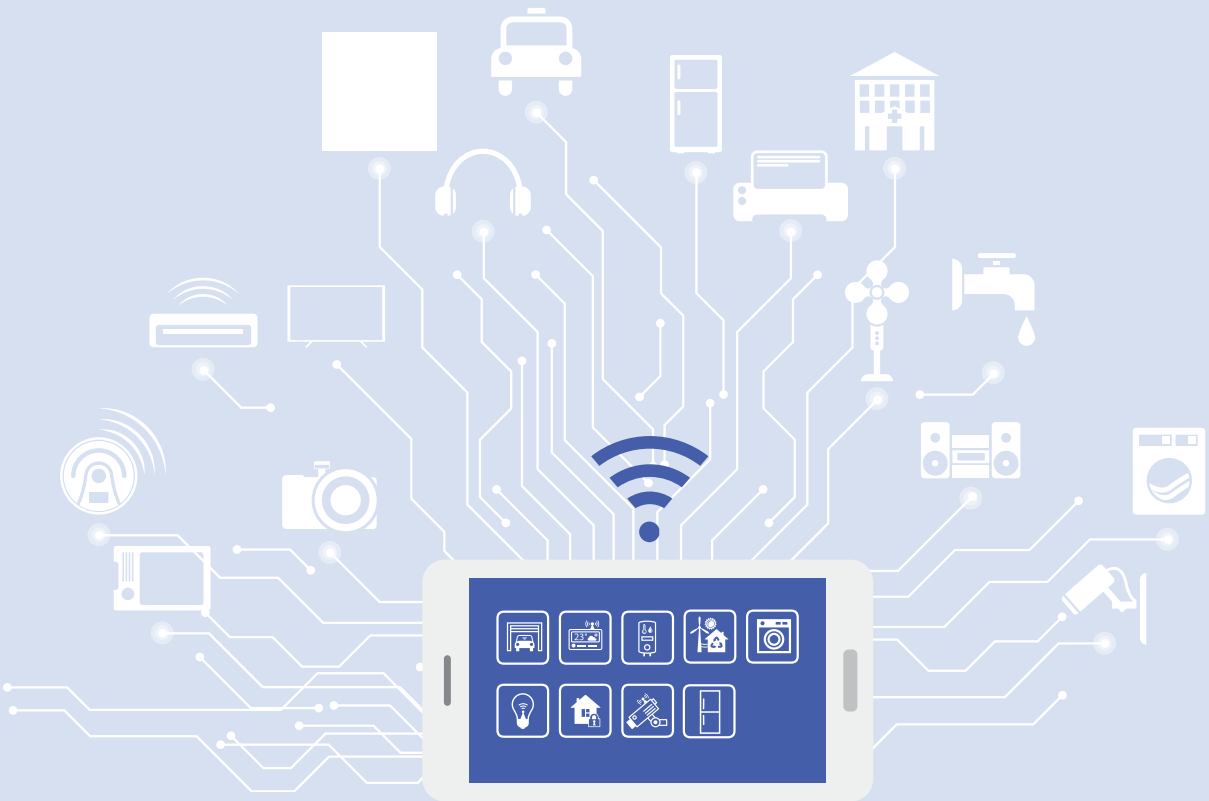
KISA 안내·해설 | KISA-GD-2019-0005

사물인터넷(IoT) 보안 시험·인증 기준 해설서

STANDARD

2019. 02.



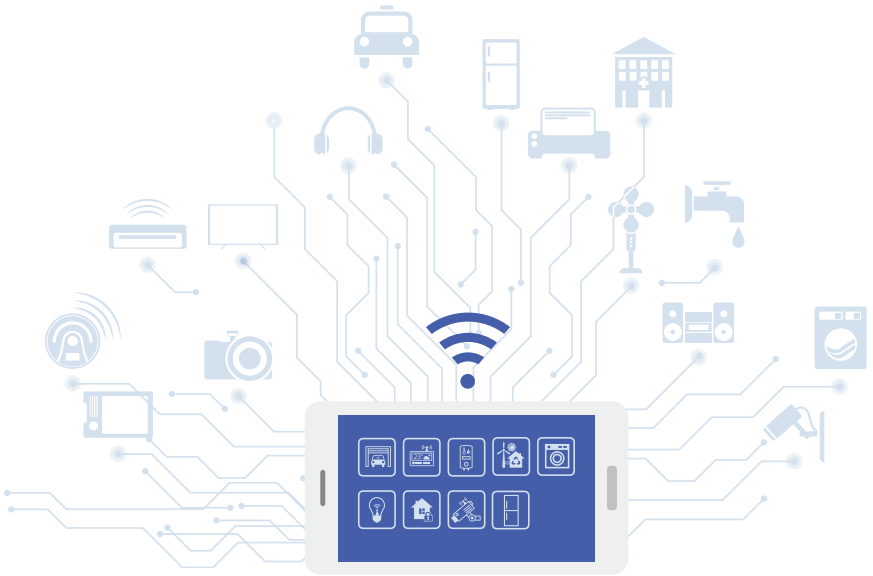
KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA 안내 · 해설 | KISA-GD-2019-0005

사물인터넷(IoT) 보안
시험·인증 기준 해설서

STANDARD

2019. 02.



KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

제1장 | 개요

제2장 | 제출물 검토 기준

제3장 | 제품 보안 기능에 대한 인증 기준

제1장

01 개요

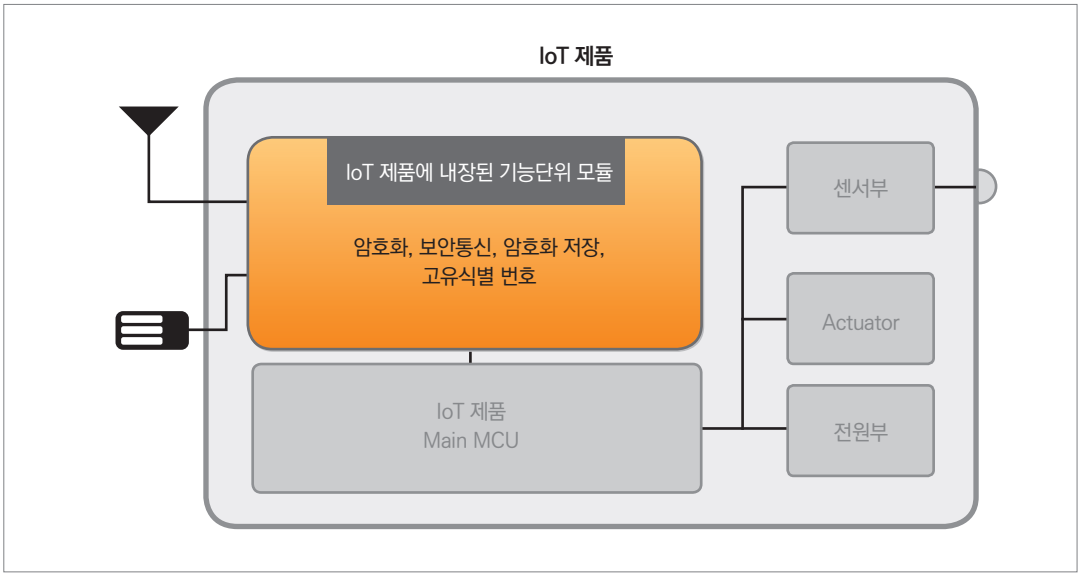
1. IoT 보안인증 대상 및 등급
2. IoT 보안인증 절차
3. IoT 보안인증 기준 구성

제1장 개요

이 장에서는 사물인터넷(Internet of Things, 이하 “IoT”라 한다) 보안인증을 위해 한국인터넷진흥원(이하“KISA”라 한다)이 인증 신청 접수부터 인증서 발급까지 보안인증 업무수행 과정의 주요절차 및 세부 활동사항을 명시한다.

1. IoT 보안인증 대상 및 등급

IoT 보안인증은 IoT 제품과 IoT 제품의 구성요소인 기능단위 모듈, IoT 제품 관리 등의 목적으로 IoT 제품과 연동하는 모바일 앱을 대상으로 한다.



☑ IoT 제품 : 네트워크 기반의 특정 서비스가 가능한 형태의 제품

☑ 모듈 : IoT 제품에 내장된 통신기능과 암호화 기능을 보유한 기능단위 모듈로, 모듈 단독으로 서비스 제공이 어려우며 다음과 같이 최소한의 보안기능이 내재되어야 함

- 통신 모듈 내 제품의 고유 식별번호 보유
- 알려진 프로토콜기반의 보안 통신 또는 암호화 통신 기능 내장
- 중요 데이터 암호화 저장
- 암호화키 암호화 저장

☑ 모바일 앱(App) : 스마트 폰 등 휴대용 단말기에서 설치되어 동작하는 소프트웨어

IoT 보안인증 등급은 IoT 제품(모듈 및 앱 포함)에 요구되는 보안기능 요구사항을 기반으로 LITE, BASIC, STANDARD와 같이 3개 등급으로 분류되며, 해당 등급의 보안기능 요구사항을 모두 만족하는 경우 해당 등급 기반의 인증서가 발급된다. 그리고, 해당 등급의 보안요구사항과 추가적인 보안기능 요구사항을 만족하는 경우 해당 등급에 '+'가 표시된다.

IoT 제품은 LITE~STANDARD 등급, 모바일 앱은 BASIC 등급, 모듈은 LITE+ 등급을 기준으로 적용한다.

<table>
<tr><th rowspan="2">등급</th><th rowspan="2">내용</th><th colspan="2">변경 이력</th><th rowspan="2">비고</th></tr>
<tr><th>前(2018년)</th><th>後(2019년)</th></tr>
<tr><td>Lite 등급</td><td>제품 보안성 유지를 위한 최소한의 조치 항목</td><td>없음</td><td>(신설) Lite 등급</td><td rowspan="2">센서 등 펌웨어 기반의 소형제품에 적합</td></tr>
<tr><td>(Lite+ 등급)</td><td>Lite 등급의 보안항목 및 추가 보안 항목</td><td>없음</td><td>(신설) Lite+ 등급</td></tr>
<tr><td>Basic 등급</td><td>해킹사례 등이 보고된 취약점 개선에 필요한 핵심조치 항목</td><td>'Lite 등급' (23개 항목)</td><td>명칭변경 (Lite → Basic)</td><td rowspan="2">저 사양 OS 탑재한 중소형 제품에 적합</td></tr>
<tr><td>(Basic+ 등급)</td><td>Basic 등급의 보안항목 및 추가 보안 항목</td><td>없음</td><td>(신설) Basic+ 등급</td></tr>
<tr><td>Standard 등급</td><td>국제적인 요구수준의 종합적 보안조치 항목</td><td>'Standard 등급' (41개 항목)</td><td>현행 유지</td><td>중대형 스마트가전 제품 등에 적합</td></tr>
</table>

2. IoT 보안인증 절차

인증을 받고자하는 신청인은 'IoT 제품 보안시험신청서'와 제출물(인증대상 IoT 제품, 보안요구사항 준수명세서, 제품기능 설명서 등)을 KISA에 제출한다. 신청서 및 제출물에 이상이 없는 경우 시험신청 접수증이 발급되며, 시험일정 협의를 거쳐 계약을 체결한다. 계약 체결 후 제출문서 검토 및 보안기능 시험을 통해 기준 적합여부를 평가하며, 필요 시 미흡한 항목에 대해 신청인에게 보완조치를 요청한다. 인증기준을 모두 만족할 경우 결과보고서 검토 후 인증서를 발급한다.

