관리구분 : □관리본 □비관리본

문서번호 : TCP-2020/R02 : 2024

관리번호 :

신·구내용대비표

번호	세부항목	현 행	개 정 안
10	인증 유효기간	(없음)	10 인증 유효기간 인증 유효기간은 인증서의 인증연월일을 기준으로 3년으로 하며 2028년 3월 31일을 초과하지 않는다. 단, 2024년 3월 31일까지 발급된 인증서는 2027년 3월 31일까지 유효하다.
11	기타 사항	10 기타 사항 (시행일) 본 인증기준은 2023년 3월 1일부터 시행한다.	11 기타 사항 (시행일) 본 인증기준은 2024년 4월 1일부터 시행한다.

관리구분 : □관리본 □비관리본
문서번호 : TCP-2020/R02 : 2024
관리번호 :

공공기관용 무선 영상전송장비 보안 성능품질 TTA Verified 인증 기준

TTA 한국정보통신기술협회
Telecommunications Technology Association

제·개정 이력 현황

개정번호	제·개정일	개정쪽	제·개정내용
00	2022.7.29	-	인증 기준 마련에 따른 제정
01	2023.2.28	P9	“7.20 영상 저장 시 암호화” 필수 항목으로 변경
02	2024.3.29	P13 P13	“10 인증 유효기간” 추가 “11 기타 사항” 시행일자 변경

목 차

1 적용 범위 4
2 관련 규격 4
3 인증대상 4
4 약어 5
5 시험 환경 6
6 시험 항목 구분 6
7 공통 시험항목 및 인증기준 7
8 인증 유형별 시험항목 및 인증기준 10
9 인증 마크 표시 13
10 인증 유효기간 13
11 기타 사항 13

1 적용 범위

본 문서는 정보통신 제품 및 서비스에 대한 인증 요령 제12조 및 공공기관용 영상정보처리기기 보안 요구사항에 따라 무선 영상전송장비의 보안 성능품질에 대하여 시험하고 인증하는 것을 적용범위로 한다.

2 관련 규격

[1] 정보보호시스템 및 네트워크 장비 국가용 보안요구사항, NIS
[2] 정보통신망연결기기 등 정보보호인증기준, KISA
[3] 영상정보 처리기기 설치·운영 가이드라인, 2015. 1., 행정자치부
[4] 공공기관용 IP카메라 보안 성능품질 TTA Verified 인증기준, TTA
[5] 공공기관용 NVR 보안 성능품질 TTA Verified 인증기준, TTA

3 인증대상

3.1 인증대상 정의

이미지 센서로부터 획득한 영상 데이터를 전송하는 장치로서 본 문서에서 정의한 인증 유형에 속해야 한다.

3.2 유형별 시험범위

인증 유형은 다음과 같으며, 유형별로 공통 시험항목과 인증 유형별 시험항목을 만족해야 한다.

o 웨어러블캠 : 사람 또는 사물의 영상 등을 촬영하여 영상을 전송하는 장치로 일정 공간에 설치되어 있지 않고 몸에 걸치거나 휴대하는 형태의 영상 기기이다.

※ 웨어러블캠 외의 인증범위에 대해서는 추가 예정

3.3 인증대상 장비의 인증 전제 조건

1) 인증대상 장비는 공공기관이 공공시설물의 유지, 관리 용도로 사용하는 것을 목적으로 하는 제품을 대상으로 한다.
2) 인증대상 장비는 인가된 관리자만 장비를 반출 및 반입하여 운용하는 환경이다.
3) 인증대상 장비의 인가된 관리자는 제품 관리에 대하여 적절히 교육받았고, 운용기관이 마련한 관리자 지침에 따라 정확하게 의무를 수행한다.
4) 이동통신 망을 통하여 전달되는 네트워크 경로는 신뢰할 수 있는 것으로 간주한다.
5) 인증대상 장비에 S/W가 포함될 경우, S/W 설치 PC는 인가된 관리자만 사용해야 한다.
6) 인증대상 장비는 운용 계정별 권한을 별도로 부여하지 않고 관리자 권한으로 한다.

7) 인증대상 장비 관리를 위한 중앙 통제 시스템은 별도로 존재하지 않는다.
8) 인증대상 장비와 통신하는 서버 및 PC는 최신 버전의 백신으로 업데이트하여 사용해야 한다.
9) 인증대상 장비 구성품 중 앱이 있을 경우 추후 별도로 규정한다.

