

공개키 기반 IoT 보안 플랫폼



ioTrust™

이문형 저사장

moon.lee@entrustdatacard.com



CONTENTS

1 제안 목적

2 제품 개요

3 주요 특징

4 아키텍쳐 구성

5 구축 예시



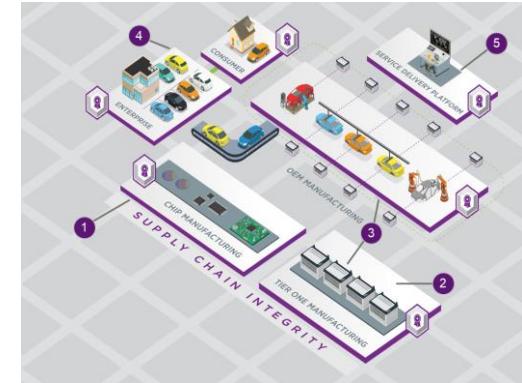
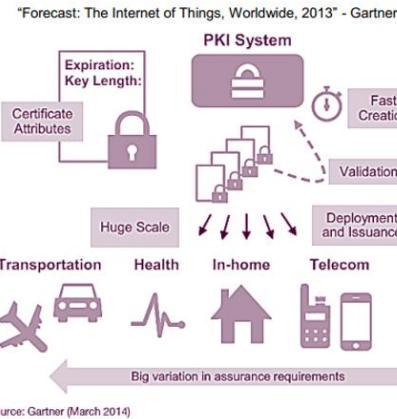
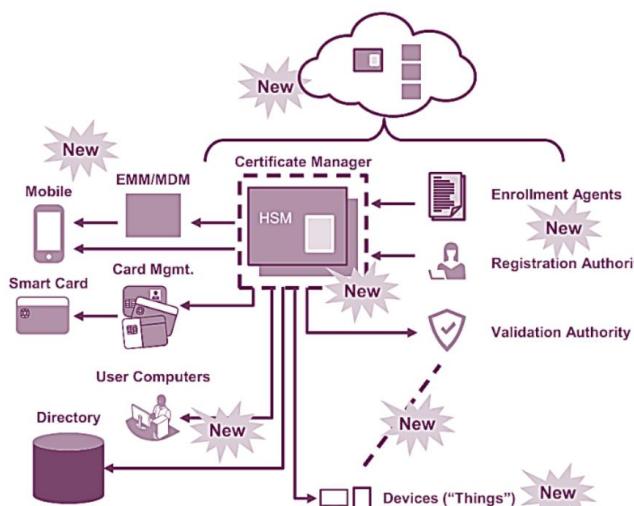
1. 제안 배경

IoT(Internet of Things) 환경에서 공개키기반(PKI) 기술의 역할

제안 배경

1

IoT 시장 성장



"Gartner는 PKI가 IoT, 이동성 및 클라우드로 인해 발생하는 새로운 요구사항의 결과로 부활하고 있다고 주장했습니다."
(2017, PKI Is Gearing Up for the Internet of Things)

Gartner®

"인증할 디바이스들(devices)을 검토할 때 실제 상호운영성을 제공하는 유일한 실제 표준은 PKI(Public Key Infrastructure, 공개키기반)뿐이다."

IEEE SPECTRUM



2. 제품 개요

PKI(공개키) 기반 IoT(Internet of Things) 보안 플랫폼 솔루션

제품 개요 2

제품명	아이오토러스트(ioTrust)
제조사(공급사)	엔트러스트 데이터카드 (한국총판 : (주)한국공인인증서비스)
제품 개요	<ul style="list-style-type: none"> ▪ 고유한 디바이스 식별 ▪ 펌웨어 사이닝(Signing) ▪ 안전한 키관리 ▪ 자동업데이트 ▪ 엔드포인트 모니터링 ▪ 아이덴티티 라이프사이클 관리 ▪ 안전한 통신(TLS, 데이터 암호화) ▪ 디바이스 프로비저닝



1994년
세계 최초 공개키기반(PKI)
상용제품 출시

Authority

20여년간 글로벌
인증/보안 리더
(인증/보안 전문기업)

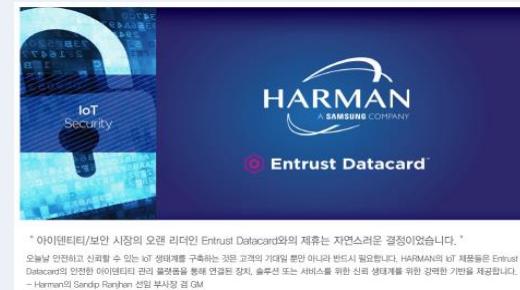
NIST FIPS 140-2 Certificate
(No.0016)



CC EAL 4+ Certificate
(383-4-127-CR)



HARMAN(삼성) 인증/보안 파트너



* IoT 인증/보안 시장의 오랜 리더인 Entrust Datacard와의 제휴는 자연스러운 결정이었습니다.
오늘날 안전하고 신뢰할 수 있는 IoT 생태계를 구축하는 것은 고의의 기지랄 뿐만 아니라 반드시 필요합니다. HARMAN의 IoT 제품들은 Entrust Datacard의 안전한 이더넷 터미널 장치, 출루션 또는 서비스를 위한 신뢰 생태계를 위한 강력한 기반을 제공합니다.
– HARMAN의 Sandip Ranjan 부사장 경 GM



