

사물인터넷(IoT) 보안 플랫폼 – ioTrust

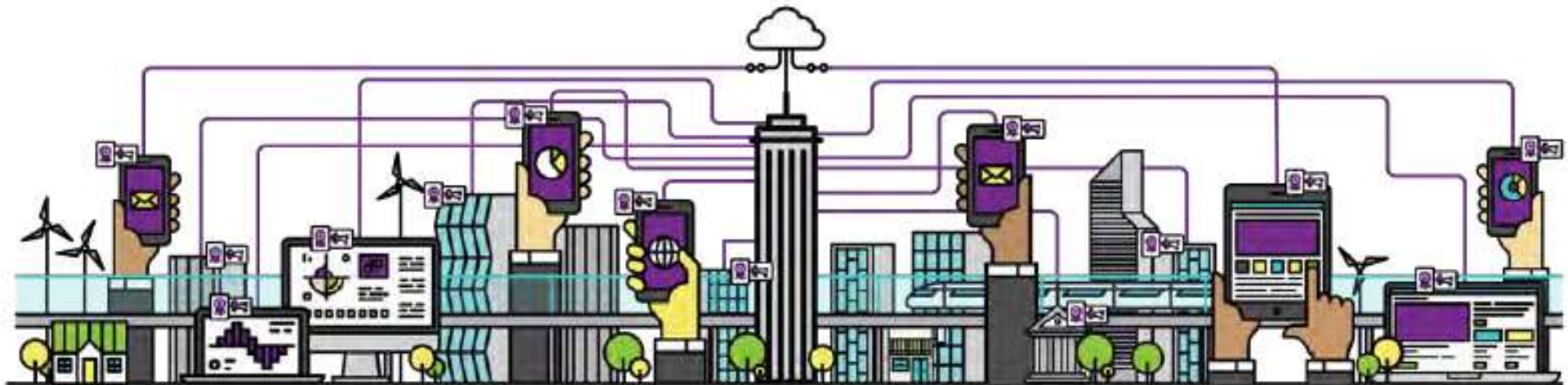


Summary

디지털 ID로 보안: IoT is CoT(Certificate of Things)

