2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

Session 1-3

커넥티드카 보안 기술 및 동향

김의석 대표이사 (아우토크립트)

[요약문]

최근의 자율주행차량(vehicle)은 Radar, Lidar, Camera등의 센서를 기반으로 자율주행기능을 구현하고, V2X 기술을 기반으로 다른 차량, 교통인프라시스템, 보행자 등과 정보를 교환함으로써 자율주행 기능을 고도화시킨다. 전자의 기능이 차량 스스로 정보를 수집하고 판단하는 동작, 즉 자율주행차량의 기본기능을 담당하는 반면, 후자의 기능은 센서의 한계를 넘어, 외부 기기와 통신함으로써 보다 다양한 정보를 수집하고, 자율주행차량(또는 운전자)이 보다 정확한 판단을 할 수 있도록 지원한다. 특히나 V2X 기술을 활용함으로써, 다양한 사고들을 효과적으로 예방하고, 효율적으로 교통환경을 개선할 수 있다.

그러나, 차량이 외부와 직접 통신하는 것은 다양한 보안 문제들을 야기할 수 있다. 차량 내부 네트워크에 대한 공격에서부터, 차량에 전달되는 메시지를 변조하거나, 임의의 메시지를 보냄으로써 차량의 안전한 운행을 오히려 방해할 수 있다. 그러므로 자율주행차량의 안전성을 확보하기 위해서는 차량자체를 안전하게 보호하고, 외부와 안전하게 통신할 수 있는 보안 체계가 반드시 필요하다. 본 발표에서는 이를 위한 주요 보안 기술들을 살펴 보고, 관련 표준들을 소개한다.

[발표자 약력]

1996년 포항공대 물리학과 학사
2010년 펜타시큐리티 개발부장
2016년 펜타시큐리티 아우토크립트 사업본부장
2019년 아우토크립트 대표이사
관심분야 : 차량 보안, V2X/SCMS, ISO 15118 기반의 Plug&Charge, CAN Network 보안