3. 주요 특징

▣ ioTrust의 가치 - IoT 보안 인프라를 제공하는 강한 보안 플랫폼

주요 특징

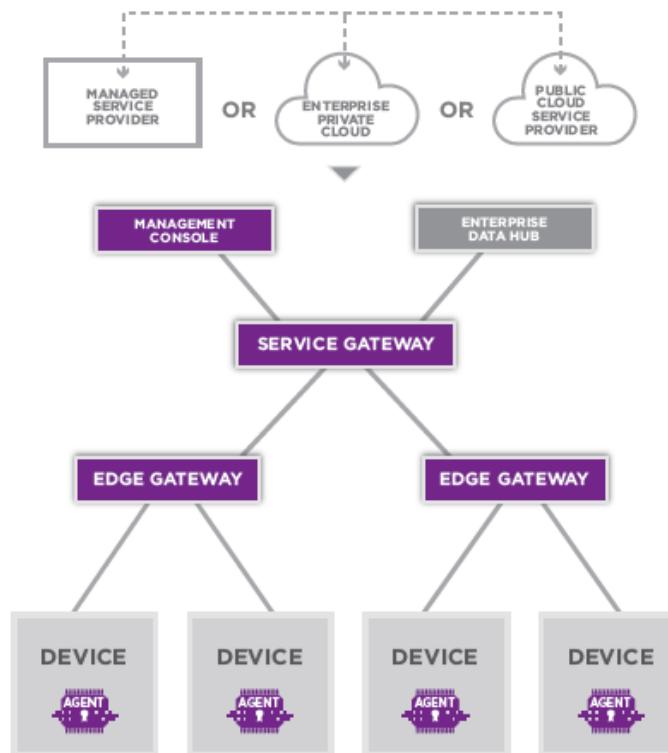
3

강력한 보안, 간편한 구축 기반 IoT 생태계를 보호하기 위한 강한 보안 플랫폼

응용 프로그램 및 데이터 플랫폼, 클라우드 환경 모두 지원

ioTrust 가치:
"Things"과 응용 프로그램간에
보안 인프라 제공

서로 다른 종류의 "Things"
기준 또는 신규 모두 지원



디바이스 통합 및 데이터 보호

아이덴티티 관리 :
제조에서 운영까지

모든 종류의 장치에
대한 인증 및 인가

데이터 수집 관리

공급망 무결성

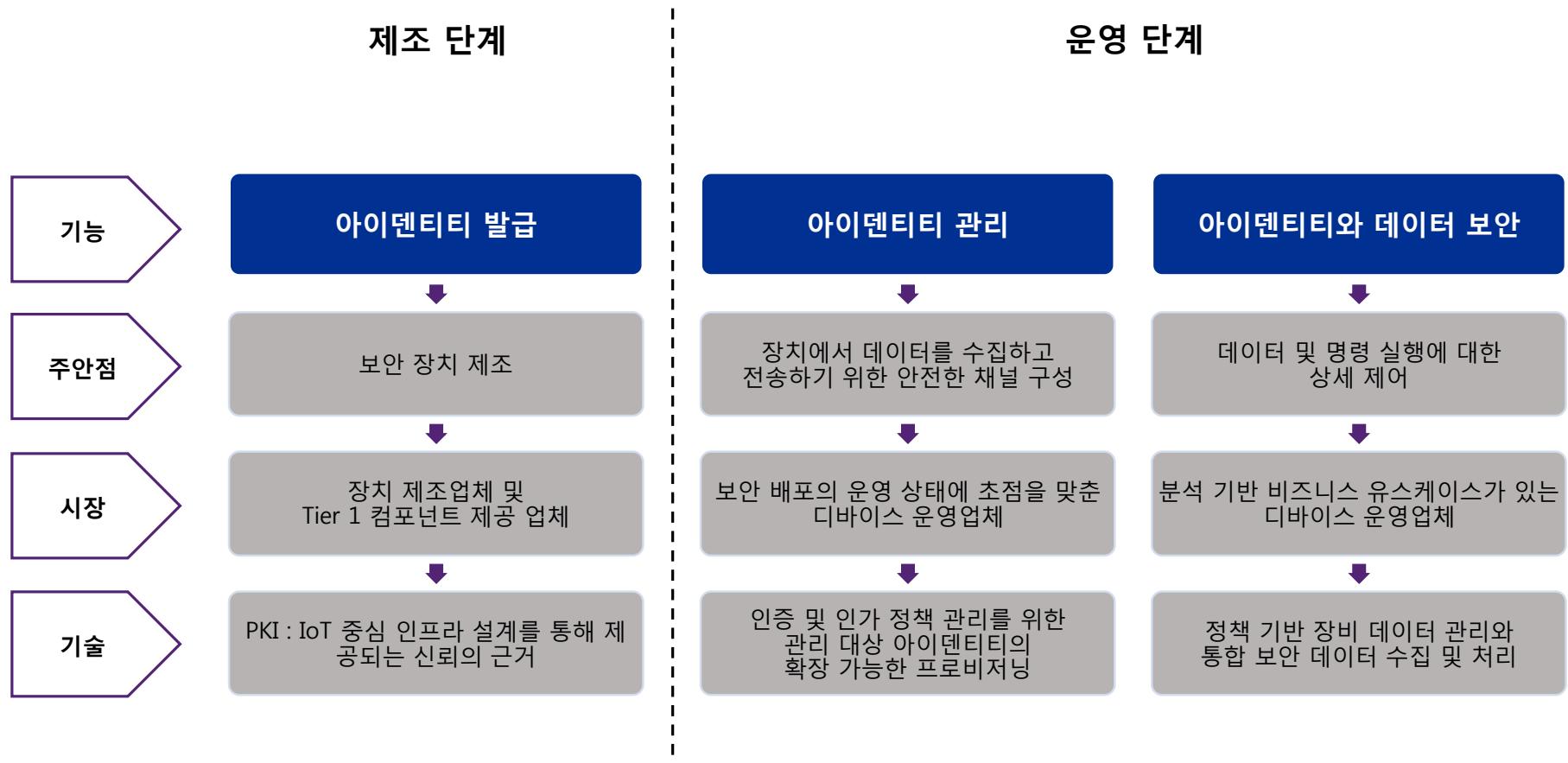
안전한 자동 등록과
프로비저닝



3. 주요 특징

- 다양한 요구사항을 수용하는 계층적인 보안 플랫폼 구성

주요 특징 3



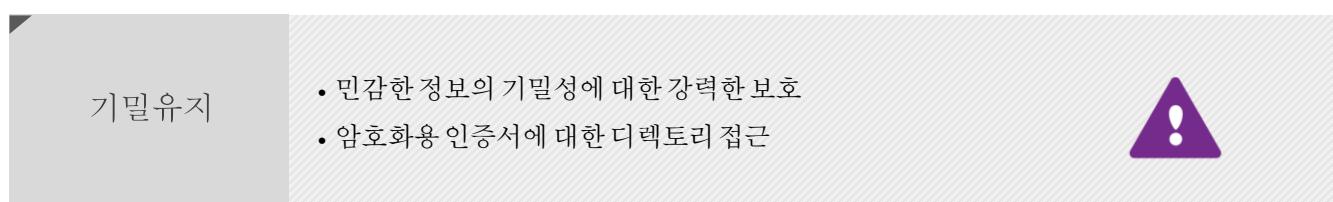
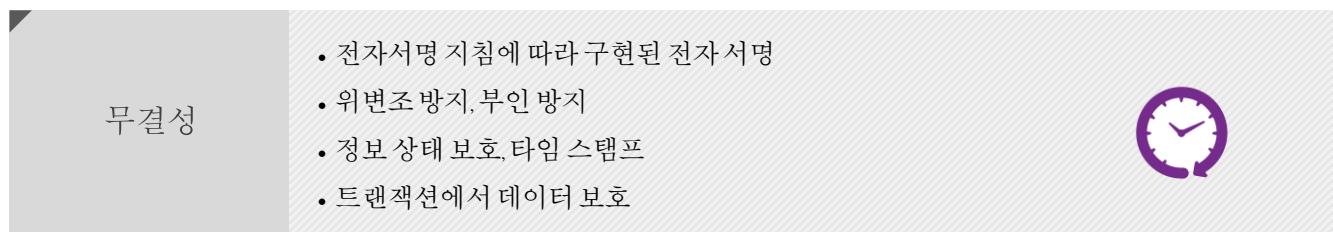
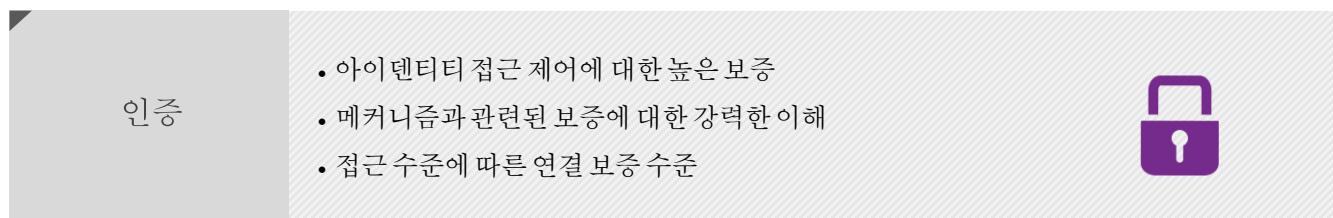
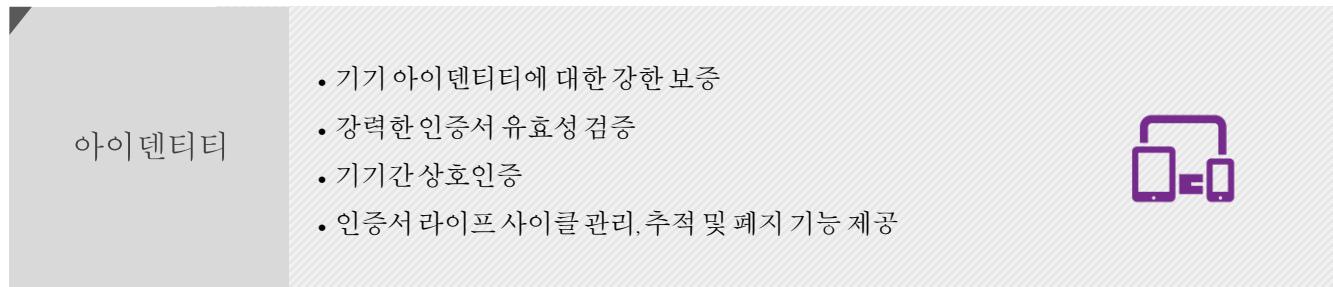


3. 주요 특징