사물인터넷(IoT) - 보안 플랫폼

Certificate of Things

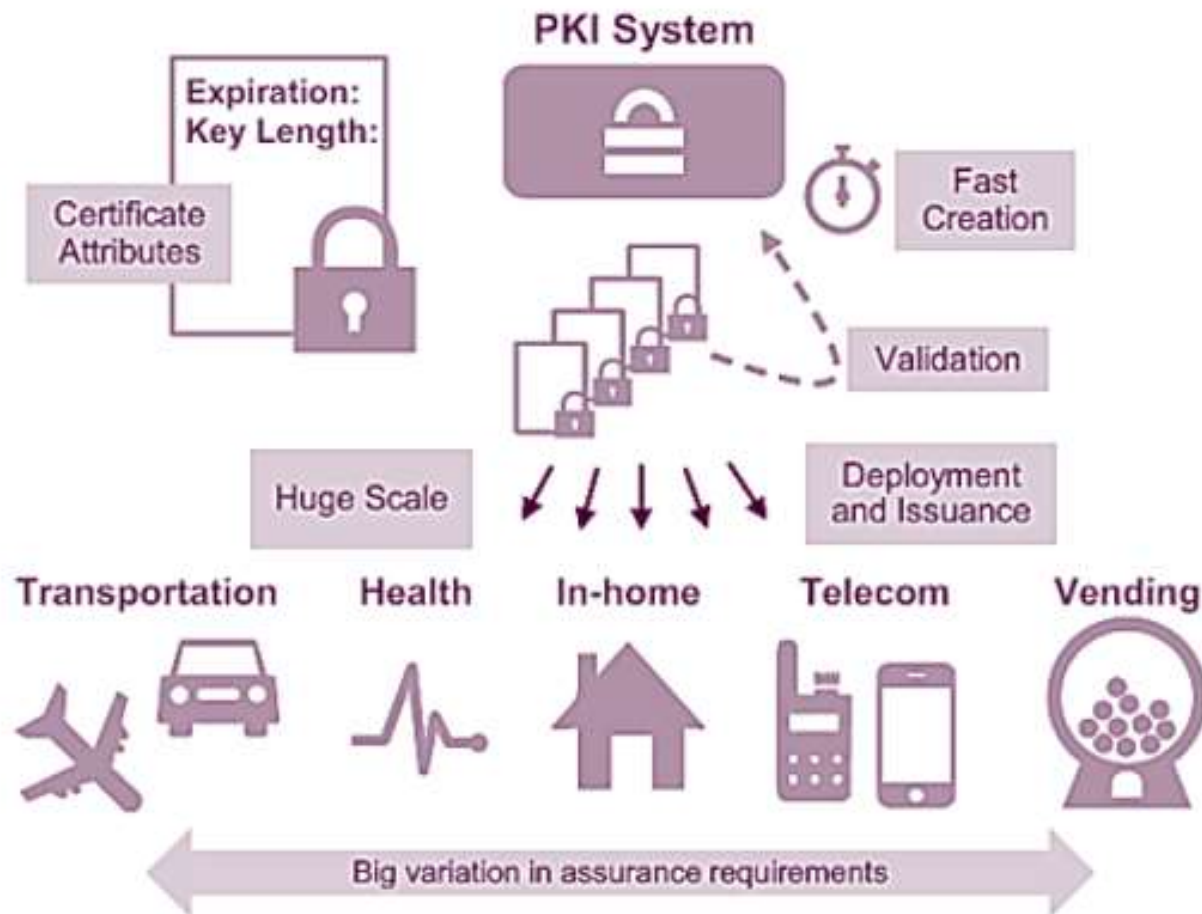




1. IoT와 PKI

IoT는 다양한 사물들(Things)이 인터넷(Internet)과 연결

"Forecast: The Internet of Things, Worldwide, 2013" - Gartner



Source: Gartner (March 2014)



"인증할 디바이스들(devices)을 검토할 때 실제 상호운용성을 제공하는 유일한 실제 표준은 PKI(Public Key Infrastructure) 뿐이다. " (2014, Looking for the Key to Security in the Internet of Things)

Gartner

"Gartner는 PKI가 IoT, Mobility 및 Cloud로 인해 발생하는 새로운 요구사항의 결과로 부활하고 있다고 주장했습니다." (2016, PKI Is Gearing Up for the Internet of Things)

THALES

"보안 기술 전문 업체인 Thales는 PKI를 사용하는 어플리케이션의 배포에서 IoT가 가장 빠르게 증가하는 추세라고 발표했습니다. (2018, PKI의 IoT 배포는 2015 년 이후 23 % 증가했습니다)



2. 제품 개요

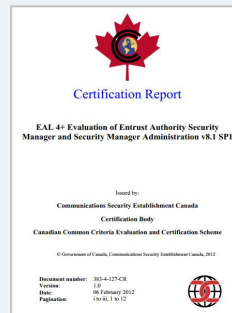
PKI(공개키) 기반 IoT(Internet of Things) 보안 플랫폼 솔루션

제품명 아이오퍼스트(ioTrust)	
제조사(공급사) 제품 개요	엔트러스트 데이터카드 (한국총판 : (주)한국공인인증서비스) - 고유한 디바이스 식별 - 펌웨어 사이닝(Signing) - 안전한 키관리 - 자동업데이트 - 엔드포인트 모니터링 - 아이덴티티 라이프사이클 관리 - 안전한 통신(TLS, 데이터 암호화) - 디바이스 프로비저닝 

NIST FIPS 140-2 Certificate
(No.0016)



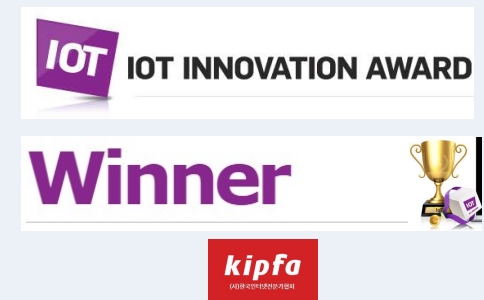
CC EAL 4+ Certificate
(383-4-127-CR)



국정원 검증 암호모듈(KCMVP) 내장
[검증번호 : CM-115-20216]



IoT 어워드 대상 수상(Security)
[2018, kipfa]