3. IoT 보안인증 기준 구성

IoT 보안인증 기준은 LITE, BASIC, STANDARD로 구분되어 있으며, 본 해설서에서는 STANDARD에 대해 기술하고 있다. STANDARD 등급의 경우, IoT 제품만 적용 가능하다.

(1) '인증' 유형

[○: 필수적용, –: 적용대상아님, 선택: 적용가능, +: 등급추가사항, N/A: 해당사항없음]

보안항목	보안인증 기준		적용 대상	
			제품	앱/모듈
사용자 인증	AU1–1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	○	–
	AU1–2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	○	–
	AU1–3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	○	–
	AU1–4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	○	–
	AU1–5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	○	–
	AU1–6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	○	–
	AU1–7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	○	–
	AU1–8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	○	–
인증정보의 안전한 사용	AU2–1	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	○	–
	AU2–2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	○	–
	AU2–3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	○	–
제품 인증	AU3–1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	○	–
	AU3–2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	○	–

(2) '암호' 유형

[○: 필수적용, –: 적용대상아님, 선택: 적용가능, +: 등급추가사항, N/A: 해당사항없음]

보안항목	보안인증 기준		적용 대상	
			제품	앱/모듈
안전한 암호 알고리즘 사용	CR1–1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	–
안전한 키 관리	CR2–1	암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.	○	–
안전한 난수 생성	CR3–1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	○	–

(3) '데이터 보호' 유형

[○: 필수적용, –: 적용대상아님, 선택: 적용가능, +: 등급추가사항, N/A: 해당사항없음]

보안항목	보안인증 기준		적용 대상	
			제품	앱/모듈
전송 데이터 보호	DP1–1	제품 간 전송되는 중요정보는 암호화해야 한다.	○	–
	DP1–2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	○	–
저장 데이터 보호	DP2–1	제품에 저장되는 중요정보는 암호화해야 한다.	○	–
	DP2–2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	○	–
정보흐름 통제	DP3–1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	○	–
안전한 세션관리	DP4–1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	○	–
	DP4–2	세션 ID는 예측할 수 없는 값이어야 한다.	○	–
개인정보 보호	DP5–1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	○	–

(4) '플랫폼 보호' 유형

[○: 필수적용, –: 적용대상아님, 선택: 적용가능, +: 등급추가사항, N/A: 해당사항없음]

보안항목	보안인증 기준		적용 대상	
			제품	앱/모듈
소프트웨어 보안	PL1–1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	○	–
	PL1–2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	○	–
	PL1–3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	○	–
	PL1–4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	○	–
안전한 업데이트	PL2–1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	○	–
	PL2–2	업데이트 실패 시 롤백 기능을 지원해야 한다.	○	–
	PL2–3	업데이트 수행 전 무결성 검사를 수행해야 한다.	○	–
보안 관리	PL3–1	불필요한 서비스는 제거하거나 비활성화해야 한다.	○	–
	PL3–2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	○	–
	PL3–3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	○	–
	PL3–4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	○	–
감사기록	PL4–1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	○	–
	PL4–2	감사기록에 대한 보호 기능을 제공해야 한다.	○	–
타임스탬프	PL5–1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	○	–

(5) '물리적 보호' 유형

[○: 필수적용, –: 적용대상아님, 선택: 적용가능, +: 등급추가사항, N/A: 해당사항없음]

보안항목	보안인증 기준		적용 대상	
			제품	앱/모듈
물리적 인터페이스 보호	PH1–1	외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.	○	–
	PH1–2	비인가자의 내부 포트 접근을 방지해야 한다.	○	–
무단조작 방어	PH2–1	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	○	–

제2장

02

제출물 검토 기준

1. 보안요구사항 준수명세서(Security Requirement Specification)
2. 제품 사용 설명서(Manual)
3. 시험서(Testing Document)

제2장 02 제출물 검토 기준

이 장에서는 IoT 보안인증을 위해 신청인이 제출한 제출물에 대한 검토 기준에 대해 설명한다.

1. 보안요구사항 준수명세서(Security Requirement Specification)

SR.1 IoT 보안인증 기준 적용 항목 식별

(1) 요구사항

- 인증대상 IoT 제품에 적용된 IoT 보안인증 기준 항목 체크(표 이용 가능)

(2) 확인사항

- 제품 보안기능 시험 및 제출 문서 검토 등을 통해 적용 기준이 정확한지 확인하고, 누락된 기준이 존재하는지 확인

SR.2 비적용 사유 식별

(1) 요구사항

- 인증대상 IoT 제품에 적용되지 않은 항목 체크(표 이용 가능)

(2) 확인사항

- 제품 보안기능 시험 및 제출 문서 검토 등을 통해 비적용 기준이 적절한지 확인하고, 적용이 필요한 경우 기준 적용 요청

2. 제품 사용 설명서(Manual)

MA.1 제품 버전 및 구성요소 식별

(1) 요구사항

- 인증대상 IoT 제품을 유일하게 식별할 수 있는 제품명과 버전 식별
- 인증대상 IoT 제품을 구성하고 있는 구성요소(하드웨어, 소프트웨어) 식별

(2) 확인사항

- 제품 버전 및 구성요소를 정확하게 식별하였는지 확인(외관, GUI/CLI 등)

MA.2-1 제품 주요 기능 설명

(1) 요구사항

- 인증대상 IoT 제품에 구현 및 제공하는 보안기능 설명

(2) 확인사항

- 제품에 구현되어 서비스를 제공하는 보안기능이 정확하게 설명되었는지 확인
- 누락된 보안기능이 있는 경우, 설명서 보완 요청

MA.2-2 제품의 모든 기능 설명

(1) 요구사항

- 인증대상 IoT 제품에 구현 및 제공하는 모든 보안기능 설명

  ※ MA.2-1(Lite) 요구사항을 포함하므로, Standard 적용시 MA.2-2 요구사항 선택 · 반영

(2) 확인사항

- 제품에 구현되어 서비스를 제공하는 모든 기능(보안기능 포함)이 정확하게 설명되었는지 확인
- 누락된 기능이 있는 경우, 설명서 보완 요청

MA.3-1 제품 보안기능과 관련된 명령어 및 사용 방법 기술

(1) 요구사항

- 안전한 IoT 제품 운영을 위한 보안기능 관련 명령어 식별
- 식별된 명령어 사용방법 및 효과 설명

(2) 확인사항

- 식별된 명령어 사용방법이 정확한지 확인
- 보안기능과 관련된 누락된 명령어가 존재하는 경우, 설명서 보완 요청

MA.3-2 제품의 모든 외부 인터페이스 식별

(1) 요구사항

- 안전한 IoT 제품 운영을 위한 보안기능 관련 명령어를 포함하여 인증대상 IoT 제품의 모든 외부 인터페이스(물리적인 입·출력 포함)를 식별

  ※ MA.3-1(Lite) 요구사항을 포함하므로, Standard 적용시 MA.3-2 요구사항 선택 · 반영

- 식별된 외부 인터페이스 사용을 위한 명령어(매개변수 포함) 사용방법 및 효과 설명

(2) 확인사항

- 모든 외부 인터페이스가 식별되었는지 확인(예, 포트스캔 등 이용)
- 식별된 외부 인터페이스 관련 명령어 사용방법이 정확한지 확인
- 누락된 인터페이스 및 명령어가 존재하는 경우, 설명서 보완 요청

MA.4 보안 관련 이벤트 목록 기술

(1) 요구사항

- 인증대상 IoT 제품 설치, 구동 등 제품 운영간 발생하는 다양한 이벤트(에러메시지 포함) 중 보안과 관련된 이벤트 목록 식별

(2) 확인사항

- 보안 관련 이벤트가 모두 식별되었는지 확인

MA.5 제품 보안을 보장하는데 필요한 제품 설정 및 환경 요구사항

(1) 요구사항

- 안전한 IoT 제품 사용 및 운영을 위한 제품 설정 및 환경 요구사항 설명

(2) 확인사항

- 사용자가 이해하기 쉽게 보안기능 관련 설정 및 환경 요구사항을 기술하고 있는지 확인

3. 시험서(Testing Document)

TE.1 제품에 구현된 보안 요구사항별 시험 수행

(1) 요구사항

- SR.1 항목에 따라 시험대상 IoT 제품에 적용된 IoT 보안인증 기준에 대해 IoT 제품의 보안기능이 정상 동작하는지 시험한 내용 기술
- 개발자에 의해 자체적으로 수행한 취약성 점검 결과 기술

(2) 확인사항

- SR.1 항목에 식별된 모든 보안 요구사항에 대한 시험이 이루어졌는지 확인
- 신청업체의 시험결과를 동일하게 수행하여 IoT 제품의 보안기능이 정상 동작하는지 확인
- 개발자에 의해 자체적으로 수행한 취약성 점검을 반복 수행하여 취약성 존재 여부 확인

제3장

제품 보안 기능에 대한 인증 기준

1. 인증(AU, Authentication)
2. 암호(CR, Cryptography)
3. 데이터 보호(DP, Data Protection)
4. 플랫폼 보호(PL, Platform Protection)
5. 물리적 보호(PH, Physical Protection)

제3장 03 제품 보안 기능에 대한 인증 기준

이 장에서는 IoT 보안 시험·인증 기준에 대해 설명한다.

