시험 성적서

한국정보통신기술협회 공공안전서비스단 주소: 경기도 성남시 분당구 분당로 47 전화: 031-780-9111, Fax: 031-724-0161	성적서번호:TTA-19-1004	

1. 의 뢰 자

o 기 관 명 : ㈜두원전자통신

o 주 소 : 경기도 부천시 석천로 397, 부천테크노파크 쌍용3차 301동 408호

2. 시료 : 영상보안시스템용 IP 카메라

o 모델명 : DWX-2003 (파생모델명: DWX-2003M, DWX-2003L, DMX-2003, DMX-2003L, DOX-2003, DHD-2000H, DHD-2000HC, DHD-2100B)

3. 시험기간 : 2020.6.8. ~ 2020.6.12.

4. 시험방법

o 인증기준 : 공공기관용 IP카메라 보안 성능품질 TTA Verified 인증기준(TCP-2012/R03:2019)

o 시험방법 : 시험결과 참조

5. 시험결과 : 시험결과 참조

이 성적서의 시험결과는 의뢰자에 의해 제공된 시료에 한하며 용도 이외의 사용을 금합니다.

확 인	작성자	승인자
	성 명 : 김태영 (서명) 김태영	성 명 : 박동영 (서명) 박동영

2020. 6. 22.

한국정보통신기술협회 회장 (인)

TPG-0024-1-A(00)

※ You can verify the forgery and authenticity by the barcode at the end of this document.

시험결과:

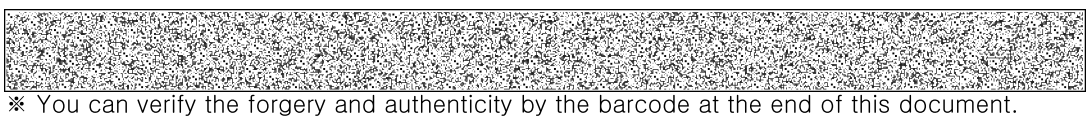
㈜두원전자통신

영상보안시스템용 IP 카메라
(모델명: DWX-2003 [파생모델명: DWX-2003M, DWX-2003L, DMX-2003, DMX-2003L, DOX-2003, DHD-2000H, DHD-2000HC, DHD-2100B])

공공기관용 보안 성능품질 TTA Verified 인증시험
(보안 ☑ 성능품질 ☐)

※ You can verify the forgery and authenticity by the barcode at the end of this document.

목 차



한국정보통신기술협회(TTA) 공공안전서비스단은 ㈜두원전자통신에서 시험 의뢰한 영상보안시스템용 IP 카메라에 대하여 공공기관용 보안 성능품질 TTA Verified 인증시험 성적서를 제출한다. 시험결과는 본 성적서의 시험 환경, 의뢰 제품 모델및 본 성적서에 명시된 버전에만 국한된다.

1 시험 개요

1.1 시험 목적

이 시험은 ㈜두원전자통신에서 의뢰한 영상보안시스템용 IP 카메라에 대하여 “공공기관용 IP 카메라 보안 성능품질 TTA Verified 인증기준(TCP-2012/R03:2019)”에 따라 TTA Verified 인증을 위한 기능 및 성능 확인이 목적이다.

1.2 시험대상장비

본 시험의 시험대상장비(DUT: Device under Test)는 카메라가 촬영한 감시 영상을 저장하고 Internet Protocol 을 활용해 전송하는 네트워크 감시용 카메라이다. 그림 1 은 시험대상장비를 나타낸다.

- 모델명 : DWX-2003
- 파생모델명 : DWX-2003M, DWX-2003L, DMX-2003, DMX-2003L, DOX-2003, DHD-2000H, DHD-2000HC, DHD-2100B
- Firmware(S/W) Version : HS19_SWU1_V1.0.0.18

그림 1. 시험대상장비

1.3 시험 환경

영상보안시스템용 IP 카메라의 보안 기능 시험 구성은 그림 2 와 같다.

