호해야 함
20		보안 저장 메커니즘에 대한 적절한 기밀 보호	6.4.3 [SSM-3]	6.4.3 [SSM-3]	6.4.3 [SSM-3]	SSM-1에 따라 요구되는 각 보안 저장 메커니즘은 저장하는 기밀 보안 매개변수와 기밀 네트워크 기능 구성의 비밀을 지속적으로 보호해야 함
21	6.5 [SCM] 보안 통신 메커니즘	보안 통신메커니즘의 적용 가능성	6.5.1 [SCM-1]	6.5.1 [SCM-1]	6.5.1 [SCM-1]	장비는 네트워크 인터페이스를 통해 보안 자산 및 네트워크 자산을 다른 개체와 통신할 때 항상 안전한 통신 메커니즘을 사용해야 함

		EN 18031:2024				
		구분	적용 요구사항			보안요구사항
			-1	-2	-3	
22		보안 통신 메커니즘에 대한 적절한 무결성 및 진위성 보호	6.5.2 [SCM-2]	6.5.2 [SCM-2]	6.5.2 [SCM-2]	SCM-1에 따라 요구되는 각 보안 통신 메커니즘은 통신되는 보안 자산과 네트워크 자산의 무결성과 진위성을 보호하기 위한 모범 사례를 적용해야 함
23		보안 통신 메커니즘에 대한 적절한 기밀성 보호	6.5.3 [SCM-3]	6.5.3 [SCM-3]	6.5.3 [SCM-3]	SCM-1에 따라 요구되는 각 보안 통신 메커니즘은 통신되는 보안 자산과 네트워크 자산의 기밀성을 보호하기 위해 모범 사례를 적용해야 함
24		보안 통신 메커니즘에 대한 적절한 리플레이 보호	6.5.4 [SCM-4]	6.5.4 [SCM-4]	6.5.4 [SCM-4]	SCM-1에 따라 요구되는 각 보안 통신 메커니즘은 리플레이 공격으로부터 통신되는 보안 자산 및 네트워크 자산을 보호하기 위해 모범 사례를 적용해야 함
25	6.6 [RLM] 복원성 메커니즘	복원성 메커니즘의 적용성 및 적절성	6.6.1 [RLM-1]	-	-	장비는 네트워크 인터페이스에서 서비스 거부 (DoS) 공격의 영향을 완화하고 공격 후 정의된 상태로 돌아가기 위해 복원 메커니즘을 사용해야 함
26		로깅 메커니즘의 적용 가능성	-	6.6.1 [LGM-1]	6.6.1 [LGM-1]	장비는 개인정보 자산 및 그 보호와 관련된 내부 활동(이벤트라고 함)에 대해 로깅 메커니즘을 사용해야 함
27	6.6 [LGM] 로깅 메커니즘	로그 데이터의 영구 저장	-	6.6.2 [LGM-2]	6.6.2 [LGM-2]	LGM-1에 따라 요구되는 로깅 메커니즘은 관련 이벤트에 대한 로그 데이터를 장비의 영구 저장소에 저장해야 함
28		지속적으로 저장되는 최소 이벤트 수	-	6.6.3 [LGM-3]	6.6.3 [LGM-3]	LGM-1에 따라 요구되는 로깅 메커니즘을 통해 장비의 영구 저장소에 저장된 모든 로그 데이터는 항상 다음을 포함해야 함 - 최소 개수의 최신 이벤트 - 최신 이벤트
29		지속적으로 저장된 로그	-	6.6.4 [LGM-4]	6.6.4 [LGM-4]	LGM-1에 따라 요구되는 로깅 메커니즘을 통해 장비의 영구 저장소에 저장된 모든 로그