□ 다양한 보안 요구사항을 수용하는 ioTrust 보안 플랫폼이 제공하는 보안

주요 특징

3



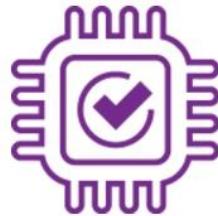


3. 주요 특징

□ X.509 등 다양한 프로토콜 지원 기반 아이덴티티와 데이터 보안

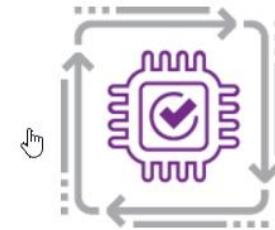
주요 특징

3



아이덴티티 발급

- X.509 및 ECC 인증서를 기반으로 하는 제조사 아이덴티티(관리되지 않음)의 안전한 대량 및 주문형 발급
- 자격 관리
- SCEP, EST, CMPV2를 통한 아이덴티티 등록 보안
- 공급망 검증



아이덴티티 관리

- IoT 아이덴티티의 실시간 수명주기 관리
- 안전한 소프트웨어 및 하드웨어 키 스토어
- 콘솔 및 기기에서 아이덴티티 관리 용 API (예 : P11 인터페이스 및 REST 서비스)
- 검증된 게이트웨이 및 엔드 포인트 클라이언트 통합
- 안전한 COAP 및 MQTT 라이브러리
- TLS 1.2+, TPM 및 HSM 지원



아이덴티티와 데이터 보안

- 데이터 암호화 자동화
- 상호 인증된 TLS 연결
- 양방향 데이터 파이프와 메시지 라우팅
- 저장 후 전달 데이터 전달
- 데이터 스트림 처리
- Modbus, CANOpen 프로토콜 통합
- 인프라 모니터링 및 경고
- 자동 연결 진단