AUTOCRYPT

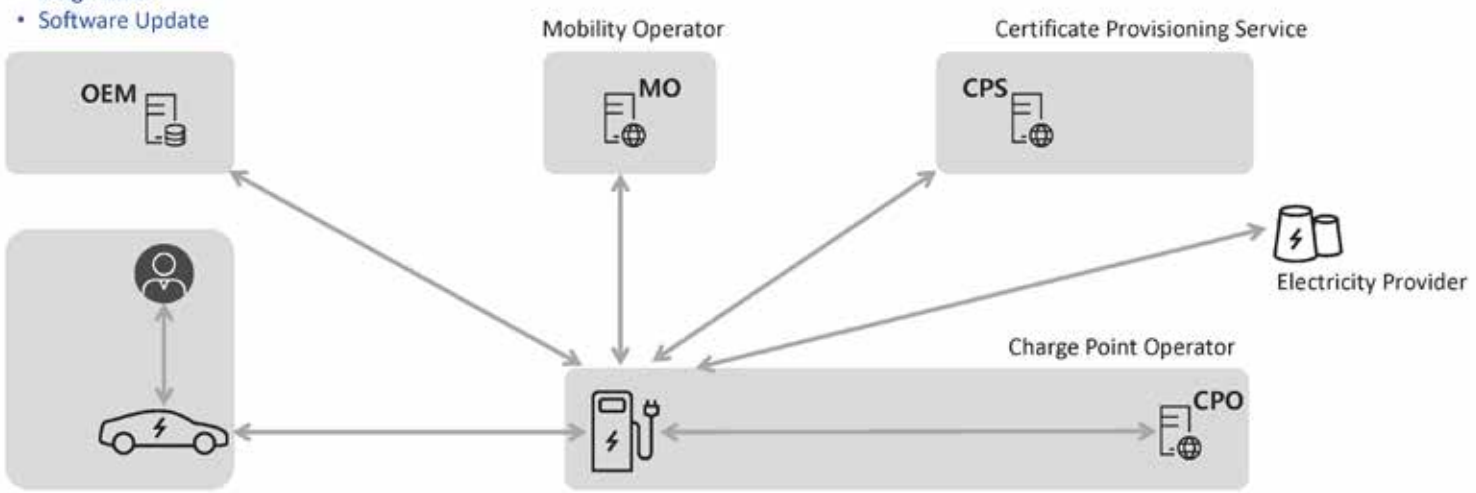
TU-Automotive AWARDS

TU-Automotive Awards
Best Auto Cybersecurity
Product/Service 2019

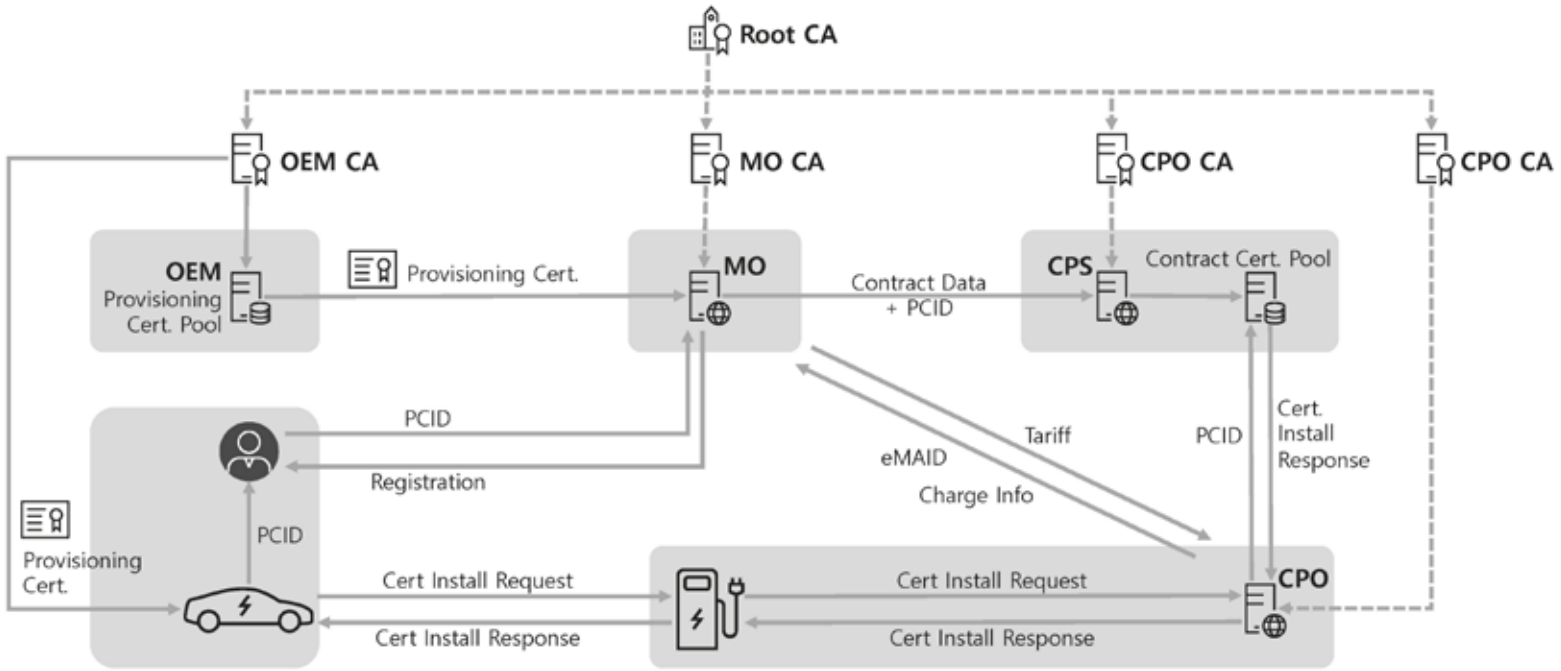
Momentum Technologies

Momentum Technologies : SPACE - Electrification

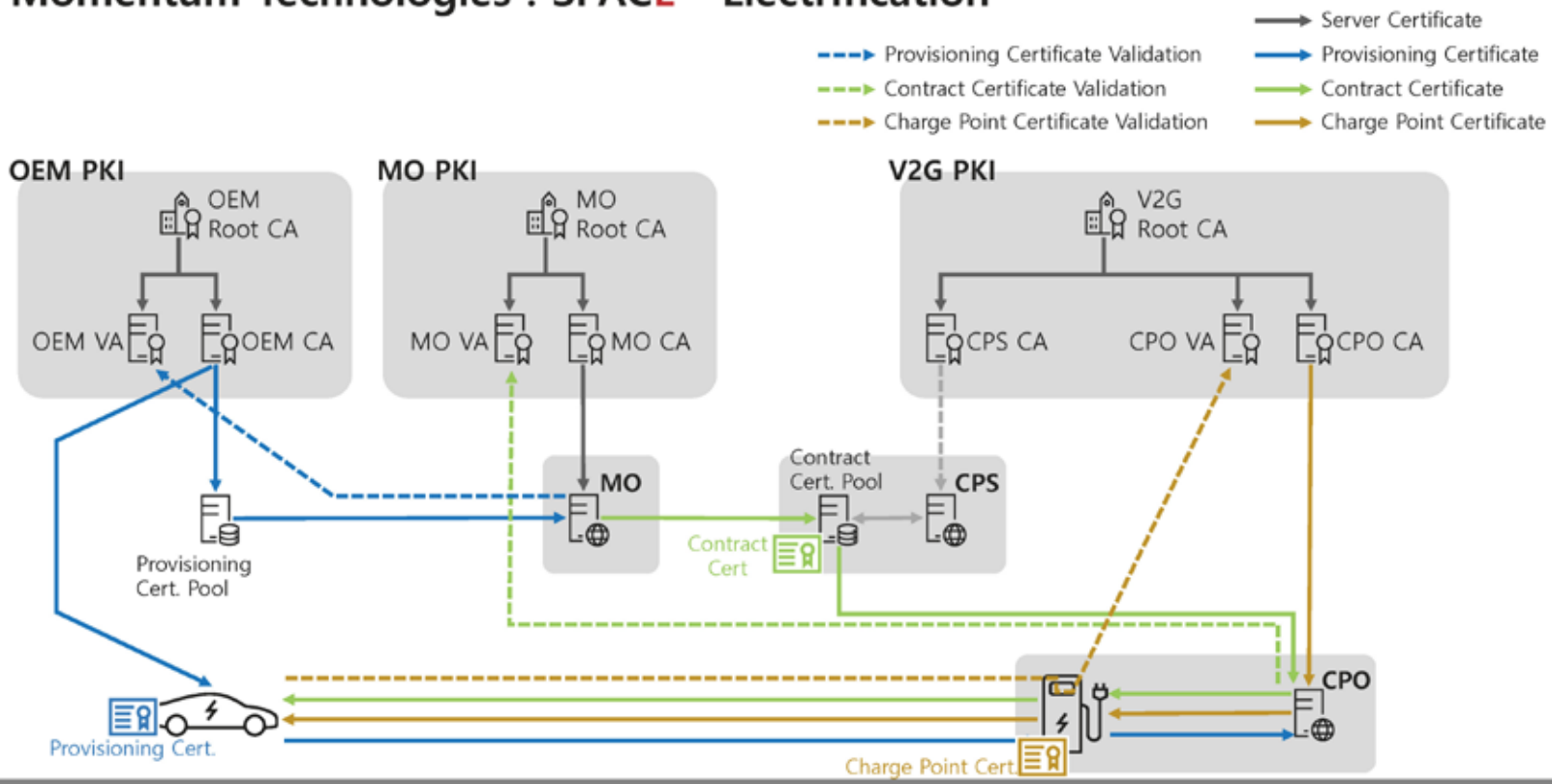
- Diagnostics
- Software Update



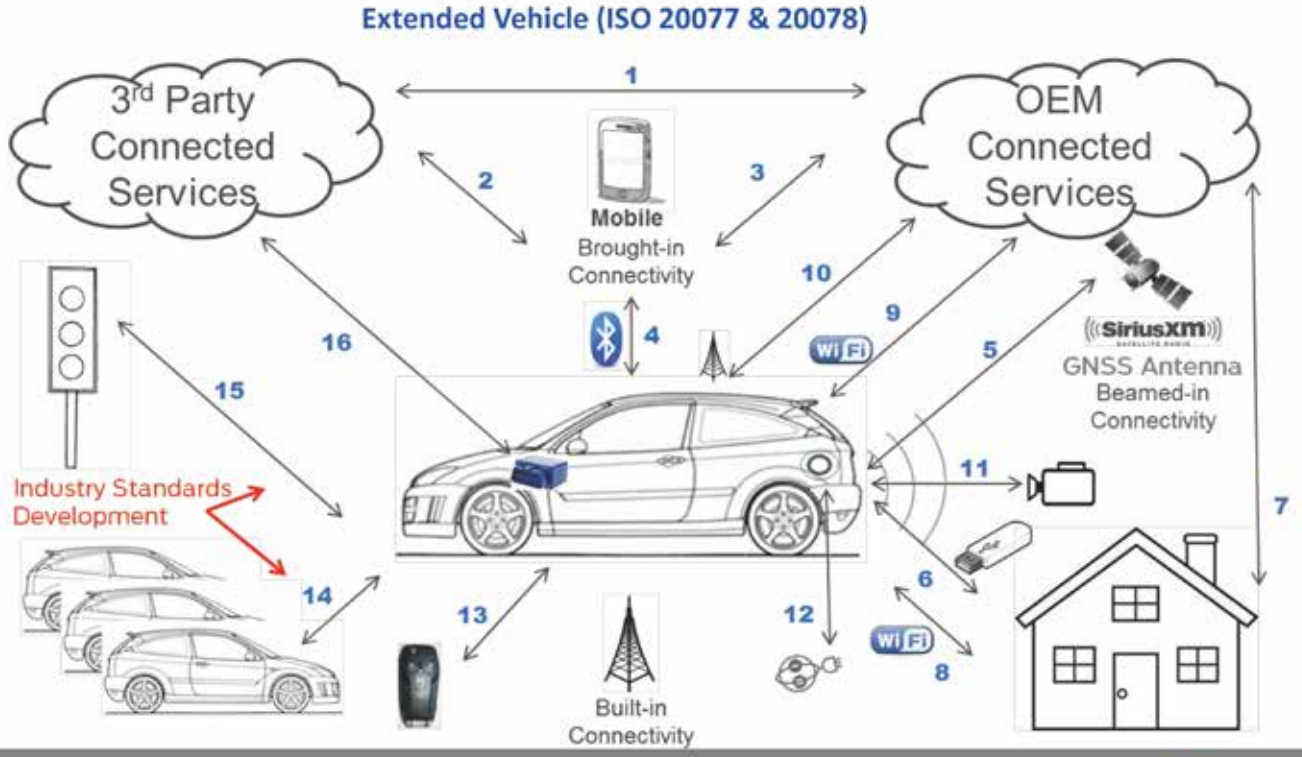
Momentum Technologies : SPACE - Electrification



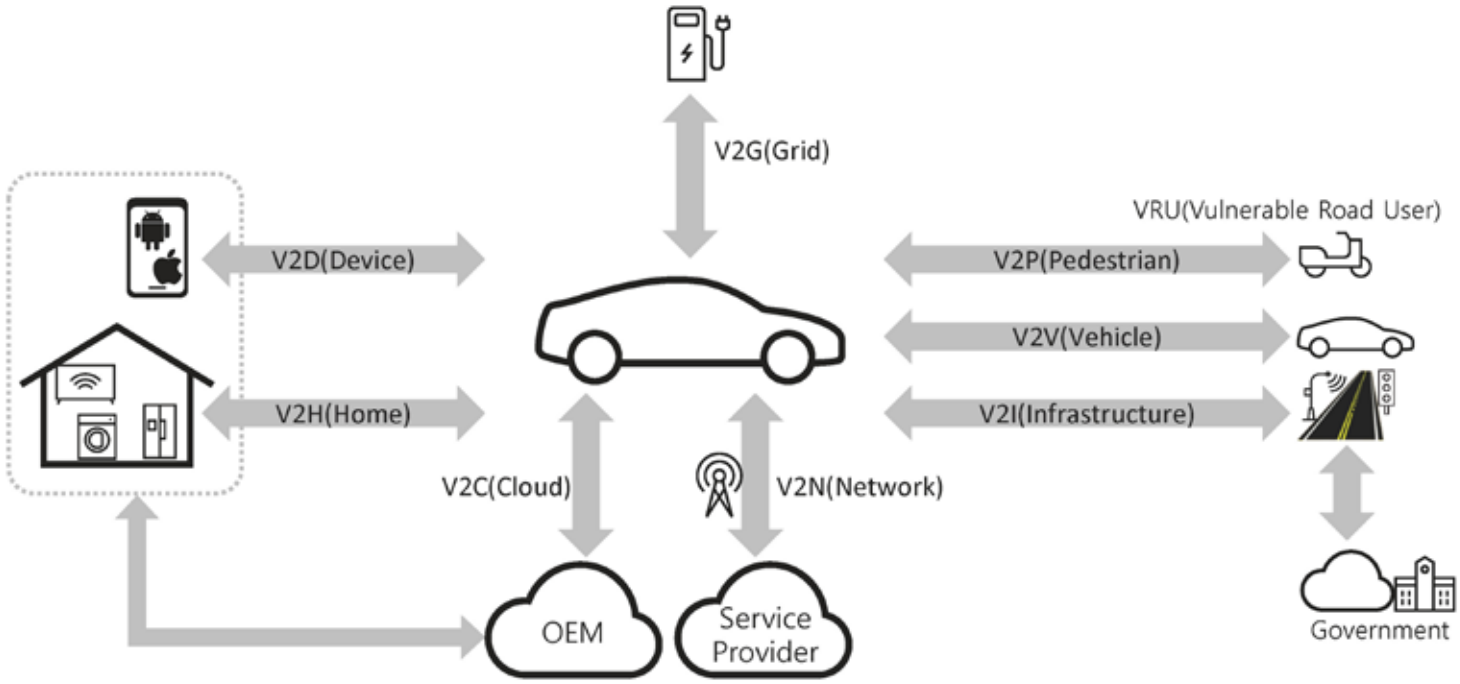
Momentum Technologies : SPACE - Electrification



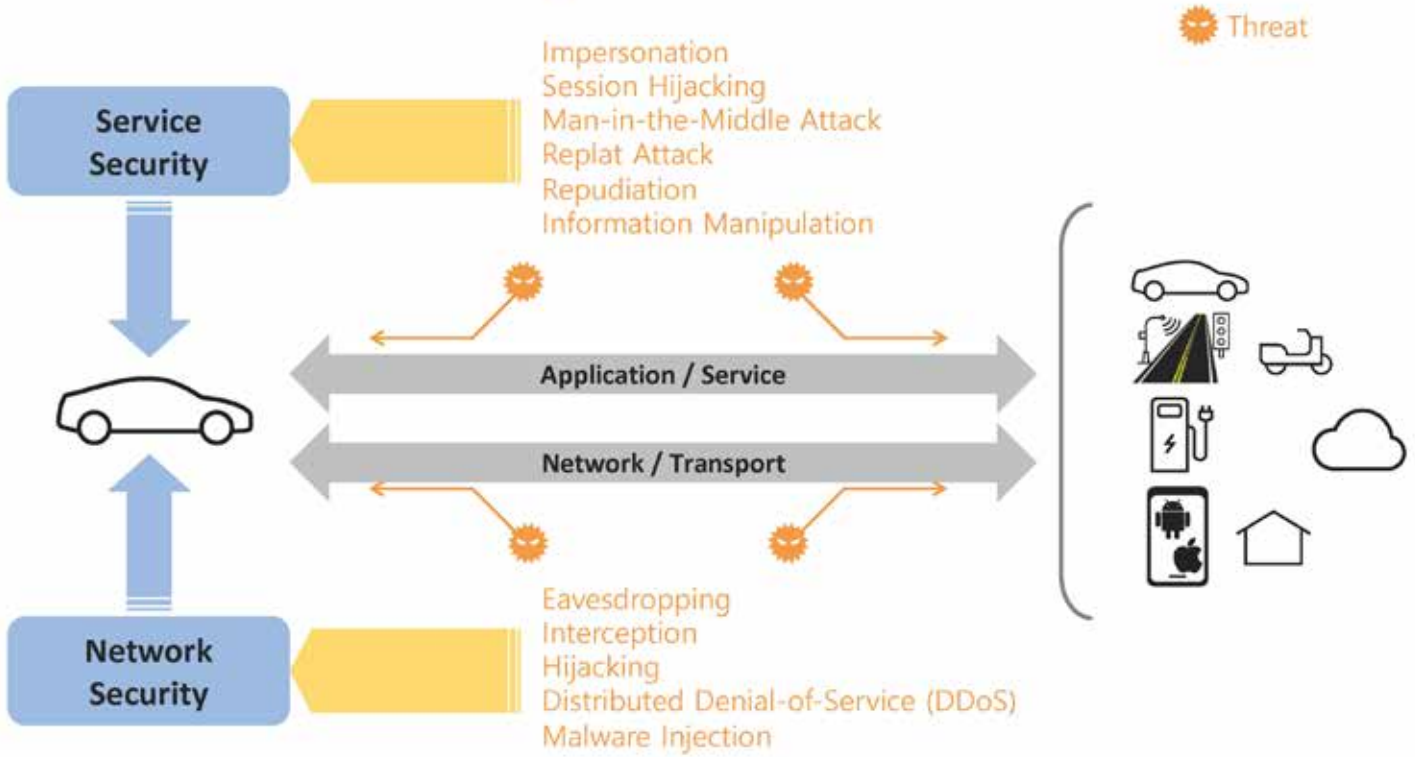
Momentum Technologies : SPACE - Connectivity