EN 18031:2024						
	구분		적용 요구사항			보안요구사항
			-1	-2	-3	
		데이터의 시간 관련 정보				데이터에는 다음이 포함되어야 함 - 장비에서 실시간을 사용할 수 있는 경우 타임스탬프, - 장비에서 실시간을 사용할 수 없는 경우 시간 관련 정보
30	6.7 [NMM] 네트워크 모니터링 메커니즘	네트워크 모니터링 메커니즘의 적용성 및 적절성	6.7.1 [NMM-1]	-	-	장비가 네트워크 장비인 경우, 장비는 처리하는 네트워크 간의 네트워크 트래픽에서 DoS 공격 지표를 감지할 수 있는 네트워크 모니터링 메커니즘을 제공해야 함
31	6.7 [DLM] 삭제 메커니즘	삭제 메커니즘의 응용성	-	6.7.1 [DLM-1]	-	장비는 사용자가 장비에 저장된 개인 데이터와 민감한 보안 매개변수를 삭제할 수 있도록 하는 삭제 메커니즘을 제공해야 함
32	6.8 [TCM] 트래픽 제어 메커니즘	트래픽 제어 메커니즘의 적용 가능성 및 적절한 것	6.8.1 [TCM-1]	-	-	장비가 네트워크 장비인 경우, 장비는 네트워크 트래픽 제어 메커니즘을 제공해야 함
33	6.8 [UNM] 사용자 알림 메커니즘	사용자 알림 메커니즘 응용성	-	6.8.1 [UNM-1]	-	장비는 개인 정보 보호 또는 개인정보 보호에 영향을 미치는 변경 사항을 장비 사용자에게 알리기 위한 사용자 알림 메커니즘을 제공해야 함
34		적절한 사용자 알림 정보	-	6.8.2 [UNM-2]	-	UNM-1에 따라 요구되는 사용자 알림 메커니즘을 통해 제공되는 알림 내용에는 최소한 다음이 포함되어야 함 - 변경 사항에 대한 설명; 및 - 변경 사항이 개인 정보 보호 및 개인정보 보호에 미치는 영향에 대한 설명
35	6.9 [CCK] 기밀 암호화 키	적절한 CCK	6.9.1 [CCK-1]	6.9.1 [CCK-1]	6.7.1 [CCK-1]	장비 사용 중에 장비에 사전 설치되거나 생성되는 기밀 암호화 키는 다음을 제외하고 최소 112비트의 보안 강도를 지원해야 함 : - 특정 보안 메커니즘에 의해서만 사용되는 CCK로 편차가 식별되고 ACM, AUM, SCM, SUM 또는 SSM 섹션의 조건에 따라 편차가 식별되고 근거가 되는 경우

		EN 18031:2024				
		구분	적용 요구사항			보안요구사항
			-1	-2	-3	
36		CCK 생성 메커니즘	6.9.2 [CCK-2]	6.9.2 [CCK-2]	6.7.2 [CCK-2]	기밀 암호화 키의 생성은 다음을 제외하고는 모범 사례 암호화를 준수해야 함 : - 특정 보안 메커니즘을 위한 CCK생성, ACM, AUM, SCM, SUM 또는 SSM 섹션의 조건에 따라 편차가 식별되고 근거가 되는 경우
37		사전 설치된 CCK에 대한 정적 기본값 방지	6.9.3 [CCK-3]	6.9.3 [CCK-3]	6.7.3 [CCK-3]	사전 설치된 기밀 암호화 키는 다음과 같은 경우를 제외하고는 장비마다 실질적으로 고유해야 함 : - 권한 있는 기관이 통제하는 조건에서 초기 신뢰 관계를 설정하는 데만 사용되는 CCK, 또는 - CCK는 장비의 의도된 기능에 필요한 공유 매개변수
38		공개적으로 알려진 악용 가능한 취약성이 없는 최신 소프트웨어 및 하드웨어	6.10.1 [GEC-1]	6.10.1 [GEC-1]	6.8.1 [GEC-1]	장비에는 공개적으로 알려진 악용 가능한 취약점이 포함되어서는 안 됨 이러한 취약점이 악용될 경우 보안 자산과 네트워크 자산에 영향을 미칠 수 있음
39	6.10 [GEC] 일반 장비 기능	관련 네트워크 인터페이스를 통한 서비스 노출 제한	6.10.2 [GEC-2]	6.10.2 [GEC-2]	6.8.2 [GEC-2]	공장 출하 시 기본 상태의 장비는 다음 항목만 노출되어야 함 : - 네트워크 인터페이스 - 네트워크 인터페이스를 통한 서비스를 통한 장비 설정 또는 장비의 기본 작동에 필요한 보안 자산 또는 네트워크 자산에 영향을 미침
40		옵션 서비스 및 관련 노출된 네트워크 인터페이스 구성	6.10.3 [GEC-3]	6.10.3 [GEC-3]	6.8.3 [GEC-3]	공장 기본 상태에 포함되고 보안 자산이나 네트워크 자산에 영향을 미치는 네트워크 인터페이스를 통해 노출되는 선택적 네트워크 인터페이스나 선택적 서비스는 권한이 있는 사용자가 네트워크 인터페이스나 서비스를 활성화하거나 비활성화할 수 있는 옵션이 있어야 함
41		노출된 네트워크 인터페이스 및 네트워크 인터페이스를 통한 노출된 서비스의 문서화	6.10.4 [GEC-4]	6.10.4 [GEC-4]	6.8.4 [GEC-4]	장비의 사용자 문서에는 다음에 대한 설명이 포함되어야 함 : - 노출된 모든 네트워크 인터페이스 - 네트워크 인터페이스를 통해 노출된 모든 서비스는 공장 출하 시 기본 상태로 제공

