

AUTOCRYPT

Secure First, Then Ride

2022

- A SPICE CL2 획득
- Red Herring Award Top 100 Global 선정
- V2X 최상위 인증기관 'Root CA' 등록
- AUTOTECH BREAKTHROUGH AWARDS, Ride Hailing Innovation of the Year 수상
- CYBERSECURITY BREAKTHROUGH AWARDS, Automotive Cybersecurity Solution of the Year 수상
- 국제교통포럼 ITF 기업협력 보드멤버 협약
- 한국교통안전공단 수요응답형 대중교통(DRT) 수주

2021

- Forbes 아시아 100대 유망기업 선정
- 캐나다, 독일 지사 설립
- ISO27001, ISO14001, ISO9001 획득
- 완성차제조사 H사와 보안성 테스트 시스템 개발
- 완성차제조사 C사와 CAN-IDS를 비롯한 통합 보안관제시스템(SOC) 개발
- 자율주행차제조사 M사와 사용자 인증 단말 보안 솔루션 개발
- 차량SW플랫폼사 A사와 AUTOSAR 보안모듈 개발

2020

- 지능형자동차부품진흥원 자율주행시험장 인증보안솔루션 구축
- H사 중국항 C-V2X 사업 계약
- H사 해외(호주, 뉴질랜드, 푸에르토리코) Auto Premium 서비스 보안인증시스템 구축
- K 통신사 V2P 기반의 V2X 안드로이드 플랫폼 개발 사업 계약
- 울산광역시 C-ITS 보안인증시스템 구축
- TU -Automotive Awards, The Automotive Tech Company of the Year Finalist 선정
- apmaIAC Cyber Mobility Awards, Global Cyber Achievement 수상

2019

- Hsubject/ElaadNL과 전기차 충전 상호운용성 기술 개발을 위한 MOU 체결
- OECD산하 '국제교통포럼 ITF(International Transport Forum)' 가입
- 완성차제조사 S사 V2X 보안 솔루션 컨설팅
- 한국도로공사 V2X보안인증체계 실증시스템 구축사업
- 전장제조사 M사 IVI(In-Vehicle Infotainment)용 보안 솔루션 개발
- 한국지능형교통체계협회 V2X 보안인증체계 연계를 위한 인증기관(CS) 실증시스템 개발
- AutoCrypt®, TU-Automotive AWARDS 2019 Best Auto Cybersecurity Product/Service 선정
- 한국전력공사 전기차 충전을 위한 보안 인프라 구축
- 서울특별시 C-ITS 실증사업 보안시스템 구축
- 차량보안 전문기업 AUTOCRYPT(주)(아우토크립트) 분할 창업

2018

- 한국전력공사 전기차 충전사업자(MO)용 인증시스템 구축
- 제주특별자치도 C-ITS 실증사업 보안시스템 구축
- 그리드위즈와 전기차 Plug and Charge 솔루션 상용화
- 모바일제조사 S사 V2P(차량과 스마트 디바이스)용 스마트폰 기반의 C-ITS 서비스 개발
- 한국도로공사 지능형 교통망구축을 위한 V2X 보안체계정보화전략계획 수립
- 철도기술연구원 열차자율주행제어시스템(T2T) 보안모듈 시제품 제작

2017

- 완성차제조사 H사 V2G(전기차 충전)을 위한 TLS/HSM 보안 기술 개발
- 교통안전공단 K-City 자율주행 실험 도시(경기도 화성)
- 여주고속도로 자율협력주행을 위한 보안인증체계 구축
- 철도기술연구원 열차제어시스템(T2T) 프로토타입 보안취약성분석 및 철도차량용 보안모듈 설계
- 전자부품연구원 스마트 자율주행협력 도로주행시스템 개발을 위한 인증센터 구축

2016

- 정보통신기술진흥센터 자율주행 스마트자동차용 이상징후 탐지 핵심기술 개발
- 한국도로공사 C-ITS 시범사업을 위한 보안인증체계 구축 (대전-세종)
- 한국산업기술평가관리원 K-BrainPower 머신러닝에 기반한 이상행위 탐지기능 개발

2015

- 국내 최초 자동차보안 솔루션 AutoCrypt® 출시
- 스마트카 방화벽 시제품 개발

2014

- 완성차제조사 H사 차량 데이터 관리시스템 (VDMS)의 보안기술 개발
- 완성차제조사 H사 텔레매틱스용 스마트폰 앱 보안검증기술 개발
- 국내 최초 차량통신 보안기술 확보(IEEE1609.2 전체 규격 구현 및 테스트베드 적용)

2013

- WAVE 통신 기반의 V2X 환경을 위한 국제 표준(IEEE1609.2:2013) 기술 개발

2012

- Patrol Car 네비게이션/텔레매틱스 시스템인증/암호화 개발 구축

2011

- 차량과 외부 스마트디바이스 연동에 대한 인증 및 암호화 적용으로 보안 향상

2007

- 완성차제조사 H사 차량 안전 진단 장치용 보안 장치(차량과 진단기기 간 보안 통신 기술)개발

협회 및 표준 활동



수상



2019 Best Auto Cybersecurity Product/Service

2020 Automotive Tech Company of the Year Finalist

2021 Automotive Tech Company of the Year Finalist



2020 Global Cyber Achievement Award



2020 Automotive Cybersecurity Company of the Year

2021 Automotive Cybersecurity Company of the Year

2022 Automotive Cybersecurity Company of the Year

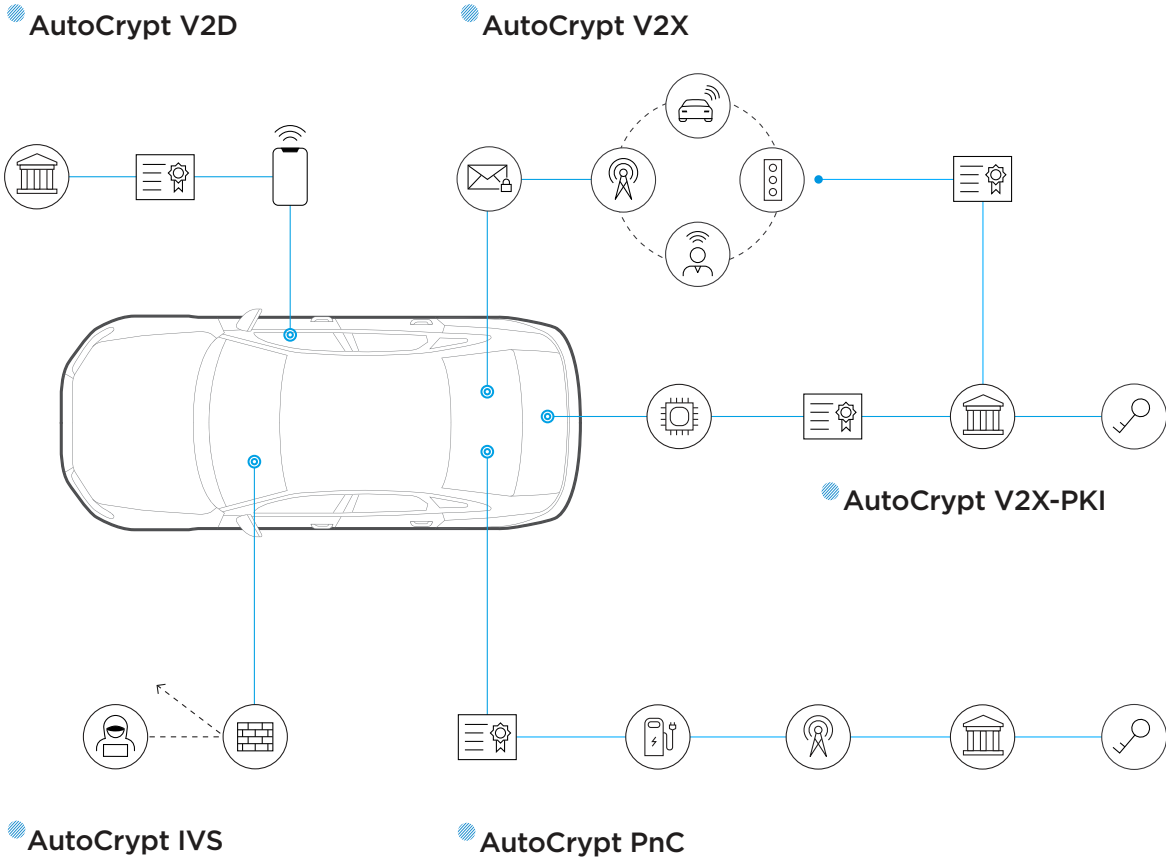


2022 Ride Hailing Innovation of the Year



2021 "100 to Watch"

Autocrypt는 차세대 지능형 교통 시스템(C-ITS)과 커넥티드 카를 위한 자동차 보안 토탈 솔루션입니다.

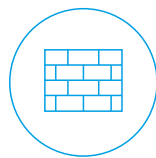


커넥티드 카에 맞춤형 된 보안 토탈 솔루션



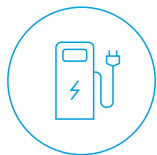
지능형 교통시스템

차세대 지능형 교통시스템 (C-ITS)통신에 필수적인 핵심 보안 요소를 제공합니다.



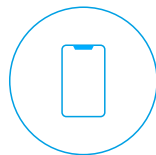
차량 내 보안

내/외부 위협으로부터 차량내부 네트워크를 보호하고 차량내 보안 업데이트 및 관리를 제공합니다.



전기차 및 충전시스템

전기차 충전시 차량과 충전기 간의 안전한 데이터 통신과 신뢰할 수 있는 상호 인증 기능을 제공합니다.



모빌리티 및 디지털 키 시스템

모바일차량 관리앱, 원격 제어시스템 등의 서비스에서 차량과 디바이스 간의 안전한 통신을 제공합니다.

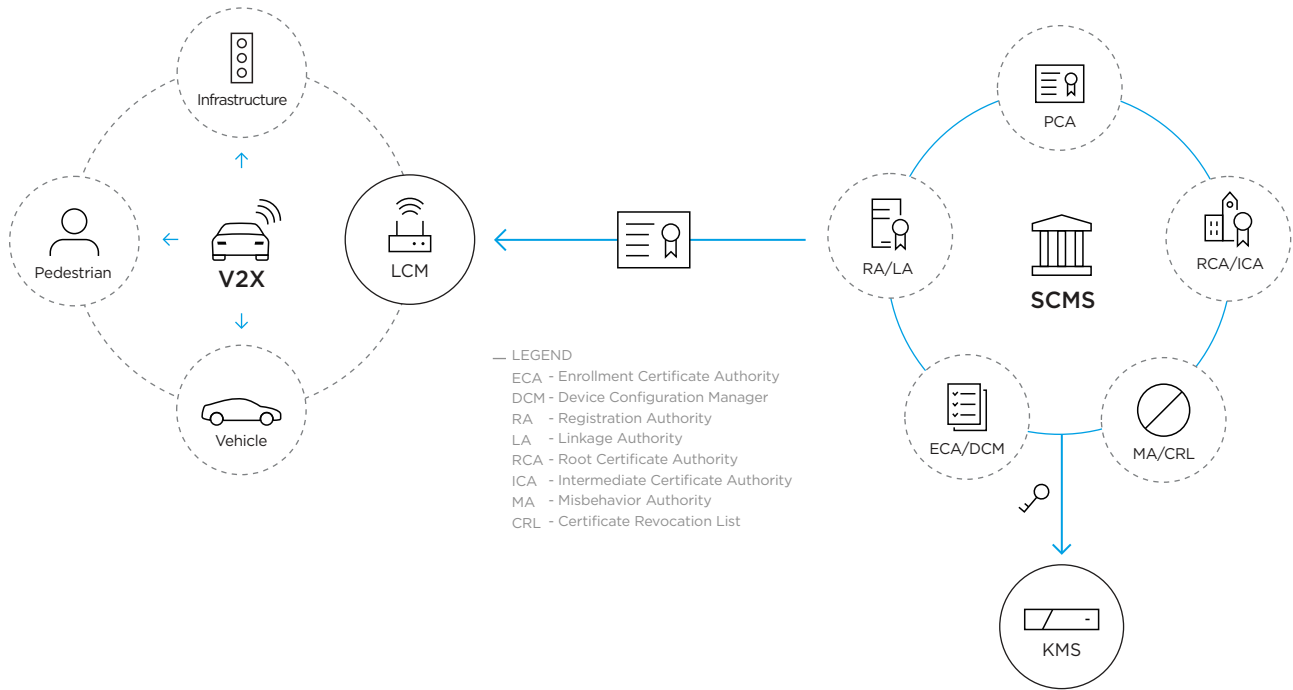
Autocrypt는 차세대 지능형 교통 시스템(C-ITS, Cooperative-Intelligent Transport System)의 안전한 보안 통신을 위한 전체 보안 솔루션을 제공합니다. Autocrypt는 CAMP(Crash Avoidance Metrics Partnership), IEEE 등 국제 주요 표준을 준수합니다.

AutoCrypt V2X

차량 및 교통 인프라를 위한 보안 통신 시스템

AutoCrypt V2X는 차량과 차량, 차량과 사람, 차량과 교통 인프라 등 모든 V2X 환경의 안전한 보안 통신을 위한 인증 및 암호화 시스템입니다.

- OBU(On-Board Unit)와 RSU(Road Side Unit) 간 BSM(Basic Safety Message) 등 보안 통신을 위한 암호화, 전자서명 제공
- 차량무선통신(WAVE, 5G)의 보안 표준규격 IEEE 1609.2.1 지원
- OBU에 설치된 AutoCrypt LCM(Local Certificate Manager)이 AutoCrypt PKI와 통신하며 인증서를 발급받고 OBU 내에 안전하게 관리



AutoCrypt V2X-PKI

차량 및 교통 인프라를 위한 PKI 인증 시스템

AutoCrypt V2X-PKI는 자동차와 자동차, 자동차와 교통인프라 시스템 간의 안전한 통신을 위해 국제 표준에서 요구하는 인증서들을 발급하고 관리합니다.

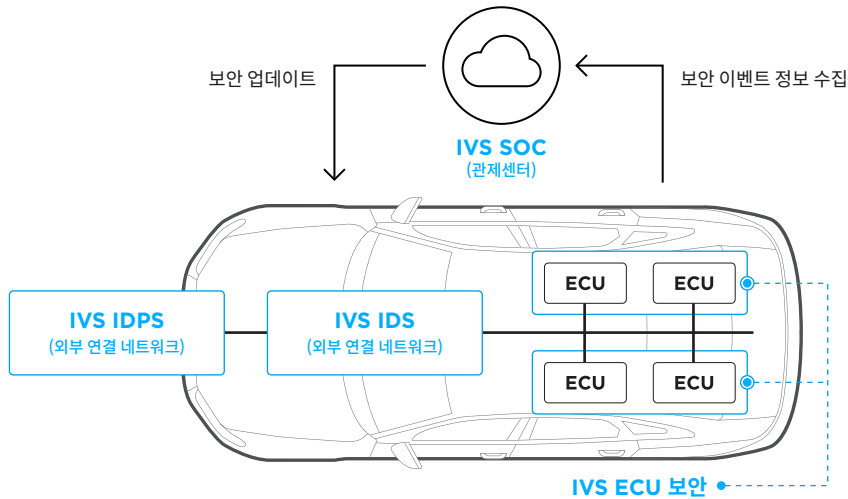
- OBU, RSU에 등록 인증서(Enrollment Certificate), ID 인증서(Identification Certificate), 익명 인증서(Pseudonym Certificate), 어플리케이션 인증서(Application Certificate) 발급
- 부정/이상 행위 검출 및 인증서 폐기 목록(CRL)관리
- 보안 표준규격 IEEE 1609.2.1(SCMS) 및 CCSA(China Communication System Association), EU CCMS(Cooperative ITS Credential Management System) 지원



AutoCrypt IVS

차량 네트워크 및 전장 보안 시스템

AutoCrypt IVS는 차량 내/외부 위협을 분석하여 요구되는 보안 기능을 차량 네트워크와 ECU에 전략적으로 적용하여 안전한 차량 보안 환경을 만들어 줍니다. 퍼징, 침투시험 등의 모의해킹을 수행하여 보안성을 검증하고 규제 대응을 준비해 드립니다. 모든 기능을 보안관제시스템으로 통합 구성하여 차량 모니터링, 보안 정책 업데이트를 운영하고, WP.29 대응의 모든 과정에서 요구되는 자료를 생성해 드립니다.



AutoCrypt IVS 항목 리스트

보안 환경 설계

TARA - 위협/리스크 분석

- 공격 경로 파악, 공격 난이도 분석
- 자산 식별, 자산 가치 분석
- 위협 대응 우선 순위 작성

보안 적용 컨설팅

- TARA 결과 적용
- 위협 완화 전략/절차 수립
- 보안 엔지니어링 설계

네트워크 보안

IVS IDPS

- 차량 외부 네트워크 공격 탐지 및 방어
- 방화벽 접근제어(Black List / White List)
- Host 기반의 DPI(Deep Packet Inspection)

IVS IDS

- 차량 내부 네트워크 공격 이상 탐지
- CAN, CAN-FD, Ethernet 등 프로토콜 탐지
- UDS, KWP, DoIP 등 진단 프로토콜 탐지

제어기 보안

HSM/TEE - 하드웨어 보안기능

- MCU 환경의 HSM 기반 보안 기능
- 리눅스/안드로이드 환경 보안 기능

Secure Boot

- 부트로더, 커널, 커널모듈 서명 검증
- 칩 환경 별 퓨징/검증 절차 구성

Secure 업데이트 - OTA

- 무선 연결에 보안 통신 적용
- 업데이트 이미지 서명 생성/검증

Secure Debug

- 키 발행 시스템 적용, 키 주입
- 장비 인증 후 디버그 포트 개방

접근 제어

- 루트 권한 제거/최소화
- 시스템 리소스 접근 제어 / 위반 탐지

파일 시스템 암호화

- 보안환경(TEE) 기반 암호화 키 운영
- 대용량의 개인/보안 정보의 저장

테스트 / 관제

SOC - 보안관제센터

- 차량 보안 이벤트와 이상 행위 수집/분석
- 보안정책/탐지규칙 업데이트, 배포
- WP.29 대응 보안 모니터링과 기록 제공

퍼징, 모의해킹

- 4세대 모델 기반 퍼징 수행
- CAN, 이더넷, 블루투스, wifi, USB
- WP.29 대응 산출물 작성

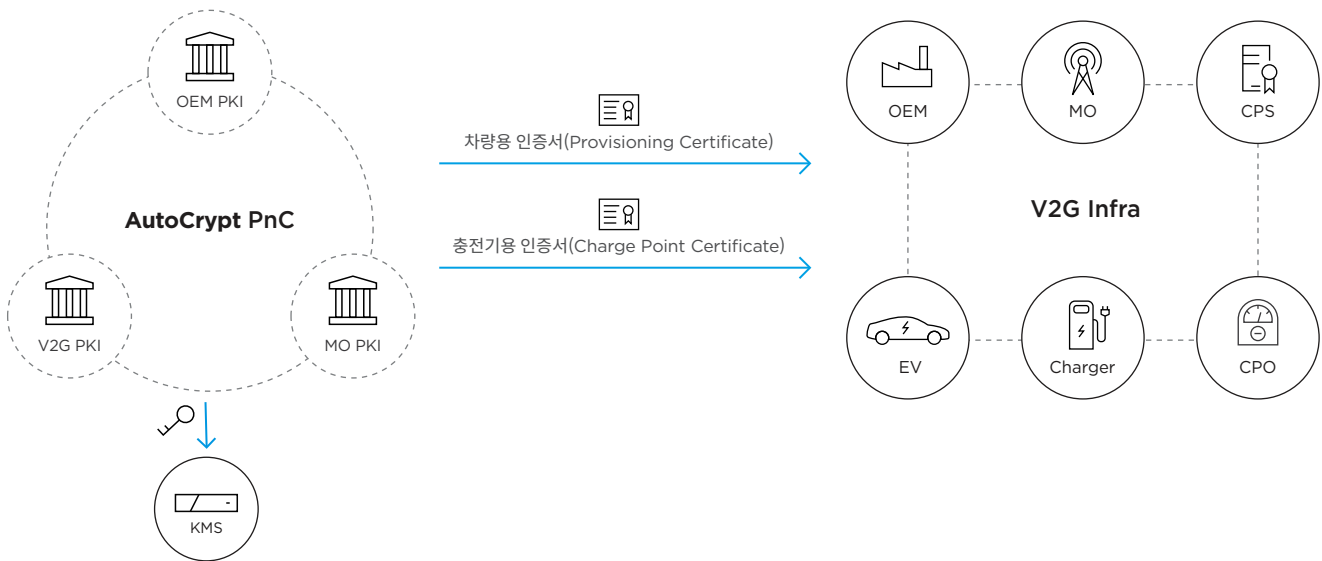
Autocrypt는 친환경 전기자동차(EV, Electric Vehicle)와 충전 장비(EVSE, EV Supply Equipment)에게 PnC(Plug & Charge) 보안과 서비스를 제공합니다. Autocrypt는 자동차 제조사, 충전기 제조사, 충전 인프라 운영 사업자(CPO, Charge Point Operator), 충전 서비스 사업자(MO, Mobility Operator)에게 보안 통신 모듈과 인증서 관리 인프라를 제공합니다.

AutoCrypt PnC

전기차 충전 시스템을 위한 보안과 PnC 서비스

AutoCrypt PnC는 PnC(Plug & Charge) 시스템의 보안 통신 및 인증 시스템을 제공합니다. AutoCrypt PnC를 통해 EV 충전 시 안전하게 PnC 서비스를 이용할 수 있습니다. AutoCrypt PnC는 PnC 환경 뿐 아니라 서비스 인프라를 위한 PKI를 제공하며, 인증, 권한부여, 결제 시스템 전반에 대한 안전하고 편리한 보안 및 서비스를 지원합니다.

- PKI 기반의 PnC 보안으로 편리하고 강력한 인증서 생성/관리/폐지, 권한부여 및 신뢰성 확보
- PKI를 기반으로 PnC 서비스를 운용하여 사용자 인증, V2G 자동 결제 및 과금 등 데이터 환경 제공
- PnC 충전을 위한 전기차와 충전기 간의 ISO-15118 표준 지원
- 충전기(EVSE)와 충전인프라간 안전한 통신을 위한 OCPP(Open Charge Point Protocol) 지원



모빌리티 서비스 디지털 키 솔루션

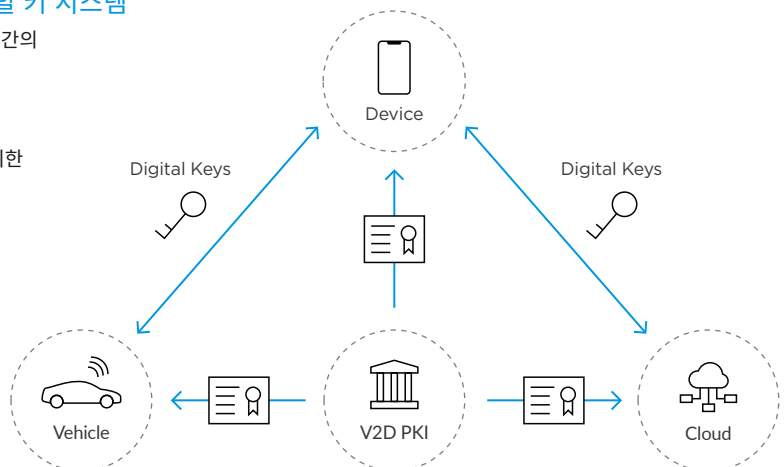
Autocrypt는 차량과 각종 스마트 기기 간 안전한 보안 통신을 지원하며, 현재 급성장 중인 자동차 공유 서비스와 자율주행차를 이용한 물류유통 서비스 등 MaaS(Mobility-as-a-Service) 사업의 기반이 되는 디지털 키를 제공합니다.

AutoCrypt V2D

차량, 모바일 기기, 클라우드 서비스를 위한 디지털 키 시스템

AutoCrypt V2D는 차량과 모바일 기기 그리고 백엔드 서비스 간의 안전한 인증 및 권한부여 등 보안 서비스를 제공합니다.

- V2D 인프라 내에서 인증서 관리를 위한 PKI 제공
- PKI를 기반으로 복수의 차량 및 복수의 스마트 기기 사용자를 위한 자동차 디지털 키의 생성, 폐기 등 인증서 관리
- NFC 통신 및 블루투스 표준 (CCC 2.0 & 3.0) 지원



AutoCrypt FMS

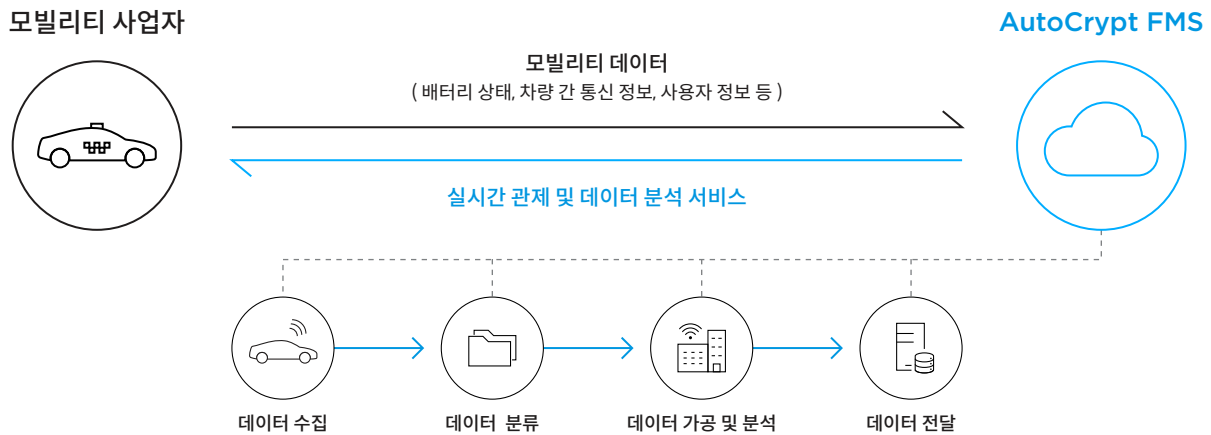
커넥티드 카 환경을 위한 진화된 Fleet Management System

AutoCrypt FMS는 차량 운영 관리시스템으로 모빌리티 서비스에서 생산되는 방대한 데이터를 수집, 분석 및 가공합니다.

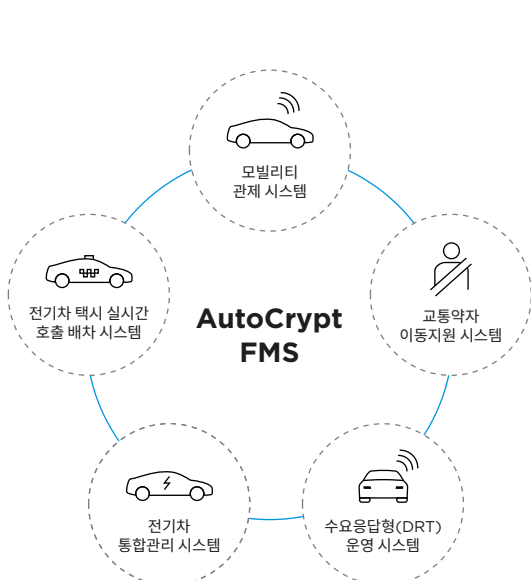
- 차량 데이터, 주행 데이터, 사용자 데이터, V2X 통신 데이터 등 다양한 모빌리티 데이터 수집
- 플러그인 방식의 데이터 수집 장치 및 소프트웨어를 통해 암호화된 환경에서 안전하고 편리하게 데이터 수집
- 수집 데이터 기반으로 비정상 운행 파악 및 차량 내 오류신호 감지
- 자체 개발한 머신러닝을 활용한 데이터 모델링, 빅데이터 기반의 상관관계 분석을 통한 인사이트 도출
- 다양한 교통 인프라 등에서 수집한 데이터 저장 및 공유, 블록체인 기반 토큰 이코노미 모델 개발

AutoCrypt FMS 구조

택시, 운송, 카셰어링 등 다양한 모빌리티 서비스에서 생산되는 데이터의 중요성과 가치는 높아지고 있습니다. 커넥티드 카 환경을 안전하게 보호하고 새로운 비즈니스를 창출하기 위해서는 모빌리티 데이터의 안전하고 간편한 수집, 분석 그리고 운영 환경에 최적화된 가공 및 활용이 필요합니다.



AutoCrypt FMS 서비스



모빌리티 관제 시스템

운수사업자 및 택시 등에서 발생하는 모빌리티 데이터를 수집, 활용해 효율성과 안정성을 높여 운영하는 관제 서비스 제공

전기차 택시 실시간 호출 배차 시스템

친환경 전기차 기반 택시 서비스를 통해 지속가능한 발전을 추구하고 미래지향적 모빌리티 서비스 제공

교통약자 이동지원 시스템

자동배차 플랫폼을 통해 효율적으로 교통약자의 이동의 자유를 보장하는 배리어프리(Barrier-Free) 서비스 제공

전기차 통합관리 시스템

안전한 전기차 주행과 관리를 위해 간편한 충전 및 차량이상진단과 BMS(Battery Management System) 데이터 수집 및 분석

수요응답형(DRT) 운영 시스템

이용객의 수요에 따라 탄력적으로 운영 가능한 DRT(Demand Responsive Transport) 서비스 제공

아우토크립트(주)

서울특별시 영등포구 여의공원로 115 B1, 1, 6, 7, 8층(여의도 세우빌딩), 07241
Tel. 02-2125-4000 E-mail. sales@autocrypt.io
www.autocrypt.co.kr

이 문서는 2023년 기준으로 제작되었습니다. 당사의 정책에 따라 내용이 추가되거나 수정될 수 있습니다.