1 인증(AU, Authentication)

1.1 사용자 인증

AU1-1 **처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.**

(1) 요구사항

- 초기 인증정보를 사용하지 않는 경우 인증정보를 새롭게 설정하도록 해야 하며, 초기 인증정보를 사용하는 경우 초기 인증정보 입력 후 해당 인증정보를 변경할 수 있도록 해야 함
- 위 항목은 사용자가 IoT 제품의 포장 박스를 개봉한 후, 제품 내 사용자 인증이 필요한 기능에 처음 접근을 시도할 때 수행되어야 하며, 초기 인증정보를 사용하는 경우는 해당 시점에 초기 인증정보의 입력 후 수행되어야 함
- IoT 제품의 사용자 인증이 필요한 기능을 처음 사용할 때에는 사용자가 인증정보를 설정하거나 초기 인증정보를 변경하도록 요구하는 단계를 거친 후, 해당 기능이 사용 가능하도록 해야 함
- 인증 정보 변경 시 초기 혹은 이전 인증정보와 동일한 값으로 설정할 수 없도록 해야 함

(2) 확인사항

- 새로운 IoT 제품을 시동하여 사용자 인증이 필요한 기능에 접근을 시도한 후, 인증정보를 설정하도록 요구하거나 초기 인증정보를 입력하도록 요구하는 지 확인함

- 초기 인증정보의 입력을 요구하는 경우 초기 인증 후에 이를 변경하도록 요구하는 지 확인함
- 인증정보 변경 시 초기 인증정보와 동일한 값으로 설정을 시도하여 이를 허용하는지 확인함
- 인증정보 설정 혹은 초기 인증번호를 변경하지 않고 우회하여 사용자 인증이 필요한 기능에 접근할 수 있는지 확인함

AU1-2 **관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증기능이 선행되어야 한다.**

(1) 요구사항

- IoT 제품의 설정, 사용자 계정 및 권한 관리 등의 관리서비스 접근 시 사용자에 대한 식별 및 인증을 수행해야 함
- 개인을 식별할 수 있는 영상정보와 같은 중요정보 접근 시 사용자에 대한 식별 및 인증을 수행해야 함
  ※ 중요정보 : 개인 영상정보, 인증정보(예: 비밀번호), 보안기능 설정정보 등(DP1-1 참조)
- 식별 및 인증은 아이디 및 비밀번호 메커니즘이 일반적임
- 계정에 부여된 권한에 따라 관리서비스 및 중요 정보에 대한 접근을 허용하는 경우, 일반 사용자 등 다른 권한들과 분리하여 해당 권한을 관리해야 함

(2) 확인사항

관리서비스 접근시

- IoT 제품의 관리서비스에 접근을 시도하여 인증을 요구하는지 확인함
- 계정에 부여된 권한을 통해 관리자와 일반 사용자를 구분하는 경우, 관리자 계정으로 로그인하여 관리서비스에 접근이 가능한지 확인하고 관리자 계정 로그아웃 후 일반 사용자 계정으로 로그인하여 관리서비스 접근이 거부되는지 확인함

중요정보 접근시

- IoT 제품의 중요정보에 접근을 시도하고 인증을 요구하는지 확인함
- 계정에 부여된 권한을 통해 관리자와 일반 사용자를 구분하는 경우, 중요 정보에 접근 권한이 있는계정으로 로그인하여 중요 정보에 접근이 가능한지 확인하고, 해당 계정 로그아웃 후 일반 사용자 계정(중요 정보에 접근 권한이 없는 계정)으로 로그인하여 중요 정보에 접근이 거부되는지 확인함

AU1-3 잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.

(1) 요구사항

- 잘못된 인증정보를 통한 반복된 인증 시도를 허용할 경우 무차별 대입 공격(Brute Force Attack)에 취약할 수 있으므로, IoT 제품은 잘못된 인증정보를 통한 지속적인 인증 시도에 대해 이를 적절하게 대응하는 기능을 제공해야 함
- 다음과 같은 방법으로 해당 기능을 제공할 수 있음
  a. 인증 시도 횟수를 제한하여 정해진 인증 시도 횟수 초과 시 계정 잠금 혹은 일정 시간 인증 기능을 비활성화 (인증 시도 횟수는 5회 이하, 인증 기능 비활성화 시간은 5분 이상으로 구현하도록 권고)
  b. 정해진 인증 시도 횟수 초과 시 허가되지 않은 네트워크 트래픽으로 판단하여 자동 차단 목록에 추가 (인증 시도 횟수는 5회 이하로 구현하도록 권고)
  c. 캡챠(CAPTCHA) 방식을 활용

• '잘못된 인증정보' 란?
  – IoT 제품에 저장 또는 등록되지 않은 인증정보를 말하며, 해당 정보로 인증 시도 시 실패하게 됨

(2) 확인사항

- 제출문서를 통해 잘못된 인증정보를 통한 반복된 인증 시도 시 이를 제한하는 방법을 확인하고, 제출문서에 기재된 방법이 요구사항을 대응하기에 적절한지 확인함
- 제출문서에 기재된 대로 대응 방법이 실제 구현되어 있는지 확인함

AU1-4 제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.

(1) 요구사항

- 초기 인증정보를 사용하는 IoT 제품의 경우, 제품별로 서로 다른 초기 인증정보를 가지고 있어야 함

• '초기 인증정보' 란?
  – 사용자가 처음으로 IoT 제품에 접근을 시도할 때 입력하는 정보(예, 아이디/비밀번호 등)로, 초기 인증번호 입력 후 새로운 인증정보(예, 아이디/비밀번호) 입력을 요청함

- 제조사는 IoT 제품에 불필요한 계정(예, guest 등)을 생성하여 배포하지 않아야 함

(2) 확인사항

- 동일한 제조사에서 제조된 같은 모델의 두 IoT 제품 내에 입력/설정되어 있는 초기 인증정보를 확인하여 동일여부를 확인함
- 단, AU1-1 요구사항을 만족하는 경우, AU1-4 항목은 적용된 것으로 판단한다.

AU1-5 **제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.**

(1) 요구사항

- IoT 제품에서 사용되는 사용자 계정(관리자 계정 등 모든 계정 포함)에 대해 사용자 계정 추가, 제거, 권한 부여 등의 관리를 수행할 수 있어야 함
- 역할 기반의 접근통제 모델을 사용하는 경우, IoT 제품의 모든 기능에 대해 접근권한을 명확하게 정의하고 이에 따라 권한을 부여하도록 해야 함

(2) 확인사항

- IoT 제품이 관리자 계정 외에 추가적인 사용자 계정을 지원하는 경우, 사용자 계정에 대한 생성 및 제거, 접근권한 부여가 접근권한 관리자에 의해서만 수행되는지 확인함

• '접근권한 관리자' 란?

– 사용자 계정에 접근권한을 부여할 수 있는 자로 관리자가 접근권한 관리자 역할을 함께 수행할 수 있음

AU1-6 **모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.**

(1) 요구사항

- 모든 사용자 계정은 사용자의 역할 혹은 IoT 제품의 운영 상 명확한 목적에 따라 권한이 부여되도록 해야 하며, 각 사용자 계정에 과도한 권한이 부여되지 않도록 해야 함(예, 모니터링 권한을 가진 사용자는 계정생성 권한을 보유하지 않아야 함)

• '최소 권한의 원칙(Principle of least privilege)' 이란?

– 주체의 역할 혹은 정해진 목적에 따라 필요한 정보와 리소스에만 접근하도록 설정하는 원칙

(2) 확인사항

- 제출문서에 IoT 제품에서 제공하는 모든 기능별 접근 가능한 권한이 명시되어 있는지 확인함
- 목적에 따라 혹은 사용자의 역할에 따라, 각 기능별 접근권한이 적절히 부여되었는지 확인하고, 과도하게 부여된 경우 보완 요청 필요
- IoT 제품에 대한 제출문서에 기재된 대로 각 기능과 권한이 구현되어 있는지 확인함

AU1-7 관리자 계정에 대해서는 동시 접속을 제한해야 한다.

(1) 요구사항

- 관리서비스에 동일한 관리자 계정을 이용하여 동시 접속 시 이를 제한해야 하며, 이전 접속에 대한 연결을 끊거나 새로운 접속에 대해 제한하는 기능을 제공해야 함

(2) 확인사항

- 관리자 계정으로 접속한 상태에서 동일한 관리자 계정을 통해 동시 접속을 시도하여 이를 제한하고 있는 지 확인함

AU1-8 길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.

(1) 요구사항

- IoT 제품은 사용자가 비밀번호 설정할 때 아래와 같이 길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 기능을 제공해야 함

고려사항	세부
길이	기본 9자리 이상을 권고
주기	비밀번호의 변경 주기는 6개월 이내를 권고 * 비밀번호 변경 주기가 지났을 때 사용자에게 이를 알려 위험을 인지시키고 변경하도록 유도하는 편이 좋으나, 변경의 강제성은 개발자의 선택사항임
복잡성	영문자(대 · 소) / 숫자 / 특수문자 중 3가지 이상의 규칙을 혼합한 구성으로 비밀번호가 설정되도록 권고

- 단, 납품처 혹은 특정 제품에 대한 제품 규격이 공시되어 해당 규격을 통해 비밀번호 설정 기준이 제시된 경우 이를 준수하도록 함 (예: 공공기관 납품용 CCTV의 경우 15자리 이상의 비밀번호를 요구)

(2) 확인사항

- 신청한 IoT 제품의 비밀번호 생성 규칙을 확인하고, 해당 규칙이 적절하게 적용되어 있는지 확인함

  * 참고: "패스워드 선택 및 이용안내서" 한국인터넷진흥원(https://www.boho.or.kr → 자료실 → 가이드 및 매뉴얼 → 8번 게시글)

1.2 인증정보의 안전한 사용

AU2-1 **인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.**

(1) 요구사항

- 사용자 인증 시 사용되는 인증정보는 하드코딩하거나 평문으로 저장하지 않아야 함
- 사용자 계정(및 중요 설정정보)을 파일 형태로 추출(export) 하는 기능이 있는 경우, 평문으로 생성하지 않아야 함(예, 파일 암호화 적용)
- 인증정보는 솔트를 추가하여 해쉬 함수 또는 암호 알고리즘을 사용하여 저장해야 하며, 해쉬 함수나 암호 알고리즘의 보안 강도는 112비트 이상의 보안강도를 권장함(2019년 1월 현재 기준)

  ※ SP800-131A 문서(NIST)에 따르면, 3-key TDES(보안강도 112bit)는 2023년 이후 허용되지 않으므로 기존 암호화된 데이터 복호화용으로만 사용을 권고하며, 128bit 보안강도를 가지는 암호알고리즘(예, ARIA, SEED, AES 등) 사용을 권고하고 있음

• '인증정보' 란?

  – 인증을 위해 입력해야 하는 요소(예: 비밀번호, 지문정보 등)

(2) 확인사항

- IoT 제품 내에 저장된 인증정보를 확인하여 하드코딩 되거나 평문으로 저장하고 있는지 확인

  ※ 저장 방법은 소스코드를 통해 확인

- 사용자 계정(및 중요 설정정보)을 파일 형태로 추출(export) 하는 기능이 있는 경우, 추출된 파일이 평문으로 되어 있는지 확인
- 동일한 두 개의 인증정보를 생성하여 저장된 인증정보의 형태가 다른지 확인함

AU2-2 **인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.**

(1) 요구사항

- 비밀번호가 평문으로 표시될 경우 '어깨너머 공격' 등에 취약할 수 있으므로, 비밀번호 입력 시 화면에 평문으로 노출되지 않도록 "*"등 의 기호를 사용하여 마스킹 처리해야 함

(2) 확인사항

- IoT 제품에서 제공하고 있는 모든 인증 기능에 대해 아이디/비밀번호 매커니즘을 사용하는 경우, 비밀번호가 화면에 평문으로 노출되는지 확인

AU2-3 **인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.**

(1) 요구사항

- 인증 실패의 사유 혹은 피드백 제공 시, 공격자에게 유용한 정보가 노출될 수 있으므로, 결과값을 제공하지 않아야 함

고려사항	세부
아이디 오류	공격자가 인증정보에 대한 정보를 얻을 수 있음(입력한 아이디는 등록되진 않은 아이디로 아이디를 변경하여 입력해야 함을 알 수 있음)
비밀번호 오류	공격자가 인증정보에 대한 정보를 얻을 수 있음(입력한 아이디는 등록된 아이디이며, 비밀번호를 변경하여 입력해야 함을 알 수 있음)
비밀번호 길이 오류	공격자가 비밀번호의 길이를 바꿔가며 입력함으로써 비밀번호의 길이를 쉽게 알아낼 수 있음

(2) 확인사항

- 잘못된 인증정보 입력으로 인증실패 유도 후 생성되는 알림 메시지가 인증 실패 사유 혹은 피드백을 제공하고 있는지 확인

1.3 제품 인증

AU3-1 하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.