EN 18031:2024						
	구분		적용 요구사항			보안요구사항
			-1	-2	-3	
42		불필요한 외부 인터페이스 없음	6.10.5 [GEC-5]	6.10.5 [GEC-5]	6.8.5 [GEC-5]	장비는 의도된 기능에 필요한 경우에만 물리적 외부 인터페이스를 노출해야 함
43		입력 검증	6.10.6 [GEC-6]	6.10.6 [GEC-6]	6.8.6 [GEC-6]	장비는 외부 인터페이스를 통해 수신된 입력이 보안 자산 및/또는 네트워크 자산에 잠재적인 영향을 미칠 수 있는 경우 입력을 검증해야 함
44		-	-	-	6.8.7 [GEC-7]	이 조항은 의도적으로 비움
45		장비 무결성	-	-	6.8.8 [GEC-8]	재무 데이터를 처리하는 장비는 금융 자산과 보안 자산을 처리하는 소프트웨어의 각 부분에 대해 변경 불가능하거나 암호화된 인증 권한에 따라 변경 가능한 신뢰 루트를 사용하여 제조업체 또는 하청업체가 제공한 소프트웨어의 부팅 프로세스 무결성 및 진위성을 암호화 방식으로 검증해야 함
56	6.11 [CRY] 암호화	모범 사례 암호화	6.11.1 [CRY-1]	6.11.1 [CRY-1]	6.9.1 [CRY-1]	장비는 다음을 제외하고 보안 자산 또는 네트워크 자산의 보호를 위해 사용되는 암호화에 대해 모범 사례를 사용해야 함 : - 특정 보안 메커니즘에 사용되는 암호화로, 편차가 식별되고 ACM 또는 AUM 또는 SCM 또는 SUM 또는 SSM 섹션의 조건에 따라 근거가 되는 경우