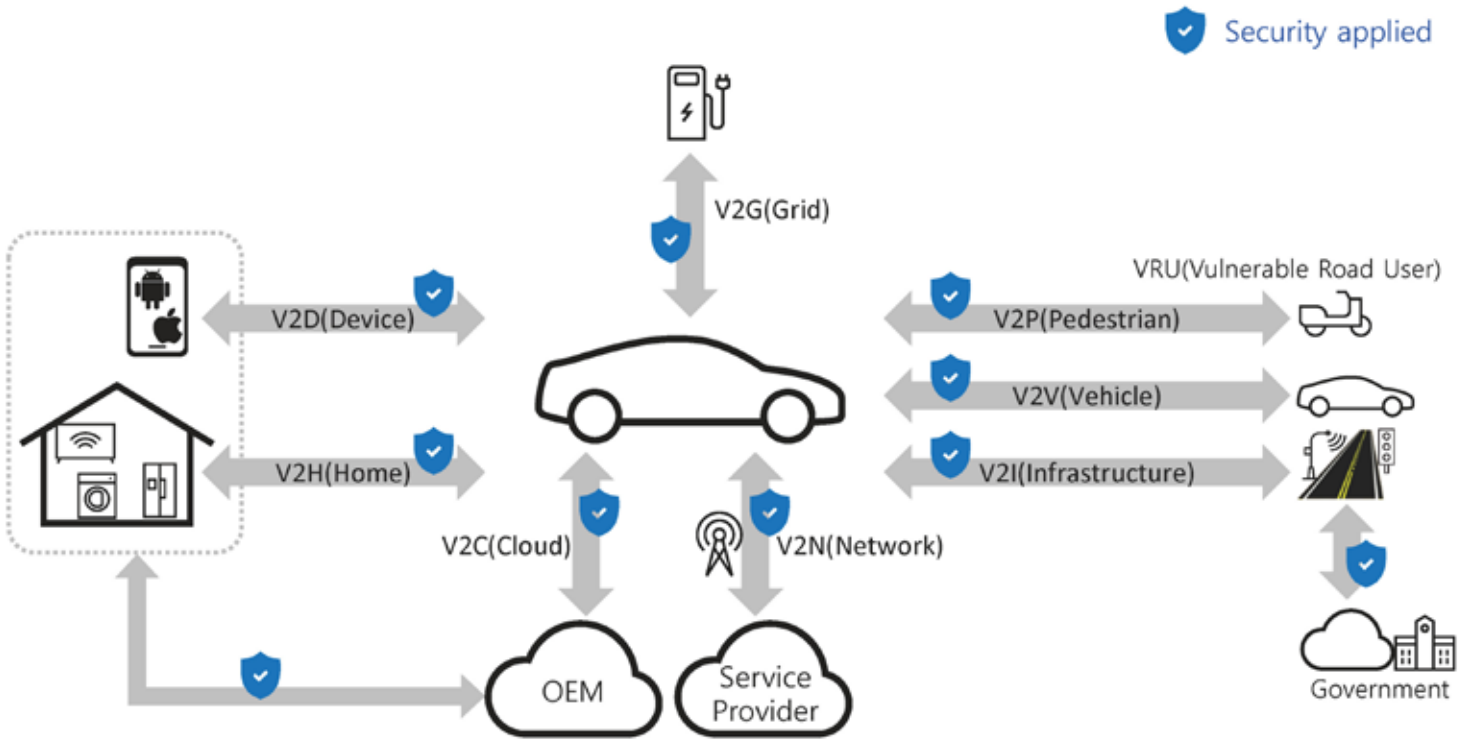
Momentum Technologies : SPACE - Connectivity



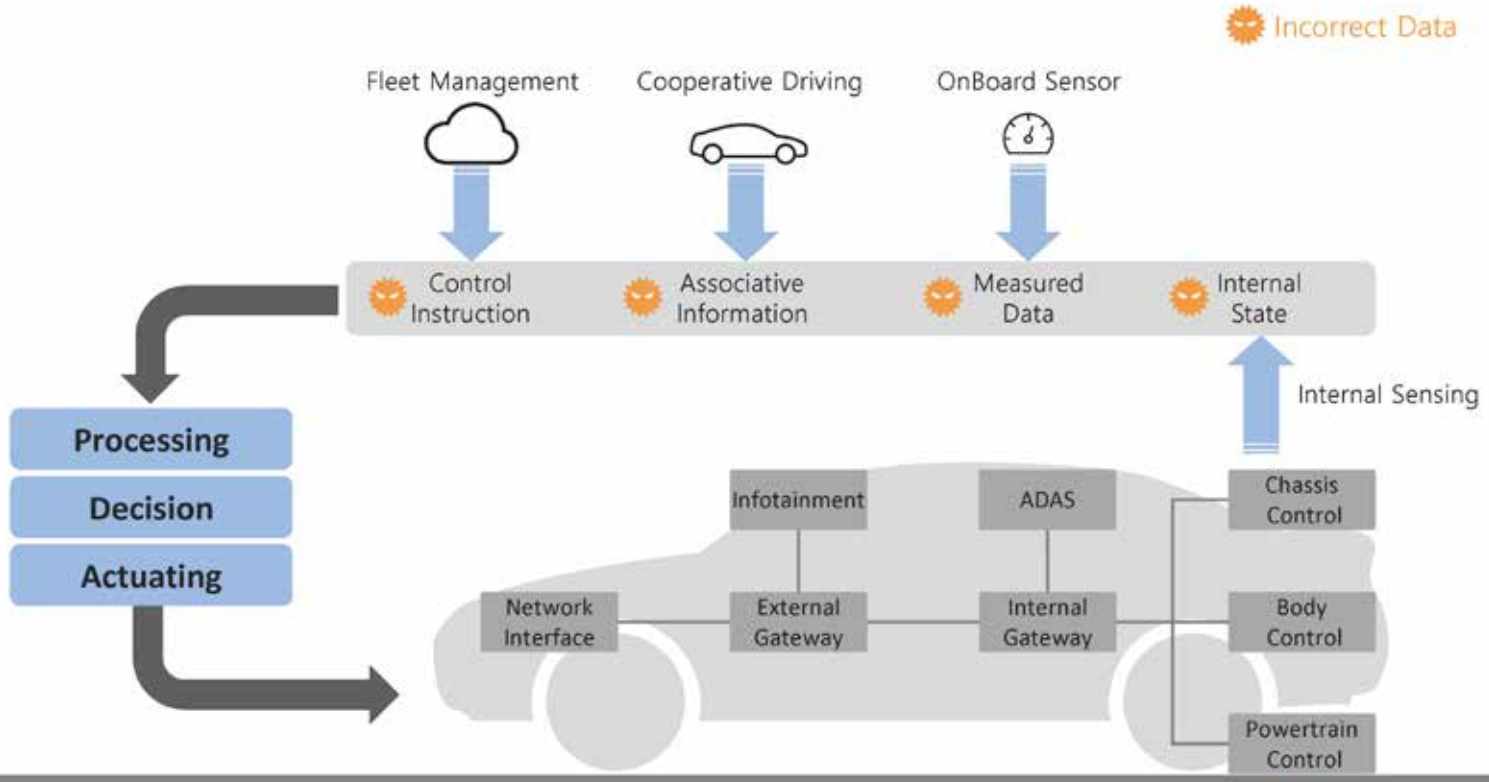
Momentum Technologies : SPACE - Connectivity



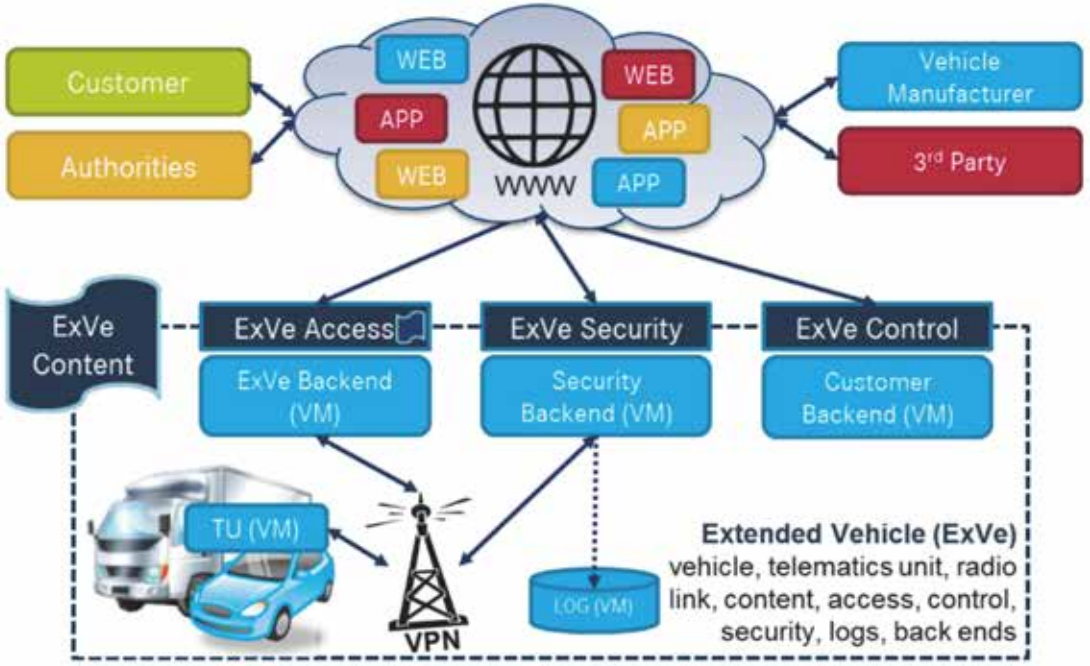
Momentum Technologies : SPACE - Connectivity