(1) 요구사항

- IoT 제품은 유추 불가능한 고유하고 변경할 수 없는 고유 식별번호를 보유해야 함
- 고유 식별번호는 네트워크 및 스마트 디바이스 분야에서 아래와 같이 사용되고 있음

• '제품 고유 식별정보' 란?

– 수많은 제품을 식별하기 위해 제조사가 제품 제조 시 각 제품에 고유하게 부여하는 번호

구분	설명
MAC Address (Media Access Control Address)	네트워크 세그먼트의 데이터 링크 계층에서 통신을 위한 네트워크 인터페이스에 할당된 고유 식별자(48bit)
Home ID (Z-wave)	Z-wave 네트워크의 ID를 지칭함 (32bit)
IMEI (International Mobile Equipment Identity, 국제 모바일 단말기 인증번호)	스마트폰 제품의 고유번호로 사용됨 제조사가 휴대폰 출고 시 부여됨 승인코드 8자리, 모델 일련번호 6자리, 검증용 숫자 1자리(총 15자리)

(2) 확인사항

- IoT 제품 제조사의 고유 식별번호 정책을 확인하고, 해당 정책에 따라 식별번호가 주어지는지 확인함

AU3-2 **제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.**

(1) 요구사항

- 제품 간 통신을 통한 중요 정보 전송 시 혹은 서비스 접근 시 상호인증을 선행하도록 해야 하며, 상호인증 방식은 다음과 같은 방법으로 구현될 수 있음

a. 공개키 암호 방식의 개인키를 이용한 상호인증 수행

※ 제조사(또는 서비스제공자)는 IoT 제품 제조 직후 주입되는 초기 암호키(PSK, Pre-Shared Key)를 안전하게 관리해야 하며, 초기 암호키 주입 시 인가된 직원이 안전한 장소에서, 안전한 방법으로 주입할 수 있도록 관리해야 함

b. 보안속성 값(UID, Key 등), 보안칩 기반의 상호인증 수행

c. 경량통신프로토콜인 CoAP 또는 L2M2M에 DTLS 적용하여 데이터 전송

※ 제품별 고유한 인증서를 탑재하여 서버와 handshake

d. 경량통신프로토콜인 MQTT에 TLS 적용하여 데이터 전송

※ 제품별 고유한 인증서를 탑재하여 서버와 handshake

e. 사전 등록된 서버*로 접속하여 서버에서 인증코드를 발급받아 인증하는 방식 사용

※ 서버 정보(예, IP, 호스트네임 등)가 저장된 제품은 서버 정보에 대한 무결성을 보장해야 함

f. 매뉴얼 방식으로 사용자가 상호인증(A↔B) 대상 제품(A)에 로그인 하여 상호인증 대상 제품(B)을 등록하고, 등록된 제품(B)으로 전송된 인증코드를 입력하여 상호인증 수행

※ SMS, BLE, NFC 등

(2) 확인사항

- 제품 간 통신을 통해 중요 정보 전송을 시도하여, 상호인증을 수행하는지 확인함
- 제품 간 통신을 통해 제품 제어를 시도하여, 상호인증을 수행하는지 확인함
- 단, IoT 제품에서 적용되는 표준 프로토콜에서 단방향 인증만 제공하여 상호인증을 적용할 수 없는 경우, 상호인증을 단방향 인증으로 대체할 수 있음

2. 암호(CR, Cryptography)

2.1 안전한 암호 알고리즘 사용

CR1-1 중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.

(1) 요구사항

- 암호모듈 검증대상(KS X ISO/IEC 19790* 또는 FIPS140-2**) 암호 알고리즘 사용

  * ARIA, SEED, HIGHT, KCDSA, EC-KCDSA 등 (http://www.nis.go.kr/AF/1_7_3_2.do 참고)

  ** AES, Triple-DES, RSA, ECDSA 등(http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm 참고)

종류	예시	비고
대칭키 암호	ARIA, SEED, LEA, HIGH, AES, TRIPLE-DES(TRIPLE-KEY)	-
공개키 암호	RSA, ECC	보안강도 요구사항 이상 키 길이
해시	SHA2, SHA3, HMAC	-

- 비검증 대상 암호 알고리즘 지원 시 기본값 비활성화

  ※ 기본값으로 검증대상 암호 알고리즘 사용 금지
  예시) DES, double length Triple DES, MD-5, SHA-1 비활성화, XOR, checksum, Base64 금지

- 보안강도 112bit이상 암호 알고리즘 사용 권고

  ※ SP800-131A 문서(NIST)에 따르면, 3키 TDES(보안강도 112bit)는 2023년 이후 허용되지 않으므로 기존 암호화된 데이터 복호화용으로만 사용을 권고하며, 128bit 보안강도를 가지는 암호알고리즘(예, ARIA, SEED, AES 등) 사용을 권고하고 있음

보안 강도	대칭키 암호	해쉬 함수	공개키 암호				암호 알고리즘 안전성 유지기간
			인수분해	이산대수		타원곡선 암호	
				공개키	개인키		
112bit	112	112	2048	2048	224	P-224/B-233	~2030년
128bit	128	112	3072	3072	256	P-256/B-283	2030년 이후
192bit	192	192	7680	7680	384	P-384/B-409	
256bit	256	256	15360	15360	512	P-512/B-571	

- 메모리 및 저장용량 제한으로 일반적인 암호 알고리즘의 사용이 어려운 경우경량화 암호 알고리즘(HIGHT, LEA 등) 사용 가능

- KISA* 및 NIST**에서 배포한 각 표준알고리즘의 테스트 벡터값을 활용하여 구현의 정확성 검증 후 사용

  * http://seed.kisa.or.kr

  ** http://csrc.nist.gov/groups/STM/cavp

- 부채널 분석* 에 대한 대응기법이 적용된 암호 알고리즘 사용 권고

  * 암호키 사용 시 발생하는 부가정보(전력 · 전자파 량, 등)를 통해 암호키 정보를 탈취

(2) 확인사항

- KS X ISO/IEC 19790* 또는 FIPS140-2의 검증대상 알고리즘 사용 여부 확인

  * 검증필 암호모듈일 필요는 없음

- KISA* 및 NIST**에서 제시한 테스트 벡터값을 적용하여 구현 정확성 검증

  * http://seed.kisa.or.kr

  ** http://csrc.nist.gov/groups/STM/cavp

2.2 안전한 키 관리

CR2-1 **암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.**

(1) 요구사항

- 안전성이 검증된 방법(안전한 난수발생기 등)을 이용하여 암호키 생성
- 암호키 전송/저장 시 기밀성을 보장해야 함

  ※ 공개키는 반드시 기밀성을 보장할 필요는 없음

  예시) 물리적으로 안전한 H/W 영역(Secure Element, PUF등)에 보관, 암호화 키로 비밀키 등 암호화, 암호키 분산 전송/저장, 암호키 난독화 등

- 암호키 전송/저장 시 무결성을 보장해야 함(예, 해시값 생성 등)
- 암호키 사용 전 무결성 검증을 통해 변조여부 확인 후 사용
- 데이터 중요도, 노출 가능성, 노출 시 위험수준 등을 고려하여 암호키 사용기간 설정 및 암호키 갱신 수행
- 사용기간이 만료되거나 무결성이 훼손된 암호키는 즉시 파기해야 함

  예시) 암호키 저장파일, 암호키 메모리 완전삭제 등

- 암호키 파기 시 암호키 생성 관련 정보도 함께 파기해야 함

• 메모리에서 키 정보 삭제

– 암호화 저장된 정보를 복호화 할 때, 복호화키 정보가 메모리에 평문으로 로드되는 경우에는 메모리 덤프 공격으로 복호화키가 노출될 수 있으므로, 사용 후 복호화키 정보를 메모리에서 삭제해야 함

- 암호키가 저장된 메모리와 암호키가 저장된 파일은 복구할 수 없도록 영구삭제

  예시) 독일 SVITR : 7회 메모리 삭제(0x00 또는 0xFF로 6회 덮어쓴 후 0xAA로 1회 덮어쓰기 수행)
  미국 국방부 DoD 5220.22 : 메모리 3회 삭제(0x35, 0xCA, 0x97으로 3회 덮어쓰기 수행)
  사용자 지정 횟수만큼 지정값(고정값, 난수값 등)으로 덮어쓰기 수행

- 암호키 저장 공간은 물리적, 논리적 비인가 접근으로부터 보호되어야 함

  ※ 제품 내부 안전한 저장소, 폐쇄형 IC, 보안USB에 저장 등

  ※ Focus Ion beam(FIB) 등 회로에 직접적인 접근을 통해 암호키등 비밀정보를 탈취할 수 있으므로 암호키 저장 공간에 대한 물리적 보호 필요

(2) 확인사항

종류	확인 방법
암호키 생성	• 안전한 난수 알고리즘 및 생성절차에 따라 생성되는지 암호키 생성 프로세스 확인
암호키 분배	• 평문으로 전송하지 않는지 암호키 분배 프로세스 확인 • 암호키 송수신 패킷을 수집 · 분석하여 암호키 정보가 통신 패킷상에 평문으로 노출되는지 확인
암호키 사용	• 사용 전에 무결성, 기밀성 등이 보장되는지 암호키 사용 프로세스 확인
암호키 저장	• 평문저장을 하지 않는지 암호키 저장 프로세스 확인 • 메모리 정보를 수집 · 분석하여 암호키 정보가 메모리상에 평문으로 존재하는지 확인
암호키 파기	• 기준에 맞는 파기 절차를 수행하는지 암호키 파기 프로세스 확인 • 파기 후 메모리 등 잔류 여부 및 재사용 가능 여부 확인
암호키 갱신	• 암호키 사용기간이 적당한지 확인 • 암호키 사용 기간에 맞게 암호키 갱신이 정확하게 수행되는지 확인 ※ 암호키 사용기간이 제품 생명주기와 같이 하는 경우, 갱신기능 불필요

2.3 안전한 난수 생성

CR3-1 **난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.**

(1) 요구사항

- 암호모듈 검증대상(KS X ISO/IEC 19790* 또는 FIPS140-2**) 난수생성 알고리즘 사용

  * http://www.nis.go.kr/AF/1_7_3_2.do 참고

  ** http://csrc.nist.gov/groups/STM/cavp/random-number-generation.html 참고

  예시) CTR_DRBG, HASH_DRBG, HMAC_DRBG

- 국가정보원 또는 NIST에서 배포한 각 표준알고리즘의 테스트 벡터값을 활용하여 구현의 정확성 검증 후 사용

  * http://www.nis.go.kr/AF/1_7_3_5/list.do

  ** http://csrc.nist.gov/groups/STM/cavp/random-number-generation.html

(2) 확인사항

- KS X ISO/IEC 19790* 또는 FIPS140-2의 검증대상 알고리즘 사용 여부 확인
- 국가정보원 또는 NIST에서 제시한 테스트 벡터값을 적용하여 구현 정확성 검증

  * http://www.nis.go.kr/AF/1_7_3_5/list.do

  ** http://csrc.nist.gov/groups/STM/cavp/random-number-generation.html

3. 데이터 보호(DP, Data Protection)

3.1 전송 데이터 보호

DP1-1 **제품 간 전송되는 중요정보는 암호화해야 한다.**

(1) 요구사항

- 제품 간에 중요정보가 전송되는 경우, 중요한 정보가 노출되지 않도록 검증된 암호알고리즘으로 암호화하여 전송해야 하며 암호화 방법과 강도는 'CR1-1'항목을 따름

  • '중요정보'란?