**FAQ**

<b>Q1) CE RED 사이버보안 시행시기가 25년 8월인데 유예될 가능성이 있나요?</b>
CE RED는 대부분 기본적인 요구사항이며 자율적인 인증으로 표준이 조화되었기에 '25년 8월에 시행 될 것으로, 시행시기 유예는 없을 것으로 보입니다.
<b>Q2) CE RED 조화표준인 EN 18031은 제3자 적합성평가가 필수인가요?</b>
CE RED 조화표준인 EN 18031은 기업이 자율적으로 검증(자가선언)이 가능합니다. 다만, 유럽의 바이어들이 EU에서 지정한 인증기관(NB)를 통한 인증서를 요구할 수는 있습니다.
<b>Q3) EU CRA법과 CE RED의 관계는 어떻게 되나요?</b>
EU CRA법이 시행(27년말) 시 CE RED의 사이버보안 조항은 자동 폐기될 예정입니다. CRA법이 CE RED보다 보안요구사항이 더 포괄적이며, 제품의 전체 수명주기를 포함한 보안요구사항을 담고 있습니다. ※ CRA는 제품 전체 라이프 사이클 관점(취약점 공개정책, 보안패치 등 포함)이며, CE RED는 제품이 시장에 출시 시점(취약점 제거 등)의 관점으로 볼 수 있음 ※ CE RED, CRA는 일관되게 접근하는 것으로 CE RED+추가조항=CRA로 볼 수 있음
<b>Q4) CCTV를 독일에 판매하려고 합니다. 어떠한 CE 적합성 평가를 받아야 하나요?</b>
<p>✓ 어떠한 유럽 CE 지침을 적용할지 고민하기(Identifying applicable EU directives)</p> <div style="border: 1px dashed gray; padding: 5px; margin: 5px 0;"> <p>무선장비지침(RE Directive 2014/53/EU) : Wi-Fi, Bluetooth 등의 무선기능이 포함              → 기존RF 시험 이외에 IoT 기기 사이버보안 평가 의무화</p> <ul style="list-style-type: none"> <li>• 전자파 지침(EMC Directive 2014/30/EU) : EMI와 EMS 테스트 모두 필요</li> <li>• 저전압 지침(LVD 2014/35/EU) : 50V에서1000V AC 또는75V에서1500V DC 범위의 전압으로 작동하는 전원공급장치</li> <li>• 유해물질 제한 지침(RoHS) : 전자 제품에 포함된 유해물질 제한</li> <li>• 폐전기전자제품지침(WEEE Directive 2012/19/EU, 독일및EU 회원국)</li> </ul> </div> <p>✓ CE 지침에 따라 제품에 적용해야 할 필수요구사항 관련 표준을 선택하기(Selecting relevant safety standards)</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <ul style="list-style-type: none"> <li>• 전기안전(LVD) EN 62368-1(전기안전), EN 60529(외함보호등급)</li> <li>• EMC EN 55032 (멀티미디어 장비 방사), EN 55035 (내성), EN 61000-3-2/3-3</li> <li>• 무선(RF) EN 301 489-1, EN 301 489-17 (EMC 무선기기), EN 300 328 (2.4GHz), EN 301 893(5GHz)</li> <li>• 사이버보안평가기준 : EN 18031-1, EN 18031-2,</li> <li>• 유해물질(RoHS) : EN IEC 63000 (물질평가)             <ul style="list-style-type: none"> <li>- 카테고리 3: IT 및 통신기기(IT and telecommunications equipment)</li> <li>- 카테고리 9: 모니터링 및 제어 기기(Monitoring and control instruments including industrial monitoring and control instruments)</li> </ul> </li> <li>• 폐가전 지침(WEEE) 적용 및 지역내 등록 대리인 찾기</li> </ul> </div>

- 카테고리 2: 스크린, 모니터 및 100cm<sup>2</sup> 이상의 화면을 포함하는 장비 (모니터 기능이 있는 CCTV의 경우)
- 카테고리 5: 소형 장비류 (외부 치수가 50cm 이하인 소형 CCTV)
- 카테고리 6: 소형 IT 및 정보통신장비 (네트워크 기능이 있는 IP 카메라 등)

✓ 적합성평가기관(NB)을 찾고(유럽 NANDO 시스템에서 검색) 적합성평가절차 실시(Notified body assessment)

- <https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies>

✓ 제품 외부시험(적합성평가기관, 적합성평가기관 계약시험기관) 또는 자체시험실시하기(External or internal lab testing)

- NANDO 사이트의 글로벌 인증기관, 회원국 시험인증 기관확인
- NANDO 적합성 평가기관 글로벌 한국지사 문의
- 중기부 및 산업부 등록 컨설팅기관 문의
- 산업부 해외인증 지원단 문의(02-6240-4770 또는 "해외인증지원단" 검색)

✓ 기술문서 만들기(Compilation of technical documentation)

- 제품개요(A general description of the product).
- 제품 디자인,설계도, 부품 및 회로 배치도(Conceptual product design and manufacturing drawings and, where appropriate, schemes of components, circuits, etc).
- 제품디자인, 설계를 이해 할 수 있는 명세서(Descriptions and explanations needed for the understanding of those drawings and schemes.)
- 적용한 조화표준 또는 비조화 표준(A list of the harmonized and non-harmonized standards applied in full or in part during the conformity assessment process).
- 시험성적서 및 리스크평가 파일(Test reports and risk assessment file).
- 제품 필수요소에 대한 적합성평가 문서Copies of conformity documentation for critical product components.
- 사용설명서Instructions for use.
- DoC문서A copy of the Declaration of Conformity.
- 모듈A 또는B+C 또는H 절차에따른NB 적합성평가서(A copy of the EU type-examination certificate according to module A or B+C or H)

✓ DoC 선언서 작성하기(Creation of a Declaration of Conformity)

✓ 제품에 CE 표시하고, 관련 라벨 붙이기(Product marking and labelling)

**Q5) 25년 8월 1일 이전에 유럽법인 창고(또는 유통차 창고 등)에 입고되어 있는 제품의 경우도 CE RED 사이버보안을 적용해야 하나요?**

네, EU RED 지침에서 “플레이싱 온 더 마켓(placing on the market)”은 해당 제품이 최초로 EU 경제영역 (EEA) 내에 공급(또는 인도)되어 유통망에 진입하는 최초의 시점(‘making available on the market’) 을 의미 하고 있습니다.

