ECU의 디지털 면역 체계 확보

네트워크로 연결된 차량의 IT 보안은 ECU 제조 단계에서부터 시작되어야 합니다.

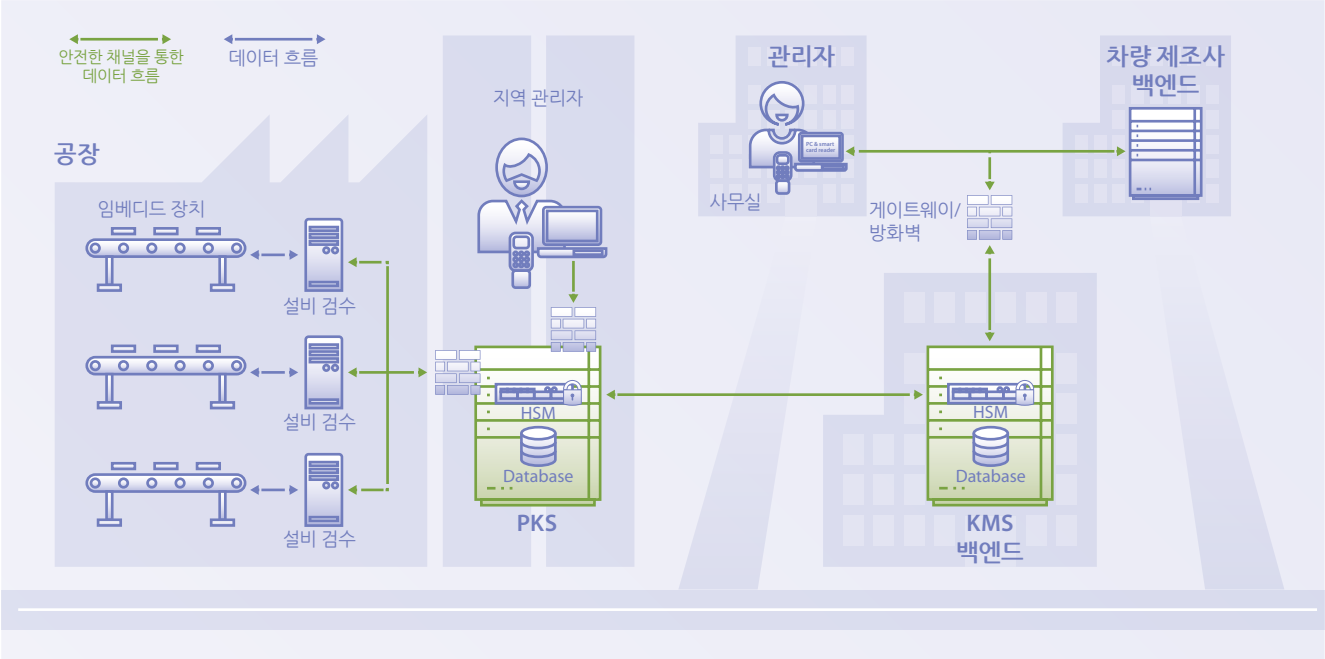
안전한 데이터 교환에 필수적인 암호화 키 관련정보를 ECU(Electronic Control Unit)에 저장하는 과정에서 보안을 확보하면서도 ECU 요구사항을 충족시킬 수 있는 방법은 무엇일까요? 정답은 백엔드의 중앙집중형 키 관리(KMS) 와 분산형 프로덕션 키 서버(PKS)로 구성된 통합 솔루션입니다.

사이버 공격으로부터 차량을 보호할 때 Control Unit은 문자 그대로 제어 장치로써 핵심적인 역할을 담당합니다. ECU는 암호화 키가 있어야만 자체 인증할 수 있으며, ECU는 자체 인증이 되어야만 전기 시스템 내의 데이터 교환 및 외부와의 데이터 교환이 가능합니다. 이 때 특히 어려운 과제는 다양한 차량 플랫폼을 위한 ECU들은 처음부터 차량제조업체(OEM)별 고유한 키 관련정보와 인증서를 제공 받아야 한다는 점입니다. ECU 제조사가 ECU 생산할 때부터 이러한 키 관련정보와 인증서를 제공받는 것이 가장 이상적입니다.