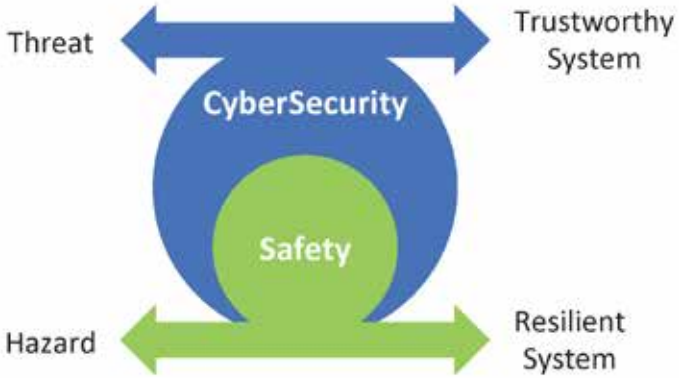
Momentum Technologies : SPACE – Autonomous Driving



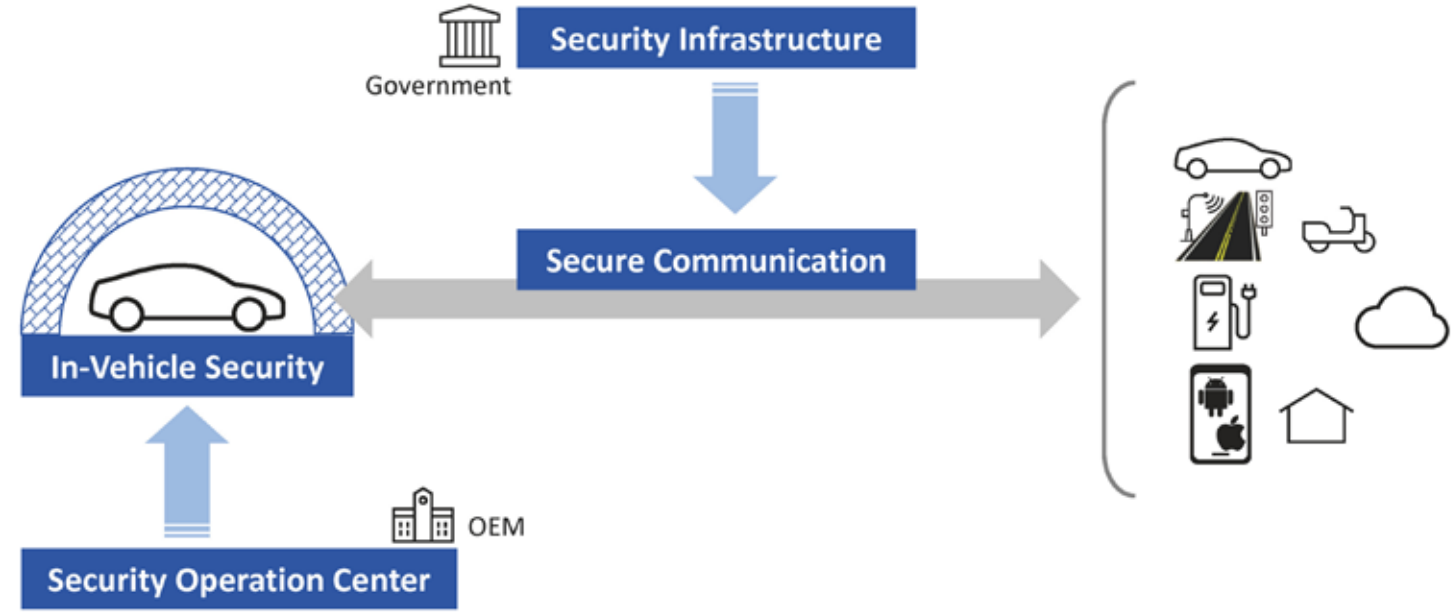
Momentum Technologies : SPACE – Service Platform



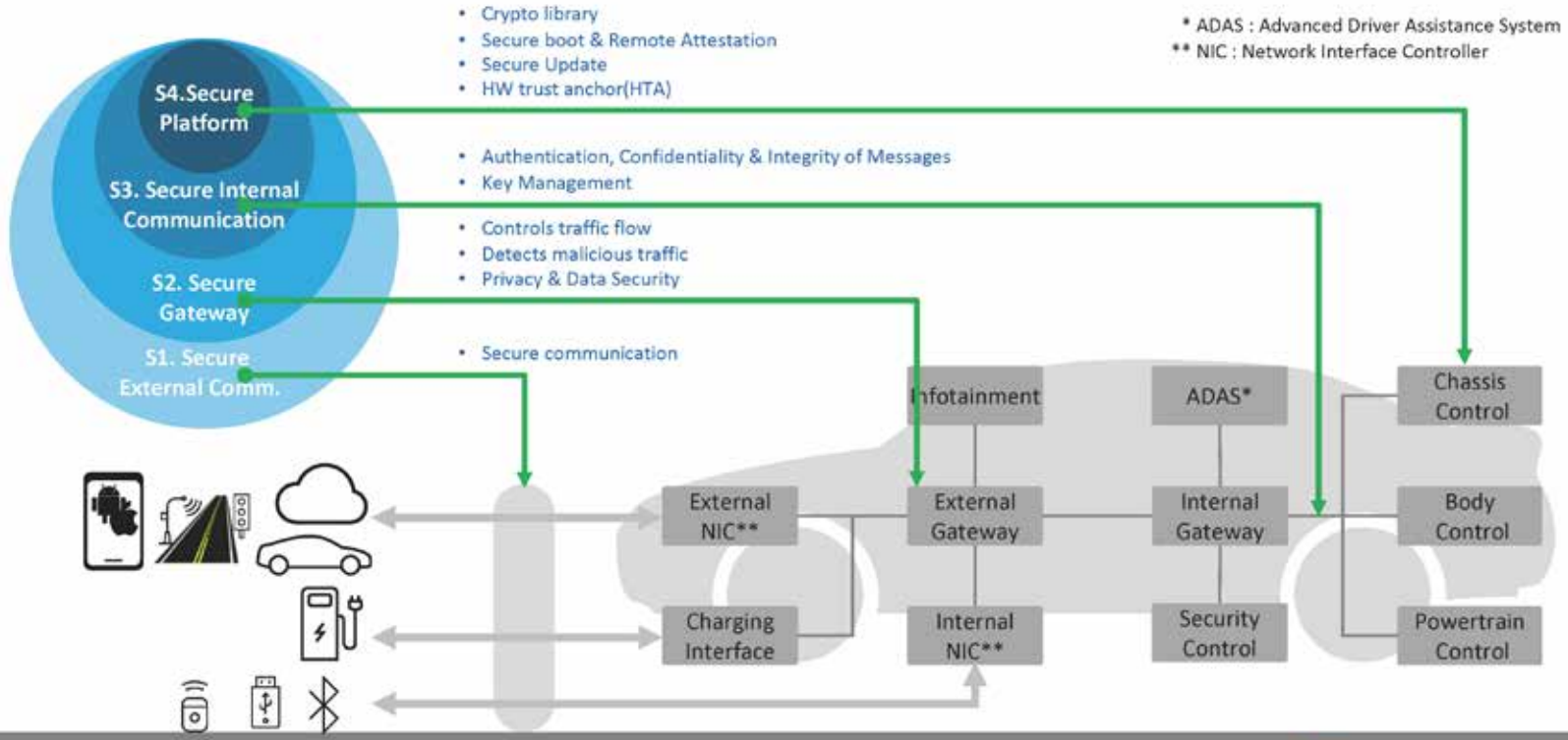
Momentum Technologies : SPACE – CyberSecurity



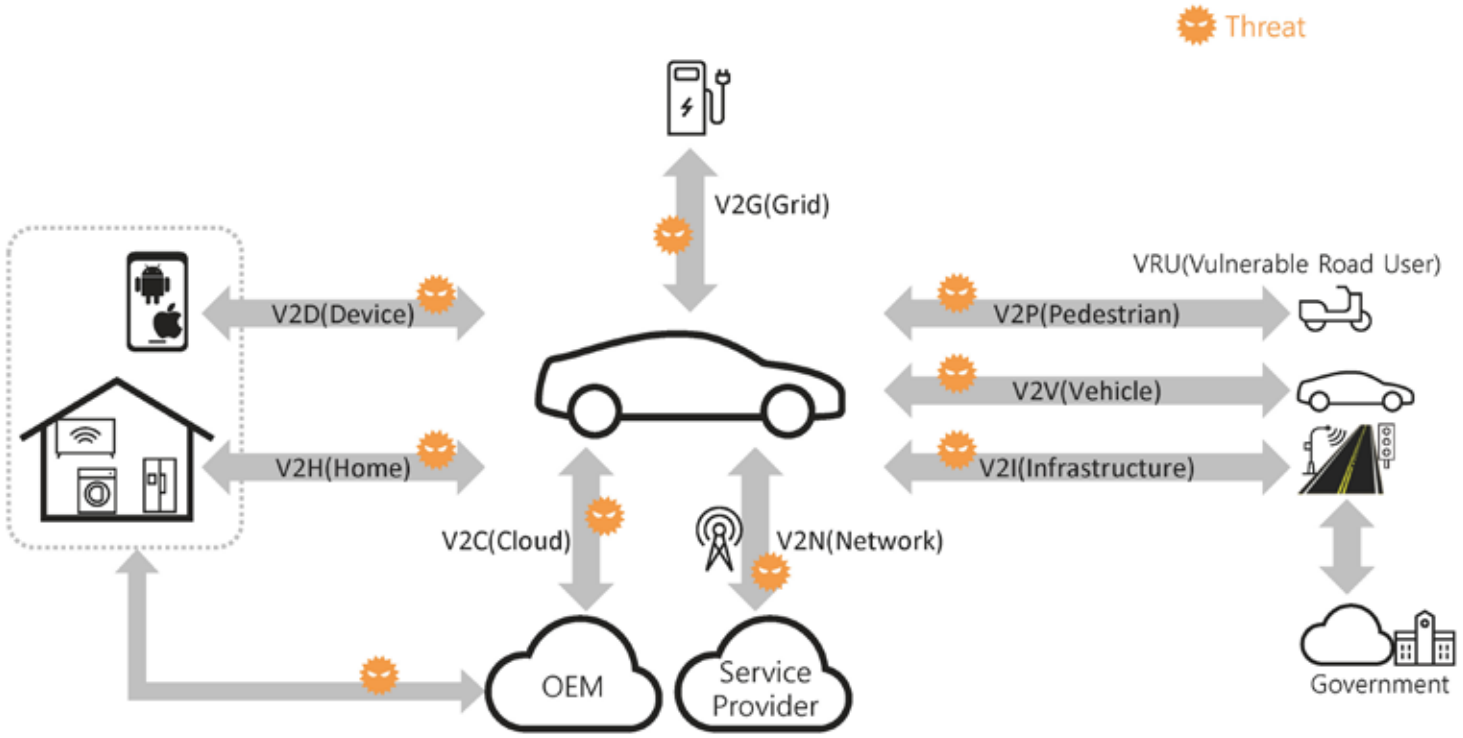
Momentum Technologies : SPACE – CyberSecurity