따라서 2025년 8월 1일 이전에 이미 유럽법인 창고(또는 유통사 창고 등)에 입고되어 있는 물품은, 이미 시장에 출시된 (placed on the market) 것으로 볼 수 있으며

유럽법인 창고에 없는 상태로, 2025년 8월 1일 이후에 새롭게 한국 본사 등에서 EU로 ‘수출’되어 들어오는 물량이 있다면, 해당 물량은 ‘2025년 8월 1일 이후에 시장에 최초로 공급’ 되는 것으로 보아 사이버보안 요건을 충족해야 하는 것으로 판단됩니다.

## 참고자료

- 한국인터넷진흥원, 2023, EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점
- EU Commission, EN 18031-1:2024, Common security requirements for radio equipment. Internet connected radio equipment
- EU Commission, EN 18031-2:2024, Common security requirements for radio equipment. Radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
- EU Commission, EN 18031-3:2024, Common security requirements for radio equipment. Internet connected radio equipment processing virtual money or monetary value
- EU Commission, GUIDANCE ON THE APPLICATION OF THE HARMONISED STANDARDS SERIES EN 18031:2024 IN SUPPORT OF COMMISSION DELEGATED REGULATION 2022/30
- Directive 2014/53/EU : Radio Equipment Directive (RED) (제3조 제3항 (d), (e), (f))
- Commission Delegated Regulation (EU) 2022/30 supplements the Radio Equipment Directive (RED) by introducing cybersecurity, personal data privacy, and fraud protection requirements for certain radio equipment : 특정무선기기에 대한 사이버보안, 개인정보보호, 위변조 보호 기준
- Commission Delegated Regulation (EU) 2023/2444: Commission Delegated Regulation (EU) 2022/30 규정에 따른 무선기기 필수요구사항(사이버보안) 적용과 관련된 사항 개정 시행일 변경규정
- Guide to the Radio Equipment Directive 2014/53/EU

Part. 03  
무선기기  
(CE RED  
Cybersecurity)

## 사이버보안 : CE-RED 부록

- |                     |    |
|---------------------|----|
| 1. 제품 설명 및 세부 시험절차서 | 29 |
| 2. 하드웨어 설계도         | 35 |

 부록 1. 제품 설명 및 세부 시험절차서

## 제품 설명 및 세부 시험절차서

제출일자	xxx.xxx.xxx
신청기업	
신청표준	예) EN 18031-1
제 품 군	예) IP 카메라
제 품 명	예) OO제품 또는 OOO 앱
모 델 명	

### 1. 제품 주요 기능 설명

--

### 2. 제품 사양

구분	사 양	
신청표준	EN 18031-1	
제품구분	예) 기기, 모바일앱 등	
제품분류	예) 도어록, 월패드, 시스피커 등	
제 품 명		
모 델 명		
제품버전		
제 조 사		
하드웨어	PCB 정보	
	Main MCU	
	외부 Memory	
	Storage	
	무선통신	
	유선통신	
	외부 인터페이스	
	내부 인터페이스	
소프트웨어	소프트웨어기능	
	개발 언어	
OS 종류		
펌웨어 버전		
업데이트 방식		

#### 4. 통신모듈

##### 4.1 무선통신

구분	시스템 사양		
예) Bluetooth	표준	예) Bluetooth 4.0 BLE	
	비표준		
	암호방식 및 수준	예) 보안통신, 보안모드1/보안레벨3	
	통신모듈	모델번호	예) KISA-CC2540
		제조사	예) KTKT
펌웨어 버전		예) V2.1.3	