차량제조업체 키 관련정보의 안전한 배포

이에 대한 효과적인 솔루션은 전통적인 키 관리 솔루션(Key Management Solution, KMS)을 중앙 백엔드로 두고 여기에 분산형 프로덕션 키 서버(Production Key Server, PKS)를 결합시키는 것입니다. PKS는 생산 설비에 설치되어 KMS와 통신하게 됩니다. 차량제조업체가 이러한 솔루션을 이용하면 차량제조업체의 특수 ECU에 자체적인 키 관련정보를 저장하는 과정을 ECU 공급업체의 기존 생산 인프라에 완벽히 통합시킬 수 있기 때문에 큰 장점을 누릴 수 있습니다.

첫째, 차량제조업체는 키 관련정보가 담긴 데이터 패킷을 KMS에 공급합니다. 키 관련정보는 중앙에 저장 되었다가 요청이 들어올 경우 안전한 데이터 교환을 통해 생산 현장으로 분배되고, 바로 사용 가능한 상태로 PKS에 저장됩니다. (그림 참고)



키 관리 솔루션(KMS) 및 프로덕션 키 서버(PKS)를 통한 통합 키 배포 및 주입 합니다.

설비 검수(EOL Tester)를 통한 키 주입

키 관련정보는 ECU 생산 현장에서 관련된 설비 검수 단계에 맞춰 ECU에 저장됩니다. 설비 검수는 공장의 PKS에서 개별 키 패키지를 불러내어 ECU가 생산되는 동안 마치 '디지털 예방주사'처럼 개별 ECU에 '주입'합니다. 동시에 PKS는 각 ECU에 어떠한 암호화 키가 주입 되었는지 기록합니다. 마지막으로 PKS는 요청을 받은 경우 백엔드의 중앙 KMS를 통해 소위 검증 파일을 생산 현장으로부터 차량제조업체로 보냅니다. 이를 통해 차량제조업체는 ECU에 올바른 암호화 키 관련정보가 저장 되었는지 확인할 수 있게 됩니다.

솔루션의 장점은 높은 수준의 보안과 가용성입니다.

온라인에 연결되어 있지 않아도 안전하게 저장 가능

이번 솔루션의 장점은 높은 수준의 보안과 가용성입니다. PKS의 자체 보안 소프트웨어와 하드웨어 보안 모듈(HSM)은 인가되지 않은 접근으로부터 PKS를 보호합니다. 또한 PKS는 지속이 아닌 필요한 시점에 따라 백엔드에 접속하여 데이터를 동기화하거나 업데이트를 수행하며, 충분한 여유분의 암호화 데이터를 확보합니다. 즉, PKS는 지속적인 인터넷 연결 여부와 상관없이 운영되기 때문에 잠재적인 온라인 공격에 큰 영향을 받지 않습니다.

사용자는 PKS의 KMS 백엔드 접속 할 시점을 자유롭게 결정할 수 있습니다. 키 재고가 사전 정의된 최소 기준 이하로 떨어지면 서버가 새로운 키를 자동 요청합니다. 따라서 생산 중인 ECU에 투입할 키 관련정보가 언제나 충분히 준비되어 있어 네트워크 연결 장애로 인해 발생할 수 있는 고비용 생산 중단을 사전에 방지할 수 있습니다. PKS는 언제나 운영 상태가 유지됩니다.

전세계 ECU 생산 현장에서 적용되고 있는 솔루션

ECU 데이터에 대한 안전하고 정확한 암호화 키 공급은 거의 모든 차량내 IT 보안 기능의 근간입니다. KMS-PKS 통합 솔루션은 키 관리 보안에서부터 키 관련정보의 ECU 저장 및 주입 보안, 그리고 기록 및 검증을 모두 포괄함으로써 차량제조업체의 복잡한 암호화 자료 처리 메커니즘을 커버합니다. 바로 이러한 이유 때문에 오늘날 전세계의 다양한 차량제조업체들이 ECU 생산에 이러한 솔루션을 적용하고 있습니다. ■

저자

크리스챤 웨커(Christian Wecker): 에스크립트, PKS 프로덕트 매니저
마이클 루크(Michael Lueke): 에스크립트, KMS 선임 프로그램 매니저

영문 원문으로 보기