  – 인증정보(예:비밀번호), 암호키(예:개인키, KEK, DEK), 개인 영상정보, 결제정보 등을 말하며, 제품의 특성에 따라 다른 정보(예: CCTV의 경우, 촬영 영상)들도 중요한 정보가 될 수 있음. 단, 제품 인증(등록)을 위한 고유 식별 정보는 중요정보에 해당하지 않으나 제품 특성에 따라 변경 가능함

- 암호키를 전송하는 경우 기밀성과 무결성을 보장해야 하며 자세한 내용은 'CR2-1'항목을 따름

(2) 확인사항

- 전송되는 중요정보 목록을 확인함
- 중요정보를 암호화한 암호알고리즘을 확인함
- 전송 방법이 무엇인지 확인함

DP1-2 알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.

(1) 요구사항

- 중요정보 암호화 전송 시 보안 프로토콜을 사용하는 경우에는 신뢰된 보안 프로토콜을 사용해야 함
- 신뢰할 수 있는 보안 프로토콜을 사용하는 경우라도, 버전, 모드, 옵션 등에 따라 취약성이 존재하므로 안전하게 설정해야 함

유형	보안 프로토콜 사용방법
Bluetooth	BLE(Bluetooth Low Energy)는 BLE 4.0/4.1를 포함하여 낮은 버전의 제품은 보안모드 1의 보안레벨 3(암호화된 인증 페어링)을 적용해야하고, BLE 4.2 제품 및 서비스는 보안모드 1의 보안레벨 4(암호화된 저전력 보안연결 인증)를 적용해야 함
Zigbee	ZigBee의 CCM 운영모드는 AES-CBC-MAC-128(보안강도 128비트 이상의 메시지인증) 또는 AES-CCM-128(보안강도 128비트 이상의 암호화 및 메시지인증)로 선택적으로 사용해야 함
Z-Wave	Z-Wave 인증을 받고 S2(시큐리티 2) 프레임워크를 적용해야 함
WiFi	WPA2 방식을 적용해야 함 ※ WPA2-PSK의 경우 초기 무선랜 인증 시 4-way 핸드셰이킹 단계의 무선 패킷수집을 통해 비밀키 유추가 가능하다는 문제가 있으므로 비밀키는 특수문자를 포함한 임의의 문자를 사용하여 최대한의 자릿수를 사용
SSL/TLS	TLS 최신 버전(예 : TLS 1.2 및 TLS 1.3 활성화 및 TLS 1.1 이하 비활성화)을 사용하고, 안전한 암호알고리즘 조합을 적용 ※ 안전한 암호 알고리즘 조합 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 등

(2) 확인사항

- 전송되는 중요한 정보 목록을 확인함
- 통신 채널 별 보안 프로토콜의 적합성을 확인함
- 중요정보를 암호화한 암호알고리즘을 확인함

3.2 저장 데이터 보호

DP2-1 **제품에 저장되는 중요정보는 암호화해야 한다.**

(1) 요구사항

- 제품에 중요정보가 저장되는 경우, 중요한 정보가 노출되지 않도록 검증된 암호알고리즘으로 암호화하여 저장해야 하며 암호화 방법과 강도는 'CR1-1'항목을 따름
- 중요정보를 암호화하기 위해 정보가 저장된 저장소를 암호화하거나 중요정보만 암호화할 수 있음
- 개인 영상, 인증정보, 중요 설정정보 등과 같은 중요정보를 파일로 추출하여 저장하는 기능이 있는 경우, 해당 파일 또는 해당 중요정보를 암호화할 수 있어야 함
- 암호키 저장 시에는 기밀성과 무결성을 보장해야 하며 자세한 내용은 'CR2-1'항목을 따름

  • 메모리에서 키 정보 삭제

  – 암호화 저장된 정보를 복호화 할 때, 복호화키 정보가 메모리에 평문으로 로드되는 경우에는 메모리 덤프 공격으로 복호화키가 노출될 수 있으므로, 사용 후 복호화키 정보를 메모리에서 삭제해야 함

- 개인정보 저장 시에는 암호화, 마스킹 등 비식별화 기능을 제공할 수 있어야 하며 자세한 내용은'DP5-1'항목을 따름
- 개인 영상정보와 같이 저장 용량이 큰 정보의 경우, 특정영역 마스킹 또는 부분 암호화 적용, 자체인코딩(BASE64 등 알려진 단순한 인코딩 제외)을 통해 중요정보 암호화 요구사항을 대체할 수 있음

(2) 확인사항

- 저장되는 중요정보 목록을 확인함
- 중요정보를 암호화한 암호알고리즘을 확인함
- 저장 방법이 무엇인지 확인함

DP2-2 **사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.**

(1) 요구사항

- 제품의 폐기 또는 업데이트, 교체 등의 요구 발생 시 중요정보를 사용할 수 없도록 삭제* 기능(예, 공장초기화, 중요정보 삭제 등)을 제공해야 함

• '완전삭제' 권고

– 완전삭제는 미국 NIST SP 800-88, 독일 VISITR, 호주 ACSI 33 표준 등을 따르기를 권고함, 단, 적용이 어려울 경우 해당 정보의 기록영역을 0x00, 랜덤한 값, 0x00 순으로 3회 이상의 덮어쓰기를 할 수 있음

(2) 확인사항

- 삭제되는 중요한 정보 목록을 확인함
- 중요한 정보를 삭제하는 방법을 확인함

3.3 정보흐름통제

DP3-1 **허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.**

(1) 요구사항

- 네트워크 기능을 보유하는 제품*의 경우, 허가되지 않은 네트워크 트래픽**을 차단하는 기능을 제공해야 함

• '네트워크 기능 보유 제품'이란?

– 홈게이트웨이, 월패드 등 네트워크 중계 역할을 담당하는 제품

• '허가되지 않은 네트워크 트래픽'이란?

– 네트워크 접근통제 정책에 등록되지 않은 제품에서 발생되는 트래픽

- 제품에서 특정 포트 오픈이 필요할 경우, 기본적으로 모든 트래픽을 거부(Deny)로 설정해야 하며, 사용자의 요구에 의해 특정 포트를 허가(allow)해야 함

※ 관리자에게만 제공되는 웹페이지 등은 미리 정의된 IP만 접근할 수 있도록 IP기반필터링 기능 제공

※ 'AU1-3' 잘못된 인증정보를 통한 반복 인증시도로 제한된 ID는 허가되지 않은 네트워크 트래픽으로 차단되며, 관리자에 의해 해제될 수 있음

- SNMP를 사용하는 제품의 경우, SNMP V3 이상의 버전을 적용해야 함

※ SNMP V3 : SNMP V1, V2와는 다르게 패스워드를 암호화하여 전송함. 무작위 대입공격에 취약하지 않도록, 디폴트명 사용 금지 및 패스워드 조합규칙 준수가 필요하며, 사용하는 암호알고리즘은 암호 유형 기준을 따름

※ SNMP V1, V2를 사용해야 하는 경우, 쓰기(write) 방지(read 권한만 제공), 디폴트 및 공개된 커뮤니티 이름 사용 금지(예, public, admin 등), 디폴트 패스워드 사용 및 평문저장 금지, MIB 데이터 내 기밀정보 사용 삭제 등의 보안 방법을 적용해야 함

(2) 확인사항

- 네트워크 트래픽 허용 및 차단 목록을 확인함
- 허가된 프로토콜 목록 및 등록사유를 확인함

3.4 안전한 세션관리

DP4-1 **세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.**

(1) 요구사항

- 세션 생성 및 연결(예, 로그인) 이후 일정 시간동안 세션을 사용하지 않는 경우, 제품은 세션을 잠그거나 세션을 종료시켜야 함

  • '일정시간'이란?

  – 제품의 특성에 따라 사용자가 설정한 세션 잠금 및 세션 종료 시간
  예) 민감한 제어 명령 처리가 포함되는 세션은 30초 이후 세션을 잠금 또는 종료, 민감하지 않은 제어 명령 처리 세션은 10분 이후 잠금 또는 종료

- 세션 잠금 및 세션이 종료된 후, 재접속 할 경우에는 재인증을 수행해야 함
- 모니터링 모드로 동작 시에는 세션 잠금 요구사항을 적용하지 않아도 무관

(2) 확인사항

- 세션 잠금 또는 세션 종료 시간(제품 특성에 적합 여부)을 확인함
- 세션 잠금·종료 후 재접속 시, 재인증 수행 여부를 확인함

DP4-2 **세션 ID는 예측할 수 없는 값이어야 한다.**

(1) 요구사항

- 해당 요구사항은 네트워크 세션 ID에 대한 내용으로 주로 HTTP 프로토콜에 적용됨
- 사용자 인증 등에 사용하는 세션 ID가 순차적으로 늘어나는 경우, 예측하기 쉽거나 재사용이 가능할 수 있으므로, 예측할 수 없도록 설정해야 함

- 안전한 난수 알고리즘을 적용하여 최소 128비트의 길이로 생성되도록 권고함
- 세션 인증시 마다 세션ID는 변경되어야 하고, 사용된 세션 ID는 재사용할 수 없도록 폐기되어야 함

(2) 확인사항

- 세션 ID 생성 방법을 확인함(세션간 연관성 확인)
- 사용중이거나 사용된 세션을 재사용하여 연결되는지 확인함

3.5 개인정보 보호

DP5-1 **제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.**

(1) 요구사항

- 제품에서 처리하는 개인정보는 중요정보로 분류되며, 저장 및 전송 시 비식별화 조치되어야 함

• '비식별화'란?

– 개인정보의 일부 또는 전부를 삭제하거나 다른 정보로 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별하기 어렵도록 하는 일련의 조치(공공정보 공유 · 개발에 따른 개인정보보호 지침, 2013.8.30.)

• '개인정보'란?