보안 기능 시험은 패킷 스니핑 장비, 네트워크 프로토콜 분석기, 보안 기능 시험기 등을 이용하여 시험한다. DUT 는 기본적으로 공장 초기화 상태에서 시험하고, 필요 시 DUT 의 설정을 변경하여 시험한다.

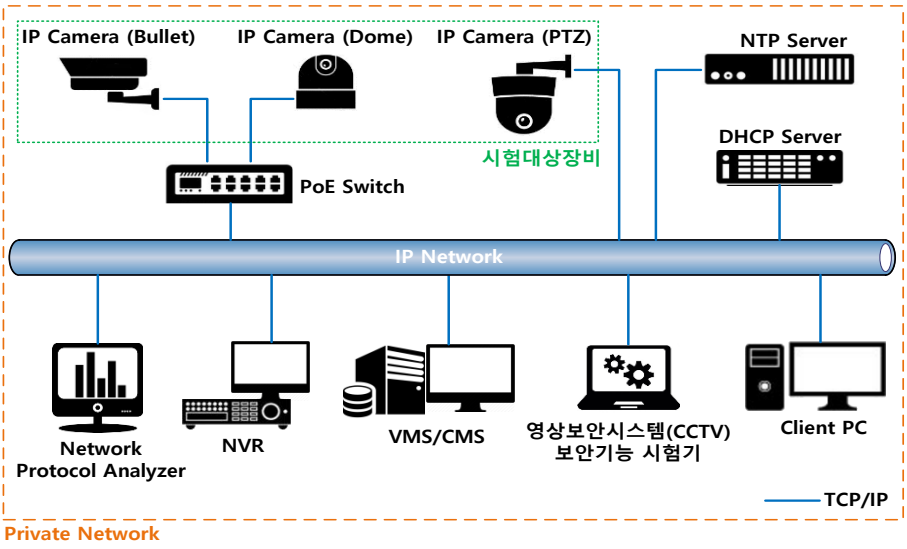


그림 2. 보안기능 시험 환경도

1.4 시험 장비

본 시험에 사용한 시험 장비는 표 1 과 같다.

표 1. 시험 장비

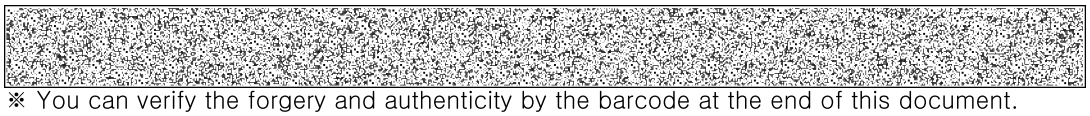
장비명	모델명	제조사
보안 기능 시험기	영상보안시스템(CCTV) 보안 기능 시험기	㈜서브
네트워크 프로토콜 분석기	Wireshark	Wireshark Foundation
PoE 스위치	SF220-24P-K9-EU	CISCO

2 시험 내용 및 결과

2.1 보안 기능 시험(TCP-2012/R03:2019)

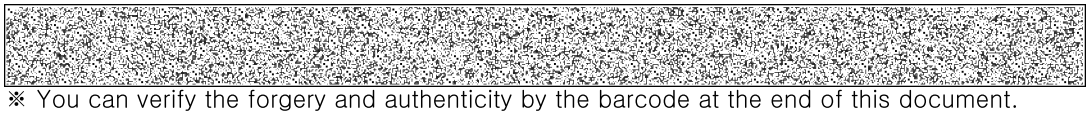
※ 본 시험에 웹 취약성 분석 관련 시험은 포함되어 있지 않음.