3. 주요 특징

□ 파트너 생태계

Primary Vertical Market Segment						
Industry Verticals >>	Auto	Industrial (Manufacturing, Energy / Utilities)	Telecom	Medical Devices	BFSI	
Primary Use-cases	Integrated Vehicle Health Management (IVHM)	Predictive Maintenance	Predictive Maintenance - Energy Generation and Distribution	Supply-Chain & Asset Monitoring: Retail	Predictive Health Monitoring	Usage based Insurance
	Warranty & Support Optimization - Remote Diagnostics	Quality Management	Smart Building Automation		Clinical Decision Support	Payment Processing
	Location & Capacity Based Services	Automation & Performance Management	Smart City / Smart Grid	Customer Experience Management: Smart Energy, Smart Auto	Telemedicine	Bespoke Financial Products
Vertical Market						
Objective: Revenue Generation	Device Manufacturer	Device Manufacturer	Device Manufacturer	Device Manufacturer	Device Manufacturer	Device Manufacturer
	Denso, Continental AG, Delphi, Panasonic, Hyundai, TRW, Mitsubishi	Siemens, Rockwell Automation, Emerson, GE, ABB, Schneider Electric, Bosch, Yaskawa, Hanwha, Hitachi, Fujitsu, Resmed, Legrand, Cradlepoint, Bosch, Thales		Ericsson, Nokia, NEC, Huawei	JnJ, Baxter International, Abbott, Medtronic, Boston Scientific, Hitachi	Sourcing in alliance with ODM or Telco
	OEM and Device Operators	Device Operators	Device Operators	Device Operators	Device Operators	Device Operators
	Transportation / Logistics Venders	Ingersoll Rand, GE, ABB, Johnson Controls, UTC	Enbridge, PG&E, DTE, Duke, Suncor, Trans-Canada, EVN	ATT, T-Mobile, NTT, Deutsche Telekom, BT, SingTel	Abbott, JnJ, Atena, SCA, Cardinal Health, United Health	Desjardins, AllState, Liberty Mutual, BoA, TD, RBC
Supporting Horizontal Market Segment						
Horizontal Ecosystem						
Objective: Ecosystem Expansion	Silicon	OS & IaaS	Sensors	ODM & Hi-tech	ISV & Platform Vendors	Vertical Solutions Providers
	Infineon, Intel, NXP, Qualcomm, Telit, Altair Semi, Gemalto	Google, Wind River, MSFT / Azure	OleumTech, B-SCADA, Novus	Cisco, Juniper, Nexcom, Kontron, Mediatek, Advantech, Quanta, Flextronic, Dell	PTC, Microsoft, AWS, Google, GE-Predix	Switch Automation, Iconics