분류	개인정보 종류
고유식별정보	주민번호, 여권번호, 운전면허번호, 외국인등록번호
민감정보	사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 병력(病歷), 신체적 · 정신적 장애, 성적(性的) 취향, 유전자 검사정보, 범죄 경력정보 등 사생활을 현저하게 침해할 수 있는 정보
개인식별정보	이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 생년월일, 성별 등
개인관련정보	학력, 직업, 키, 몸무게, 혼인여부, 가족상황, 취미 등
인증정보	비밀번호, 바이오정보(지문, 홍채, 정맥 등)
신용정보/금융정보	신용정보, 신용카드번호, 계좌번호 등
의료정보	건강상태, 진료기록 등
위치정보	개인 위치정보 등
자동생성정보	IP정보, MAC주소, 사이트 방문기록, 쿠키 (cookie) 등
가공정보	통계성 정보, 가입자 성향 등
제한적 본인식별정보	회원번호, 사번, 내부용 개인식별정보 등

※ 소프트웨어 개발보안 가이드(2017.1., 행정자치부/KISA)

- 비식별화 조치 방법으로는 가명처리(Pseudonymization), 총계처리(Aggregation), 데이터 삭제(Data Reduction), 데이터 범주화(Data Suppression), 데이터 마스킹(Data Masking) 등이 있음

  ※ 개인정보 비식별 조치 가이드라인(2016) 또는 빅데이터 개인정보보호 가이드라인 해설서(2015) 참조

- 개인 영상정보의 경우, 특정영역 마스킹 또는 부분 암호화를 적용을 통해 비식별화 요구사항을 대체할 수 있음
- 개인정보를 기반으로 서비스를 제공하거나 서버에 개인정보를 저장하는 경우, 개인정보 보호법 및 동법 시행령 등 관련법규의 요구사항을 만족해야 함

(2) 확인사항

- 제품에서 처리되는 개인정보의 종류를 확인함
- 개인정보 비식별화 방법의 적절성을 확인함

4. 플랫폼 보호(PL, Platform Protection)

4.1 소프트웨어 보안

PL1-1 **보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.**

(1) 요구사항

- 보안항목을 고려하여 제품을 설계하고, 보안약점을 최소화하여 안전하게 구현하는 것을 목적으로 함
- 제품은‘소프트웨어 개발보안 가이드(행정안전부/한국인터넷진흥원)’를 참고하여 시큐어코딩을 적용해야 함

(2) 확인사항

- 개발기관에서 자체적으로 소스코드 보안약점 점검 및 보완조치한 결과가 적절한지 확인함
- 소스코드 보안약점 분석 도구를 이용하여 소프트웨어에 대한 보안약점을 점검하고, 보안약점이 존재하는지 확인함

PL1-2 **알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.**

(1) 요구사항

- 기존에 알려진 보안취약점을 내포한 프로토콜, 라이브러리, API, 패키지, 오픈소스 등을 사용하여 개발된 소프트웨어의 경우, 펌웨어, 운영체제도 보안에 취약할 수 있으므로 제품을 점검하여 보안 취약점을 제거해야 함
- 알려진 보안취약점 공개영역(예, KrCERT, CVE, NVD, Security Focus, 논문 등)을 통해 제품에 해당하는 보안취약점 존재 여부를 확인하고 제거해야 함

• 알려진 보안취약점
  – 예) XSS, SQLi, CSRF, 버퍼 오버플로우, 퍼징, 서비스 거부(DoS) 공격 등

(2) 확인사항

- 상용 또는 신뢰할 수 있는 공개용 보안취약점 점검도구를 사용하여 개발 제품의 보안 취약점 점검 및 제거 여부를 확인함

PL1-3 **소스코드 분석 방지를 위해 난독화를 적용해야 한다.**

(1) 요구사항

- 해당 요구사항은 주로 소스코드 복원이 용이한 JAVA(및 Android JAVA)로 개발된 제품에 적용될 수 있음
- 공개된 역공학 도구를 통해 중요 로직이나 키 정보 등을 추출할 수 있으므로 적절한 수준의 보호방법을 적용해야 함
- 소스 코드 난독화 도구(또는 컴파일러 옵션을 활용한 난독화)를 적용하여 메모리 보호 기법을 적용해야 함
- 패키지 구성 요소 중 중요 정보를 선별하여 난독화를 해야 함
- 펌웨어의 경우, 필수적으로 난독화 적용이 어려울 경우 선택적으로 난독화 적용을 권고함

(2) 확인사항

- 난독화 적용 방법(난독화 도구 등)을 확인함
- 제품에 대한 소스코드 복원을 시도하여 난독화 여부를 확인함

PL1-4 주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.

(1) 요구사항

- IoT 제품의 정상동작을 보장하기 위해서는 주요 설정 값 및 실행코드에 대한 무결성 검증이 수반되어야 함
- 제품 시동 시(필수), 사용자 요청 또는 주기적으로(선택) 무결성 검증 수행

• 무결성 검증 대상

– 제품 구동에 영향을 미치는 설정 값, 암호화키, 보안기능 및 제품의 중요 기능에 관련된 실행코드, 업데이트 서버 주소 등

• 무결성 검증 방법

– (예시) 위변조 시 영향이 큰 경우: HMAC, RSA서명 방식 적용
– (예시) 위변조 시 영향이 크지 않은 경우: SHA-2 family 허용
– (예시) 위변조 시 영향이 미미한 경우: SHA-1, MD-5, Checksum 허용

- 무결성 검증 실패(오류) 시 적절한 대응 절차를 수행해야 함

• 무결성 검증 실패 시 대응 절차

– 관리자에게 알림(이메일, 팝업, 경고음 등), 무결성 오류 이전 설정값 및 실행코드로 복구, 제품에서 제공하는 기능 잠금 및 서비스 중단, 공장초기화 수행 등

(2) 확인사항

- 시동 시 무결성 기능이 실행되는 지 확인함
- 사용자 요청 시 또는 주기적으로 무결성 기능이 실행되는 지 확인함
- 무결성 검증 실패 시 적절한 대응 절차를 수행하는 지 확인함

4.2 안전한 업데이트

PL2-1 업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.

(1) 요구사항

- 인가된 사용자(관리자)에 의해 업데이트가 진행되어야 함

(2) 확인사항

- 업데이트는 인가된 사용자(관리자)에 의해서만 수행될 수 있도록 업데이트 수행 전 사용자 인증 기능을 제공하는지 확인함

  • 사용자 인증 방법

  – 아이디, PIN입력, 소유자 보유 카드 태깅 등 사용 가능

PL2-2 업데이트 실패 시 롤백 기능을 지원해야 한다.

(1) 요구사항

- 업데이트를 위한 안전한 프로세스를 정의해야 함
- 업데이트 실패 시 안전한 상태로의 복구 될 수 있도록 롤백 기능을 지원해야 함

(2) 확인사항

- 기능 시험을 통해 업데이트 실패 시 롤백 기능의 존재 여부를 확인함
- 기능 시험을 통해 롤백 후, 제품이 정상 동작하는지 확인함

PL2-3 업데이트 수행 전 무결성 검사를 수행해야 한다.

(1) 요구사항

업데이트 알림 및 사용자 선택	업데이트 알림 기능을 제공하는 경우, 사용자가 업데이트를 적용할 수 있도록 해야 함 ※ 단, 사용자가 업데이트 알림을 받고 업데이트를 적용하지 않을 수 있음
업데이트 서버 주소 무결성	업데이트 서버 주소는 주요 설정 값에 포함되므로, 'PL1–4'항목에 따라 서버 주소 변경여부가 확인되어야 함
업데이트 파일 무결성	업데이트 파일 다운로드 후, 업데이트 파일 설치 전 업데이트 파일에 대한 무결성 검증을 수행하여 무결성에 오류가 발생한 경우 설치를 금지해야 함

(2) 확인사항

- 업데이트 알림 기능 제공 여부 및 사용자에 의해 업데이트를 적용할 수 있는지 확인함
- 업데이트 서버 주소를 포함한 주요 설정 값에 대한 무결성 검사가 수행되는지 확인함
- 업데이트 수행 전 업데이트 파일에 대한 무결성 검사를 수행하는지 확인하고, 무결성 오류 시에도 업데이트가 진행되는지 확인함

4.3 보안 관리

PL3-1 **불필요한 서비스는 제거하거나 비활성화해야 한다.**

(1) 요구사항

- 제품에서 제공하는 필요 서비스를 정의해야함
- 불필요한 서비스(예, Telnet, FTP, UPnP, SNMP)는 비활성화 해야함
- 외부 접속을 허용할 경우 접근 IP 제한, 접근 비밀번호 설정 등의 추가적인 보안 조치를 수행해야 함
- 인가된 사용자에 의해서만 서비스 활성화 기능이 수행되어야 함

• '인가된 사용자' 란?

– 관리서비스 접근이 허용된 사용자('AU1-5' 항목 참조)

(2) 확인사항

- 제품에서 제공하는 서비스(포트) 및 목적, 용도 등을 확인함
- 포트 스캔 등을 통해 불필요한 서비스가 존재하는지 확인함
- 외부 접속 포트 사용 시, 해당 포트 접근을 위한 추가적인 보안 조치를 확인함
- 인가된 사용자에 의해 서비스 활성화 가능 여부를 확인함

PL3-2 **원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.**

(1) 요구사항

- 관리자는 원격관리를 신뢰할 수 있는 환경에서 수행해야 함

• '원격관리' 란?

– 원격 조종자로 하여금 해당 시스템에 물리적으로 접근권한이 있는 것처럼 시스템을 제어하게 해주는 소프트웨어 및 프로그래밍 모음 등을 모두 일컬음

• '신뢰할 수 있는 환경' 이란?

– 내부망, 사전 지정된 원격 관리용 IP, 안전한 채널(TLS, SSH등)이 적용된 시스템 등

(2) 확인사항

- 지정되지 않은 IP로 접근 또는 안전하지 않은 채널로 접근 시, 원격관리 서비스가 가능한지 확인함

PL3-3 **3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.**

(1) 요구사항

- 개발 시 사용되는 3rd party 라이브러리 및 모듈은 알려진 취약점이나 결함이 존재하지 않는 최신 버전을 사용하여야 함
- 3rd Party 소프트웨어는 최신 보안패치가 적용된 버전을 사용하여야 하며, 사용자(관리자) 매뉴얼에 안전한 운영환경을 제공해야 함

(2) 확인사항

- 소프트웨어 정보 홈페이지를 통해 최신 소프트웨어 버전의 사용 여부를 확인함

• 확인방법

– 어플리케이션 및 Bootloader, Busybox, OpenSSL, OpenSSH, Linux를 포함한 소프트웨어에 대한 보안 취약점 점검

- 시험대상 제품에 적용된 3rd party 소프트웨어(라이브러리)가 IoT 보안인증기간이 변경되는 경우, 신청업체로부터 패치 일정을 받아서 해당 요구사항을 처리할 수 있음

※ 단, 신청업체가 제출한 패치 일정을 준수하지 않는 경우 기 발급된 인증서 취소 사유가 될 수 있음

PL3-4 하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.