번호	시험 항목	인증 기준	필수 여부	판정
1	최초 비밀번호 변경	• 장비를 공장 초기화한 후 최초 장비 접속 및 최초 서비스 접속 시 관리자 기본(Default) 비밀번호 유지는 제한 되어야 하며 반드시 안전한 패턴으로 변경되어야 한다. 1) 장비 접속 - 웹 브라우저, 로컬 콘솔 등 2) 서비스 접속 - SSH, HTTP/HTTPS, RTSP, FTP, TELNET, SNMP 등	필수	PASS
2	비밀번호 조합 구성	• 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)	필수	PASS
3	비밀번호 최소길이 설정	• 비밀번호의 최소 길이를 관리자가 설정할 수 있는 기능을 제공해야 한다. ※ 최소 길이의 기본값은 9 자리 이상이어야 한다.	선택	PASS
4	비밀번호 15 자리 이상 입력가능	• 비밀번호는 15 자리 이상 입력이 가능해야 한다.	선택	PASS



번호	시험 항목	인증 기준	필수 여부	판정
5	인증 실패 시 장비접속 제한기능	• 지정된 횟수(기본값 5 회 이하) 이상 인증 실패 시 일정 시간 (기본값 5 분 이상) 장비 접속을 제한하는 기능을 제공해야 한다.	필수	PASS
6	인증 실패 시 장비접속 제한시간 설정기능	• 인증 실패 시 장비 접속 제한 시간을 관리자가 설정할 수 있는 기능을 제공해야 한다.	선택	PASS
7	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.	필수	PASS
8	입력 비밀번호 마스킹 기능	• 입력되는 비밀번호를 화면에서 볼 수 없도록 마스킹하는 기능을 제공해야 한다.	필수	PASS
9	비밀번호 암호화 저장 기능	• 비밀번호를 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	필수	PASS
10	비밀정보 읽기 방지 기능	• 장비에 저장된 모든 비밀정보(비밀번호, 대칭키, 개인키 등)를 읽거나 유추할 수 없어야 한다. • 비밀정보 평문 저장 및 Base64 단순 인코딩 등은 제한한다.	필수	PASS
11	사용자 인증	• HTTP 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다. • RTSP 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다. • SOAP 사용자 인증으로 WSSE UsernameToken 의 PasswordDigest 인증 방식을 SHA-1 이상으로 사용해야 한다. • 기타 사용자 인증방식을 “(대분류)암호지원”을 참조하여 안전한	필수	PASS

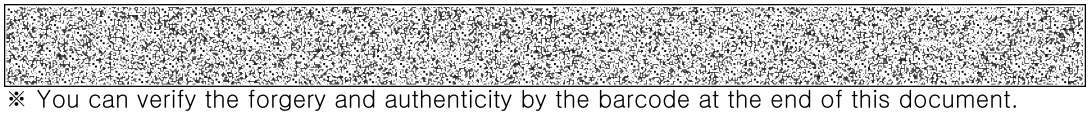
번호	시험 항목	인증 기준	필수 여부	판정
		방식을 사용해야 한다.		
12	암호 알고리즘 보안 강도 만족 여부	• 암호화 및 해시 알고리즘의 보안강도는 112bit 급 이상을 만족해야 한다. (예시) - 해시(SHA-224/256/384/512 등) - 대칭키암호(SEED, ARIA-128/192/256, AES-128/192/256 등) - 공개키암호(RSA 2048 등) - 전자서명(RSA-PSS-2048/3072, ECDSA/KCDSA/EC-KCDSA 등)	필수	PASS
13	국가용 암호 알고리즘 사용 여부	• 국가용 암호 알고리즘의 사용을 권고한다. - 국정원장 승인 알고리즘, 국가사이버안전센터 안내 참조	선택	해당사항 없음
14	VLAN 기능	• VLAN 기능 제공시 IEEE Std 802.1q-2011 이상을 지원해야 한다.	선택	해당사항 없음
15	IP Filtering 기능	• 특정 IP 주소에서의 접속을 허용/차단할 수 있는 기능을 제공해야 한다. ※ Black List(Deny), White List(Allow) 동작 확인	필수	PASS
16	ACL 기능	• 장비별 다음과 같은 ACL 기능을 제공해야 한다. - Source IP Address 정보 또는 Source Port Number 정보	선택	해당사항 없음
17	원격 관리용 IP 주소 지정 기능	• 원격 관리 서비스 용도의 IP 주소를 지정하는 기능을 제공해야 한다. - IP 주소 지정은 대역이 아닌 개별 주소 등록만 가능해야 함	필수	PASS
18	원격관리서비스 활성화/비활성화 기능	• 공장 초기화 상태에서 원격 관리 서비스는 비활성화되어 있어야 한다. • 관리자가 원할 때 원격 관리 서비스를 활성화/비활성화 할 수 있는 기능을 제공해야 한다. - 원격 관리 서비스 : SSH, HTTP/HTTPS, FTP, TELNET, SNMP 등 - 로컬 콘솔 포트가 없는 경우 : HTTPS 만 활성화 허용	필수	PASS



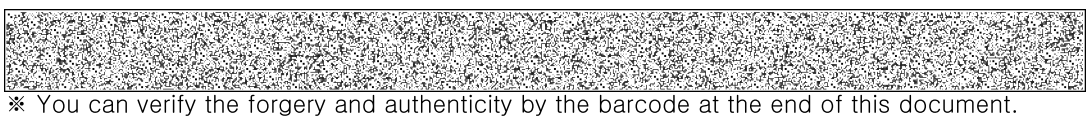
번호	시험 항목	인증 기준	필수 여부	판정
		- 로컬 콘솔 포트가 있는 경우 : HTTPS 도 활성화 금지		
19	웹 표준방식 지원	• HTML5 등의 웹 표준방식을 지원해야 한다. ※ Active X, EXE 가 지원될 경우 해당 기능에 대한 ON/OFF 가 가능해야 한다.	선택	해당사항 없음
20	SNMP V3 지원 기능	• SNMP 를 지원하는 경우, SNMP 는 V3 이상을 지원해야 한다. - 암호화 방식에 대한 상세는 "암호지원" 참조	조건부 필수	해당사항 없음
21	펌웨어/소프트웨어 버전 확인 기능	• 관리자가 어플리케이션/펌웨어의 현재 버전을 확인할 수 있는 기능을 제공해야 한다.	필수	PASS
22	펌웨어 업데이트 검증 기능	• 펌웨어 업데이트 시 해시값 비교 또는 전자서명 등을 제공해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조 (MD5 등 사용제한, SHA256 이상 사용권고)	필수	PASS
23	일정시간 미사용시 세션 잠금/종료 기능	• 일정시간 관리자 활동이 없는 경우 세션을 잠그거나 종료하는 기능을 제공해야 한다. (예시) 기본값 10 분 이하 ※ 본 항목의 기능은 ON/OFF 가 허용됨 ※ 관리자 활동 : 관리자 계정으로 접속하여 설정을 변경할 수 있는 로컬/원격 세션의 모든 활동	필수	PASS
24	동시접속 세션 수 제한 기능	• 시험대상장비에 원격으로 접속하는 관리자의 동시 접속 세션을 하나만 허용하거나 동시 접속 세션 수를 제한 기능을 제공해야 한다. ※ 본 항목의 기능은 ON/OFF 가 허용됨	선택	해당사항 없음
25	하드웨어 자체검사 기능	• Embeded-HW 형 장비에 한하여, 장비 구동 시(Power On) 주요 하드웨어에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. (예시) - CPU, 메모리, 플래시 메모리, 네트워크 인터페이스 등	조건부 필수	PASS

번호	시험 항목	인증 기준	필수 여부	판정
		※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함		
26	소프트웨어 자체검사 기능	• 장비 구동시(Power On) 또는 어플리케이션 로딩 후 주요 프로세스에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. (예시) - 식별 및 인증 프로세스 - 정보흐름통제 프로세스 - 보안관리 프로세스 등 ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함	필수	PASS
27	자체검사 내용 및 결과 확인 기능	• 시험대상장비가 수행한 자체검사 내용 및 결과를 관리자가 확인할 수 있는 기능을 제공해야 한다. (예시) - 화면 출력 - 디스플레이 화면 - 감사데이터 생성 등	필수	PASS
28	자체검사 실행 기능	• 관리자가 항목 25,26 의 자체검사를 직접 실행하는 기능을 제공해야 한다.	선택	해당사항 없음
29	소프트웨어 무결성 검사 기능	• 시험대상장비 구동 시(Power On) 또는 구동 이후 주요 소프트웨어에 대한 무결성 검사 기능을 제공해야 한다. ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함	선택	해당사항 없음
30	무결성 검사 실행 기능	• 관리자가 소프트웨어 무결성 검사를 직접 실행하는 기능을 제공해야 한다.	선택	해당사항 없음
31	설정 백업/복원시 무결성 검사 기능	• 장비 설정 백업/복원 시 설정 파일에 대한 무결성 검사 기능을 제공해야 한다.	선택	해당사항 없음

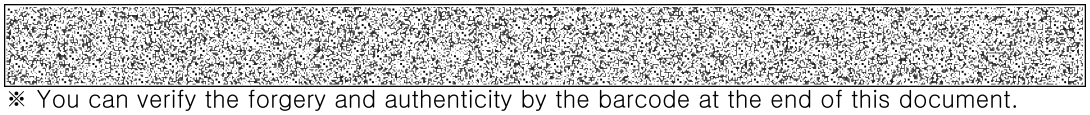
번호	시험 항목	인증 기준	필수 여부	판정
32	계정별 접근권한 설정 기능	• 관리자 계정별 접근권한을 설정하는 기능을 제공해야 한다.	필수	PASS
33	운영모드 변경용 비밀번호 생성 기능	• 운영모드 변경이 가능할 경우, 운영모드 변경용 비밀번호를 관리자가 생성/재설정할 수 있는 기능을 제공해야 한다. ※ 비밀번호 생성 관련 부분은 안전한 비밀번호 설정 기능을 참고	조건부 필수	PASS
34	운영모드 변경 시 추가 인증 기능	• 운영모드 변경이 가능할 경우, 운영모드 변경 시 추가 인증을 수행하는 기능을 제공해야 한다.	조건부 필수	PASS
35	중요 명령 사용 제한 기능	• 장비 상태를 변경하는 중요 명령(기능)에 대한 접근은 로컬 콘솔(콘솔포트 연결)로 제한하는 기능을 제공해야 한다. (중요 명령) - 재부팅, 디버깅(부트롬 접속, 메모리 수정/덤프)	선택	해당사항 없음
36	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" 참조	필수	PASS
37	별도 서버와 연동시 암호통신 수행 기능	• 별도 서버(로그서버 등)와 원격으로 장비 연동 시 암호통신 프로토콜을 이용한 신뢰된 채널을 제공해야 한다. (예시) - HTTPS, SSL/TLS, SSH - 암호화 방식에 관련된 부분은 "암호지원" 참조	선택	해당사항 없음
38	TLS 1.2 이상 지원 기능	• TLS 프로토콜은 TLS 1.2(RFC 5246) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	필수	PASS
39	SSH 2.0 이상 지원 기능	• SSH 를 지원하는 경우, 프로토콜은 SSH v2(RFC 4251~4254) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	조건부 필수	PASS



번호	시험 항목	인증 기준	필수 여부	판정
40	OpenSSH, OpenSSL 버전 확인 기능	• 암호통신을 위해 OpenSSH, OpenSSL 을 사용하는 경우 버전을 확인하는 기능을 제공해야 한다.	필수	PASS
41	감사데이터 생성 기능	• "붙임"에 해당하는 감사 데이터들을 생성하는 기능을 제공 해야 한다. ※ 감사 데이터 세부내역은 "붙임" 참조	필수	PASS
42	감사데이터에 최소 정보 포함 기능	• 감사데이터에는 최소한 다음의 정보가 포함되어야 한다. - 사건 발생 일시 - 사건 유형 - 사건 발생 주체(ID, IP 주소) - 사건의 결과(성공 또는 실패)	필수	PASS
43	감사 증적 초과시 관리자 확인 기능	• 감사증적 크기가 로그 저장 용량의 일정 기준(예: 90% 이상) 초과 시 관리자가 알 수 있는 기능을 제공해야 한다.	필수	PASS
44	감사 증적 초과시 대처 조치 기능	• 감사증적 크기가 로그 저장 용량의 일정 기준(예: 90% 이상) 초과 시 '외부로의 로그 백업 또는 오래된 내용 덮어쓰기' 등 대처 조치를 해야 한다.	필수	PASS
45	외부 로그서버 전송 기능	• 감사데이터를 외부 로그 서버로 전송하는 기능을 제공해야 한다.	선택	해당사항 없음
46	감사 데이터 접근 제한 기능	• 인가된 관리자만 감사데이터에 접근할 수 있어야 한다.	필수	PASS
47	감사 데이터 암호화 저장 기능	• 감사데이터를 장비 내부에 저장할 경우 암호화하여 저장하는 기능을 제공해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	선택	해당사항 없음
48	개인키 암호화 저장 기능	• 장비 내에 저장된 개인키는 암호화되어 저장되어야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	필수	PASS
49	인증서/개인키의 안전한 생성	• 장비 내에서 인증서/개인키를 생성하는 경우, 안전한 방법으로 생성해야 하며, 인증서/개인키의 하드코딩 및 장비간 공통된 개인키의 일괄 사용을 하지 않아야 한다.	필수	PASS



번호	시험 항목	인증 기준	필수 여부	판정
50	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	필수	PASS
51	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	필수	PASS
52	지원 명령어 확인	• OPTIONS 메시지로 지원하는 RTSP 명령어가 확인되어야 한다.	필수	PASS
53	세션 확인	• DESCRIBE 메시지로 제공 가능한 세션 내역이 확인 되어야 한다.	필수	PASS
54	연결 설정	• SETUP 메시지로 원하는 세션 연결 설정이 가능해야 한다.	필수	PASS
55	전송 시작	• PLAY 메시지로 영상 데이터 전송을 시작할 수 있어야 한다.	필수	PASS
56	전송 종료	• TEARDOWN 메시지로 영상 데이터 전송을 종료할 수 있어야 한다.	필수	PASS
57	기본 Flow 적용	• TLS 표준상의 기본 Flow 가 적용되는지 확인한다.	필수	PASS
58	인증서 적용	• TLS 연결 과정에서 서버 측의 인증서가 클라이언트에게 전달되는지 확인한다. • Certificate Request 를 지원하는 경우, TLS 연결 과정에서 클라이언트	필수	PASS



번호	시험 항목	인증 기준	필수 여부	판정
		측의 인증서가 서버로 전달되는 지 확인한다.		
59	전자서명	• TLS 연결 과정에서 전자서명 역할을 하는 Certificate Verify 를 전송하는 지를 확인한다.	선택	해당사항 없음
60	국제 표준 암호 알고리즘 수용 및 협상	• 적용된 암호화 알고리즘이 2 개 이상일 경우, 상호간 협상에 의하여 우선순위에 따라 암호화 알고리즘을 선택하여 적용하는 지를 확인한다. ECC 적용 장비의 경우, 별도 규격인 IETF RFC 4492 규격을 준용하여 파라미터 및 키를 생성하고 전송하는 지 확인한다.	필수	PASS
61	RTP 암호화 및 복호화	• 암호화된 RTP 메시지를 네트웍상에서 캡쳐하여 영상이 재생되는 지를 확인하며, 클라이언트에서 정상적으로 복호화를 수행하여 영상 재생이 되는 지를 확인한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	필수	PASS
62	영상 저장 시 암호화	• 영상 데이터를 장비 내부에 저장할 경우 암호화하여 저장해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조 ※ 음성 데이터는 저장하지 않아야 함	선택	해당사항 없음
63	영상 백업 시 암호화	• 영상 데이터를 장비 외부로 반출할 경우 암호화하여 반출해야 한다. • 반출하는 영상 데이터에 대한 무결성 검증 값 생성 및 확인이 가능해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조	조건부 필수	해당사항 없음