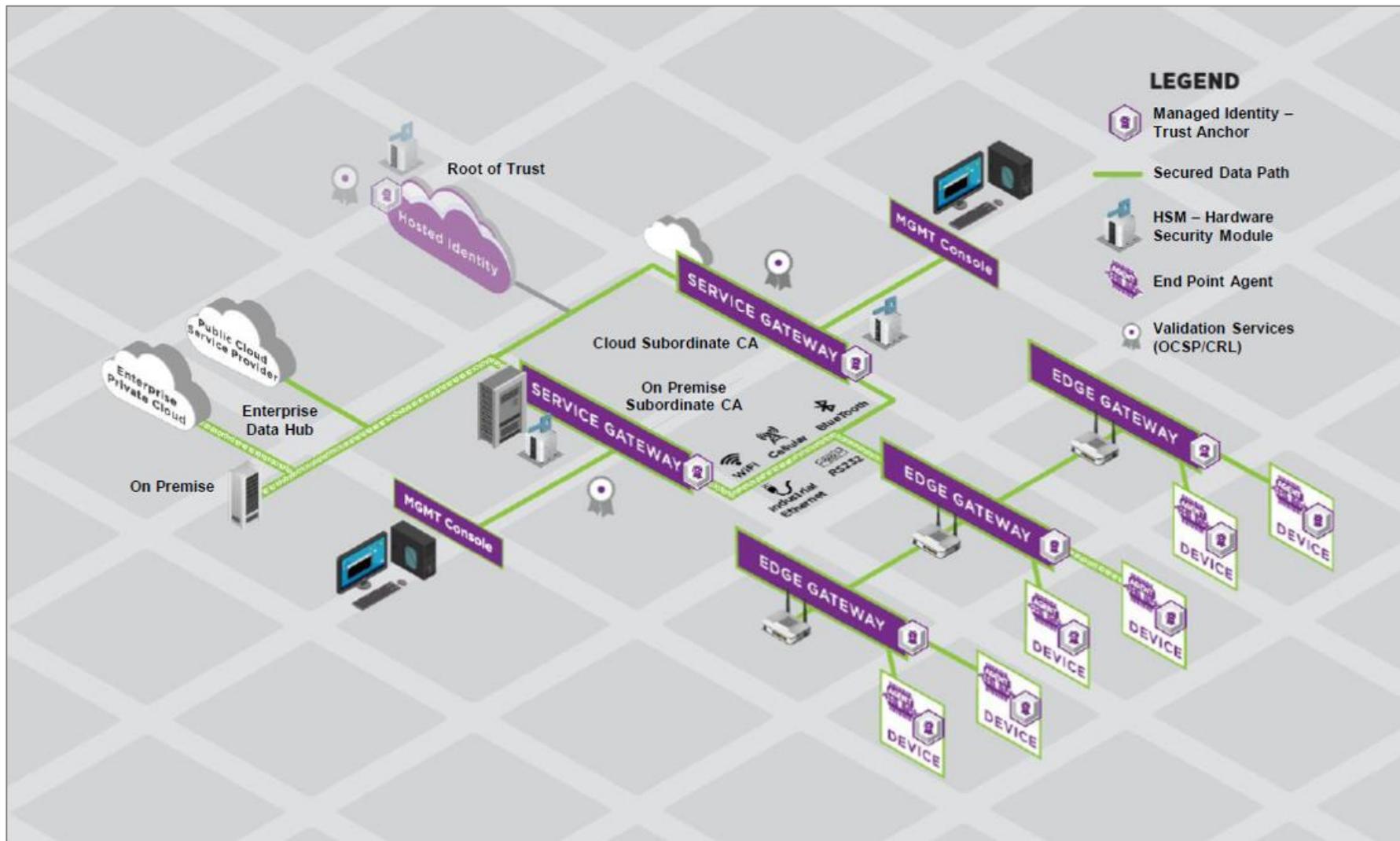


4. 아키텍쳐 구성 – 신뢰 모델

□ 공개키 기반 신뢰 모델

아키텍쳐 구성

4



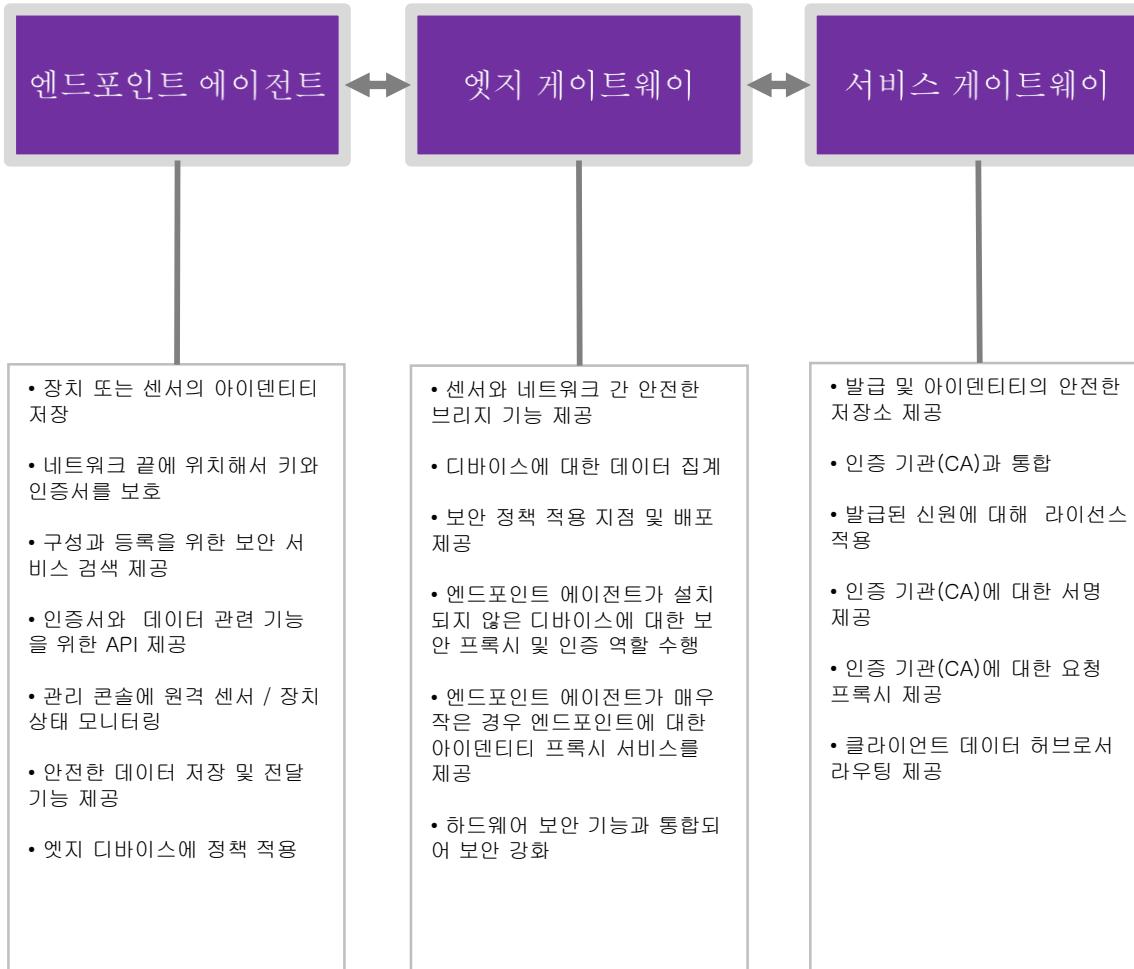


3. 주요 특징

3단계 모델(엔드포인트 에이전트-엣지 게이트웨이-서비스 게이트웨이)로 **긴밀한 연계**

주요 특징

3



Key Features	
셀프서비스 플랫폼	<ul style="list-style-type: none"> Policy Management Monitoring & Reporting Audit & Compliance* Edge Analytics Integration* Subscription Management Entitlement Management Usage Metering
지원 네트워크와 프로토콜	<ul style="list-style-type: none"> Wi-Fi, 2G/3G/4G/LTE Ethernet, Industrial Ethernet ZigBee USB RS-232/485 RFID Bluetooth MQTT, AMQP, CoAP, REST
디바이스 관리	<ul style="list-style-type: none"> Enrollment & Provisioning Device Supply Chain Control Equipment Data Model & Policy Enforcement
디바이스 보호	<ul style="list-style-type: none"> Authentication & Authorization Credential Management Application Code Signing* Certificate Lifecycle Management
데이터 보호	<ul style="list-style-type: none"> Secure Transport & Data Encryption Filtering & Aggregation*



4. 아키텍쳐 구성



아키텍쳐 구성

4

Issuance & Licensing

- 발급 및 신원 저장소의 안전한 지점을 제공
- 인증 기관(CA)과 통합
- 발급된 신원에 대해 라이선스 적용
- 인증 기관(CA)에 대한 보안 서명 및 요청 Proxy 제공
- 클라이언트 데이터 허브로서 라우팅

API Layer

Data Service

MQTT

AMQP

App Data

Telemetry

Enrollment Service

Identity

Config

SCEP

EST

COAP

File

Storage Layer

Data Queue

Encrypted File Storage

Entitlement Licensing Layer

Usage Collection

Feature Enablement

Policy Management

Identify Management

Authentication & Authorization

Data Collection & Routing



4. 아키텍쳐 구성

 Edge Gateway

아키텍쳐 구성 4

Secure Proxy & Policy Enforcement

- Edge Gateway는 Sensor와 WAN(Wide Area Network)간에 안전한 네트워크 브리지를 제공
- 장치에 대한 데이터 집계
- 보안 정책 적용 지점 및 배포 제공
- 엔드포인트 에이전트가 설치되지 않은 디바이스에 대한 보안 프록시 및 인증자 역할
- 엔드포인트 에이전트가 없는 제약된 엔드포인트에 대한 Identity Proxy 서비스를 제공
- 하드웨어 보안 기능과 통합되어 향상된 보안을 위한 신뢰할 수 있는 플랫폼 모듈