4 약어

AES	Advanced Encryption Standard
ARIA	Academy, Research Institute, Agency
FTP	File Transfer Protocol
FTPs	File Transfer Protocol Secure
HTML5	Hypertext Markup Language 5
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IP	Internet Protocol
LTE	Long Term Evolution
NTP	Network Time Protocol
RSA	Rivest, Shamir, Adleman
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
sFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity
WPA	WiFi Protected Access

5 시험 환경

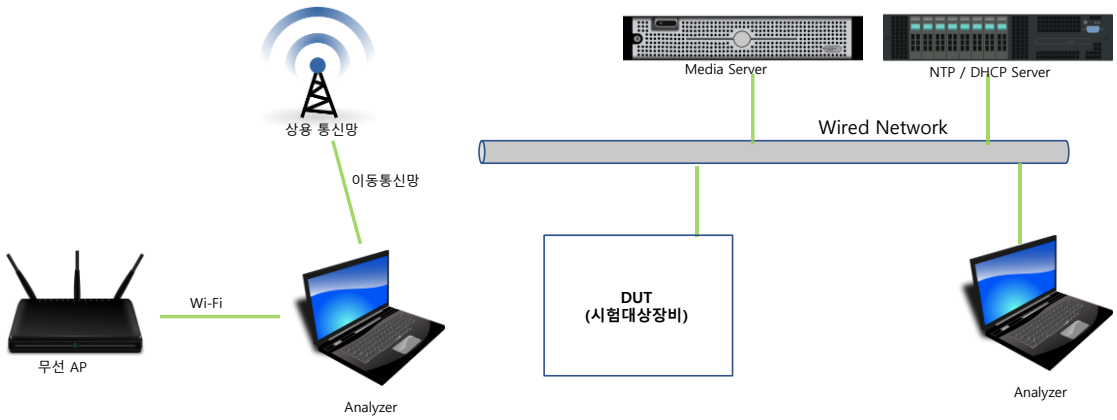

그림 1. 시험환경 구성도

시험 환경 구성은 그림 1과 같다. 시험대상장비는 기본적으로 공장 초기화 상태에서 시험하고, 필요 시 장비의 설정을 변경하여 시험한다. 시험대상장비가 가지고 있는 영상 전송 방법에 따라 유선 통신과 무선 통신(Wi-Fi, LTE 등) 인터페이스를 확인한다. 또한, 시험대상장비에 따라 시험 구성은 달라질 수 있다.

6 시험 항목 구분

시험항목의 실시 여부는 다음과 같은 조건을 따른다.

- [필수]: 인증을 위해 반드시 시험하는 항목
- [조건부필수]: 관련 기능이 구현된 경우에 반드시 시험하는 항목
- [선택]: 시험의뢰업체가 희망할 경우 시험하는 항목

인증 대상 장비가 다수개의 구성품으로 조합될 경우 적용되는 시험항목은 각 구성품 별로 모든 시험항목을 적용할 수 있고, 경우에 따라 구성품별로 시험항목을 상이하게 적용할 수 있다. 인증 대상 장비의 구성품 별 개별 시험항목의 적용 여부는 인증기관 시험원이 장비 검토 후 결정하여 수행한다.

7 공통 시험항목 및 인증기준

대분류	중분류	번호	시험 항목	인증 기준
식별 및 인증	관리자 기본(default) 비밀번호 변경 기능	1	[필수] 최초 비밀번호 생성/변경 강제	• 장비를 공장 초기화한 후 최초 장비 접속 및 최초 서비스 접속 시 관리자 기본(Default) 비밀번호에 대해 아래의 사항을 만족해야 한다. - 관리자 기본(Default) 비밀번호가 있는 경우, 비밀번호 변경이 강제되어야 함 - 관리자 기본(Default) 비밀번호가 없는 경우, 비밀번호 생성이 강제되어야 함 1) 장비 접속 - 웹 브라우저, 로컬 콘솔 등 2) 서비스 접속 - SSH, HTTP, HTTPS, RTSP, FTP, TELNET, SNMP 등 • 최초 비밀번호 생성/변경 기능이 일반적인 비밀번호 생성/변경 기능과 동일하지 않은 경우, 해당 기능은 공장초기화 이후 처음 1 회만 동작해야 한다.
		2	[필수] 최초 비밀번호 생성/변경 취약점 대응	• 최초 비밀번호 생성/변경 기능이 일반적인 비밀번호 생성/변경 기능과 동일한 경우, 해당 기능의 반복 동작이 허용되지만 반드시 안전한 사용자 인증이 요구되어야 한다.
	안전한 비밀번호 설정 기능	3	[필수] 비밀번호 생성 안정성	• 생성하는 비밀번호는 9 자리 이상이어야 한다. • 숫자, 영문 대문자, 영문 소문자, 특수문자 중 3 가지 조합 이상으로 비밀번호를 생성할 수 있어야 한다. - 숫자(0-9) - 영문자 대문자(A-Z) - 영문자 소문자(a-z) - 특수문자(!, @, #, $, %, ^, &, *, (,) 등)
		4	[선택] 비밀번호 최소길이 설정	• 비밀번호의 최소 길이를 관리자가 설정할 수 있는 기능을 제공해야 한다. ※ 최소 길이의 기본값은 9 자리 이상이어야 한다.
		5	[선택] 비밀번호 15 자리 이상 입력가능	• 비밀번호는 15 자리 이상 입력이 가능해야 한다.
	인증 실패 대응 기능	6	[필수] 인증 실패 시 장비접속 제한기능	• 지정된 횟수(기본값 5회 이하) 이상 인증 실패 시 일정 시간 (기본값 5 분 이상) 장비 접속을 제한하는 기능을 제공해야 한다.
		7	[조건부 필수] 인증 실패 시 관리자 통보 기능	• 지정된 횟수(기본값 5 회 이하) 이상 인증 실패 시 관리자가 즉시 확인할 수 있는 수단을 통해 통보해야 한다. - 알람, 문자메시지, 이메일 등의 수단

대분류	중분류	번호	시험 항목	인증 기준
		8	[필수] 에러 메시지에 인증 실패 사유 미포함 기능	• 인증 실패 시 인증 실패 사유를 에러 메시지에 포함하지 않아야 한다. (인증 실패 사유 예시) - 잘못된 계정을 입력하였습니다. - 잘못된 비밀번호를 입력하였습니다. ※ UI 뿐만 아니라 네트워크 상의 응답 메시지에도 실패 사유가 포함되지 않아야 한다.
	인증 피드백 보호 기능	9	[필수] 입력 비밀번호 마스킹 기능	• 입력되는 비밀번호를 화면에서 볼 수 없도록 마스킹하는 기능을 제공해야 한다.
데이터보호	인증 데이터 보호 기능	10	[필수] 비밀번호 암호화 저장 기능	• 비밀번호를 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다. • 장비에서 백업할 수 있는 설정 파일 등에 비밀번호가 포함된 경우, 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다. • 웹 브라우저 등을 통해 장비 외부에서 비밀번호를 설정 받을 시 이를 암호 알고리즘(비대칭키 암호 등)을 이용하여 안전하게 전송해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조
		11	[필수] 비밀정보 읽기 방지 기능	• 장비에 저장된 모든 비밀정보(비밀번호, 대칭키, 개인키 등)를 읽거나 유추할 수 없어야 한다. • 비밀정보에 대한 평문 처리 및 Base64 단순 인코딩 등은 제한한다.
		12	[필수] 비밀번호 임의 복구 기능 제한	• 비밀번호 찾기 또는 2 차 비밀번호 등의 임의 복구 기능을 제공하지 않아야 한다.
		13	[필수] 인증 정보 재사용 방지	• 안전한 사용자 인증 절차 없이 세션 ID, 쿠키 등의 세션 정보만으로 인증 여부를 판단하지 않아야 한다. • 사용자 비밀번호는 암호화된 상태로 전송해야 한다.
	저장 데이터 보호 기능	14	[조건부 필수] 설정값 암호화 저장 기능	• 설정값을 외장 메모리(microsd 카드 등)에 저장하여 설정을 변경할 수 있는 경우, 제품 설정값은 안전하게 저장해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조
암호지원	암호사용	15	[필수] 암호 알고리즘 보안 강도 만족 여부	• 암호화 및 해시 알고리즘의 보안강도는 112bit 급 이상을 만족해야 한다. ※ 알고리즘의 보안강도는 한국인터넷진흥원의 “암호 알고리즘 및 키 길이 이용 안내서” 최신본을 참조 (예시) - 해시(SHA-224/256/384/512) - 대칭키암호(SEED, ARIA-128/192/256, AES-128/192/256) - 공개키암호(RSA 2048) - 전자서명(RSA-PSS-2048/3072, ECDSA/KCDSA/EC-KCDSA)
		16	[필수] 국가용 또는 국제표준 암호 알고리즘 사용	• 정보보호시스템 및 네트워크 장비 국가용 보안 요구사항 권고 암호 알고리즘을 참조하여 국제표준 암호알고리즘 사용을 해야 한다.

대분류	중분류	번호	시험 항목	인증 기준
보안관리	안전한 업데이트 기능	17	[필수] 펌웨어/소프트웨어 버전 및 모델명 확인 기능	• 펌웨어/소프트웨어의 현재 버전을 확인할 수 있는 기능을 제공해야 한다. • 시험대상장비의 UI에서 모델명을 확인할 수 있어야 한다.
		18	[필수] 펌웨어/소프트웨어 업데이트 검증 기능	• 펌웨어/소프트웨어에 대한 해시 값 정보(모델명, 펌웨어/소프트웨어 파일명, 버전 정보 포함)를 홈페이지에 게시해야 한다. - SHA256 이상 사용
	안전한 세션 관리 기능	19	[필수] 일정시간 미사용시 세션 잠금/종료 기능	• 일정시간 관리자 활동이 없는 경우 세션을 잠그거나 종료하는 기능을 제공해야 한다. - Default ON, 기본값 10분 이하 ※ 본 항목의 기능은 ON/OFF가 허용됨
영상 저장 보안	영상 저장 시 암호화	20	[필수] 영상 저장 시 암호화	• 영상 데이터를 장비 내부에 저장할 경우 암호화하여 저장해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조 ※ ON/OFF 기능 사용 가능
	오디오 데이터 저장 제한	21	[필수] 오디오 데이터 저장 제한	• 기본 설정 상태에서 오디오 데이터 저장 기능을 사용할 수 없어야 한다. ※ 오디오 ON/OFF 기능 필수
인증 심의 항목	무단은닉 하드코딩 방지 이행	22	[필수] 암호 및 암호화키 하드코딩 방지 이행각서 공문	• 이행각서 공문 접수 - 주내용 : 방지 이행 약속 및 불이행시 관련 제품군에 대한 인증 취소 사전동의 (공문 내용) - "무단은닉 및 하드코딩된 암호 및 암호화키 없음" 선언 - "운용 모드 변경 (개발자/디버깅 모드) 관련 유/무" 선언 - "보안 및 성능품질 열화행위 하지 않음" 선언 - "백도어 없음" 선언
	채증 자료 제출	23	[필수] 구동 소프트웨어 채증 자료 제출	• 시험당시 구동 소프트웨어(어플리케이션 등) 해시 값 파일 제출 ※ 소스코드가 아닌 원본 소프트웨어 검증용 해시 값 또는 펌웨어 파일, 설치 파일 제출

8 인증 유형별 시험항목 및 인증기준

■ 웨어러블캠

대분류	중분류	번호	시험 항목	인증 기준
전송 데이터 보호	제품과 원격으로 연결된 모든 통신 수단간 안전한 암호통신 프로토콜 사용	1	[필수] 원격 접속시 암호통신 수행 기능	• 원격으로 접속 시 암호통신 프로토콜을 이용한 신뢰된 채널을 제공해야 한다. - (예시) HTTPS, SSL/TLS, SSH - 암호화 방식에 관련된 부분은 암호지원 시험항목(공통 시험항목 15번, 16번) 참조 - 제품 구성 요소간 데이터 전송시에도 동일하게 적용한다.
		2	[필수] TLS 1.2 이상 지원 기능	• TLS 프로토콜은 TLS 1.2(RFC 5246) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(공통 시험항목 15번, 16번) 참조
		3	[조건부필수] SSH2.0 이상 지원 기능	• SSH 를 지원하는 경우, 프로토콜은 SSH v2(RFC 4251~4254) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(공통 시험항목 15번, 16번) 참조
		4	[필수] OpenSSH, OpenSSL, 웹서버 모듈 버전 확인 기능	• 암호통신을 위해 OpenSSH, OpenSSL 을 사용하는 경우 버전을 확인하는 기능을 제공해야 한다. • 웹서버를 사용하는 경우 웹서버 모듈 버전을 확인하는 기능을 제공해야 한다. • 버전의 표기는 패치 버전 정보를 포함해야 한다.
감사 기록	감사데이터 생성 기능	5	[필수] 감사데이터 생성 기능	• 주요 감사사건에 대해 감사기록을 생성하는 기능을 제공해야 한다. - 관리자/사용자에 대한 식별 및 인증 성공/실패 기록 - 제품 설정 변경내역 기록 - 업데이트 정보 기록 - 단말 고유 식별자 등록 및 변경 이력 - 공장초기화(※공장 초기화 시에도 로그 이력은 유지해야 함)
	감사데이터에 최소 정보 포함 여부	6	[필수] 감사데이터에 최소 정보 포함 기능	• 감사데이터에는 최소한 다음의 정보가 포함되어야 한다. - 사건 발생 일시(※ NTP 서버나 운영체제에서 제공하는 시간 정보를 반영해야 함) - 사건 유형 - 사건 발생 주체 (ID, IP 주소) - 사건의 결과 (성공 또는 실패) - 인증정보(ex:비밀번호), 암호키 등의 정보는 감사기록에 포함되지 않아야 함
	감사데이터 보호 기능	7	[필수] 감사데이터 접근 제한 기능	• 인가된 관리자만 감사데이터에 접근할 수 있어야 한다.
	오류 검사 기능	8	[조건부 필수] 하드웨어 자체검사 기능	• Embeded-HW형 장비에 한하여, 장비 구동 시(Power On) 주요 하드웨어에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. - CPU, 메모리, 플래시 메모리, 네트워크 인터페이스 등

대분류	중분류	번호	시험 항목	인증 기준
자체보호				※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료를 제출해야 함
		9	[필수] 소프트웨어 자체검사 기능	• 장비 구동시(Power On) 또는 어플리케이션 로딩 후 주요 프로세스에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. - 식별 및 인증 프로세스 - 정보흐름통제 프로세스 - 보안관리 프로세스 등 ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함
		10	[필수] 자체검사 내용 및 결과 확인 기능	• 장비가 수행한 자체검사 내용 및 결과를 관리자가 확인할 수 있는 기능을 제공해야 한다. (예시) - 화면 출력 - 디스플레이 화면 - 감사데이터 생성 등
인증서 관리	개인키 암호화 저장 확인	11	[필수] 개인키 암호화 저장 기능	• 장비 내에 저장된 개인키는 암호화되어 저장되어야 한다. – 암호화 방식에 관련된 부분은 암호지원 시험항목(공통 시험항목 15번, 16번) 참조
	인증서/개인키/대칭키 확인	12	[필수] 인증서/개인키/대칭키의 안전한 생성	• 장비 내에서 인증서/개인키/대칭키를 생성하는 경우, 안전한 방법으로 생성해야 하며, 인증서/개인키/대칭키의 하드코딩 및 장비간 공통된 개인키/대칭키의 일괄 사용을 하지 않아야 한다.
영상전송 보안	영상 전송 보안	13	[필수] 영상 전송 시 암호화	• 웹 브라우저 등에 영상을 전송하기 위한 암호통신 프로토콜 기반의 신뢰된 채널을 제공해야 한다. – (예시) HTTPS, TLS • HTTPS Tunneling(RTP/RTSP/HTTPS/TCP) 방식으로 영상 데이터를 송신할 수 있어야 한다. – 암호화 방식에 관련된 부분은 암호지원 시험항목(공통 시험항목 15번, 16번) 참조 • FTP 전송시 FTPs, sFTP 등 암호화 채널로 전송해야 한다.
	무선 채널	14	[조건부 필수] Wi-Fi 를 통한 영상 전송 시 암호화	• WPA2 또는 WPA3 를 사용할 수 있어야 한다.
		15	[조건부 필수] 이동통신 망을 통한 영상 전송	• LTE/5G 등 이동통신 망 채널을 통해 전송한 영상이 정상적으로 재생되는 지를 확인한다.

대분류	중분류	번호	시험 항목	인증 기준
영상 백업 보안	영상 백업 시 암호화	16	[조건부 필수] 영상 백업 시 암호화	• 장비에 저장된 영상 데이터를 외부로 백업/다운로드하는 것이 가능한 경우, 암호화하여 백업/다운로드해야 한다. • 백업/다운로드하는 영상 데이터에 대한 무결성 검증 값 생성 및 확인이 가능해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(공통 시험항목 15번, 16번) 참조 ※ 백업을 위해 별도 SW를 이용할 경우에만 본 시험항목 적용
장비 관리	관리 보안	17	[선택] 분실시 대응 기능	o 관리자는 장비 분실, 도난 등의 사고 발생시 원격으로 앱초기화 또는 원격소거, 로그아웃, 잠금, 저장 자료 삭제 등의 보안 기능을 실행할 수 있어야 한다.
		18	[조건부 필수] 외부 인터페이스	o USB 등 외부 인터페이스가 존재할 경우, 인가된 관리자만 접속가능해야 한다.

9 인증 마크 표시

인증된 제품에 대해서는 TTA Verified 마크의 사용을 승인한다.

공공기관용 무선 영상전송장비
보안 성능품질
(TTA-V-YY-XXX)

10 인증 유효기간

인증 유효기간은 인증서의 인증연월일을 기준으로 3년으로 하며 2028년 3월 31일을 초과하지 않는다. 단, 2024년 3월 31일까지 발급된 인증서는 2027년 3월 31일까지 유효하다.

11 기타 사항

(시행일) 본 인증기준은 2024년 4월 1일부터 시행한다.