[암호화 모듈사양서]
암호화 모듈 Model: DUSS

[무선브리지 세부 사양서]
무선브리지 적용모델
X5NM X5NB X525
NR2 N5 N52 N2H

SUNGJIN RF

X5NM, X525, X5NB 무선브리지 사양서

1. 특징
- 802.11.an 300Mbps이며 2X2 MIMO다중입출력장치 통신방식을 적용.
- 이동체 등에 적용하도록 제로센스로밍(핸드오프) 기능을 기본 탑재하여 별도의 추가 소프트웨어가 필요하지 않음.
- 무선브리지의 웹GUI페이지 메뉴내용은 한국어를 지원하여 설정, 변경이 용이하다.
- 핸드오프 지연시간은 50ms
- 사이트 탐색을 위한 Wave View 스펙트럼 아날라이저 기능 탑재.
- 각종 악성바이러스 차단 및 네트워크 관련 제어를 설정하여 외부의 침입을 사전에 차단하는 기능을 탑재.

가. 통신방식
- MIMO 다중입출력
- CSMA/TDMA지원

나. 무선장치 전용 소프트웨어 IP Discovery tool프로그램은 시스템 작동을 확인 및 내부 접속 을 위한 관리용 Tool이다.

[무선장치의 Main은 다양한 OS Tool를 지원한다]
- RSSI를 Color bar와 수치 값으로 무선링크상태를 모니터링과 안테나조정이 가능하다.
- 자체 OS Tool에서 무선장치와 접속된 모든 네트워크 장치의 Ping Test를 할 수 있다.
- Ping test는 유저가 지정한 packet size를 지정하여 지연시간, 손실 율을 모니터링 할 수 있다
- 스펙트럼 아날라이저 기능과 사이트검색 툴은 무선장치 주변에 타 장치를 검색하여 본 장치에 혼신과 간섭요인을 파악하여 우회 주파수를 선택 운용 할 수 있다.
- 네트워크 스피드테스트 툴은 두 장치간 통신에 최대 실효데이터를 측정하며 양방향, 수신, 송신의 실시간 실효데이터를 자체 테스트 할 수 있다.
- Main페이지 GUI는 실시간 통신하는 실효데이터의 트래픽을 그래프로 표시하며 LAN, WLAN 유선, 무선 두 개의 실시간 그래프를 표시한다.
- STATION모드는 무선장치의 리스트를 보여주며 신호상태, 송수신속도, 손실 율, 접속 시간, 동작상태를 표시한다.
- 시스템LOG는 장치의 동작상태, 변동 이력을 볼 수 있다.
- AP는 4개의 멀티 SSID지원한다.
- 장치 자체WEB에서 제품의 일련번호, 프로그램버전, MAC주소, CPU사용 상태, 메모리상태 등을 모니터링 한다.
- 다국어 지원: 한국어, 영어, 중국어, 터키어, 스페인어, 아랍어

다. 무선 보안
- 무선브리지는 아래와 같은 암호화를 지원 한다.

WPA, WEP, WPA-TKIP, WPA-AES, WPA2, WPA2-TKIP, WPA2-AES, WPA 4KEY, 128bit
- MAC ACL을 지원하며 특정한 MAC을 연결 또는 제한 한다.
- 무선링크 후에는 성능의 최적화에 대해 다른 패킷 크기로 통신테스트 할 수 있다
- 각종 통계 정보를 검토, 무선설정, TX / RX 정보, 이더넷 통계, 장치 정보. 표시.
- PIN(SSID) 코드 기능은 PTP, PTM site의 보안모드를 설정할 수 있다.
- Web 접근제한
- WISP지원

라. 네트워크 보안

무선브리지는 외부로부터 침입을 차단하기 위해 아래와 같은 기능을 지원한다.

- Bridge는 DHCP, Static 지원.
- 네트워크 외부침입 감지, 차단기능: 포트감지스캔, 동기화 공격탐지, 스루핑 공격탐지, TCP널 스캔탐지, Finger스캔탐지, 핑 테스트 감지, 핑 공격탐지, 조각공격감지, ACK검색 속임수탐지, NetBIOS침투스캔감지.
- 네트워크 포트 침투차단 제어: FTP, SSH, TELNET, HTTP, DNS
- 바이러스 차단: Worm Virus, Shock Virus, Netbus Horse, Netspere Horse, Shake Virus, Hackers Horse

[네트워크 일반}

- 네트워크 VLAN 추가 지원.
- 이더넷 1포트 10/100/1G자동 지원.
- 트래픽 쉐이핑 제어로 통신상의 송신, 수신 데이터 량을 제어.
- 동보제한 설정, 블랙&화이트 사이트 제어, 특정사이트 제어.
- 다이나믹DNS설정, SNMP사용 설정,
- 클라이언트속도 전체 또는 분류제한.

마. 무선 일반사항

- 통신거리는 자동, 수동모드 설정가능.
- 무선브리지는 스펙트럼 아날라이저 기능을 탑재하여 주변 사이트 채널 검색, 신호크기, 채널 스캔대역폭 조정, 혼신여부, 4.9GHz~6GHz까지 스캔, 다양한 메뉴측정 툴을 지원한다.
- 자동모드 ACK설정으로 통신상에 지연을 최소화.
- 장치 외부에 무선링크 상태 모니터링용 4개의 시그널 LED를 장착하여 통신상태 확인가능.
- Ping Watchdog 지원.
- 통신중인 장치간의 통신거리 표시.
- Web Server, SSH Server, Telnet Server, NTP Client, Dynamic DNS, System LOG등 지원.
- KSD9502 염수분무시험 합격
- 안테나이득에 따라 송신출력이 자동조정 기능.
- 실시간 데이터 처리량은 반 이중 90MB를 지원한다.
- WMM설정으로 AP, Station장치의 매개변수 설정.
- AP와 AP간 통신이 가능한 APWDS 통신 기능.
- SSID숨김 기능, DFS자동 탐지 기능.

바. 본체는 IP-67규격 다이케스팅 케이스 재질을 사용한 소형 경량급이며 분체 도장을 하여 염분에 의한 부식이 없으며 백화현상이나 도색부분이 벗겨지지 않고 무광 분체도장한 제품이다.

사. 안테나 및 본체를 쉽게, 다양한 각도 조정이 가능한 알루미늄 다관절 브라케트를 사용한다.

아. RJ-45포트는 방수용 이더넷 커넥터와 IEC기준 사용.

자. 무선장치의 전원은 기본적으로 DC24V PoE로 구동되나, 태양전지 및 배터리로 구동하기 위해서 DC12V~ DC28V으로도 작동되며 용도에 따라 DC인젝터를 공급한다.

차. 장치를 고정하는 알루미늄 다관절 브라케트를 수직, 수평 POLE등 다양한 위치에도 고정할 수 있으며 브라켓 방향 조정은 수직350도, 수평 360도 조정이 가능해야 하며 70mm의 POLE에 고정할 수 있다.

카. 무선장치는 통신이 가능하도록 먼저 셋팅하고, 그 후 POLE에 고정하여 4단계 고휘도 LED RSSI상태를 모니터링 한다.

타. 무선장치는 육안으로 장치의 동작상태를 확인하기 위하여 LAN접속용 LED램프, 전원LED 램프 등이 부착되어 있다.

파. 스마트 폰, 노트북에서 검색되지 않는 주파수 사용이 가능하다.

하. 무선장치내부에 써지 보호기 장착. ESD16Kv. IEC61000-4-2(ESD), IEC61000-4-5(Surge) 기준 준수.

2. 제원

- 무선기술: MIMO다중 입출력 프로토콜 CSMA/TDCA 적용
- 운용모드: 점대점(Point to Point,) 점대다(Pint to Multi Point)
- 운용주파수: 5745~5825MHz (World 5150~5825MHz, 4920MHz ~ 6020MHz)
- 변조방식: BPSK, QPSK, 16QAM
- 송신출력: 10dBm (max27dBm)
- 수신감도: MCS0 -94 ~ MCS15 -73 dBm
- 채널대역폭: 5,10,20,40MHz
- 이너넷 포트: 10/100/1000 Ethernet IEEE 802.3
- 써지보호: Built-in (IEC 61000-4-2 (ESD) and IEC 61000-4-5 (SURGE))
- 무선속도: Max 300Mbps
- Packet지연시간: 2 ms (64 bytes packet)
- 데이터 암호화: 본체 4중 보안. Hardware based AES, 국정원 인증 **ARIA,SEED, 보안1등급 VSL1** 탑재(외장형 선택품목)
- 암호화 모듈은 유지보수 및 펌 웨어 업로드와 관리가 용이하도록 외장용으로 설치한다(제품 내장 장착 가능)
- 동작온도: -40°C (-40 F) ~ +85°C (+185 F)
- 습기: 0 ~ 90 % (non-condensing)
- 크기mm: X5NM 가로228 세로228 두께76. X5NB 가로183 세로183 두께43. X525 가로371 세로371 두께95
- 무게Kg: X5NM 1.7Kg X5NB 1.5Kg X525 4.3Kg
- 전원: POE 24 VDC, (DC12V~28V 300mA)
- 전원입력: 100 – 240 VAC
- 소비전류: 4 W

무선안테나 사양서

1. 지향성 이중편파 패치 안테나

1) 기능

무선브리지의 다중입출력 이중편파를 사용한 안테나.

X5NM	X525	N5
2) 특성		
▪ 주파수 범위 : 5150 – 5850MHz ▪ 이 득 : 18dBi X2 이중편파 ± 0,5 dBi ▪ VSWR GHz : ≤ 1,5 ▪ F/B Ratio-dB: 20 ▪ 임피던스Ω: 50 ▪ 빔 폭 : 수평16° 수직16° ▪ 커 넥 터 : UFL x2 MIMO ▪ 크 기 : 228*228*76 ▪ 무 게 : 1.7Kg ▪ Material: IP67,Aluminum die casting	▪ 주파수 범위 : 5150 – 5850MHz ▪ 이 득 : 25dBi X2 이중편파 ± 0,5 dBi ▪ VSWR GHz : ≤ 1,5 ▪ F/B Ratio-dB: 28 ▪ 임피던스Ω: 50 ▪ 빔 폭 : 수평11° 수직11° ▪ 커 넥 터 : UFL x2 MIMO ▪ 크 기 : 371*371*95 ▪ 무 게 : 4.3Kg ▪ Material: IP67,Aluminum die casting	▪ 주파수 범위 : 5150 – 5850MHz ▪ 이 득 : 14dBi X2 이중편파 ± 0,5 dBi ▪ VSWR GHz : ≤ 1,5 ▪ F/B Ratio-dB: 20 ▪ 임피던스Ω: 50 ▪ 빔 폭 : 수평45° 수직20° ▪ 커 넥 터 : UFL x2 MIMO ▪ 크 기 : 180*95*44 ▪ 무 게 : 0.27Kg ▪ Material: IP65 UV플라스틱

N5S 무선브리지 사양서

1. N5S의 무선 사양은 X5NM과 동일
N5S는 N5를 섹터 안테나에 부착한 제품이며 근거리 3Km 이내의 장치와 1:N 또는 중계용으로서 다중 접속AP로 운용한다.

가. 본체는 IP-67규격 다이케스팅 케이스
나. 안테나 및 본체를 쉽게, 다양한 각도 조정이 가능한 알루미늄 다관절 브라케트를 사용한다.
다. RJ-45포트 이더넷 커넥터 IEC기준 사용.
라 무선장치의 전원은 기본적으로 DC24V PoE로 구동되나, 태양전지 및 배터리로 구동하기 위해서 DC12V~ DC28V으로도 작동되며 용도에 따라 DC인젝터를 공급한다.
마. 장치를 고정하는 알루미늄 다관절 브라케트를 수직, 수평 POLE등 다양한 위치에도 고정할 수 있으며 브라켓 방향 조정은 70mm의 POLE에 고정할 수 있다.
바. 무선장치는 통신이 가능하도록 먼저 셋팅하고, 그 후 POLE에 고정하여 4단계 고휘도 LED RSSI상태를 모니터링 한다.
사. 무선장치는 육안으로 장치의 동작상태를 확인하기 위하여 LAN접속용 LED램프, 전원LED 램프 등이 부착되어 있다.
아. 스마트 폰, 노트북에서 검색되지 않는 주파수 사용이 가능하다.
자. ESD16Kv. IEC61000-4-2(ESD) 기준 준수.

2. 제원
- 데이터 암호화: 본체 4중 보안. Hardware based AES, 국정원 인증 **ARIA,SEED, 보안1등급 VSL1** 탑재(외장형 선택품목)
- 암호화 모듈은 유지보수 및 펌 웨어 업로드와 관리가 용이하도록 외장용으로 설치한다(제품 내장 장착 가능)
- 동작온도: -40°C (-40 F) ~ +85°C (+185 F)
- 습기: 0 ~ 90 % (non-condensing)
- 전원: POE 24 VDC, (DC12V~28V 지원)
- 전원입력: 100 – 240 VAC
- 소비전류: 7.5 W

N5S 무선안테나 사양서

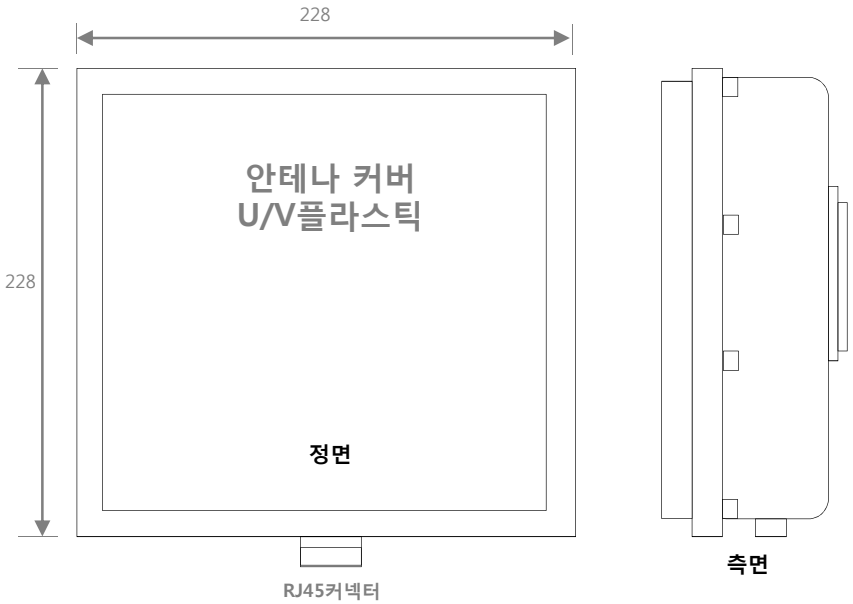
1. 지향성 이중편파 섹터 안테나

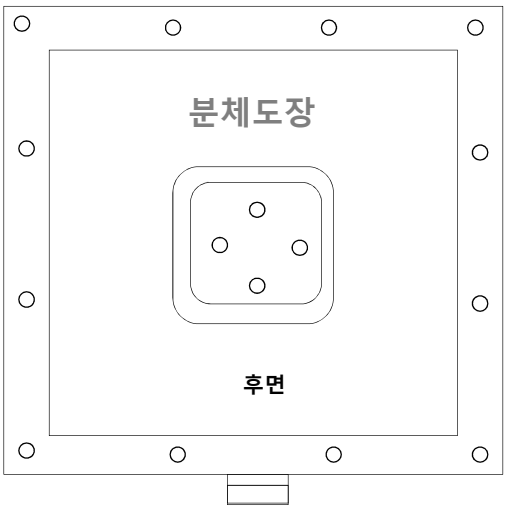
1) 기능
무선브리지의 다중입출력 이중편파를 사용한 안테나.

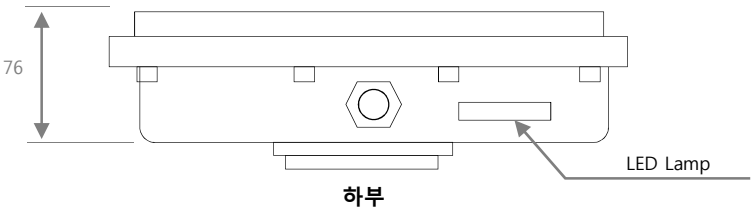
2) 특성
- 주파수 범위 : 5150 – 5850MHz
- 이 득 : 19dBi X2 이중편파 ± 0,5 dBi
- VSWR GHz : ≤ 1,5
- F/B Ratio-dB: 25
- 임피던스Ω: 50
- 빔 폭 : 수평120° 수직5°
- 커 넥 터 : UFL x2 MIMO
- 크 기 : 700*133*95
- 무 게 : 2.9Kg 브라켓 제외

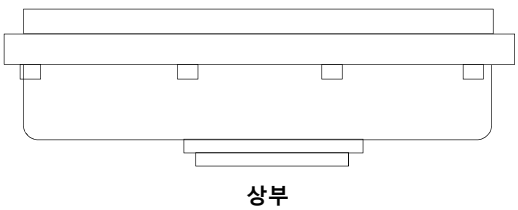
X5NM무선브리지 전체 도면

부식방지를 위한 고온 180℃ 가열한 무광 특수 분체도장



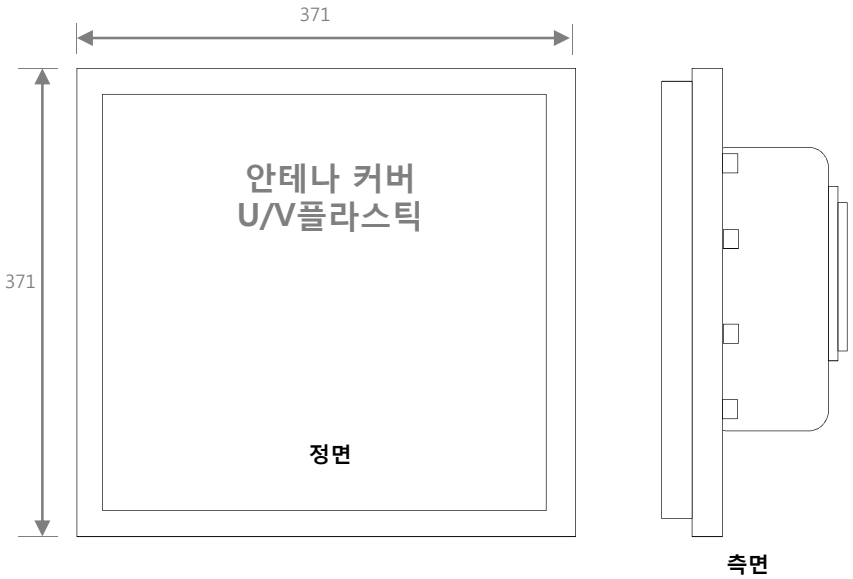


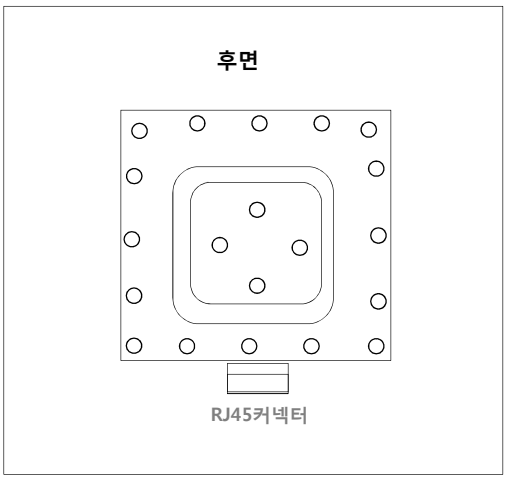


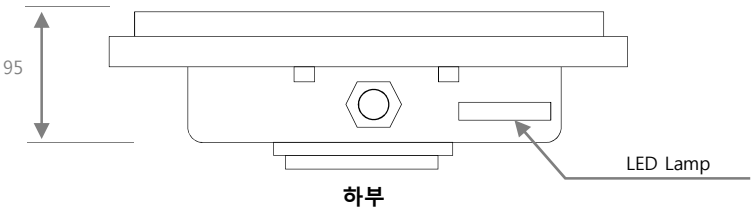


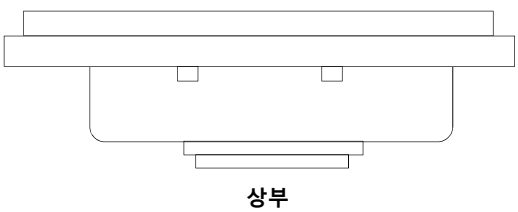
X525무선브리지 전체 도면

부식방지를 위한 고온 180℃ 가열한 무광 특수 분체도장

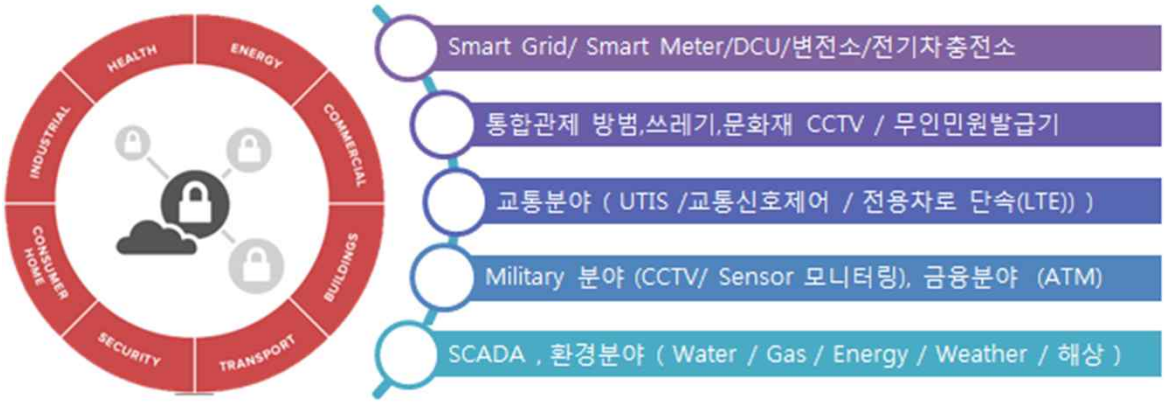








Model: DUSS　　국가정보원 KCVMP검증된 국산 암호화 ARIA, SEED 탑재



암호화 모듈은 성진알에프에서 공급하는 모든 무선브리지에 적용되며 모듈타입으로 외장형으로 착 탈이 쉽고 무선구간에서 강력한 5단계의 보안 및 암호화를 지원합니다.

■검증번호: CM-111-2021.3　■보안등급: 1등급 VSL1　■S/W명: KMULiB V2.0　■H/W명: DUSS

[무선구간의 강력한 5중화 보안적용]

1차 무선장비에서 기본 암호화 AES128bit (N5, N5S, X5NM, X5NB, X525)

2차 무선장비에서 네트워크 관련 보안설정 (N5, N5S, X5NM, X5NB, X525)

3차 오픈 포트 차단설정 (N5, N5S, X5NM, X5NB, X525)

4차 바이러스 침투 차단설정 (N5, N5S, X5NM, X5NB, X525)

5차 종단간 구간암호화를 위한 검증필암호모듈(CM-111-2021.3) 적용

[제품특징]

- 암호 알고리즘 최적화로 소형화 구현
- 대용량(영상정보) 데이터 실시간 암호화 처리가능
- 국제 표준 암호 AES선택가능
- IP계층 보안터널 구성
- 공공기관 보안적합성 만족(KCMVP 검증필암호모듈) 사용
- 대칭 키, 공개 키 기반 상호인증 지원으로 안전성 확보
- 소형 시설물 및 단말장비에 적합
- 안전성이 뛰어난 키 유도함수 알고리즘 사용
- 난수 기반 양방향 인증으로 Rogue 단말 차단
- 홀로그램 스티커 봉인을 통한 물리적 보안
- 모듈타입으로 쉽게 착/탈 및 유지보수와 업그레이드 용이
- 성진알에프에서 공급하는 전 제품 및 타사 제품에도 적용 가능

[보안등급]
시험기준(KS X ISO/IEC 24759)의 보안영역 중 본 암호모듈에 해당하는 10개의 영역 모두 보안등급 VSL1을 만족한다.

시험영역	보안등급	시험영역	보안등급
암호모듈 명세	1	암호모듈포트와 인터페이스	1
역할, 서비스 및 인증	1	유한상태모델	1
물리적 보안	N/A	운영환경	1
암호 키 관리	1	설계보증	1
자가 시험	1	암호모듈 보안정책	1
기타 공격에 대한 대응	1	전자파 간섭/전자기 적합성	N/A

[사용목적]
유무선용 데이터 암호장비

[주요기능]
Ethernet port와 Serial port로 입.출력되는 데이터를 KCMVP 검증 암호모듈을 적용하여 암.복호하는 장비로서 중요 시설물의 데이터를 보호할 수 있다.

[활용분야]
① 임대 망을 사용한 시설물 데이터 전송
② 교통, 방범, 방재용 CCTV 영상정보 전송
③ 공공기관의 센서데이터 등과 같은 공공정보 전송
④ 중요 시설물의 데이터 전송
⑤ 일반 VPN의 암호화를 필요로 하는 구간 암호화
⑥ 재택근무 또는 출장 시 외부에서 인터넷전화 또는 PC를 사용

■ 암호화 장비 사양서

암호 모듈	국가사이버안전센터 검증필 획득한 검증필암호모듈 탑재 (KMULiB v2.0, CM-111-2021.3)
암호모듈 규정	2015년 8월 개정된 신 규정 검증 기준을 통과한 검증필암호모듈 탑재
검증필 보호함수	ARIA(128, 192, 256), SEED(128), LEA(128, 192, 256)
	ECB, CBC, CTR, CCM, GCM
	SHA-224, SHA-256, SHA-384, SHA-512
	HMAC, CMAC, GMAC
	RSAES(2048, 3072)
	ECDSA(p-224, p-256), ECKCDSA(p-224, p-256)
	DH(2048, 224), ECDH(p-224, p-256)

PART	SPEC
CPU	Core Processor 800MHz 이상
Memory	Mobile DDR SDRAM 256MB X 1, EMMC 8GB X 1
RS-232	RS-232/485 겸용 Port 2EA
ETHERNET	GIGA bit RJ-45 Port 2EA
POWER	DC12V (DC JACK ø2.0)
Dimensions	78mm(W) x 111mm(H) x 23mm(D)
Operation Temp	-30℃ ~ +80℃
Throughput	암/복호화 성능 100Mbps 이상

■ 암호모듈 탑재 내역

탑재된 검증필암호모듈 소개

암호모듈명	검증번호	개발사	모듈형태	검증일	효력만료일
RTCrypto_v1.0	CM-114-2021.3	리턴트루(주)	S/W 라이브러리	2016-03-31	2021-03-31
SECUI CRYPTOU V1.0	CM-113-2021.3	(주)시큐아이	S/W 라이브러리	2016-03-31	2021-03-31
KEPCRYPTO V1.0.0	CM-112-2021.3	한국전력공사 전력연구원	S/W 라이브러리	2016-03-31	2021-03-31
KMULiB v2.0	CM-111-2021.3	국민대학교	S/W(라이브러리)	2016-03-09	2021-03-09

■ 암호모듈 알고리즘

검증필암호모듈 암호알고리즘 소개(http://service1.nis.go.kr)

분류		암호알고리즘	참조표준	
블록암호		SEED, ARIA, LEA, HiGHT	KS X 1213-1(2009) TTAS.KO-12.0004/R1 (2005) ISO/IEC 18033-3 (2010)	
블록암호 운영모드	기밀성	ECB,CBC,CFB,OFB,CTR	KS X 1213-2 (2009) TTAS.KO-12.0025 (2003) TTAS.KO-12.0131 (2010)	
	기밀성/인증	CCM, GCM		
해시함수		SHA-224/256/384/512	ISO/IEC 10118-3 (2004) ISO/IEC 10118-3 Amd 1 (2006)	
메시지 인증코드	해시기반	HMAC	ISO/IEC 9797-2 (2011)	
	블록기반	CMAC,GMAC	KS X 1213-2 (2009) ISO/IEC 9797-1 (2011) NIST SP 800-38D	
난수발생기		HASH_DRBG,CTR_DRBG, HMAC_DRBG	ISO/IEC 18031 (2005) NIST SP 800-90	
공개키암호		RSAES	ISO/IEC 18033-2 (2006)	2048, 3072
전자서명		RSA-PSS, KCDSA, ECDSA, EC-KCDSA	ISO/IEC 14888-2 (2008) ISO/IEC 14888-3 (2006) TTAS.KO-12.0001/R1 (2000) TTAS.KO-12.0015 (2001)	P-224, P-256
키 설정 방식		DH, ECDH	ISO/IEC 11770-3 (2008)	P-224, P-256

Model: DUSS 보안 제품 암호화 모듈

GiGa Ethernet + 232/485 + 검증필암호모듈 VPN 장비

방안 : 유선 VPN

- ✓ 유선 + 검증필암호모듈 + VPN + 서비스 에이전트
- ✓ Ethernet(10-100, 1G), Serial(232, 485)
- ✓ KC 인증필 / CE 인증필

iPhone 6 plus

DUSS의 KC 인증서

DUSS의 CE 인증서

PART	SPEC
CPU	Core Processor 800MHz 이상
Memory	Mobile DDR SDRAM 256MB X 1, EMMC 8GB X 1
RS-232	RS-232/485 겸용 Port 2EA
ETHERNET	GIGA bit RJ-45 Port 2EA
POWER	DC12V (DC JACK ø2.0)
Dimensions	78mm(W) x 111mm(H) x 23mm(D)
Oper. Temp	-30℃ ~ +80℃
Throughput	암/복호화 성능 200Mbps 이상
암호모듈	국가사이버안전센터 검증필 획득한 검증필암호모듈 탑재
암호모듈 규정	2015년 8월 개정된 신규정 검증기준을 통과한 검증필 암호모듈 탑재
검증필 보호함수	ARIA(128, 192, 256), SEED(128), LEA(128, 192, 256)
	ECB, CBC, CTR, CCM, GCM
	SHA-224, SHA-256, SHA-384, SHA-512
	HMAC, CMAC, GMAC
	RSAES(2048, 3072)
	ECDSA(p-224, p-256), ECKCDSA(p-224, p-256)
	DH(2048, 224), ECDH(p-224, p-256)

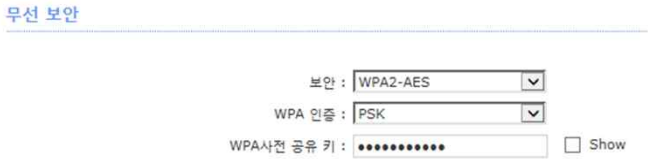
[무선브리지의 자체보안 강화]

1. 보안기본: 외부침입을 감지하여 차단.

2. 보안서비스: 포트침입을 감지하여 차단.

3. 바이러스 차단: 악성바이러스 감지하여 차단.

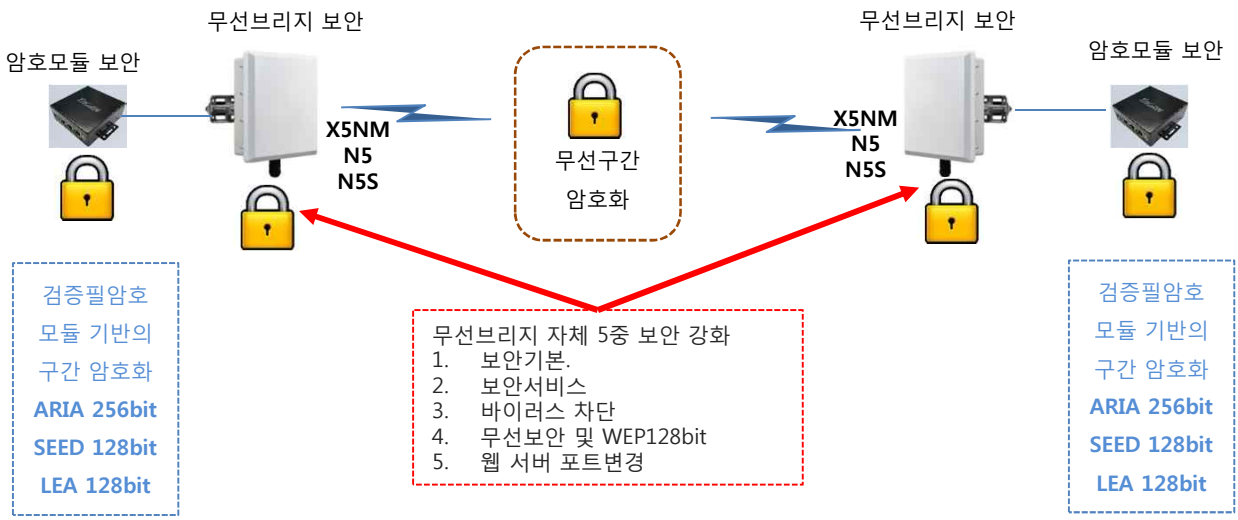
4. 무선보안: 무선보안설정



5. 무선보안: WEP 64bit / 128bit보안설정

5. 웹 서버 포트변경: 포트80을 변경하여 웹 접근 차단

[무선브리지와 암호모듈의 2중 보안 구성]



무선링크 1:N구성

[무선구간 강력한 5중화 보안 적용]

1차 무선장비에서 기본 암호화 AES128bit

2차 무선장비에서 네트워크 관련 보안설정

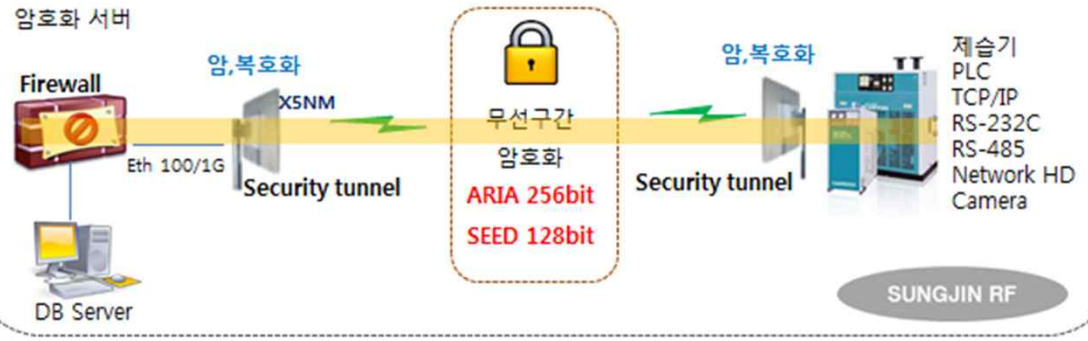
3차 오픈 포트 차단설정

4차 바이러스 침투 차단설정

5차 암호화 모듈 적용

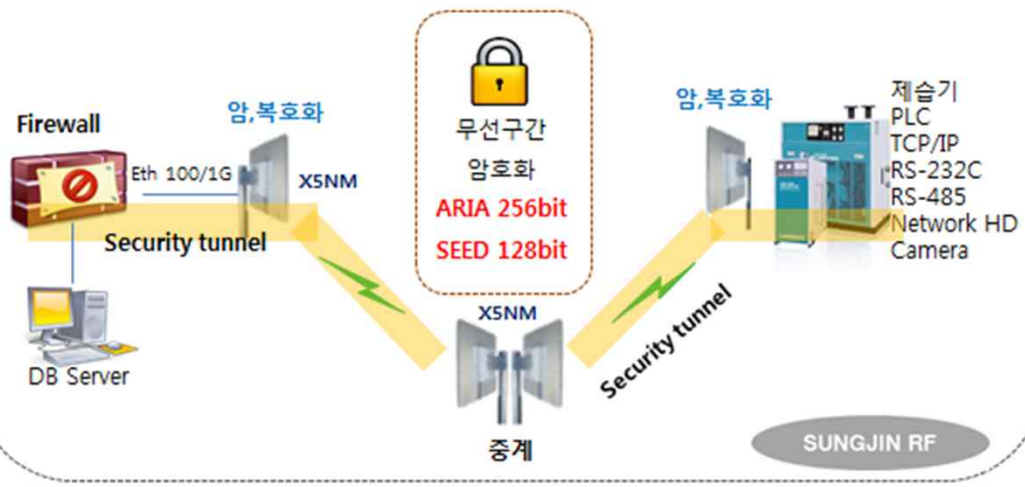
SUNGJIN RF

무선링크 1:1구성

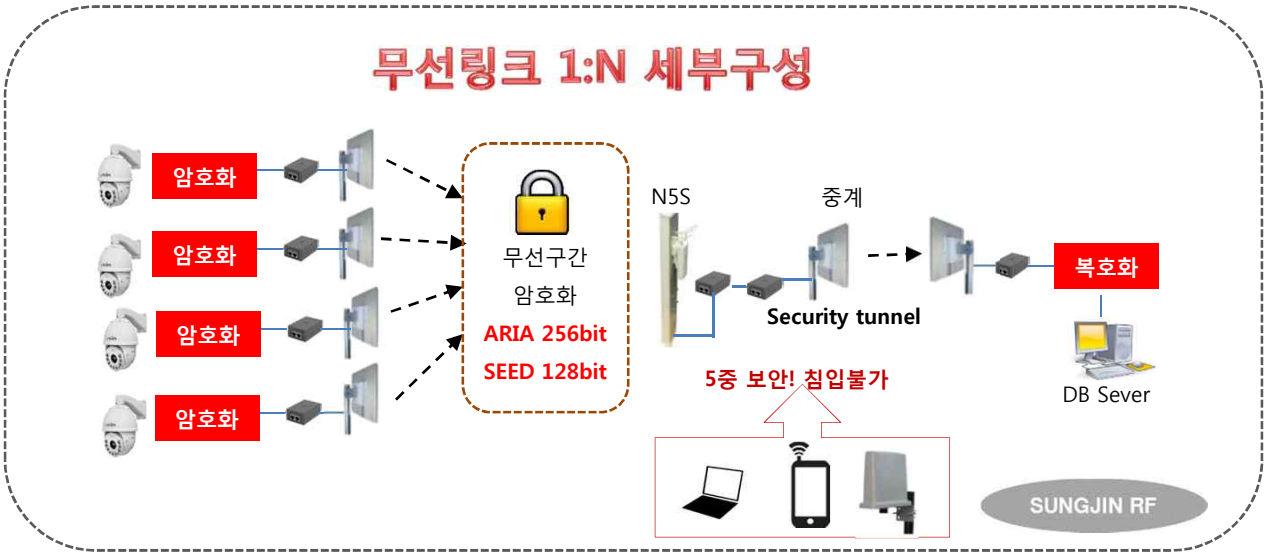


SUNGJIN RF

무선링크 중계 구성



SUNGJIN RF



■암호모듈 적용 제품

● 추천! A타입 암호화 모듈 외장형

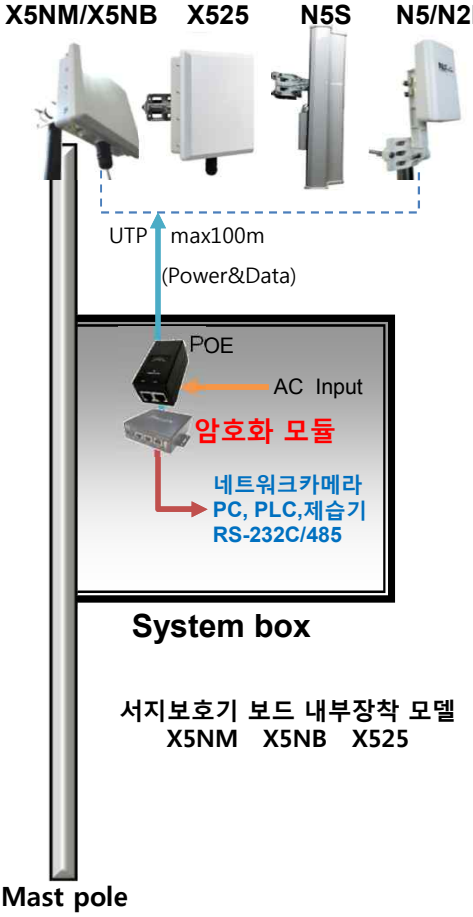
- 고장 발생시 교체가 쉽다.
- 유지보수, 점검이 용이하다.
- 암호모듈 펌 웨어 업그레이드 용이.
- 시리얼포트 사용 용이.

● 비 추천 A타입 암호화 모듈 일체형

- 고장 발생시 모두 교체.
- 유지보수, 점검 불편.
- 암호모듈 펌 웨어 업그레이드 불편.
- 시리얼포트 사용 불편.

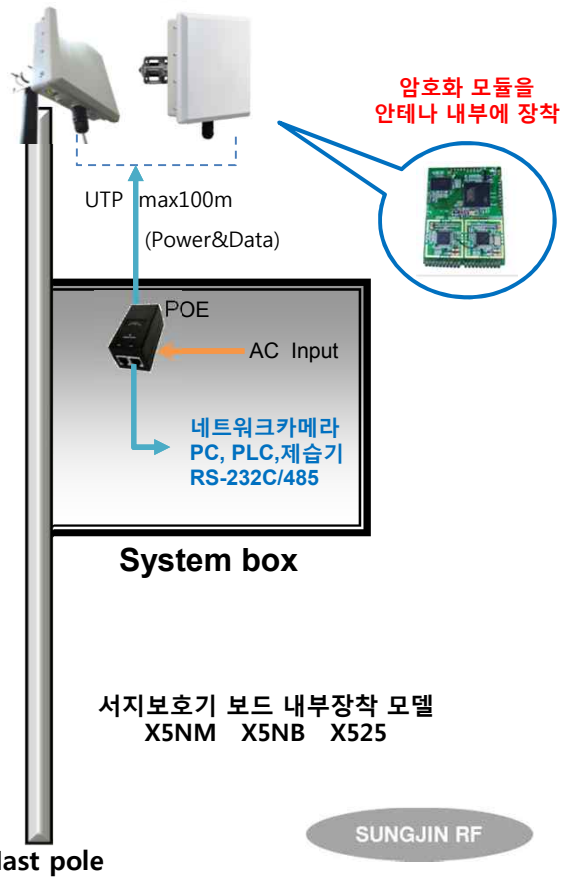
A- 암호모듈 외장용 적용장비 Wireless bridge

X5NM/X5NB X525 N5S N5/N2H



B- 암호모듈 일체형 적용장비 Wireless bridge

X5NM/X5NB X525



■ 부록1　　검증암호모듈 관련 법적 근거 (관계법령)

관계 법령 (전자정부법)[법률 제13459호, 2015.8.11., 타법개정, 시행 2016.2.12.]

전자정부법 제56조(정보통신망 등의 보안대책 수립 시행)

③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관,유통함에 있어서 위조, 변 조, 훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. **"전자정부"**란 정보기술을 활용하여 행정기관 및 공공기관(이하 "행정기관 등"이라 한다)의 업무를 전자화하여 행정기관 등의 상호 간의 행정업무 및 국민에 대한 행정업무를 효율적 으로 수행하는 정부를 말한다.
2. "행정기관"이란 국회、법원、헌법재판소、중앙선거관리위원회의 행정사무를 처리하는 기 관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다) 및 그 소 속 기관, 지방자치단체를 말한다.
3. "공공기관"이란 다음 각 목의 기관을 말한다.
   가.「공공기관의 운영에 관한 법률」제4조에 따른 법인、단체 또는 기관
   나.「지방공기업법」에 따른 지방공사 및 지방공단
   다. 특별법에 따라 설립된 특수법인
   라.「초、중등교육법」,「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교
   마. 그 밖에 대통령령으로 정하는 법인、단체 또는 기관

관계 법령(전자정부법 시행령)[시행 2016.2.12.] [대통령령 제26980호, 2016.2.12., 타법개정]

제2조(적용범위)

이 영은 **「전자정부법」**(이하 "법"이라 한다)에 따른 중앙행정기관(대통령 소속 기 관과 국무총리 소속 기관을 포함한다. 이하 같다)과 그 소속 기관, 지방자치단체 및 공공기관(이하 "중앙행정기관등"이라 한다)의 업무에 대한 전자적 처리에 적용한다.(개정 2014.7.28)

제69조(전자문서의 보관.유통관련 보안 조치)

① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관、유통할 때에는 법 제 56조 제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.

1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입、운용
2. 전자문서가 보관、유통되는 정보통신망에 대한 보안대책의 시행

② 행정기관의 장이 제1항의 보안조치를 이행하는 경우에는 미리 국가정보원장에게 보안성 검토를 요청하여야 한다.

■ 부록2 암호기술 적용의 필요성(관계법령)

관계 법령 (지식경제부고시 제2012-129호)

지능형전력망 정보의 보호조치에 관한 지침(지식경제부 고시 제2012-129호, 2012.6.20. 시행) 산업통상자원부 고시

✦ 목적: 지능형전력망의 구축 및 이용촉진에 관한 법률 제26조제3항에 따라 지능형전력망 정 보의 신뢰성과 안전성을 확보하기 위해 지능형전력망 사업자가 준수해야 할 보호조치의 세부 적 기준을 정함

✦ 정의

-지능형전력망 정보: 지능형전력망의 구축 및 이용을 위한 광 또는 전자적 방식으로 처리되어 부호, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료 또는 지식

-지능형전력망사업자: 전력망의 구축 및 이용에 관한 재화 또는 지능형전력망을 이용한 서비스를 제 공하는 사업으로서 다음 중 하나에 해당하는 사업을 영위하는 자

✓ 지능형전력망 기반 구축사업 **✓ 지능형전력망 기기 및 제품 제조사업** **✓ 지능형전력망 서비스 제공사업**

✦ 정의

-지능형전력망 기반구축사업자: 지능형전력망을 이용하여 전기를 공급하거나 전력계통의 운영에 관한 사업을 수행하는 송전사업자, 배전사업자, 구역전기사업자, 한국전력거래소

-지능형전력망 서비스제공사업자: 지능형전력망을 이용한 서비스를 제공하는 수요반응 관리서비스 제공사업, 전기차 충전 서비스 제공사업 또는 기타 서비스 제공사업 수행하는 자

-정보통신망: 전기통신사업법 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집.가공.저장.검색.송신 또는 수신하는 정보통신체계

-지능형전력망 기기: 지능형전력량계, 데이터수집장치, 센서, 충전기, 신 재생 발전원, 소규모 발전 기 등 지능형전력망에 연결되는 기기 또는 설비

-정보보호시스템: 정보의 수집.가공.저장.검색.송신 또는 수신 중에 정보의 유출, 위조, 변조 등을 방지하기 위한 하드웨어 및 소프트웨어

✦ 적용범위 : 이 지침은 지능형전력망 사업자에 대하여만 적용한다.

✦ 제7조(무선통신망 보안)

① 지능형전력망 기반구축사업자는 운영실과 정보통신실 내부 통신에 대해 무선통신망을 사용 하지 못함

② 지능형전력망 기반구축사업자는 지능형전력망 기기와 정보통신실 간 무선통신망(무선랜, 3G, 근거리무선통신 등) 이용을 최소한으로 이용하여야 한다.

1. 무선통신내용 암호화 **2. 무선통신 사용자 신원 및 권한 확인**

✦제10조(암호모듈)

① 지능형전력망 사업자는 지능형전력망 시스템에 사용되는 암호모듈로 국가사이버안전센터 IT보안인증 사무국의 검증필 암호모듈을 사용하여야 한다.

② 지능형전력망 시스템에 사용되는 암호알고리즘은 보안강도 128비트 이상을 만족해야 한다.

✦제12조(지능형전력망 시스템 인증)

① 지능형전력망 사업자의 지능형전력망 시스템은 중간자 공격, 스니핑 공격을 차단하기 위하여 다른 시스템과의 통신시 상호인증을 하여야 한다.

② 지능형전력망 사업자의 지능형전력망기기는 다른 기기 또는 지능형전력망 시스템과 통신시 상대방을 상호인증 하여야 한다. 이 경우 지능형전력망 시스템은 상호인증한 상대방에 대해서 만 통신을 허용하여야 한다.

✦제13조(지능형전력망 기기 통신보안)

지능형전력망 사업자의 기기는 정보통신실 등 다른 기기 및 지능형전력망 시스템과의 통신에 있어서 다음 각 호의 보안서비스를 제공하여야 한다.

1. 통신내용이 위.변조되거나 도.감청되는 것을 방지하는 기능 제공
2. 과금과 관련된 통신(검침정보, 전력판매단가 등)에 대해서는 부인방지 기능 제공

보안적합성 vs. CMVP 검증 vs. CC인증

✦보안적합성

- 보안적합성 검증은 국가정보통신망의 보안수준을 제고하기 위해 국가.공공기관이 도입 하는 정보보호시스템에 대해 안전성을 검증하는 제도
- 국가.공공기관은 보안기능이 포함된 IT 제품 도입 시 국가사이버안전센터에 보안적합성 검증을 신청해야 하며, 검증결과 발견된 취약점을 제거한 뒤 운용
- 국가사이버안전센터가 필요성을 인정하는 정보보호시스템의 경우 안전성이 확인된 CC 인증 제품을 도입
- IT제품에 중요자료 저장.소통을 위한 암호기능이 포함될 경우 국가사이버안전센터가 안 전성을 확인한 검증필 암호모듈을 탑재

✦CMVP (Cryptographic Module Validation Program, 검증필암호모듈제도) = 개발 기관이 신청

✦CC (Common Criteria, 공통평가기준) =개발 기관이 신청

✦CC인증 제품 유형(24종) (www.itscc.kr)

- 침입차단시스템, ~~침입탐지시스템~~, 침입방지시스템(IPS), 통합보안관리 제품
- 웹 응용프로그래밍 침입차단 제품
- DDoS 대응 장비, 서버 접근통제 제품, DB 접근통제 제품
- 네트워크 접근통제 제품, 인터넷전화 보안 제품
- 무선침입방지시스템, 무선랜 인증 제품, 스팸 메일 차단시스템
- 네트워크 자료유출방지 제품, 호스트 자료유출방지 제품
- 안티바이러스 제품, ~~PC 침입차단 제품~~, 패치관리시스템
- 소프트웨어기반 보안USB, ~~매체제어 제품, PC 가상화 제품, 서버 가상화 제품~~
- 가상화 제품, 망간 자료전송 제품, 스마트카드, 복합기 완전삭제
- 소스코드 보안약점 분석도구, 스마트 폰 보안관리 제품
- 가상사설 망(VPN) 제품

- **가상사설 망.보안USB 등 중요자료 소통.저장을 위한 암호사용 시 검증필 암호모듈 탑재 필요**
- 지능형전력망에 필요한 장비들은 위의 제품 유형 중 어디에 해당?

✦CMVP검증 제품군(8종)

- 메일 암호화
- 구간 암호화
- ~~PKI 제품~~
- 통합인증(SSO)
- 디스크 파일 암호화
- 문서 암호화(DRM 등)
- ~~키보드 암호화 모듈~~
- 하드웨어 보안 토큰
- DB 암호화
- 기타 암호화

✦상기 제품은 CC는 해당사항 없음

✦검증필 암호모듈은 필수임 (출처 : http://service1.nis.go.kr)