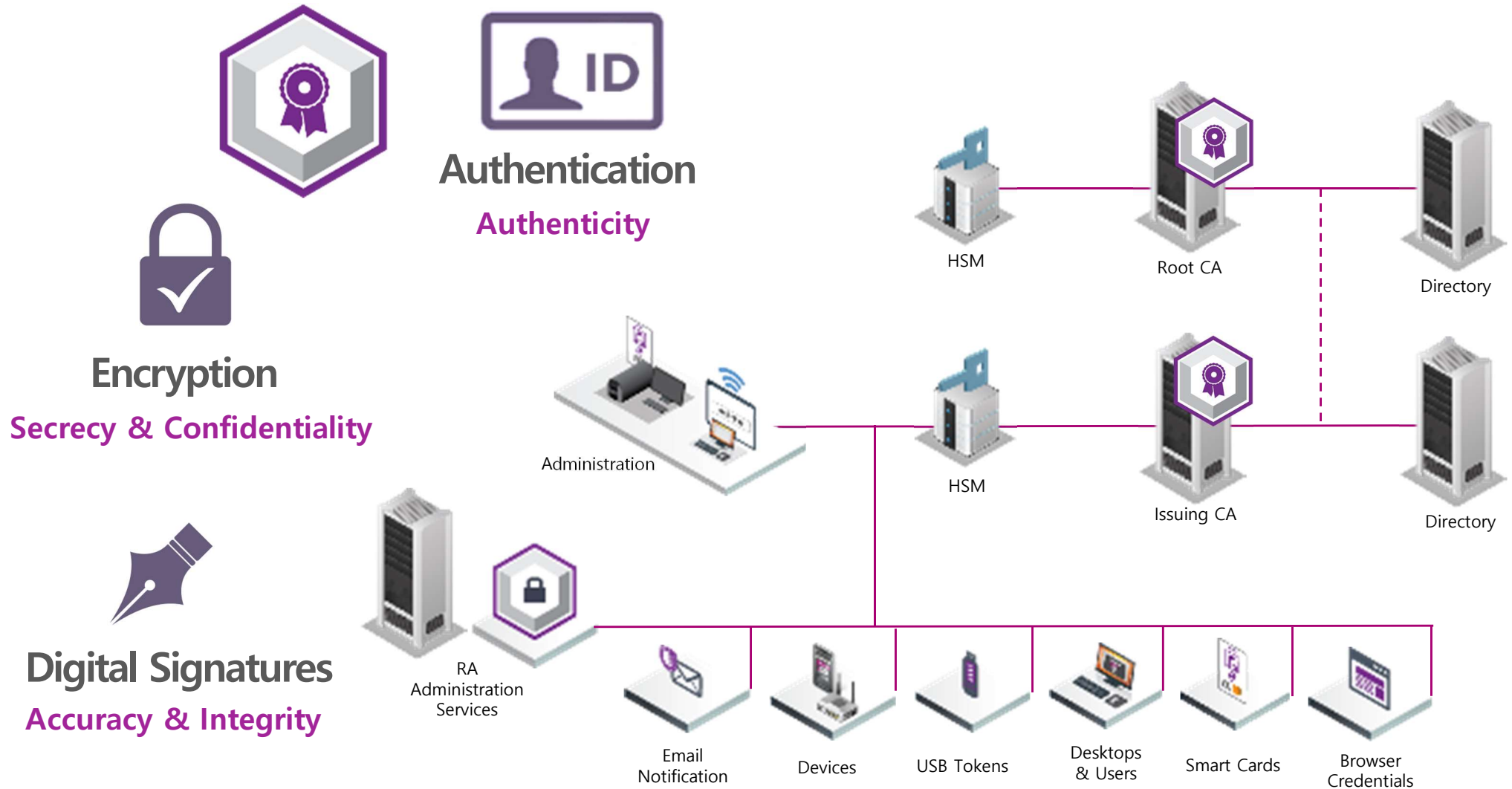


3. About PKI

PKI (Public Key Infrastructure, 공개키기반)

강력한 암호화를 사용하여 트랜잭션을 보호하고,

이를 통해 사용자에게 신뢰할 수 있는 디지털 ID를 발급하고, 안전하게 관리하는 방법





3. About PKI

다양한 보안 요구사항을 수용하는 **ioTrust 보안 플랫폼이 제공하는 보안**

1 Identity	아이덴티티	• 기기 아이덴티티에 대한 강한 보증 • 강력한 인증서 유효성 검증 • 기기간 상호인증 • 인증서 라이프 사이클 관리, 추적 및 폐지 기능 제공	
2 Authentication	인증	• 아이덴티티 접근 제어에 대한 높은 보증 • 메커니즘과 관련된 보증에 대한 강력한 이해 • 접근 수준에 따른 연결 보증 수준	
3 Integrity	무결성	• 전자서명 지침에 따라 구현된 전자 서명 • 위변조 방지, 부인 방지 • 정보 상태 보호, 타임 스탬프 • 트랜잭션에서 데이터 보호	
4 Confidentiality	기밀유지	• 민감한 정보의 기밀성에 대한 강력한 보호 • 암호화용 인증서	



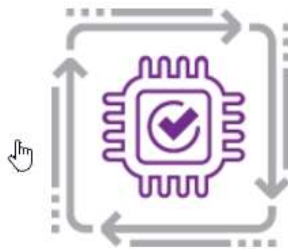
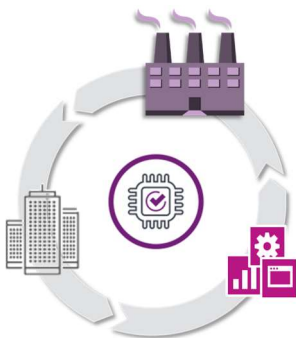
4. 주요 특징

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



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

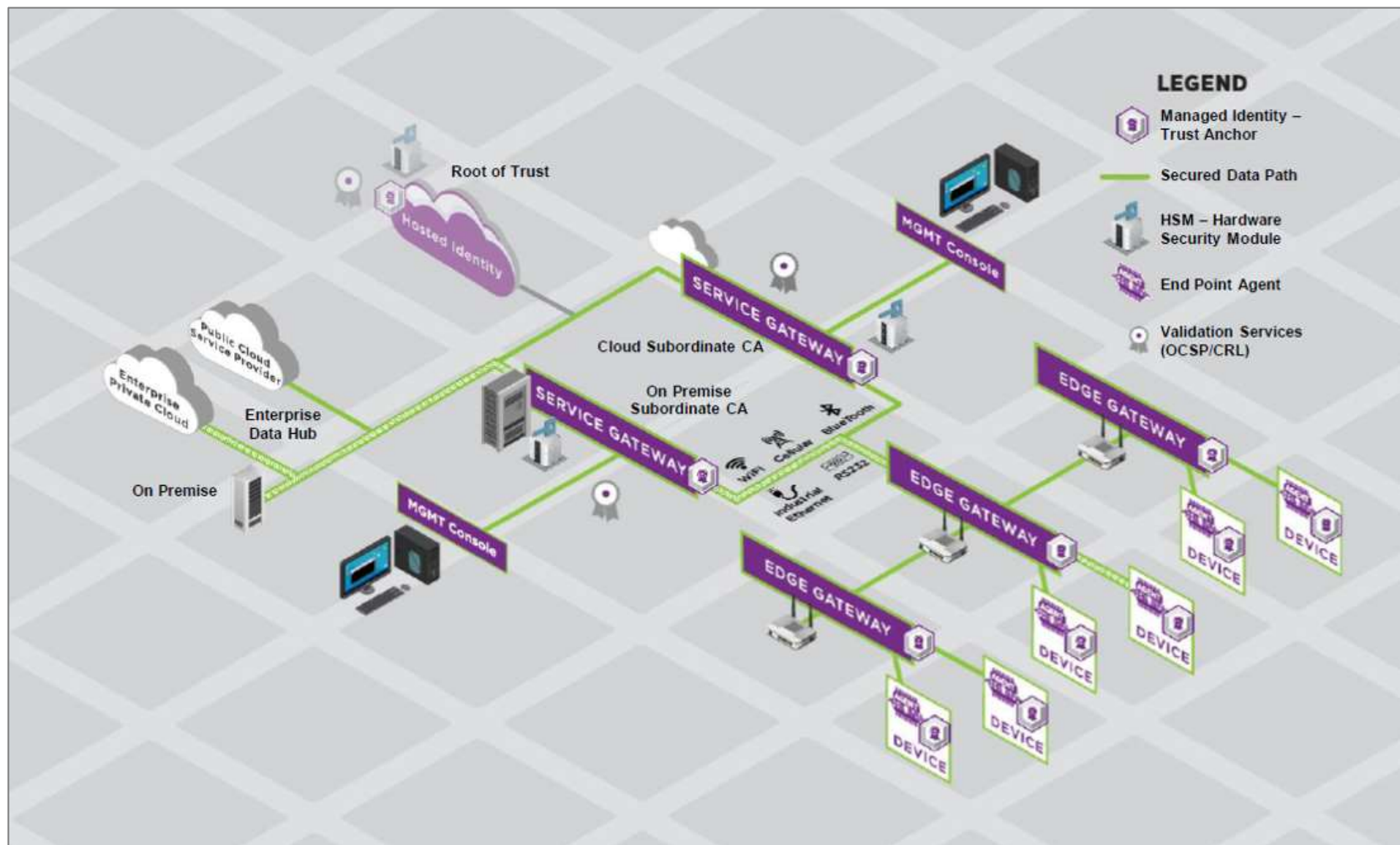
- 데이터 암호화 자동화
- 상호 인증된 TLS 연결
- 양방향 데이터 파이프와 메시지 라우팅
- 저장 후 전달 데이터 전달
- 데이터 스트림 처리
- Modbus, CANOpen 프로토콜 통합
- 인프라 모니터링 및 경고
- 자동 연결 진단





4. 아키텍처 구성 - 신뢰 모델

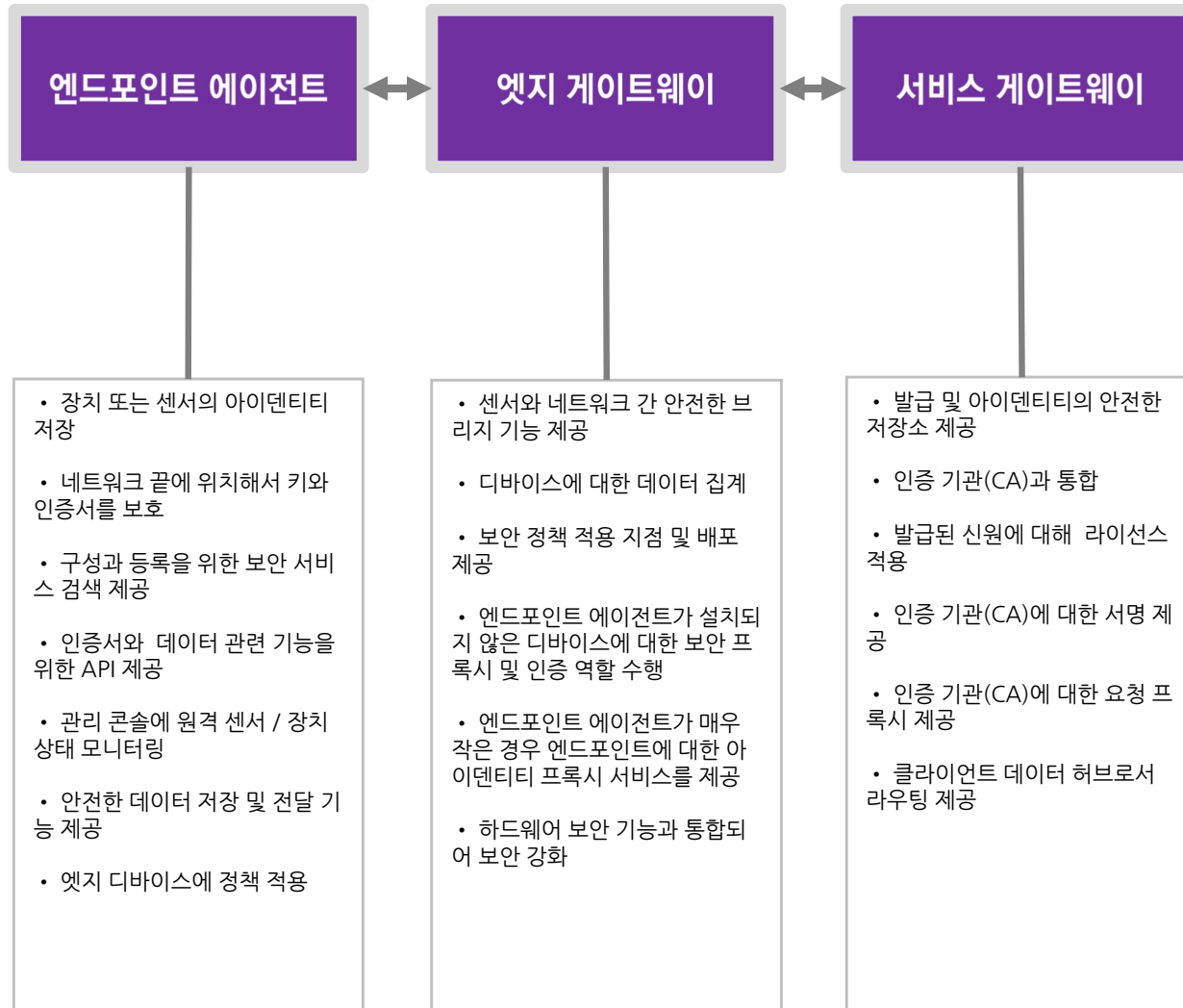
공개키 기반 구조 기반 신뢰 모델





4. 주요 특징

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



Key Features	
셀프서비스 플랫폼	• Policy Management • Monitoring & Reporting • Audit & Compliance* • Edge Analytics Integration* • Subscription Management • Entitlement Management • Usage Metering
지원 네트워크와 프로토콜	• Wi-Fi, 2G/3G/4G/LTE • Ethernet, Industrial Ethernet • ZigBee • USB • RS-232/485 • RFID • Bluetooth • MQTT, AMQP, CoAP, REST
디바이스 관리	• Enrollment & Provisioning • Device Supply Chain Control • Equipment Data Model & Policy Enforcement
디바이스 보호	• Authentication & Authorization • Credential Management • Application Code Signing* • Certificate Lifecycle Management
데이터 보호	• Secure Transport & Data Encryption • Filtering & Aggregation*



5. 구축 예시 : HARMAN(삼성) 사례

HARMAN(삼성)이 채택한 안전한 IoT 보안 솔루션 – ioTrust



* 아이덴티티/보안 시장의 오랜 리더인 Entrust Datacard와의 제휴는 자연스러운 결정이었습니다.*

오늘날 안전하고 신뢰할 수 있는 IoT 생태계를 구축하는 것은 고객의 기대일 뿐만 아니라 반드시 필요합니다. HARMAN의 IoT 제품들은 Entrust Datacard의 안전한 아이덴티티 관리 플랫폼을 통해 연결된 장치, 솔루션 또는 서비스를 위한 신뢰 생태계를 위한 강력한 기반을 제공합니다.
— Harman의 Sandip Ranjan 선임 부사장 겸 GM

AS-WAS

대칭키 암호화(PSK)

자체서명

기기도용/기기차단 어려움

Hop-to-hop 보안

AS-IS

공개키+대칭키 암호화

전자서명(인증서체인)

인증서 폐기 가능

상호 기기 인증

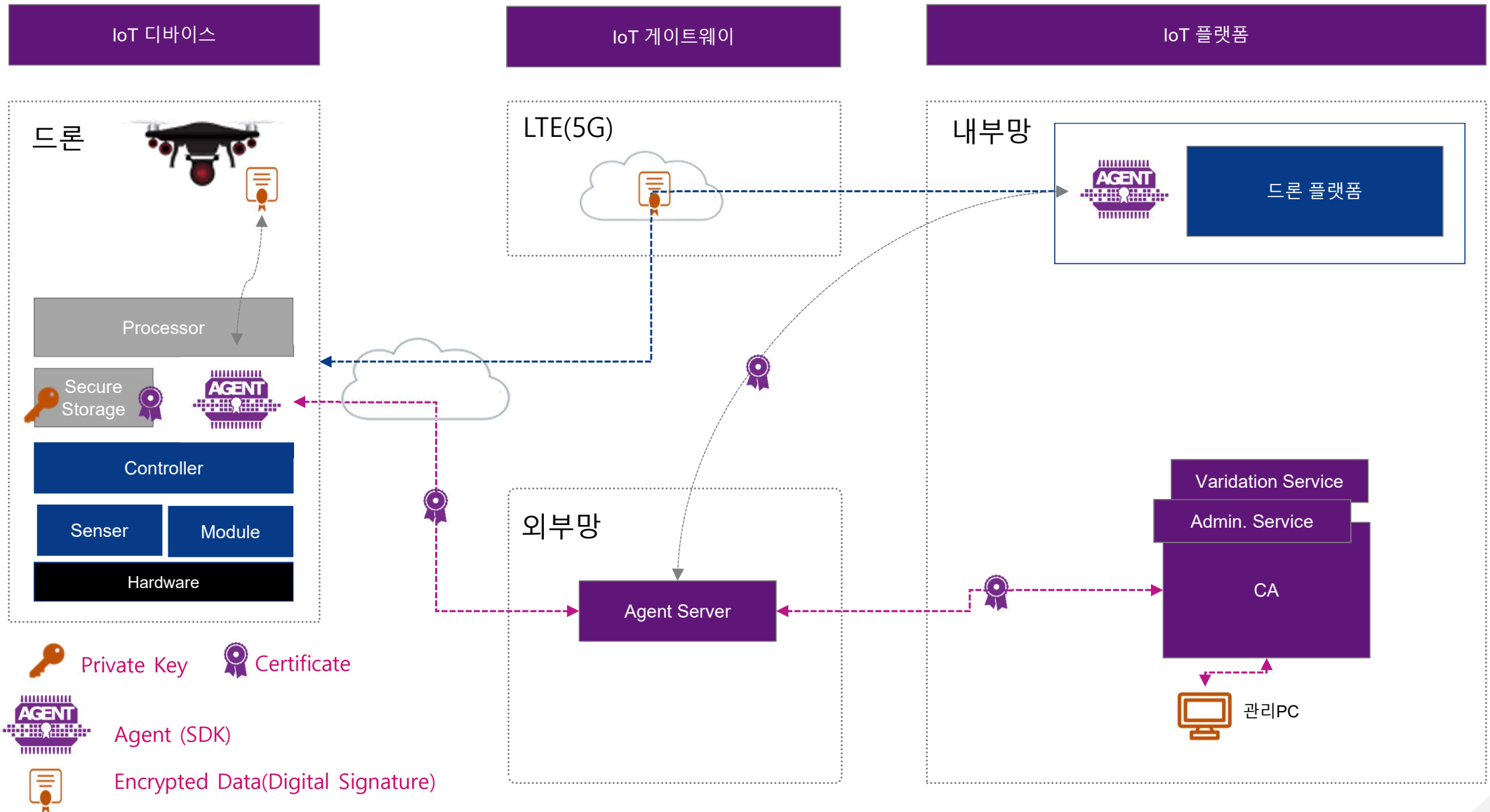


오디오 자동차 전장장비 기업 '하만'은 아이오투러스트를 도입했다. 하만은 오디오 브랜드로 유명하지만 자동차 전장 분야 선도 기업이다. 하만 사업 분야 중 커넥티드 서비스(Connected Service)는 IoT 서비스와 솔루션 사업부다. 초기 하만은 IoT 솔루션에서 사용하는 게이트웨이와 센서 등 엔드포인트 장치 인증과 데이터 보안을 위해 파일시스템에 보관하는 비밀키(PSK) 방식을 채택했다. 비밀키의 외부 도용 위험이 크고 하드웨어 보안 업그레이드가 어려웠다. 하만은 IoT 기기를 배치하기 전에 인증과 보안 문제를 해결하려고 아이오투러스트를 도입했다. 아이오투러스트 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

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

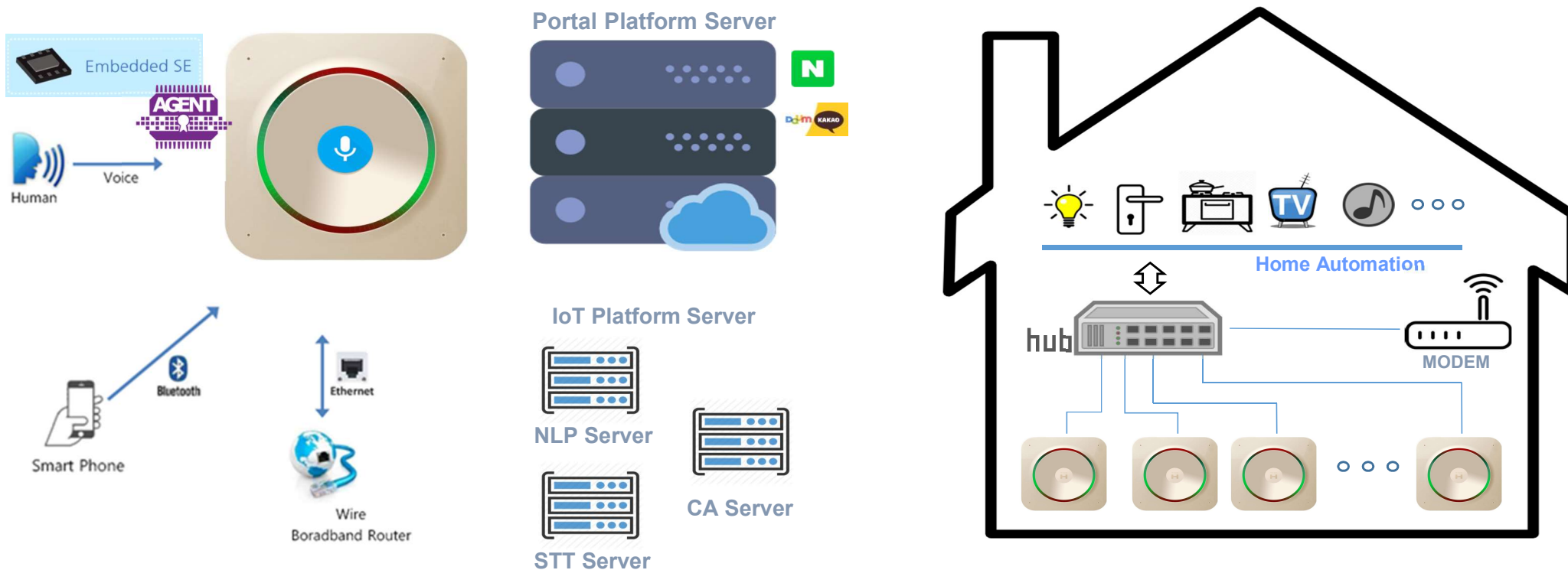




5. 구축 예시 : Secure Element 사례

하드웨어보안모듈 – Embedded SE

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



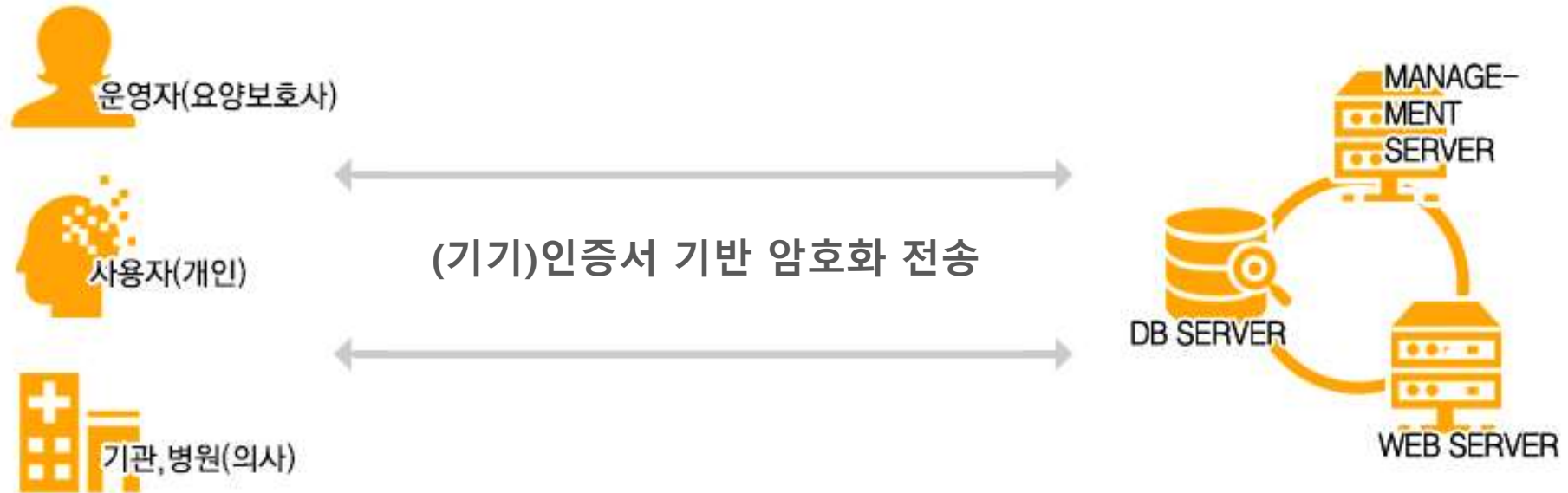
Agent (SDK)

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

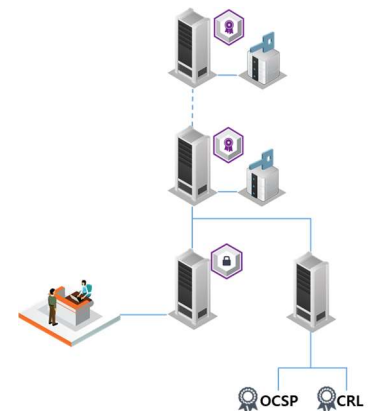


5. 구축 예시 : Secure microSD 사례

하드웨어보안모듈 – microSD



공개키기반

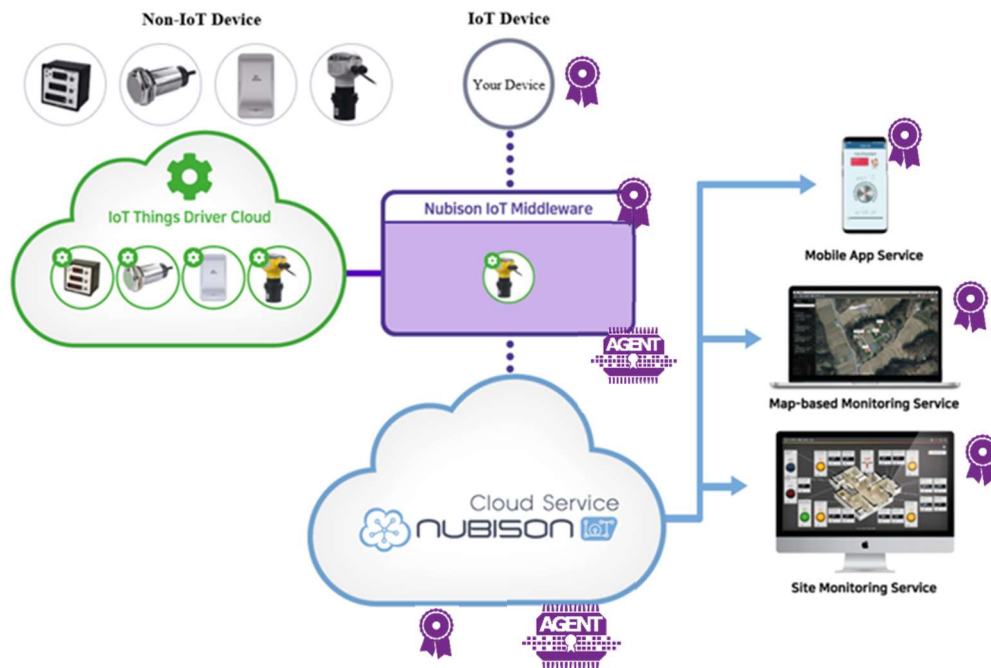




5. 구축 예시 : IoT Cloud 서비스 사례

IoT 플랫폼 기반 보안 구성

상호 기기인증과 강력한 암호화



Certificate & Security

강력한 암호화를 사용하여 데이터 통신을 보호하고, 이를 통해 기기에 신뢰할 수 있는 디지털 인증서를 발급하고, 안전하게 관리하는 방법을 제공합니다.



IoT 인증서(디지털 신원정보) 발급



IoT 인증서를 안전하게 관리



강력한 암호화로 IoT 데이터 보호



인증서 관리 에이전트 제공



6. 레퍼런스

☐ NASA, 전자여권, 인터폴, 스위트 등

포천 500대 글로벌 기업		금융 서비스	
항공우주 & 운송			
통신			
공공기관 및 정부			



7. 플랫폼 : Things

☐ 디지털 ID로 보안 : IoT is CoT(Certificate of Things)

Certificate Provider

IoT is a Certificate of Things

Managed Service by Cloud, on-Premise, Hybrid





별첨 01. Entrust Overview

Entrust® Securing Digital Identities & Information



Securing Your Digital Life

About Entrust

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

구 분	Entrust
홈페이지	www.entrust.com
개요	✓ Privately held ✓ Headquartered in Minneapolis, Minnesota, USA ✓ Founded in 1969 ✓ Over \$600M in annual revenue ✓ 2,000+ employees in 34 worldwide locations ✓ Sales, service and support covering 150+ countries ✓ 10M+ identity and payment credentials issued daily ✓ Billions of transactions managed annually
제품 & 서비스	✓ SSL Certificates ✓ ID card Printers ✓ Authentication ✓ Digital Signing Certificates ✓ Financial Card Printers ✓ ioTrust IoT Security ✓ Central Card Issuance ✓ PKI(Public Key Infrastructure) ✓ Credit Card Embossers ✓ Passport Systems





별첨 02. Why Entrust PKI

1. 세계 여러 정부가 엔트러스트를 선택하였습니다.
 - 35개국 이상의 정부가 가장 크고 복잡한 신뢰 환경에서 사용
 - 특히 전자여권 환경에서 사용
 - 150개국 이상의 고객을 보유
2. 20여년간 고객 기술지원 이력을 보유하고 있습니다.
 - 중단없는 업그레이드 기술지원이 가능
 - 전세계 34개소 지사와 2,000여명 직원을 보유
3. PKI 테크놀로지의 글로벌 리더이며, 국제표준개발에 참여



Entrust Datacard™

Trusted Identities | Secure Transactions™



별첨 03. Entrust infographic

Entrust는 전세계 가장 큰 디지털 아이덴티티, 트랜잭션, 신뢰된 자산을 보호하고 있습니다.



THANK YOU

www.kcert.co.kr



(주)한국공인인증서비스

- 10여년간 인증 & 보안, 전자서명 솔루션 공급
- 국내 1위 RA(인증서 대행 발급) 서비스 전문 업체
- 엔트러스트*가 선택한 국내 유일 한국총판

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