Services

Network

Service Discovery

NTP

Health

DNS

Data Store

Configuration

Data Queue

Logs

Policy Management

Data

Security

Identity Management

Activate

Suspend

Terminate

Renew

Enrollment



4. 아키텍쳐 구성

 EndPoint Agent

아키텍쳐 구성 4

Secure Key & Data Management

- 장치 또는 센서의 아이덴티티 저장
- 네트워크 끝에 위치해서 키와 인증서를 보호
- 구성 및 등록을 위한 보안 서비스 검색
- 인증서 및 데이터 관련 기능을 위한 API
- 관리 콘솔에 원격 측정 데이터 기반 센서 / 장치 상태 모니터링
- 원격 측정 데이터를 처리 할 때 안전한 저장 및 전달 기능
- 에지 장치에 정책 적용

Secure Functions

PKCS 11

Key Generation

Identity Store

Manufacturer ID

Operator ID 1..n

Data Store

Configuration

Data Queue

HW Management

TPM 1.2

Logs

Communications Module

SSL/TLS

HTTPS

SCEP

TCP/IP

REST API

MQTTS

Telemetry

UDP

Commands

COAP

Discovery

Configuration

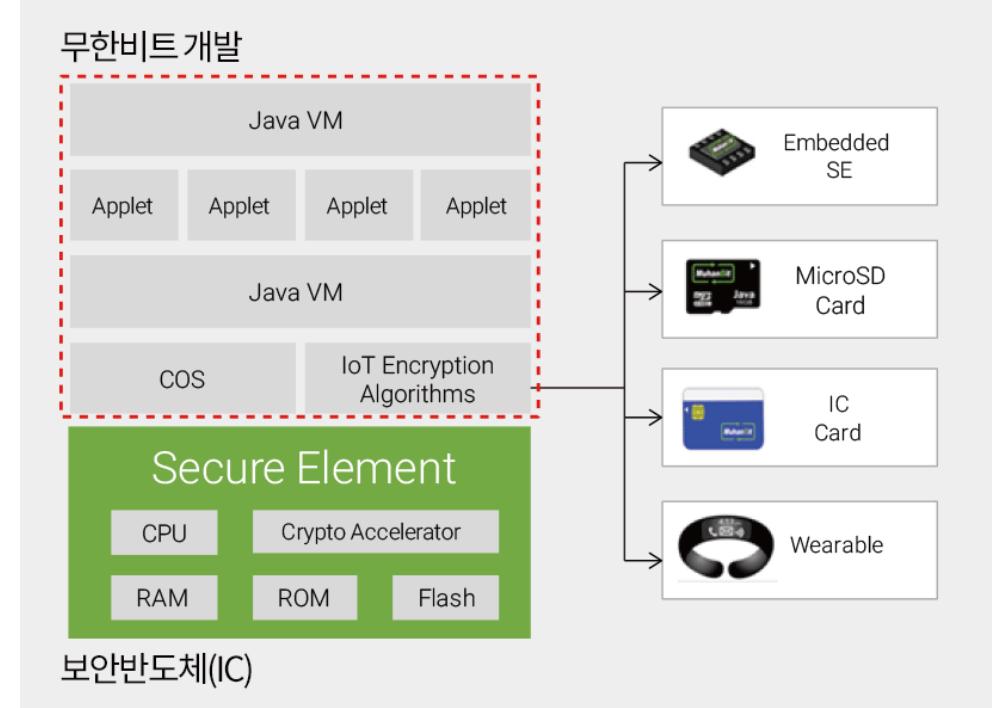
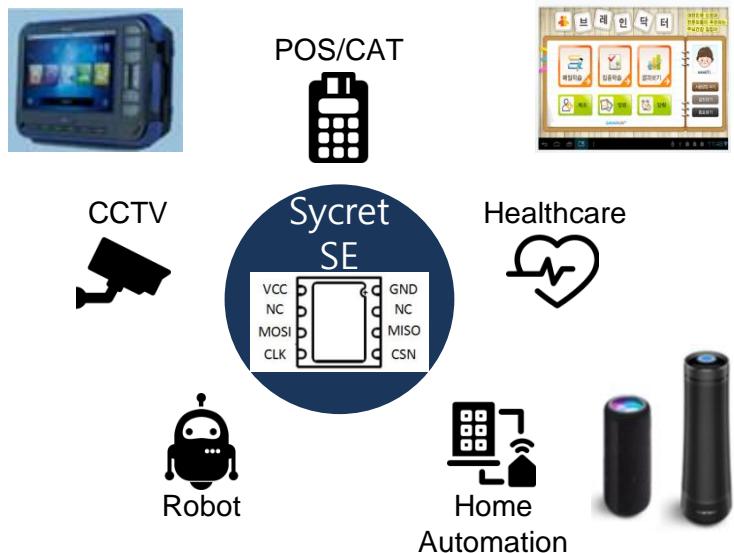


5. 구축 예시 : SE 사례

구축 예시 5

하드웨어보안모듈 - HSM

Sycret – Certificate(SE)





5. 구축 예시 : HARMAN(삼성) 사례

구축 예시

5

□ HARMAN(삼성)이 채택한 안전한 IoT 보안 솔루션 - ioTrust



2016년 기준
프리미엄 인포테인먼트 분야 1위(24%)
텔레매틱스 분야 2위(10%)
카오디오 분야 1위(41%)

매출 중 65%가 전장사업에서
발생함.