##### 4.2 유선통신

구분	시스템 사양	
예) Ethernet	표준	예) Ethernet : IEEE 802.3
	암호방식 및 수준	예) TLS 1.2

#### 5. 운영체제 정보

구분	시스템 사양	
예) Linux	OS명	예) CentOS
	버전	예) 7.1.4

구분	구분	시스템 사양
xx SW	소프트웨어 유형 (펌웨어, 범용 OS기반 어플리케이션, 모바일 App, 등)	예) Linux 기반 App. 5종 - 통신 드라이버 app. - 조명제어 App. - 관리 서비스 DB
	개발 플랫폼(언어)	예) C, JAVA
	적용 SDK 버전 (MCU 적용)	예) Atmel 사 제공 SDK 3.24 개발 플랫폼 : AT Studio 5.8
	3rd Party 라이브러리 사용 여부 및 세부	예) 보안통신 : OpenSSL 1.1.1e 예) 암호화 : Crypto++® Library 8.2 예) DB : SQLite .31.1
	통신 모듈 SW 버전 (적용 시)	예) HW 사양과 동일 ※ 통신모듈에서 동작하기 위해 사용되는 펌웨어, 라이브러리 등
	업데이트 방식	예) 업데이트 서버, FOTA, SD 카드 이용 업데이트

## 6. 소프트웨어 정보

## 7. 데이터 정보

### 7.1 수집데이터

수집경로	데이터
예) 온습도 센서	예) 온도 습도 데이터

### 7.2 저장데이터

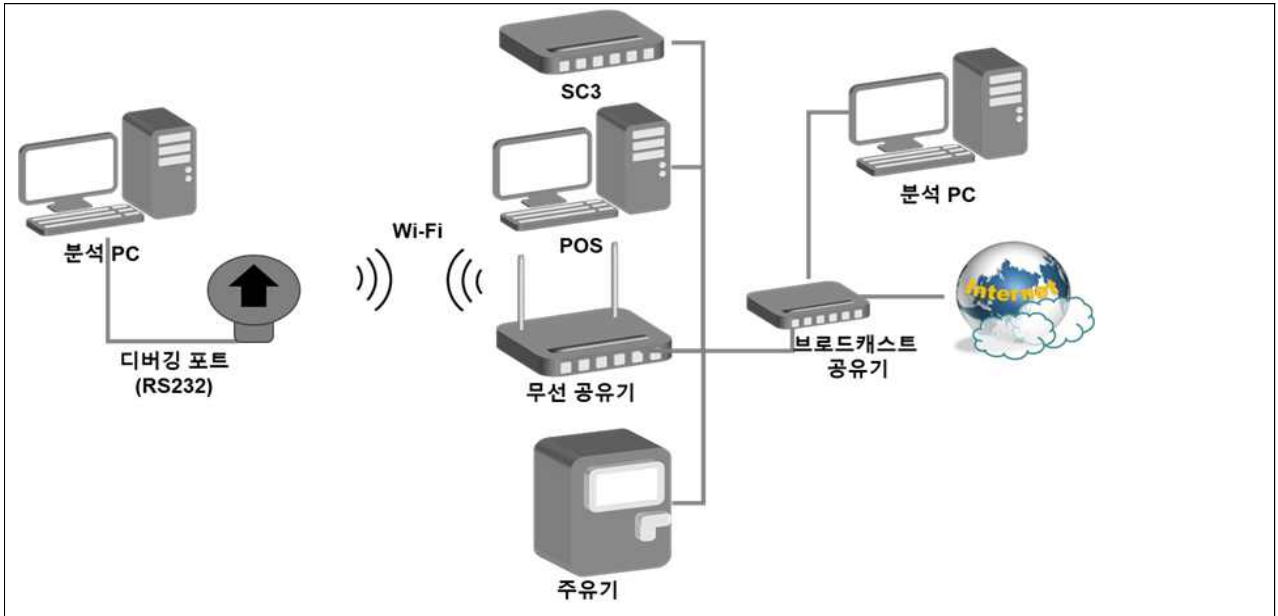
저장방법	데이터
예) 암호화 저장 (AES-128-CBC)	예) 암호키, 전화번호