(1) 요구사항

- IoT 제품 시동 시(전원 인가 시) 또는 시동 후 주요 하드웨어 및 소프트웨어에 대한 오류를 탐지할 수 있는 자체검사 기능을 제공해야 함
- 오류 탐지 시 관리자에게 오류에 대한 내용을 알릴 수 있도록 권고함

• 오류 알림 방법
  – 이메일 전송, SMS 발송, LED 점멸, 경고음 등

(2) 확인사항

- 하드웨어 및 소프트웨어 자체 시험 기능은 개발업체에서 제공한 문서 내용을 기반으로 확인함
- 하드웨어 및 소프트웨어의 오류를 발생시킨 후 자체 시험 기능이 오류를 탐지하는지 확인함
- 오류 탐지 시 사용자(관리자)에게 알림기능을 제공하는지 확인함

4.4 감사기록

PL4-1 보안과 관련된 이벤트는 감사기록을 생성해야 한다.

(1) 요구사항

- 감사기록 생성 기능을 구현해야 하며, 제품의 이상행위를 탐지 및 추적할 수 있어야 함
- 감사기록은 사건발생 일시, 유형, 사건을 발생시킨 주체의 신원, 작업내역 및 결과(성공/실패) 등을 고려하도록 권고함

• 감사기록 대상
  – 사용자 로그인 성공/실패, 제품설정 변경 내역, 기능 수행내역(보안기능 포함) 등

• 감사기록 제외 대상
  – 비밀번호, 암호키 등 민감한 정보 등

- 인가된 사용자(관리자)가 해석 할 수 있도록 감사기록을 생성하고, 검토할 수 있는 기능을 제공해야 함
- 감사기록(로그)을 제품에 저장하지 않고 외부 서버 또는 기타 저장장치로 전송할 수 있음

(2) 확인사항

- 보안관련 이벤트를 수행한 후 감사기록 로그를 확인함
- 외부 서버로 감시기록(로그)을 전송하는 경우 정상적으로 전송 및 저장되는지 확인함

PL4-2 **감사기록에 대한 보호 기능을 제공해야 한다.**

(1) 요구사항

- 감사기록의 유실 및 비인가된 변경(삭제 포함)에 대비하기 위해 감사기록을 보호하는 장치를 마련해야 함

  • 감사기록 보호하는 장치

  – 저장 공간이 일정 이상 채워지면 오래된 감사기록 덮어쓰기 또는 인가된 사용자에게 경고를 통해 저장 공간을 확보할 수 있는 기능(예, 감사기록 백업 등) 제공

- 비인가된 삭제 또는 변경이 발생하지 않도록 보호해야 함(예, 감사기록에 대한 삭제 및 변경 기능 및 UI를 제공하지 않음)
- 클라우드 등 안전성이 검증된 외부저장소를 사용하여 감사기록 저장 가능

(2) 확인사항

- 감사기록 보호 기능 확인
- 감사기록 삭제 기능 존재 여부 확인

4.5 타임스탬프

PL5-1 신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.

(1) 요구사항

- 신뢰할 수 있는 타임스탬프를 사용해서 보안 관련 사건 이벤트를 정확하게 기록해야 함
  (예, NTP 등)
- 공인된 시간 소스와 동기화를 지원해야 하며 하루에 1초 이내의 정확성을 가져야 함
  ※ 외부 NTP 서버와 연결이 어려운 경우, 운영체제 시간을 기반으로 적용할 수 있으며 RTC는 일정시간으로 사용을 제한하고 주기적으로 업데이트를 수행해야 함
- 감사기록 생성 시 신뢰할 수 있는 타임스탬프가 제공되어야 함

(2) 확인사항

- 제품의 현재 시간을 임의로 변경 및 재부팅 후 정확한 시간으로 복귀하는지 확인함

5. 물리적 보호(PH, Physical Protection)

5.1 물리적 인터페이스 보호

PH1-1 불필요한 외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.

(1) 요구사항

- 외부에 노출된 모든 인터페이스 종류와 기능은 제품 사용 설명서에 기술되어야 함
- 불필요한 외부 인터페이스에 대하여 비활성화 대책이 구현되어야 하며 제품 사용 설명서에 기술해야 함
- 필요 시, 비인가된 접근 방지를 위해 접근통제 기능을 제공해야 하며, 제품 사용 설명서에 기술해야 함

- 외부 인터페이스의 예
  - USB, Ethernet, 시리얼 통신 인터페이스(RS232, RS485 등), SD Card Slot 등

(2) 확인사항

- 외부에 노출된 인터페이스의 필요 여부는 제품 사용 설명서 또는 제조사가 제공하는 문서로 확인함
- 필요한 외부 인터페이스라도 비인가된 접속을 방지하기 위한 접근통제 기능이 적용되었는지 확인
- 불필요한 외부 인터페이스가 존재할 경우 제거하거나 비활성화 가능여부를 확인함

PH1-2 비인가자의 내부 포트 접근을 방지해야 한다.

(1) 요구사항

- 모든 내부 인터페이스 종류와 기능은 제품 사용 설명서에 기술되어야 함
- 불필요한 내부 인터페이스에 대하여 제거 또는 비활성화 대책이 구현되어야 하며 제품 사용 설명서에 기술해야 함
- 필요 시, 비인가된 접근 방지를 위해 접근통제 기능을 제공해야 하며, 제품 사용 설명서에 기술해야 함

- 내부 인터페이스의 예
  - JTAG, UART, USB, SPI, I2C, SDIO, Ethernet 등 표준/비표준 통신 인터페이스

(2) 확인사항

- 제조사에서 제출한 제품 사용 설명서를 기반으로 내부 인터페이스 유무를 확인함
- 제거가 불가능한 인터페이스는 비활성화 여부를 확인하고, 사후 관리 및 디버깅에 필요한 인터페이스는 접근통제 기능이 적용되어 있는지 확인함

5.2 무단조작 방어

PH2-1 비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.

(1) 요구사항

- 무단 조작 접근방지 및 검출 방법으로 아래와 같은 기능을 구현해야 함

• 접근 방지/검출 방법의 강도는 제품의 성능과 저장된 데이터에 따라서 조절할 수 있고 대응기술도 구현가능
※ 높은 강도의 외부 접근 방지 및 검출 방법 구현 시 제품 인터페이스 명세서에 기재

구분	설명
접근방지 방법	자체 제작된 조립 스크류(나사) 적용 (예. 별나사, 팔각나사 등), 제품 내부 몰딩, 주요 IC CAN 적용, IC 레이저마킹 삭제, 주요 통신선 내층 설계 등
접근검출 방법	파괴테입, Tamper Proofing 기능 구현
대응기술	– 케이스 내부에 그물망형상의 센서 또는 스위치를 구현 – 케이스의 변형 또는 열림을 검출 후 관리자 알람 또는 메모리 전체(민감 정보) 초기화

- 접근 방지/검출 방법은 제품의 성능과 저장된 데이터의 중요도에 따라 강도조절 가능함

(2) 확인사항

- 무단 조작 접근 방지기능과 접근 검출 방법이 구현되어 있는지 확인함

부록

유형별 IoT 보안인증 기준

IoT 보안인증 등급별 적용 기준 및 대상

등급	내용	적용 대상 유형				
		IoT 제품	앱	모듈	홈IoT 기기	홈IoT앱
Lite 등급 (10개 항목)	제품 보안성 유지를 위한 최소한의 조치 항목	○	–	–	○	○
Lite+ 등급 (10개+α 항목)	Lite 등급의 보안항목 및 추가 보안 항목	○	–	○	○	○
Basic 등급 (23개 항목)	해킹사례 등이 보고된 취약점 개선에 필요한 핵심조치 항목	○	○	–	–	–
Basic+ 등급 (23개+α 항목)	Basic 등급의 보안항목 및 추가 보안 항목	○	○	–	–	–
Standard 등급 (41개 항목)	국제적인 요구수준의 종합적 보안조치 항목	○	–	–	–	–

IoT 제품 대상 IoT 보안인증 적용 기준

보안항목		보안인증 기준		L	B	S
인증	사용자 인증	AU1–1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	○	○	○
		AU1–2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	○	○	○
		AU1–3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	–	○	○
		AU1–4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	–	–	○
		AU1–5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	–	–	○
		AU1–6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	–	–	○
		AU1–7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	–	–	○
		AU1–8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	–	–	○
	인증정보의 안전한 사용	AU2–1	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	–	○	○
		AU2–2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	–	○	○
		AU2–3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	–	○	○
	제품 인증	AU3–1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	○	○	○
		AU3–2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	–	–	○

보안항목		보안인증 기준		L	B	S
암호	안전한 암호 알고리즘 사용	CR1–1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	○	○
	안전한 키 관리	CR2–1	암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.	–	–	○
	안전한 난수 생성	CR3–1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	–	–	○
데이터 보호	전송 데이터 보호	DP1–1	제품 간 전송되는 중요정보는 암호화해야 한다.	○	○	○
		DP1–2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	–	○	○
	저장 데이터 보호	DP2–1	제품에 저장되는 중요정보는 암호화해야 한다.	○	○	○
		DP2–2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	–	–	○
	정보흐름통제	DP3–1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	–	–	○
	안전한 세션 관리	DP4–1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	–	○	○
		DP4–2	세션 ID는 예측할 수 없는 값이어야 한다.	–	–	○
	개인정보 보호	DP5–1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	–	–	○
플랫폼 보호	소프트웨어 보안	PL1–1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	–	○	○
		PL1–2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	○	○	○
		PL1–3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	○	○	○
		PL1–4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	–	–	○
	안전한 업데이트	PL2–1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	○	○	○
		PL2–2	업데이트 실패 시 롤백 기능을 지원해야 한다.	–	○	○
		PL2–3	업데이트 수행 전 무결성을 검사해야 한다.	–	–	○
	보안 관리	PL3–1	불필요한 서비스는 제거하거나 비활성화해야 한다.	–	○	○
		PL3–2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	–	○	○
		PL3–3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	–	○	○
		PL3–4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	–	–	○
	감사기록	PL4–1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	–	○	○
		PL4–2	감사기록에 대한 보호 기능을 제공해야 한다.	–	–	○
	타임스탬프	PL5–1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	–	–	○
물리적 보호	물리적 인터페이스 보호	PH1–1	불필요한 외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.	–	○	○
		PH1–2	비인가자의 내부 포트 접근을 방지해야 한다.	○	○	○
	무단조작 방어	PH2–1	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	–	–	○