삼성전자가 2017년 3월 인수



AS-WAS

AS-IS

문제점

1. PSK(Pre Shared Key) 인증서를 파일시스템에 저장
2. 자체 서명
3. 도용 위험 및 도용된 기기 차단 쉽지 않음
4. Hop-to-hop 보안을 통해 인증서버없이 보안
5. 확장성 없이 설계

ioTrust 적용 후

1. 자동으로 인증서 사전 배포
2. 안전하게 키 스토어 저장
3. 탈취위험 감소
4. TPM 제공 업그레이드
5. 환경 영향 없이 폐기
6. 상호인증 처리

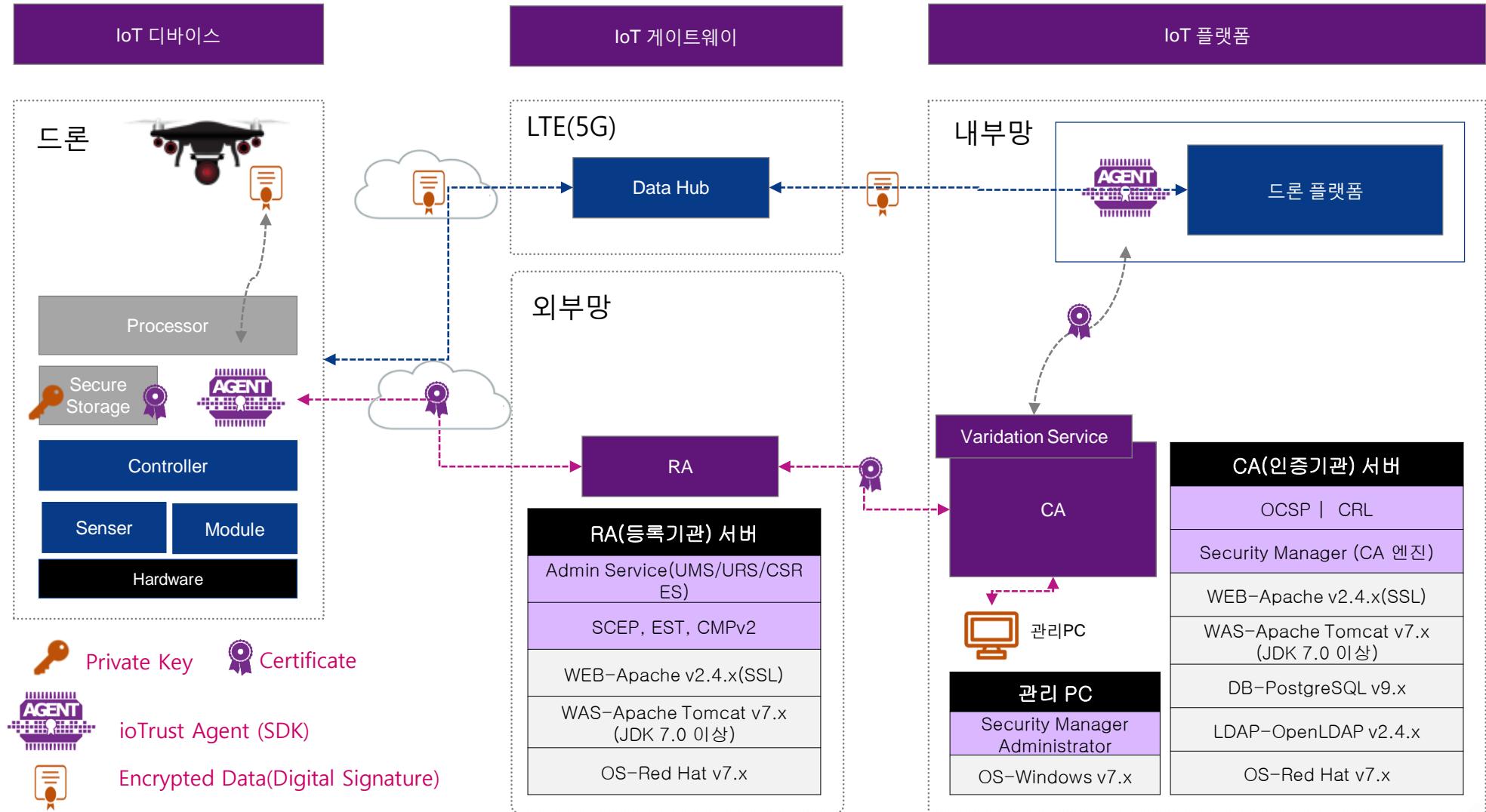
오디오 자동차 전장장비 기업 '하만'은 아이오토러스트를 도입했다. 하만은 오디오 브랜드로 유명하지만 자동차 전장 분야 선도 기업이다. 하만 사업 분야 중 커넥티드 서비스(Connected Service)는 IoT 서비스와 솔루션 사업부다. 초기 하만은 IoT 솔루션에서 사용하는 게이트웨이와 센서 등 엔드포인트 장치 인증과 데이터 보안을 위해 파일시스템에 보관하는 비밀키(PSK) 방식을 채택했다. 비밀키의 외부 도용 위험이 크고 하드웨어 보안 업그레이드가 어려웠다. 하만은 IoT 기기를 배치하기 전에 인증과 보안 문제를 해결하려고 아이오토러스트를 도입했다. 아이오토러스트 플랫폼으로 인증기관을 통한 공개키 기반 인증서 관리시스템을 도입했다. 키스토어 기반으로 인증키를 안전하게 저장해 보안을 강화하고 자동 배포 프로세스를 구성해 기기 확장에 따른 등록의 어려움도 해소했다. 손상된 기기 인증 폐기도 다른 기기와 상관없이 처리하는 IoT 생태계를 만들었다.
(전자신문, 2018.03.05)



5. 구축 예시 : 드론 사례

구축 예시 5

□ 드론 시스템 환경에서 인증기관(CA) 기반 ioTrust 보안 플랫폼 구성안

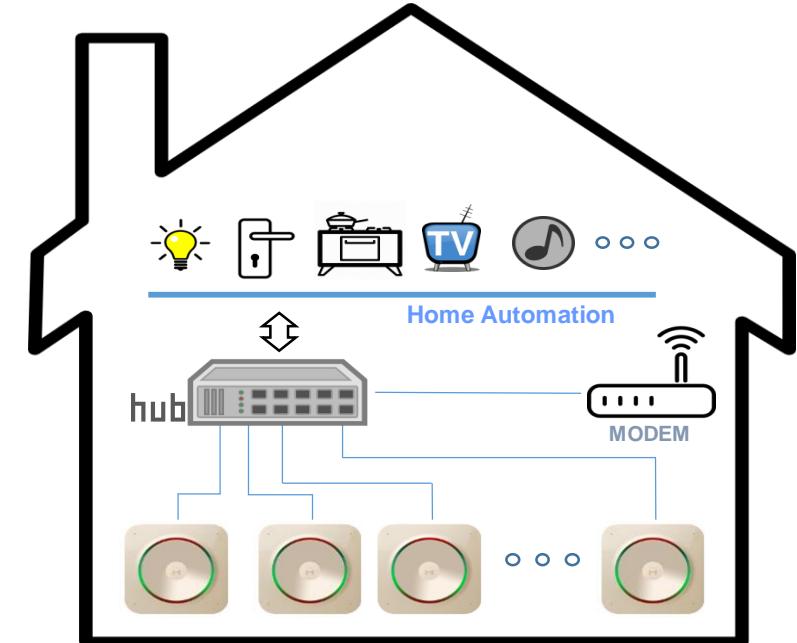
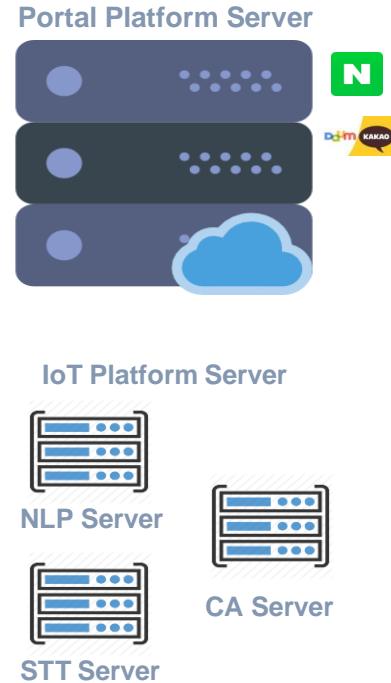




5. 구축 예시 : AI 스피커 사례

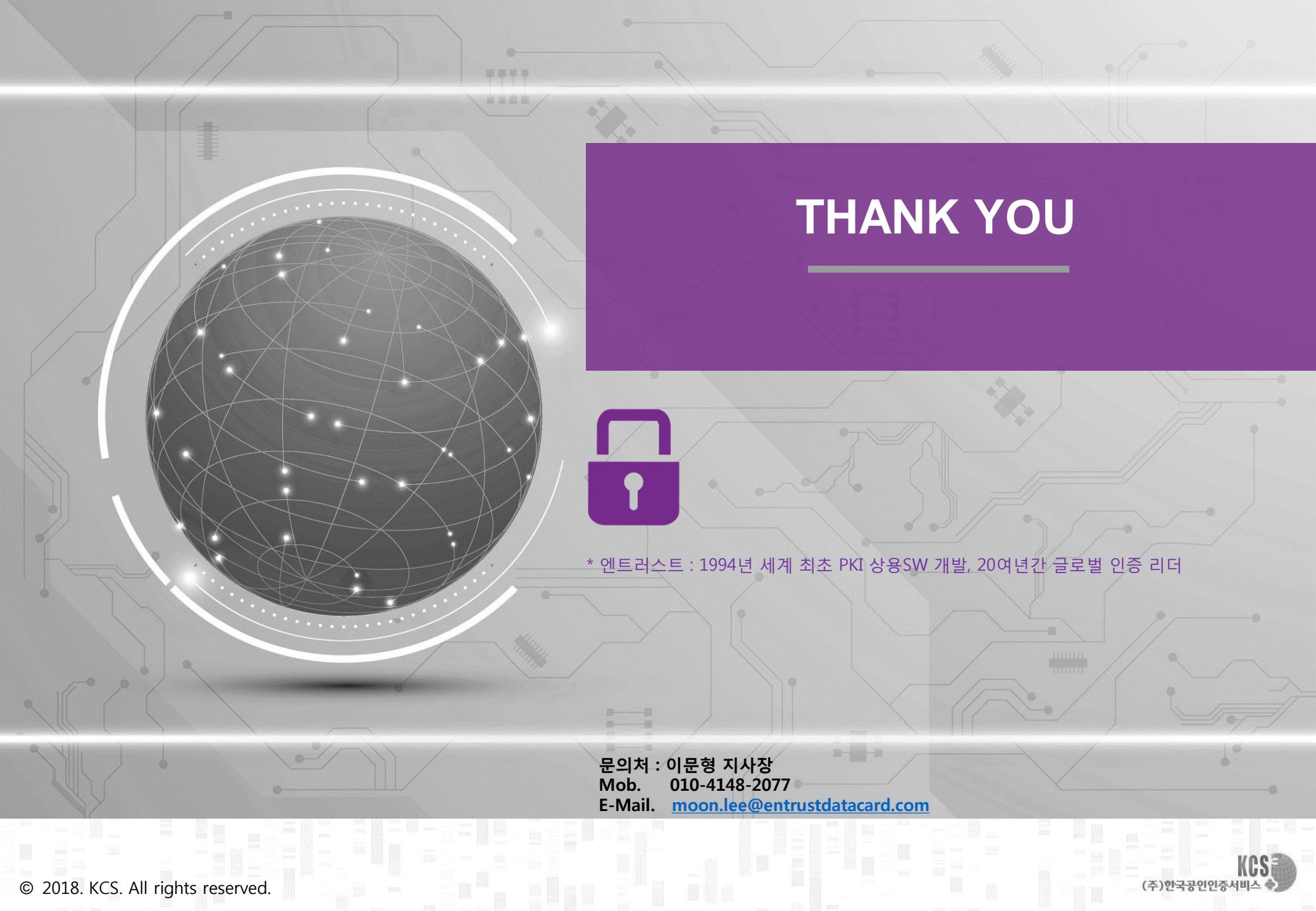
AI 스피커

빌트인 형태의 단말기로 음성인식 엔진을 탑재하여 스마트 가전제품 및 클라우드 연동 음성서비스가 가능한 단말기



ioTrust Agent (SDK)

NLP(Natural Language Processing, 자연어 처리)
STT(Speech to Text, 음성 인식)
CA(Certificate Authority, 인증기관)



THANK YOU



* 엔트러스트 : 1994년 세계 최초 PKI 상용SW 개발, 20여년간 글로벌 인증 리더

문의처 : 이문형 지사장
Mob. 010-4148-2077
E-Mail. moon.lee@entrustdatacard.com