### 7.3 전송데이터

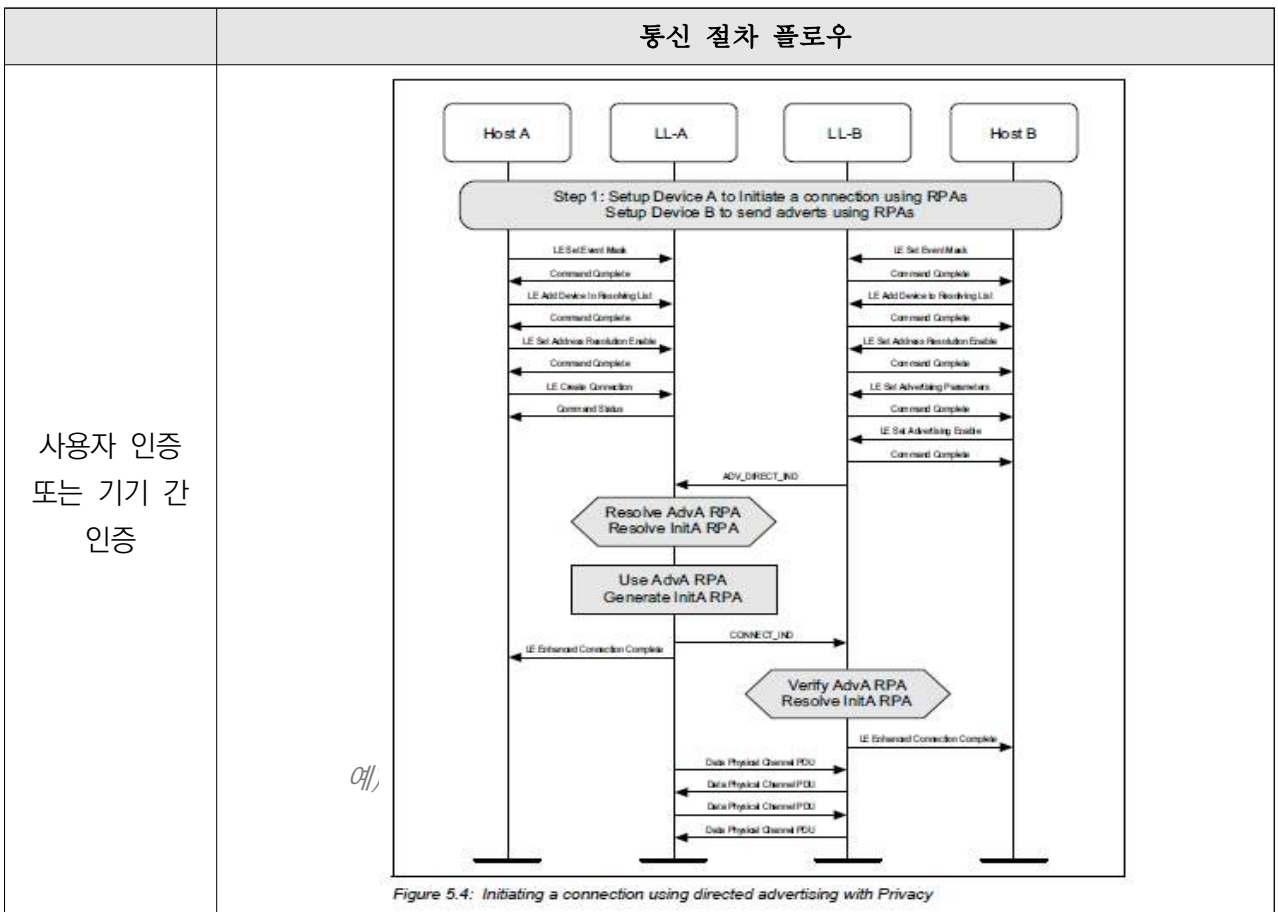
전송 구간	데이터
예) 시험제품 -> 서버	예) 영상데이터

## 8. 기기 운영환경

### 8.1 기기 운영환경 (네트워크 구성도)



### 8.2 기기 운영 절차(사용자 인증, 기기 간 인증, 데이터 전송 등 통신절차에 따른 플로우)



<p>데이터 전송</p>	<p>예)</p> <p>Figure 6.1: Sending data</p>
<p>업데이트 절차</p>	

## 부록 2. 하드웨어 설계도

# 하드웨어 설계도

제출일자	xxx.xxx.xxx
신청기업	
신청표준	예) EN 18031-1
제 품 군	예) IP 카메라
제 품 명	예) 000제품 또는 000 앱
모 델 명	

### 1. 하드웨어 사양

구분	시스템 사양
Main MCU (RF SoC 등)	예) 모델명 : STM32F103
	예) 사양 : ARM cortex M4
외부 Memory	예) Flash Memory 1GB
Storage	예) HDD 20GB
기기 외부 인터페이스	예) Micro USB : 충전용 예) SD 카드 슬롯 : 업데이트
기기 내부 인터페이스	예) JTAG : 펌웨어 다운로드 및 디버깅 예) UART : 디버깅

### 2. 기기 내부

#### 2.1 PCB 보드 상 포트 및 핀 식별

※ 시험제품 PCB 보드 상에 존재하는 모든 포트 및 핀들에 대해 식별하고 어떤 용도인지 작성이 필요

PCB Top	예)
PCB Bottom	예)

#### 2.2 내부 인터페이스 용도

포트, 핀 번호 (포트 사진)	용도 및 목적
예) 디지털 핀	예) LED 연결 핀, 통신 센서 모듈 연결 핀
예) J8	예) UART 포트 : 디버깅 로그를 확인하기 위한 포트

#### 2.3 PCB 회로 설계 사진

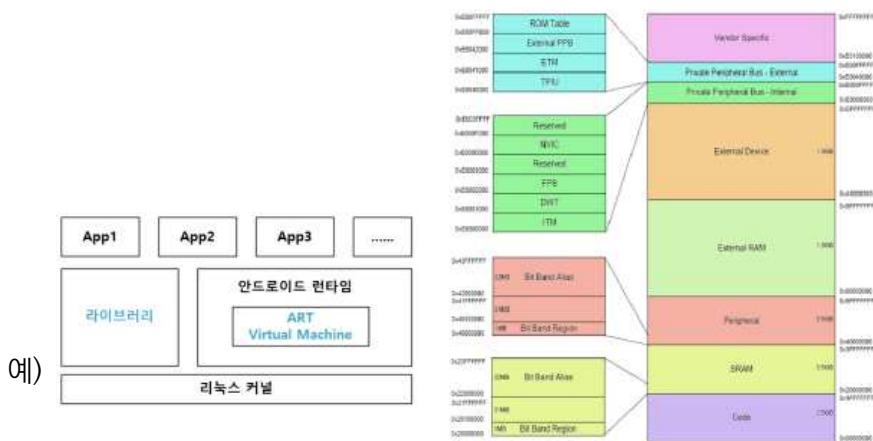
구분	〈앞면〉	〈뒷면〉
Main PCB		

### 3. 기기 외부

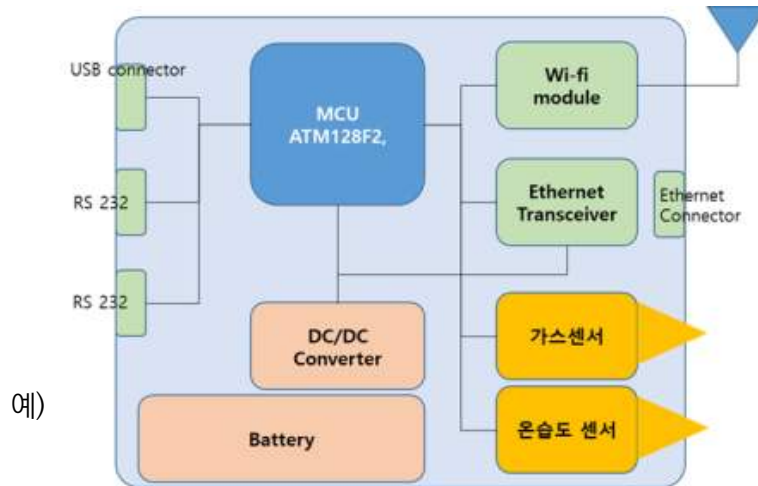
〈앞면〉	〈뒷면〉
(사진)	(사진)
〈상측면〉	〈하측면〉
(사진)	(사진)
〈좌측면〉	〈우측면〉
(사진)	(사진)

### 4. 기기 구성도

#### 4.1 기기 논리적 구성도 (소프트웨어 구현 구조 및 메모리 구조 등)



#### 4.2 기기 물리적 구성도 (하드웨어 블록 다이어그램 등)



---

## 해외인증 실무 가이드북 (05. 무선기기)

---

발행일 2025년 6월 9일

발행처 산업통상자원부 해외인증지원단

주소 06160 서울시 강남구 테헤란로 69길 5(삼성동, DT센터 3층)

전화번호 02-6240-4770

E-mail [globalcertification@ksa.or.kr](mailto:globalcertification@ksa.or.kr)

홈페이지 <https://globalcerti.kr>

감수 **KSA 한국표준협회**

작성  KTC  
한국기계전기전자시험연구원

 KISA 한국인터넷진흥원

© 수출유망품목 가이드북 (05. 무선기기)

본 저작물은 산업통상자원부 해외인증지원단 소유이므로 사전 승인 없이 무단 전재와 복제를 금합니다.

---