모바일 앱 대상 IoT 보안인증 적용 기준

보안항목		보안인증 기준		L	B	S
인증	사용자 인증	AU1-1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	–	○	–
		AU1-2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	–	○	–
		AU1-3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	–	○	–
		AU1-4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	–	–	–
		AU1-5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	–	–	–
		AU1-6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	–	–	–
		AU1-7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	–	–	–
		AU1-8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	–	–	–
	인증정보의 안전한 사용	AU2-1	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	–	○	–
		AU2-2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	–	○	–
		AU2-3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	–	○	–
	제품 인증	AU3-1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	–	N/A	–
		AU3-2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	–	–	–
암호	안전한 암호 알고리즘 사용	CR1-1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	–	○	–
	안전한 키 관리	CR2-1	암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.	–	–	–
	안전한 난수 생성	CR3-1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	–	–	–
데이터 보호	전송 데이터 보호	DP1-1	제품 간 전송되는 중요정보는 암호화해야 한다.	–	○	–
		DP1-2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	–	○	–

보안항목		보안인증 기준		L	B	S
데이터 보호	저장 데이터 보호	DP2-1	제품에 저장되는 중요정보는 암호화해야 한다.	–	○	–
		DP2-2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	–	–	–
	정보흐름통제	DP3-1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	–	–	–
	안전한 세션 관리	DP4-1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	–	○	–
		DP4-2	세션 ID는 예측할 수 없는 값이어야 한다.	–	–	–
	개인정보 보호	DP5-1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	–	–	–
플랫폼 보호	소프트웨어 보안	PL1-1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	–	○	–
		PL1-2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	–	○	–
		PL1-3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	–	○	–
		PL1-4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	–	–	–
	안전한 업데이트	PL2-1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	–	○	–
		PL2-2	업데이트 실패 시 롤백 기능을 지원해야 한다.	–	N/A	–
		PL2-3	업데이트 수행 전 무결성을 검사해야 한다.	–	–	–
	보안 관리	PL3-1	불필요한 서비스는 제거하거나 비활성화해야 한다.	–	○	–
		PL3-2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	–	선택	–
		PL3-3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	–	○	–
		PL3-4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	–	–	–
	감사기록	PL4-1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	–	선택	–
		PL4-2	감사기록에 대한 보호 기능을 제공해야 한다.	–	–	–
	타임스탬프	PL5-1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	–	–	–
물리적 보호	물리적 인터페이스 보호	PH1-1	불필요한 외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.	–	N/A	–
		PH1-2	비인가자의 내부 포트 접근을 방지해야 한다.	–	N/A	–
	무단조작 방어	PH2-1	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	–	–	–

모듈 대상 IoT 보안인증 적용 기준

보안항목		보안인증 기준		L	B	S
인증	사용자 인증	AU1-1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	선택	–	–
		AU1-2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	선택	–	–
		AU1-3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	–	–	–
		AU1-4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	–	–	–
		AU1-5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	–	–	–
		AU1-6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	–	–	–
		AU1-7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	–	–	–
		AU1-8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	–	–	–
	인증정보의 안전한 사용	AU2-1	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	–	–	–
		AU2-2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	–	–	–
		AU2-3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	–	–	–
	제품 인증	AU3-1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	○	–	–
		AU3-2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	–	–	–
암호	안전한 암호 알고리즘 사용	CR1-1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	–	–
	안전한 키 관리	CR2-1	암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.	+	–	–
	안전한 난수 생성	CR3-1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	+	–	–
데이터 보호	전송 데이터 보호	DP1-1	제품 간 전송되는 중요정보는 암호화해야 한다.	○	–	–
		DP1-2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	+	–	–
	저장 데이터 보호	DP2-1	제품에 저장되는 중요정보는 암호화해야 한다.	○	–	–
		DP2-2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	+	–	–

보안항목		보안인증 기준		L	B	S
데이터 보호	정보흐름 통제	DP3–1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	–	–	–
	안전한 세션 관리	DP4–1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	–	–	–
		DP4–2	세션 ID는 예측할 수 없는 값이어야 한다.	–	–	–
	개인정보 보호	DP5–1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	–	–	–
플랫폼 보호	소프트웨어 보안	PL1–1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	–	–	–
		PL1–2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	○	–	–
		PL1–3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	○	–	–
		PL1–4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	–	–	–
	안전한 업데이트	PL2–1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	○	–	–
		PL2–2	업데이트 실패 시 롤백 기능을 지원해야 한다.	–	–	–
		PL2–3	업데이트 수행 전 무결성을 검사해야 한다.	–	–	–
	보안 관리	PL3–1	불필요한 서비스는 제거하거나 비활성화해야 한다.	–	–	–
		PL3–2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	–	–	–
		PL3–3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	+	–	–
		PL3–4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	–	–	–
	감사기록	PL4–1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	–	–	–
		PL4–2	감사기록에 대한 보호 기능을 제공해야 한다.	–	–	–
	타임스탬프	PL5–1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	–	–	–
물리적 보호	물리적 인터페이스 보호	PH1–1	불필요한 외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.	–	–	–
		PH1–2	비인가자의 내부 포트 접근을 방지해야 한다.	선택	–	–
	무단조작 방어	PH2–1	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	–	–	–

홈IoT기기 대상 IoT 보안인증 적용 기준

보안항목		보안인증 기준		L	B	S
인증	사용자 인증	AU1–1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	선택	–	–
		AU1–2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	○	–	–
		AU1–3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	–	–	–
		AU1–4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	–	–	–
		AU1–5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	–	–	–
		AU1–6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	–	–	–
		AU1–7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	–	–	–
		AU1–8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	–	–	–
	인증정보의 안전한 사용	AU2–1	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	–	–	–
		AU2–2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	–	–	–
		AU2–3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	–	–	–
	제품 인증	AU3–1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	○	–	–
		AU3–2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	–	–	–
암호	안전한 암호 알고리즘 사용	CR1–1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	–	–
	안전한 키 관리	CR2–1	암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.	–	–	–
	안전한 난수 생성	CR3–1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	–	–	–
데이터 보호	전송 데이터 보호	DP1–1	제품 간 전송되는 중요정보는 암호화해야 한다.	○	–	–
		DP1–2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	–	–	–

보안항목		보안인증 기준		L	B	S
데이터 보호	저장 데이터 보호	DP2–1	제품에 저장되는 중요정보는 암호화해야 한다.	○	–	–
		DP2–2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	–	–	–
	정보흐름통제	DP3–1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	–	–	–
	안전한 세션 관리	DP4–1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	–	–	–
		DP4–2	세션 ID는 예측할 수 없는 값이어야 한다.	–	–	–
	개인정보 보호	DP5–1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	–	–	–
플랫폼 보호	소프트웨어 보안	PL1–1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	–	–	–
		PL1–2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	선택	–	–
		PL1–3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	선택	–	–
		PL1–4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	–	–	–
	안전한 업데이트	PL2–1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	○	–	–
		PL2–2	업데이트 실패 시 롤백 기능을 지원해야 한다.	–	–	–
		PL2–3	업데이트 수행 전 무결성을 검사해야 한다.	–	–	–
	보안 관리	PL3–1	불필요한 서비스는 제거하거나 비활성화해야 한다.	–	–	–
		PL3–2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	–	–	–
		PL3–3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	–	–	–
		PL3–4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	–	–	–
	감사기록	PL4–1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	–	–	–
		PL4–2	감사기록에 대한 보호 기능을 제공해야 한다.	–	–	–
	타임스탬프	PL5–1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	–	–	–
물리적 보호	물리적 인터페이스 보호	PH1–1	불필요한 외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.	–	–	–
		PH1–2	비인가자의 내부 포트 접근을 방지해야 한다.	○	–	–
	무단조작 방어	PH2–1	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	–	–	–

홈앱 대상 IoT 보안인증 적용 기준

보안항목		보안인증 기준		L	B	S
인증	사용자 인증	AU1–1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	선택	–	–
		AU1–2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	○	–	–
		AU1–3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	–	–	–
		AU1–4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	–	–	–
		AU1–5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	–	–	–
		AU1–6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	–	–	–
		AU1–7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	–	–	–
		AU1–8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	–	–	–
	인증정보의 안전한 사용	AU2–1	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	–	–	–
		AU2–2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	–	–	–
		AU2–3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	–	–	–
	제품 인증	AU3–1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	N/A	–	–
		AU3–2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	–	–	–
암호	안전한 암호 알고리즘 사용	CR1–1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	–	–
	안전한 키 관리	CR2–1	암호키는 안전성이 검증된 방법으로 생성 · 갱신 · 분배 · 사용 · 저장 · 파기 되어야 한다.	–	–	–
	안전한 난수 생성	CR3–1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	–	–	–
데이터 보호	전송 데이터 보호	DP1–1	제품 간 전송되는 중요정보는 암호화해야 한다.	○	–	–
		DP1–2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	–	–	–

보안항목		보안인증 기준		L	B	S
데이터 보호	저장 데이터 보호	DP2–1	제품에 저장되는 중요정보는 암호화해야 한다.	○	–	–
		DP2–2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	–	–	–
	정보흐름 통제	DP3–1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	–	–	–
	안전한 세션관리	DP4–1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	–	–	–
		DP4–2	세션 ID는 예측할 수 없는 값이어야 한다.	–	–	–
	개인정보 보호	DP5–1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	–	–	–
플랫폼 보호	소프트웨어 보안	PL1–1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	–	–	–
		PL1–2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	○	–	–
		PL1–3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	○	–	–
		PL1–4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	–	–	–
	안전한 업데이트	PL2–1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	선택	–	–
		PL2–2	업데이트 실패 시 롤백 기능을 지원해야 한다.	–	–	–
		PL2–3	업데이트 수행 전 무결성을 검사해야 한다.	–	–	–
	보안 관리	PL3–1	불필요한 서비스는 제거하거나 비활성화해야 한다.	–	–	–
		PL3–2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	–	–	–
		PL3–3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	–	–	–
		PL3–4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	–	–	–
	감사기록	PL4–1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	–	–	–
		PL4–2	감사기록에 대한 보호 기능을 제공해야 한다.	–	–	–
	타임스탬프	PL5–1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	–	–	–
물리적 보호	물리적 인터페이스 보호	PH1–1	불필요한 외부 인터페이스는 비활성화하되, 필요 시 접근통제 기능을 지원해야 한다.	–	–	–
		PH1–2	비인가자의 내부 포트 접근을 방지해야 한다.	N/A	–	–
	무단조작 방어	PH2–1	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	–	–	–

사물인터넷(IoT) 보안 시험·인증 해설서 STANDARD

인 쇄 2019년 2월
발 행 2019년 2월
발 행 처 한국인터넷진흥원
전라남도 나주시 진흥길9(KISA 본원)
인 쇄 처 호정씨앤피 Tel. (02) 2277-4718

〈비매품〉

• 본 가이드라인 내용의 무선 전재 및 복제를 금하며, 가공 · 인용하는 경우 반드시 "한국인터넷진흥원의 '사물인터넷(IoT) 보안 시험·인증 기준 해설서'" 라고 출처를 밝혀야 합니다.

* 본 가이드 관련 최신본은 한국인터넷진흥원 홈페이지(www.kisa.or.kr) 또는 정보보호산업진흥포털(www.kisis.or.kr)에서 얻으실 수 있습니다.

사물인터넷(IoT) 보안
시험·인증 기준 해설서

STANDARD

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY