Cyber Security Solution & Service

MDS 인텔리전스

CSMS인증을 위한 표준 ISO/SAE 21434에서
암호 키 및 인증서 관리를 요구

● UNECE WP.29_ List of vulnerability or attack method related to the threat

4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short **encryption keys** and long period of validity enables attacker to break encryption
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems
			26.3	Using already or soon to be deprecated **cryptographic algorithms**

● ISO 21434 [RQ-10-06]

[RQ-10-06] If specific procedures are required to ensure cybersecurity in post-development phases, these cybersecurity requirements shall be specified and allocated to the relevant entities of the operational environment.

EXAMPLE 8: Table 1 provides example requirements and procedures to ensure cybersecurity in post-development phases including their allocation.

Table 1 - Example cybersecurity requirements for post-development

Requirement	During	Allocated to
secured management of the key store	production	system production
	maintenance	service and maintenance facilities/instructions
deactivation of debug interfaces	production	hardware production
deactivation of development functions	production	deployment finalization for software
procedures to delete personally identifiable information	operations	user manual

● ISO 21434 [RQ-10-10]_use of encryption & Sercure Storage

Requirement: HSM 또는 Secure Memory 적용

펌웨어 / 바이너리의 전자 서명 및 암호화에 사용되는 암호 키는 HSM 또는 Secure Memory에 보관되어야 함.

Requirement: Secure Flash 2.0

OEM의 암호 키 유출 또는 손상으로 인해 유효하지 않은 업데이트를 허용하지 않도록 암호 키 생애주기 관리 필요
제어기 펌웨어 / 바이너리에서 암호 키를 추출할 수 없도록 해야 함.
전자 서명 및 암호화 시 안전한 암호 키/알고리즘 적용

Requirement: Secure Debug

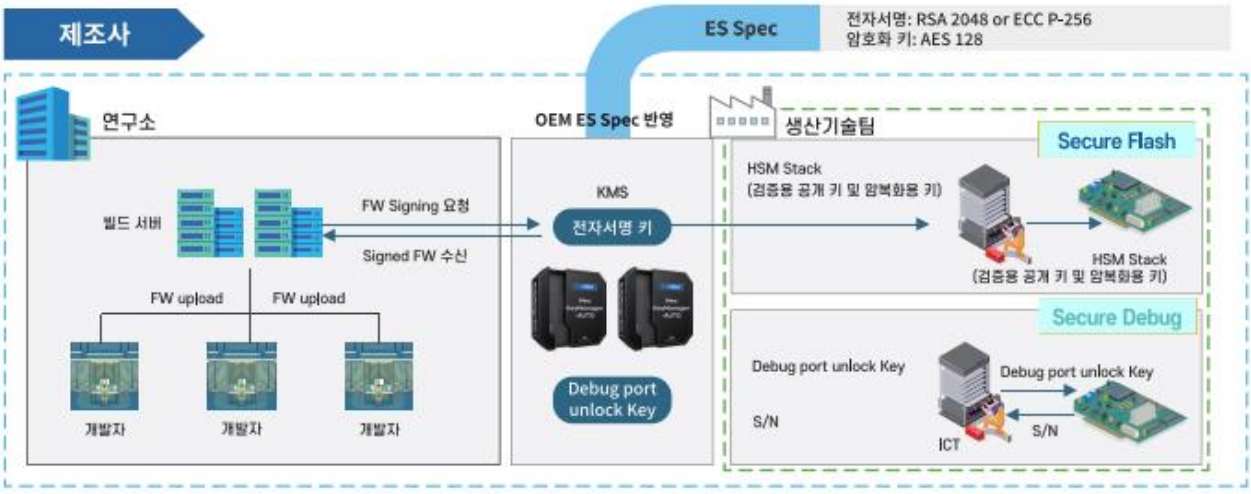
제어기 시리얼 번호 별 JTAG PW를 생성하여 제어기에 주입함으로써 JTAG 포트를 Disable

OEM Requirements

- Secure Debug 및 Disable 로직 적용 패스워드는 256bit 이상, 랜덤 값을 사용하며 인가된 최소 인원만 관리, KMIP 준수
- 지정 알고리즘과 자체 패스워드 변환 규칙을 사용, 제어기별 비밀번호 생성 및 적용 후 안전한 전달 방법 확보

Management Requirement

- When defining cybersecurity specifications, cybersecurity implications of post-development phases can be considered, e.g. secure management of the key store; deactivation of debug interface; procedures to delete personally identifiable information .. ISO_SAE 21434



Secure Flash

자동차의 전자 제어 장치(ECU, Electronic Control Unit) 및 기타 시스템에 적용되어, 자동차의 사이버 보안을 강화하고, 외부 공격으로부터 차량을 보호해야 합니다.

암호화 및 디지털 서명

업데이트된 펌웨어가 Flash에 저장되기 전에 암호화되고 디지털 서명을 합니다.
이는 외부에서의 불법적인 업데이트를 방지하고, 안전한 펌웨어가 사용되도록 합니다.

보안 플래시 메모리

일반적으로 Secure Flash는 특수한 보안 기능을 갖춘 플래시 메모리를 사용합니다.
이러한 메모리는 외부에서의 액세스를 제한하고 데이터의 안전한 저장을 보장합니다.

Secure Debug

디버그 용도의 JTAG, UART, ADB 포트는 디버그 포트 제한 원칙을 준수해야 합니다.

HSM 적용 여부

HSM 적용 여부에 따라 Secure Debug 적용 또는 MCU 업체 Debug Disable 로직 적용이 필요합니다 .

공통사항 JTAG의 경우

1) JTAG 커넥터 및 소자 미실장
2) Debug port Enable을 위한 password
   - 패스워드는 256bit 이상, 복잡도 있도록 설정해야 합니다.
   - 차종마다 다르게 설정하고, 유추 불가하도록 규칙성 제거해야 합니다.
   - 패스워드가 유출되지 않도록 철저하게 관리해야 합니다.

NeoKeyManager

암호 키 생명주기 관리	· 암호 키 생성·분배·저장·백업·복구·교체·폐기 · 암호 키 별 UUID 부여_직접적인 노출·유출방지	· ISO 27001, 전자금융 감독규정, · NIST, 국방 등 각종 암호화 규정 준수 · 다양한 자동차 OEM 및 부품사 납품
인증서 생명주기 관리	· 인증서 발급·재발급·폐기·검증 · 인증서 별 UUID 부여_직접적인 노출·유출방지	
상호 운용성	· KMIP, PKCS# 11 등 표준 프로토콜 지원 · **KMIP 호환 SDK** (C, C++, C#, Jave, Python 등) 제공 · 각종 암호화 솔루션 및 DB TDE(Oracle, Mongo DB 등) 연동지원	· 국제 키 관리 표준 프로토콜 호환성 평가 통과 및 OASIS에 등록 · 국내유일 KMIP기반 상용 KMS
물리적 보안	· **HSM(Hardware Security Module) 내장** · 생성된 암호 키의 안전한 저장 및 유출 방지 · 미 연방정부 정보처리 표준 FIPS 140-2 Lv3 인증 HSM 내장 · 국정원 검증을 획득한 암호 모듈(KCMVP) 탑재	· 보안인증 (FIPS, 국정원)
모니터링	· 접근권한 제어, 승인 프로세스 구축, 유효기간 만료일 · 알람·자동 갱신, 보안감사 로그 자동생성, 감사관리 · 승인 보고서 자동 생성 · 웹 기반 관리콘솔 제공	· 지속적인 CSMS 준수 사항 관리
협업조직 관리	· 외부 키 관리 솔루션(KMS)과 연동·승인 관리 · 회사의 조직 구조(Hierarchy) 반영한 **그룹/권한 설정** · Tier·차종·제어기 별 암호 키 접근 제어	· 상하위 KMS, OEM/Tier 간 **그룹 관리** 다수의 암호 키 관리

NeoKeyManager는 MDS인텔리전스에서 자체 개발한 전용 **어플라이언스 타입의 KMS로 HSM이 탑재된 솔루션입니다.**

● HSM Spec.

암호화 API	· PKCS#11, Java(JCA/JCE), Microsoft CAPI 및 CNG, OpenSSL
암호화	· Full Suite B 지원 · 비대칭: RSA, DSA, 디피헬만(Diffie-Hellman), 명명·사용자 정의· 브레인풀(Brainpool) 곡선 포함 ECC (타원 곡선 암호 - ECDSA, ECDH, Ed25519, ECIES), KCDSA 등 · 대칭: AES, AES-GCM, Triple DES, ARIA, SEED, RCS, RC4, RC5, CAST 등 · 해시/메시지 다이제스트/HMAC: SHA-1, SHA-2, SM3 등 · 키 유도: SP800-108 카운터 모드 · 키 래핑: SP800-38F · 난수 생성: NIST 800-90A 준수 CTR-DRBG와 함께 HW 기반 트루 노이즈 소스를 사용하여 AIS 20/31에서 DRG.4까지 준수하는 설계 방식으로 대체됨
Size	로 프로파일 PCIe 카드, 2.74" x 6.57" x .074" (69.6mm x 167mm x 187mm)
인증	FIPS 140-2 레벨 3 - 비밀번호 및 다중 요소(PED)

● Server Spec.

CPU	Intel Xeon E-2334 3.4GHz, 8M Cache, 4C/8T, Turbo (65W), 3200 MT/s
Memory	2ea * 8GB UDIMM, 3200MT/s, ECC
HDD	2ea * 600GB Hard Drive SAS ISE 12Gbps 10k 512n 2.5in with 3.5in HYB CARR Hot-Plug
	2ea * 2TB Hard Drive SATA 6Gbps 7.2K 512n 3.5in Hot-Plug
NIC	PowerEdge R350 Motherboard with Broadcom 5720 Dual Port 1GB On-Board LOM, V2
Power	Dual, Hot-Plug, Redundant Power Supply (1+1), 600W
OS	CentOS 7.9

아시아 유일의 상호 운용성 **국제 표준(KMIP) 3.0 인증을 통해 타 시스템과의 효율적인 통합**을 이루며, **OEM과 Tier 그룹 간 관리도 가능**합니다.

● Before KMIP

● After KMIP

HSM (Hardware Security Module)

● 제품 구성

Network Type HSM

· Standard 1U 19" rack mount appliance
· 4 - Gigabit Ethernet
· 10G optical Ethernet option

PCIe Type HSM

· Low Profile PCIe card
· PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

ProtectServer 3+ 외장 HSM

보안이 강화된 네트워크 암호화 서버가 암호화, 서명 및 인증 서비스를 제공하여 기본 블록체인 알고리즘 지원을 비롯한 중요 애플리케이션을 보호하는 동시에 암호 키 침해를 방지합니다. 이중 스왑형 AC 전원 공급 장치는 고가용성, 비즈니스 연속성을 지원하며 전원 공급 장치 기능과 현장 유지 관리 작업을 처리할 수 있는 유연성을 제공합니다.

ProtectServer 3 외장 HSM

변조 방지 보안 기능을 갖춘 강철 ProtectServer 3 외장 HSM 장치를 이용하면 물리적·논리적 공격을 방지할 수 있습니다.

ProtectServer 3 PCIe HSM

PCI Express x4 호환 카드는 다양한 시스템 요건을 충족하기 위해 다양한 성능 수준으로 제공됩니다.

● HSM 인증 현황

국제 CC 인증

FIPS 140-2 Lv3 인증

● HSM의 안전성 수준 [NeoKeyManager FIPS 140-2 Lv.3 인증 보유]

Level 1	· 기본적인 보안 요구 사항에 대해 평가를 받은 제품 · 물리적 보안성에 대해서는 요구되지 않고 주로 소프트웨어적 암호화 모듈에 대한 평가
Level 2	· 암호화 모듈 및 하드웨어 부문에서 보안 적합성 평가 실시 · 물리적인 장비 해체 방지 등에 대한 대책이 강구되어야 함 · 침입자가 접근하면 흔적이 남도록 함
Level 3	· 제품 분해를 막기 위한 단편적 방편 및 적극적인 대책까지 제시되는 지 평가 (침입자가 접근하면 저장된 내용을 삭제) · 무단 접근과 같이 부당한 방법의 변경 또는 오용 감지 시 해당 장치는 주요 보안 변수를 삭제
Level 4	· 물리적인 보호가 어려운 환경을 고려해 평가 · 클라우드 등 새로운 키 관리 서비스나 제품에 적용하기 위한 레벨 · 물리적/전기적 접근 시도 및 외부 환경 변화 감지 시 내용 삭제

HSE (High Speed Encryptor)

네트워크 암호화 장치

Thales Network Encryptor Series

탈레스의 SafeNet High Speed Encryptor 솔루션은 데이터 센터와 본사 간의 네트워크 트래픽부터 백업 및 재해 복구 사이트에 이르기까지, 사내 네트워크와 클라우드를 비롯하여 어디에서든 암호화가 가능한 단일 플랫폼을 고객에게 제공합니다.
탈레스의 포괄적인 네트워크 트래픽 암호화 솔루션은 L2, 3 암호화 방식을 사용하여 최상의 보안을 유지합니다.
지연 시간을 최소화하면서 최대 처리량을 보장하며, 고객의 데이터를 효과적으로 보호할 수 있도록 지원합니다.

SafeNet High Speed Encryptor 제품군

탈레스는 요구사항과 예산에 따라 기능을 적절히 구성할 수 있는 다양한 제품군의 SafeNet High Speed Network Encryptor를 제공하고 있습니다. 전 제품군은 상호 운용이 가능하며 단일 플랫폼을 사용하여 단일 고객 링크부터 분산형 네트워크까지 모두 중앙에서 관리할 수 있습니다. 각 encryptor는 최대 512건의 동시 암호화 연결을 지원할 수 있습니다. Hardware encryptor는 FIPS 140-2 Level 3 및 Common Criteria EAL +2, EAL 4+* 인증을 받았습니다

Thales CN4000 Network Encryptor Series

CN4000 시리즈는 기본형 네트워크 암호화 장치(10Mbps~1Gbps)는 작은 크기에 활용도가 좋을 뿐만 아니라, 네트워크 성능 저하 없이 보안을 제공합니다. 다목적으로 간편하며, 지사 혹은 원격 지원에 적합하며 네트워크 성능을 저해하지 않고도 비용 효율적인 고성능 암호화를 제공합니다.

SafeNet Ethernet Encryptor CN6000 Series

CN6000 시리즈의 Encryptor는 100Mbps ~10Gbps의 가변 속도 라이센스를 제공합니다. CN6140 모델은 멀티 포트 설계로 최대 40 Gbps (4x10Gbps)의 가변 속도 라이선스를 제공하여 높은 유연성과 비용 효과를 누릴 수 있습니다.

SafeNet Ethernet Encryptor CN9000 Series

초당 1천억 비트비트의 높은 보증성, 초저 대기 시간을 제공하여, 고품질의 안전한 암호화를 거친 데이터를 제공하는 CN9000 시리즈는 업계에서 가장 짧은 대기 시간 (< 2µs)으로 대용량(100Gbps) 데이터 보안을 제공합니다.

주요 특징

민감한 트래픽을 위한 강력한 보안

- 강력한 암호화와 함께 FIPS 140-2 레벨 3의 변조 방지 키 관리 기능을 제공
- 보안 통신 Suite B 암호화 알고리즘 (AES-256, ECDSA, ECDH 및 SHA512)의 사양 충족
- NIST 인증 난수생성기 키를 사용, 다중 테넌트 환경에서도 키 제어 가능

최대 성능과 높은 가용성

- 지연 시간이 거의 없으며 패킷 손실의 위험 없이 전이중 방식(FD)을 최대 속도로 작동
- 관리자에게 잠재적 문제를 조기 경고하는 기술 진단 기능을 제공
- 10Mbps~100Gbps의 네트워크 속도를 지원
- 하드웨어와 가상 솔루션 모두 제공 가능

차세대 고속 암호화 방식

- 암호화 민첩성을 갖추어 다양한 범위의 타원 및 개별 곡선에 맞는 맞춤형 암호화 지원
- 향후 변화에 따라 차세대 알고리즘 또는 맞춤형 알고리즘을 신속하게 배치 가능
- 데이터 전송 암호화에서 네트워크 독립 계층(레이어 2, 레이어 3 및 레이어 4) 및 프로토콜 비의존 데이터인 TIM(Transport Independent Mode)을 최초로 제공

MDSIT Academy (A-SPICE Provisional Assessor 교육)

개요

MDS인텔리전스에서는 **intacs® Certificated** Automotive SPICE Provisional Assessor 교육을 진행하고 있습니다. 본 교육을 통해 A-SPICE 요구사항에 대해 실무 적용 및 수행 역량을 확보하고 개발 간 IATF 16949 및 ISO 26262 프로세스를 준수하여 품질을 유지하기 위함입니다.

일 정 매달 변동 (기간: 5일)
장 소 MDS인텔리전스 본사 교육장(판교 / 상황에 따라 변동될 수 있습니다.)
비 용 365만원 (부가세 포함, 시험 응시료 1회 포함)
대 상 자동차 산업에 종사하는 시스템 및 소프트웨어 개발자, 테스트 엔지니어, PM, QC 등- 총 12명 (선착순 마감)
기 타 - 국내 유일의 한국어 교육
- 교육 교재 및 수료증 제공

커리큘럼

Day	Time	Details
Day 1	09:00 ~ 12:00	1-1 Introduction 1-2 The intacs® sheme 1-3 Motivation & Overview 1-9 Assenssment Skills & Techniques
	13:00 ~ 18:00	1-9 Assenssment Skills & Techniques 1-4 Rating 1-8 Assessment exercise "Project Management" (written scenario or role-plays)
Day 2	09:00 ~ 12:00	**Revision Day 1** 1-7 Assessment exercise "Project Management" (ctd.) 1-5 Overview Assessment Process
	13:00 ~ 18:00	2-1 PAM Overview 2-3 PAM details (Self Reading) 2-2 Assessment exercise CL1 (SWE.2, SWE.3) (written scenario or role-plays)
Day 3	09:00 ~ 12:00	**Revision Day 2** 2-3 PAM details (Self Reading) 2-2 Assessment exercise CL1 (SUP.8) (written scenario or role-plays)
	13:00 ~ 18:00	2-3 CLs 2 and 3 2-4 Ration Guidelines 2-5 Assessment exercise CLs 2 and 3 (SWE.2) (written scenario or role-plays)
Day 4	09:00 ~ 12:00	**Revision Day 3** 2-5 Assessment exercise CLs 2 and 3 (SUP.8) (written scenario or role-plays)
	13:00 ~ 18:00	2-5 Assessment exercise CLs 2 and 3 (SUP.8) (written scenario or role-plays) 2-2 Assessment exercise CL1 further processes (SWE.5, SYS.5) (written scenario or role-plays) Sample Exam (voluntary)
Day 5	09:00 ~ 12:00	**Revision Day 4** 2-5 Assessment exercise CLs 2 and 3 (SWE.5, SYS.5) (written scenario or role-plays)
	13:00 ~ 18:00	2-5 Assessment exercise CLs 2 and 3 (SYS.5) (written scenario or role-plays) Examination setup 2:00 - 2:30pm Exam 2:30 - 3:30 pm Course close & feedback 3:30-4:00 pm

신청 및 문의

교육 신청
- 교육 확정 메일 수신 후, 교육비를 입금하면 교육 참여가 확정됩니다.
- 본 교육에 소요되는 라이선스 및 교재 그리고 다른 교육 희망자에게 피해가 발생하지 않도록 노쇼 방지를 위해 불참 시 납부한 교육비는 환급되지 않습니다.

교육 문의 **담당자** 이승한 과장 **Tel** 031-601-4311 **E-mail** seunghan.lee@mdsit.co.kr

주요고객

HYUNDAI MOTOR GROUP · HYUNDAI MOBIS · HYUNDAI AutoEver · SL Corporation · SL TENNESSEE
LG전자 · LG이노텍 · LG에너지솔루션 · DAEWOO ELECTRONIC COMPONENTS · LS오토모티브
AMO AMOSENSE · AMO AMOVINA · Motonic · 계양전기 · COAVIS
BMW · JAGUAR

NeoKeyManager	자동차 사이버 보안 요구사항 대응을 위한 편리한 키관리 시스템(KMS)
HSM	안전한 키 분리 보관을 위한 FIPS 140-2 Lv3 인증받은 글로벌 No.1 하드웨어 보안 모듈
HSE	안전한 네트워크 암호화 통신부터 백업 및 재해 복구에 이르기까지 사내 네트워크와 클라우드 등 어디서든 암호화가 가능한 단일 플랫폼
A-SPICE Provisional Assessor 교육/심사	A-SPICE 요구사항에 대한 이해와 실무 적용 및 수행 역량을 확보하고, IATF 16949 / ISO 26262 프로세스를 준수하여 품질을 유지하기 위한 국내 유일의 한국어로 진행하는 intacs® 인증 교육

MDS 인텔리전스
E. nkm_biz@mdsit.co.kr
T. 031-601-4311