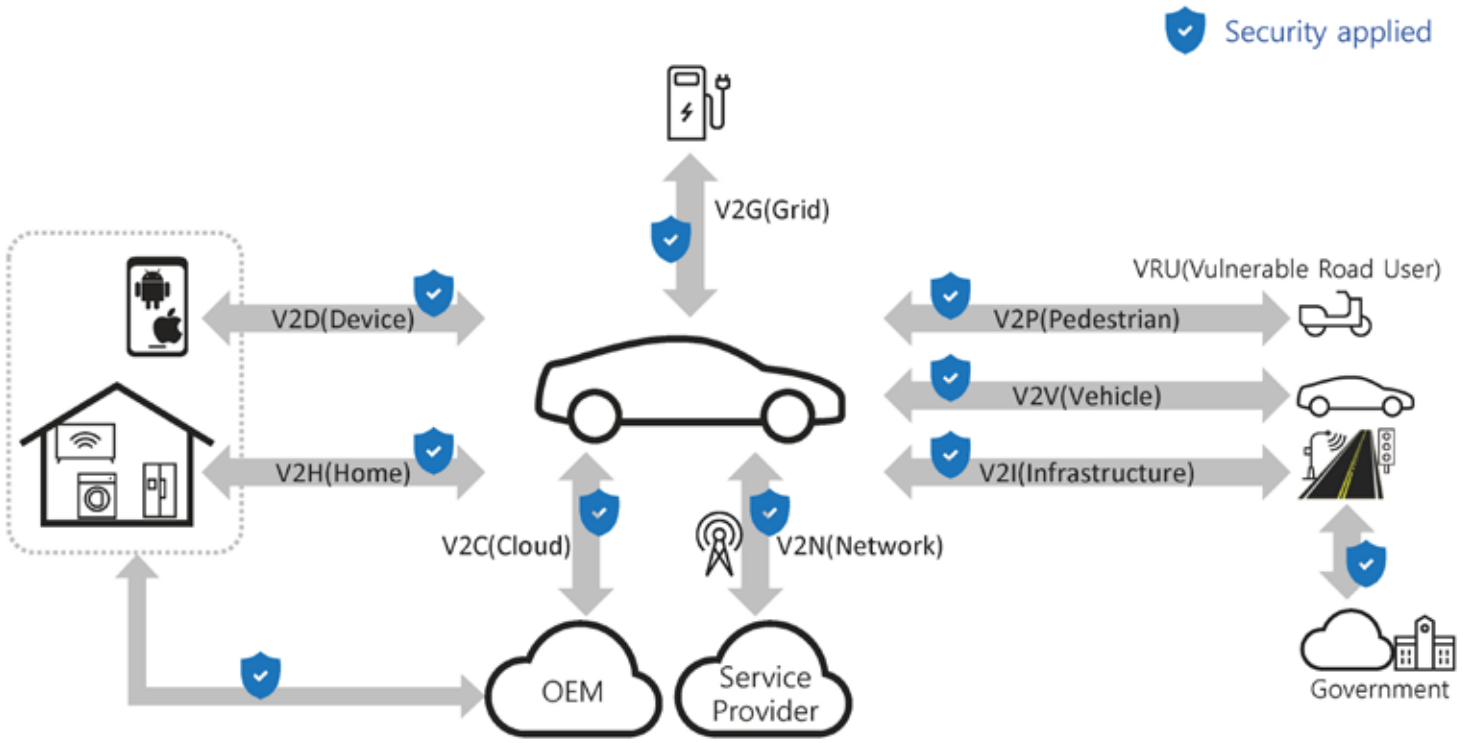
In-Vehicle Security : Layered Approach



S1. Secure External Communication – Security Threats

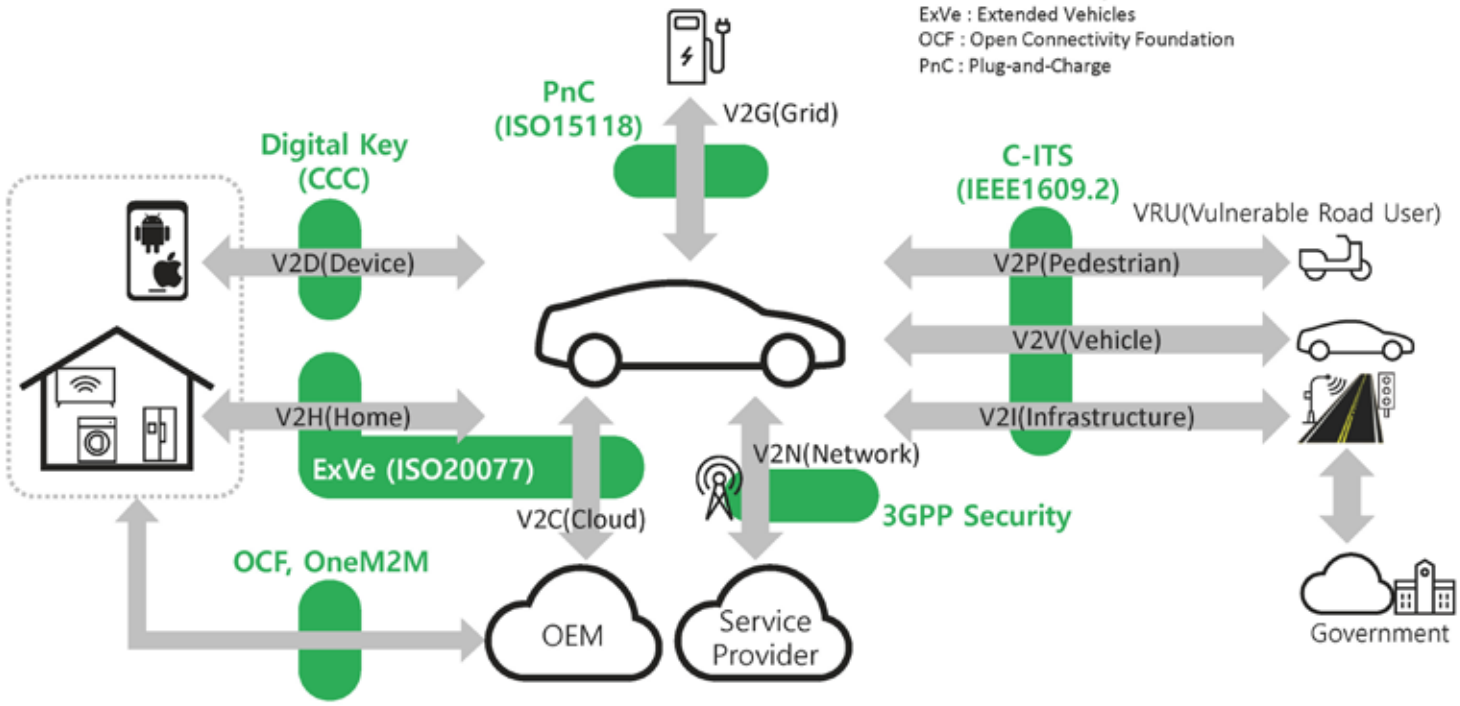


S1. Secure External Communication – Security Adoptions

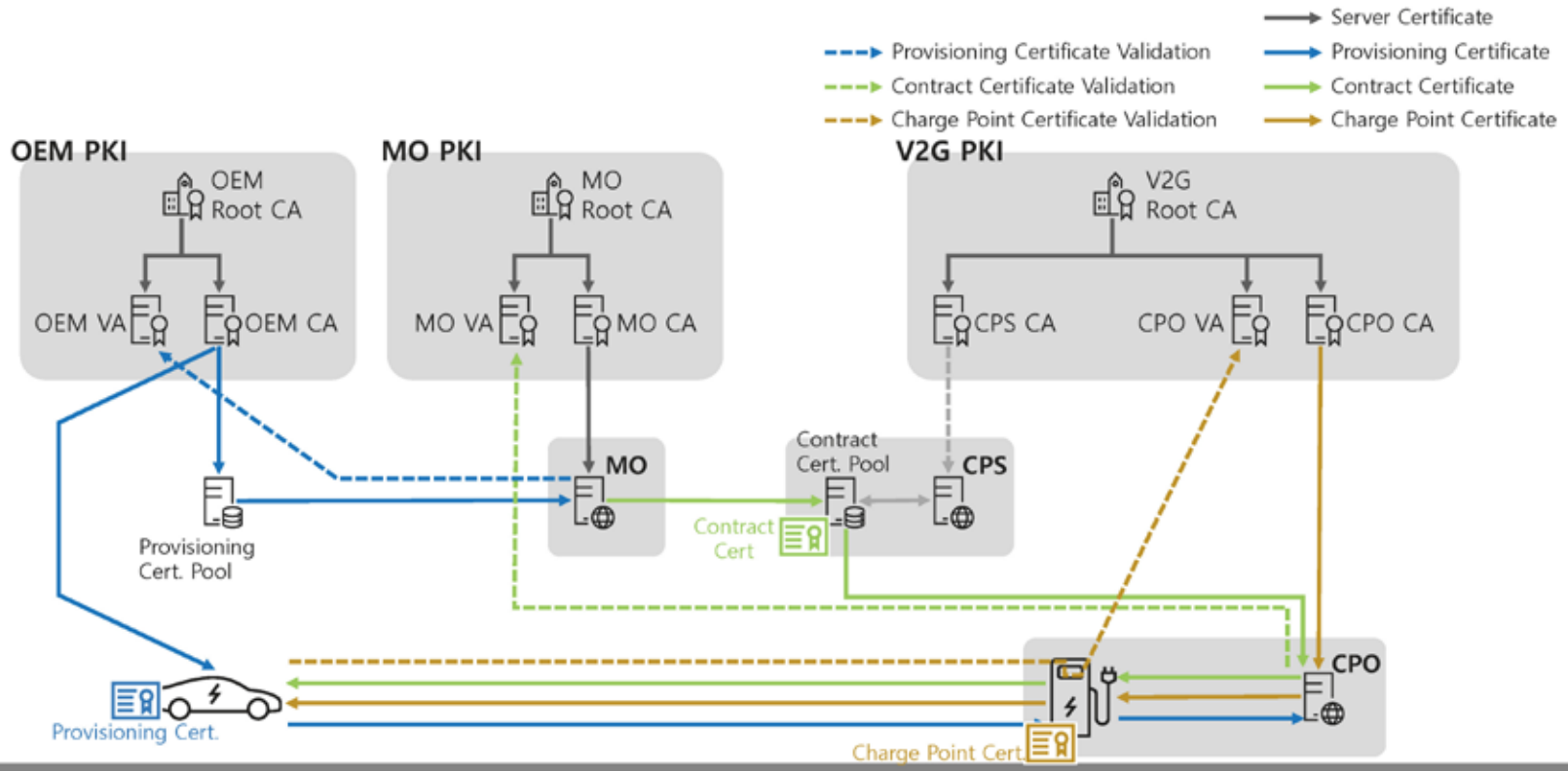


S1. Secure External Communication – Security Standards

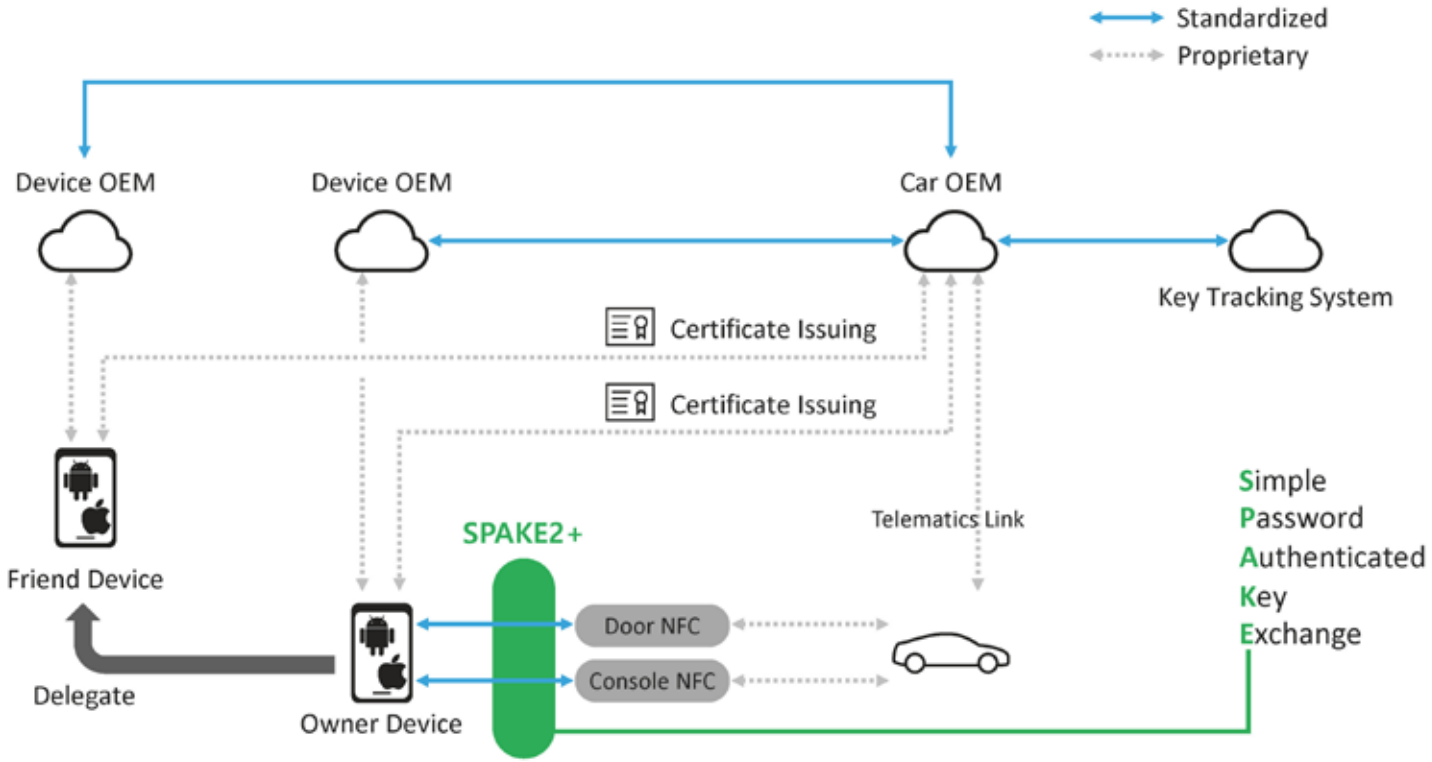
3GPP : 3rd Generation Partnership Project
CCC : Car Connectivity Consortium
ExVe : Extended Vehicles
OCF : Open Connectivity Foundation
PnC : Plug-and-Charge



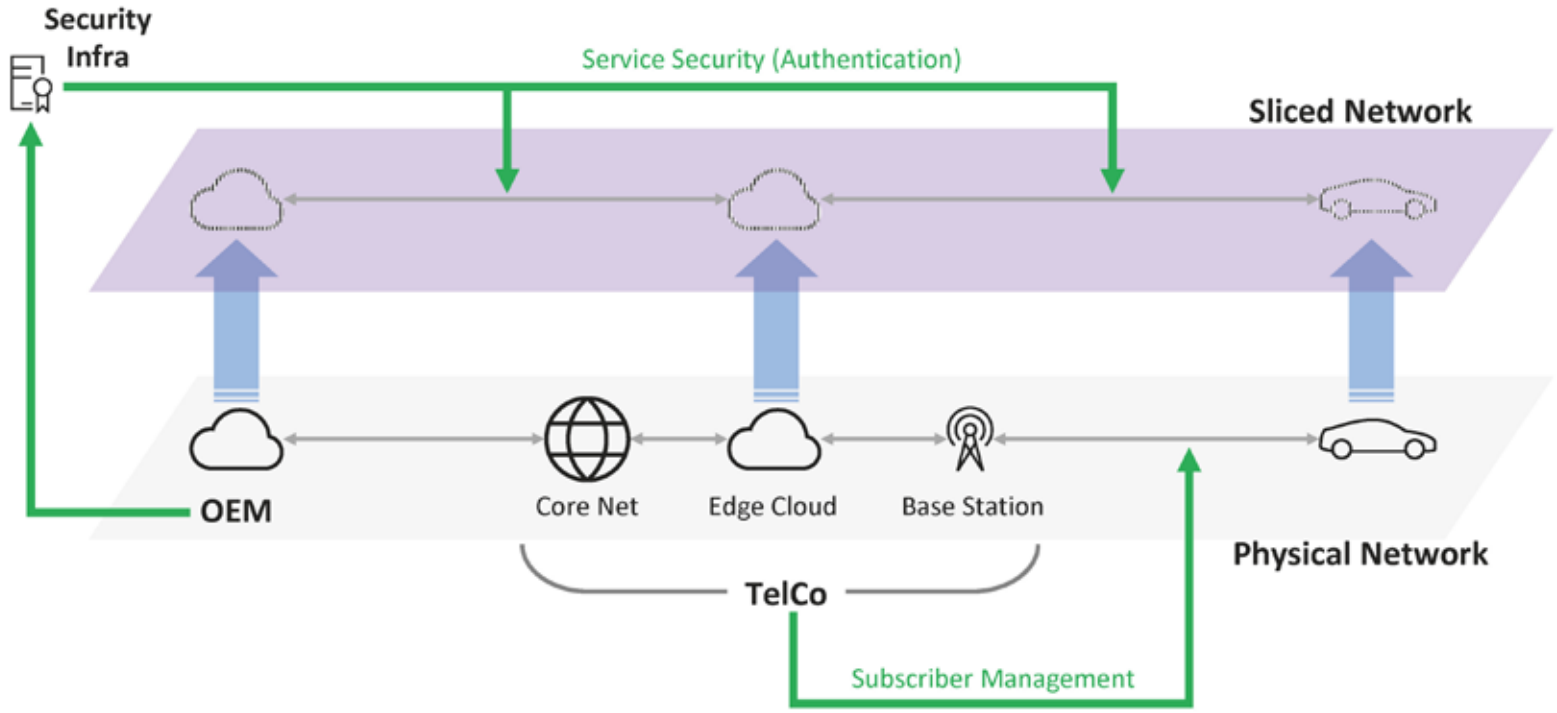
S1. Secure External Communication – V2G : PnC(Plug&Charge, ISO15118)



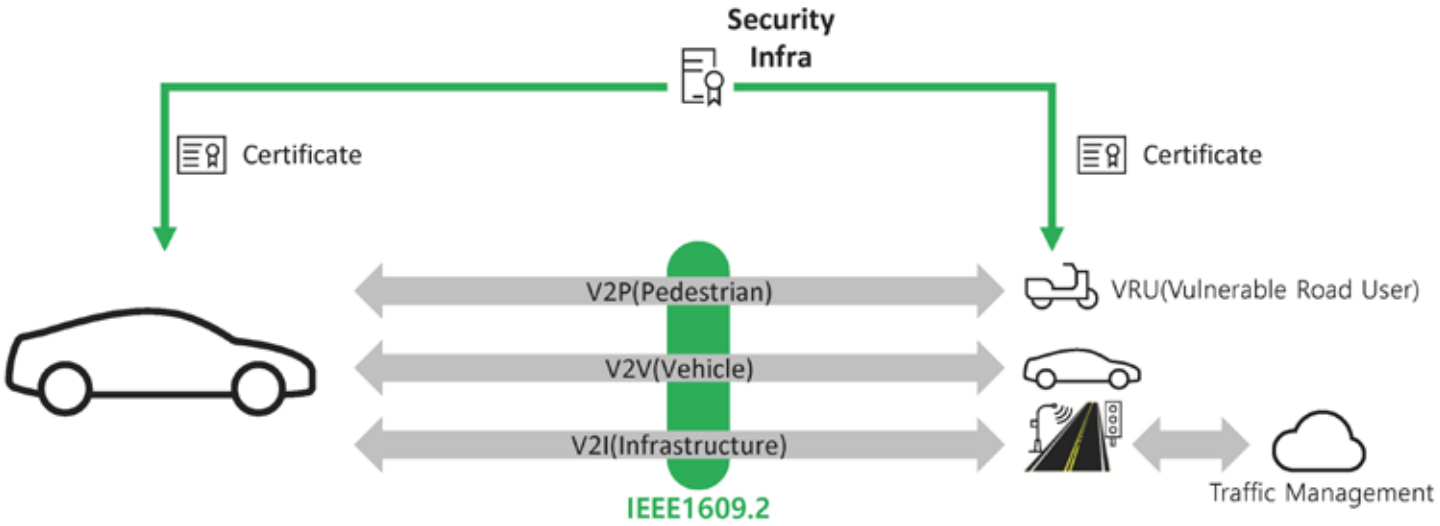
S1. Secure External Communication – V2D : CCC Digital Key



S1. Secure External Communication – V2N : 3GPP Security

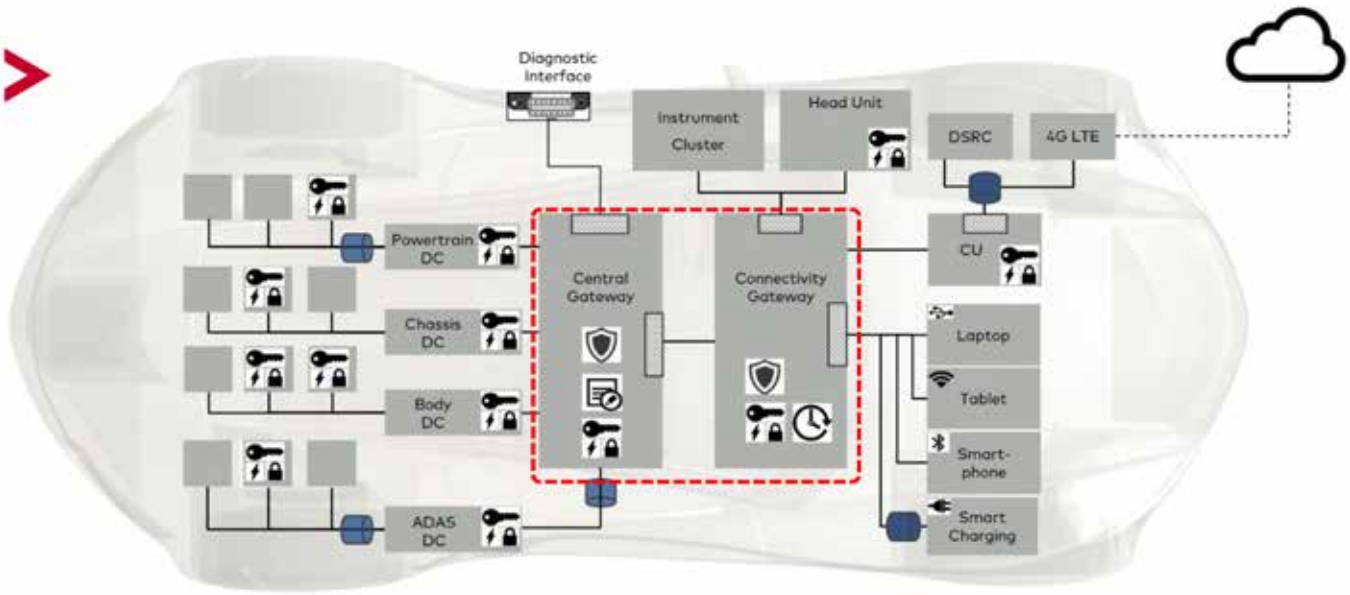


S1. Secure External Communication – V2V/V2I/V2P : IEEE1609.2

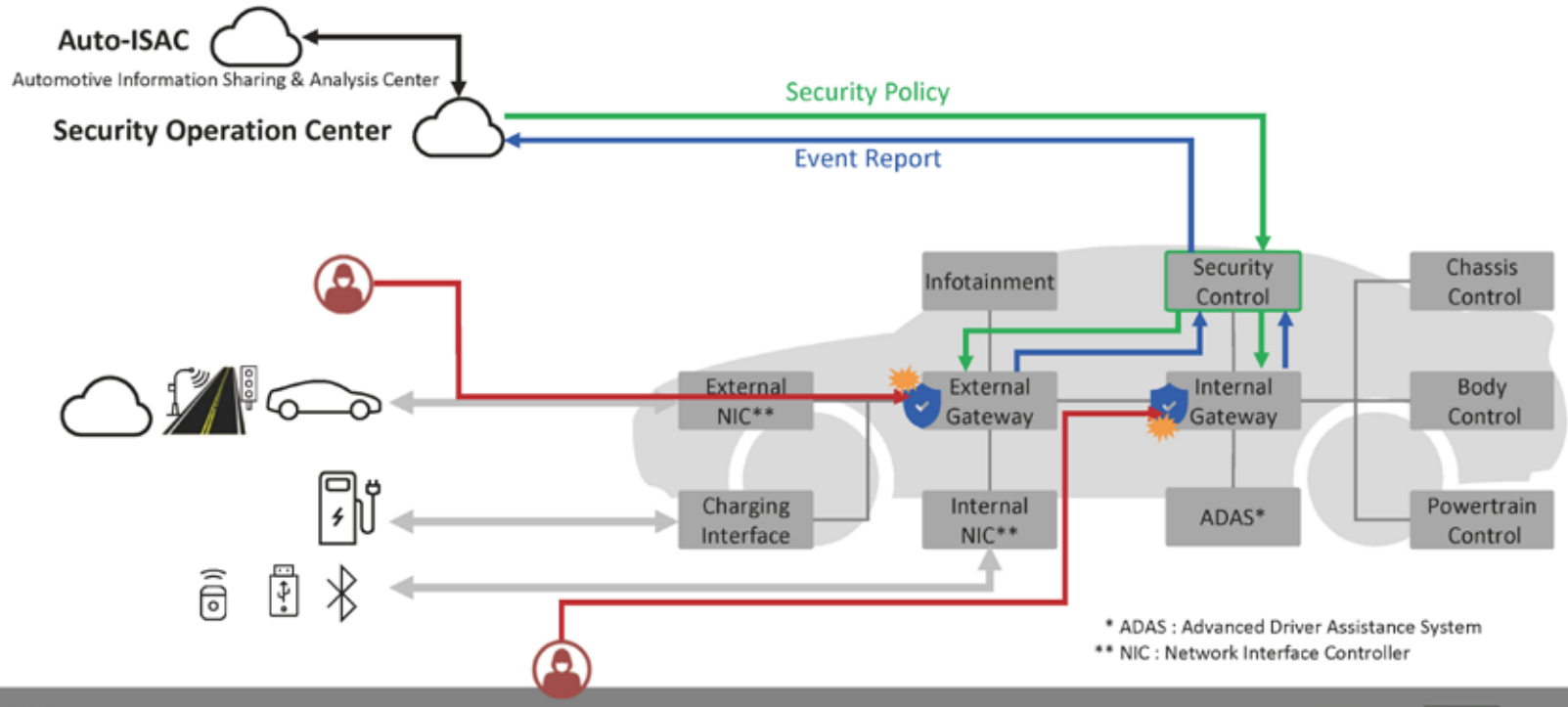


S2. Secure Gateway – "Solutions for Cybersecurity" (Vector, 2019.04)

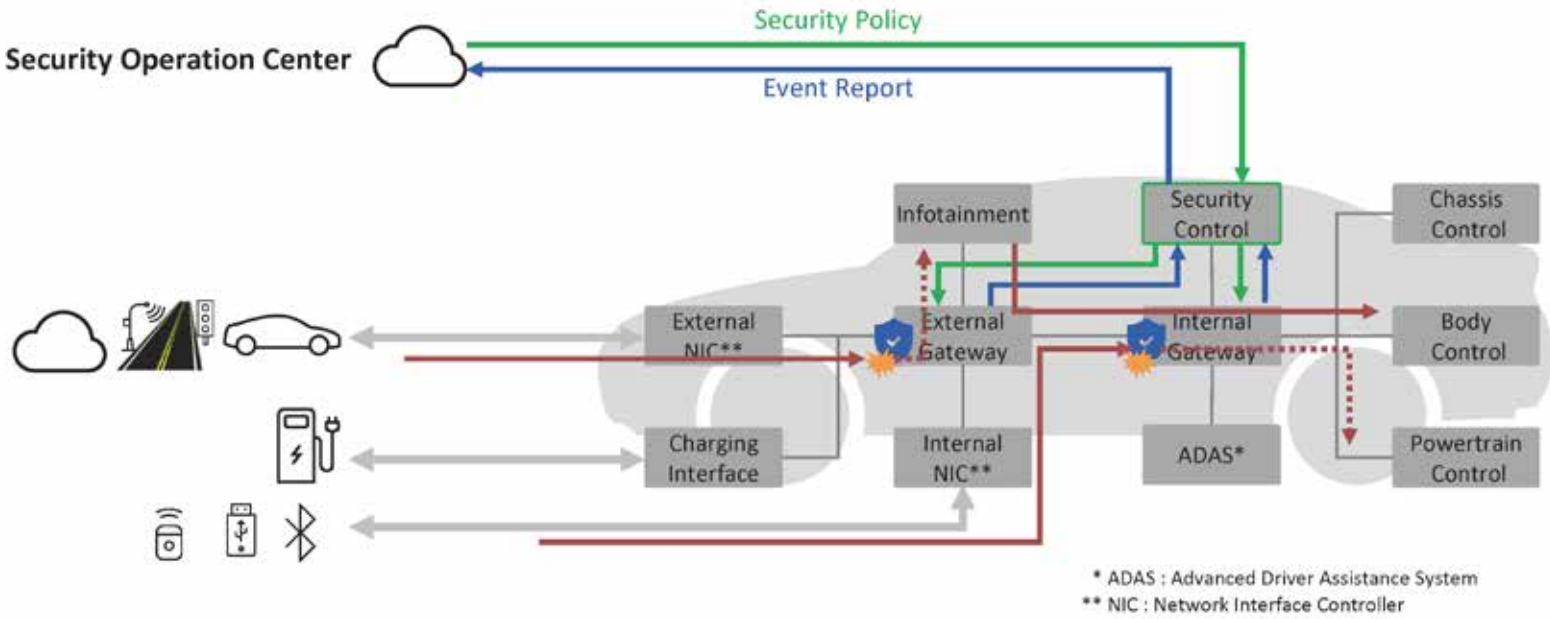
VECTOR



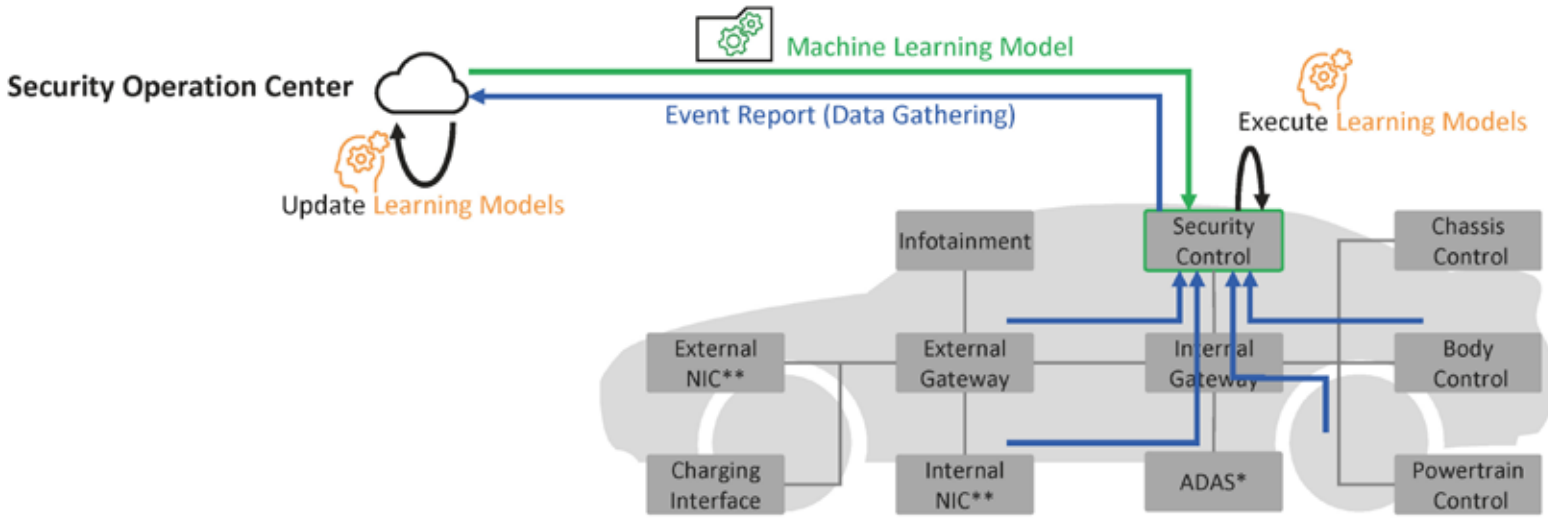
S2. Secure Gateway – Detects malicious traffic



S2. Secure Gateway – Controls traffic flow

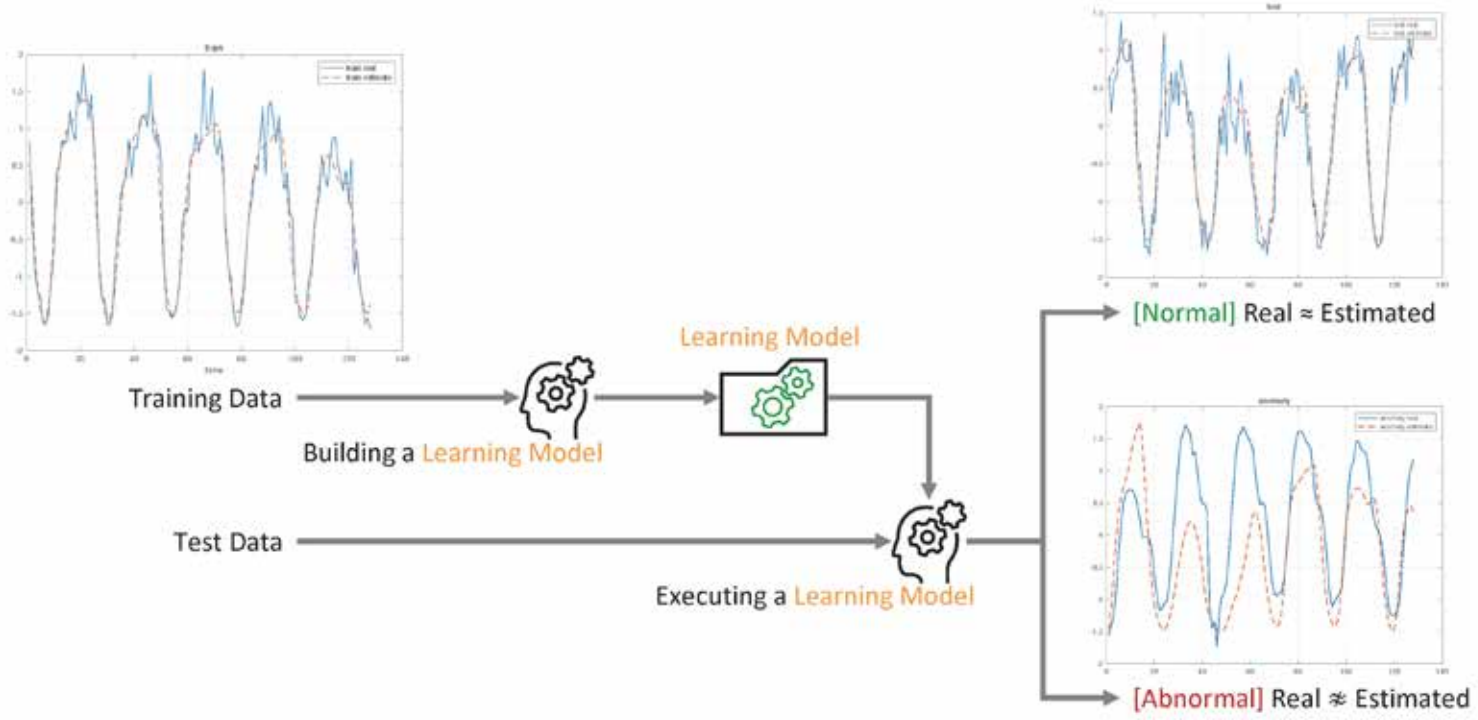


S2. Secure Gateway – Anomaly Detection (with Machine Learning)

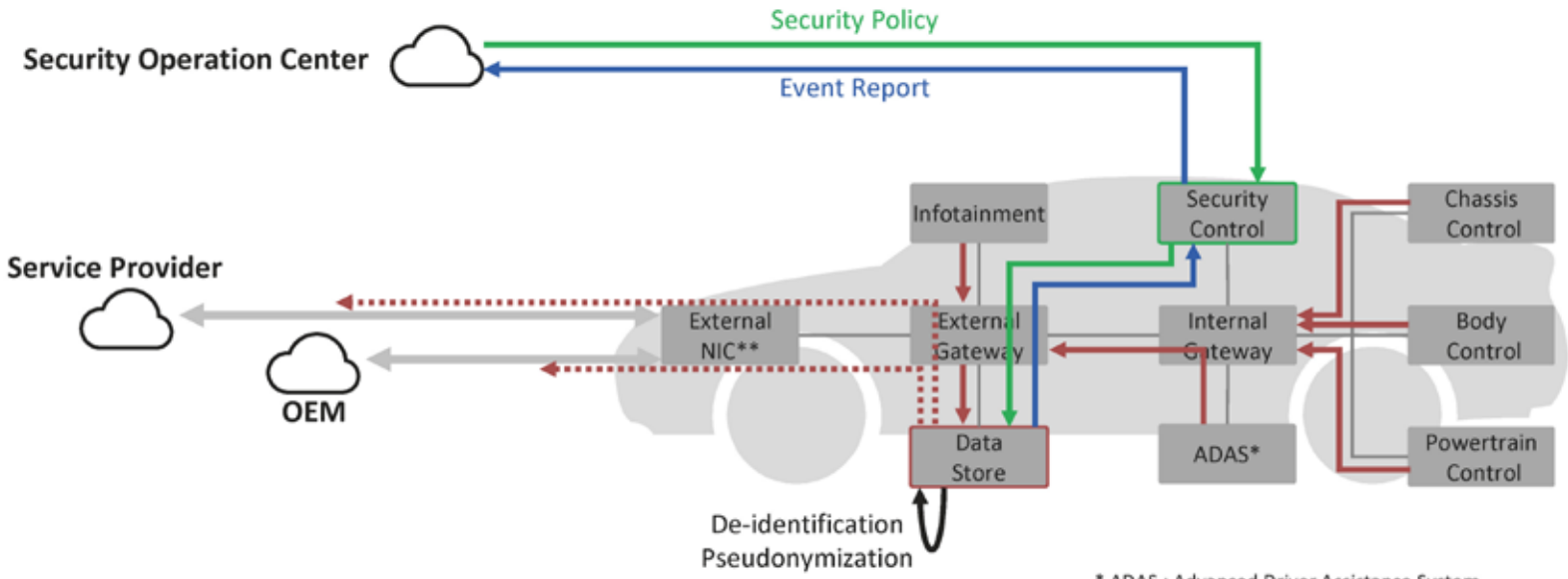


* ADAS : Advanced Driver Assistance System
** NIC : Network Interface Controller

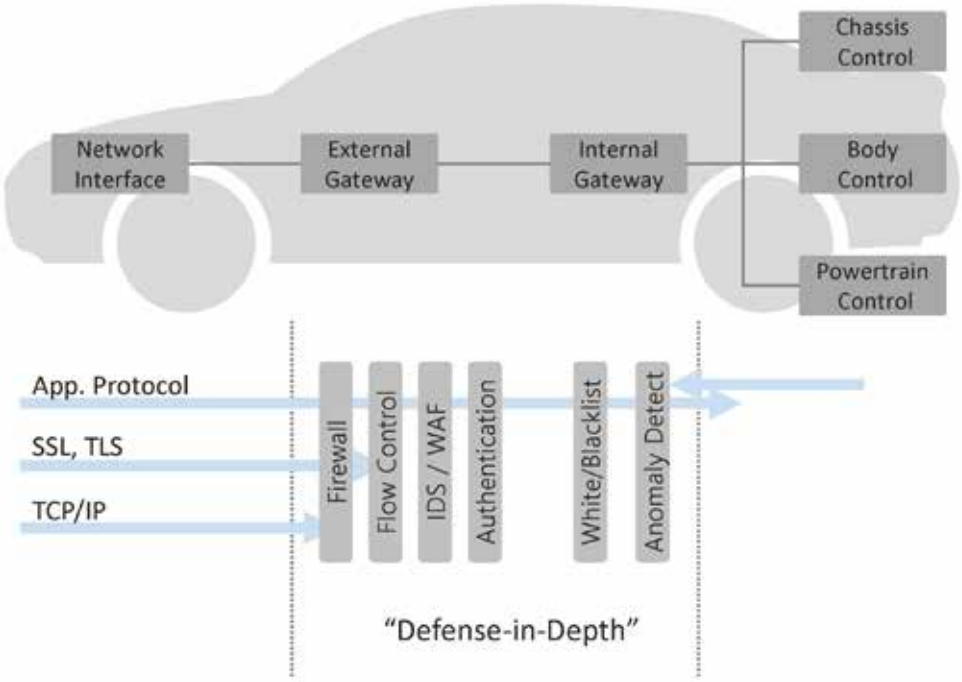
S2. Secure Gateway – Anomaly Detection (with Machine Learning)



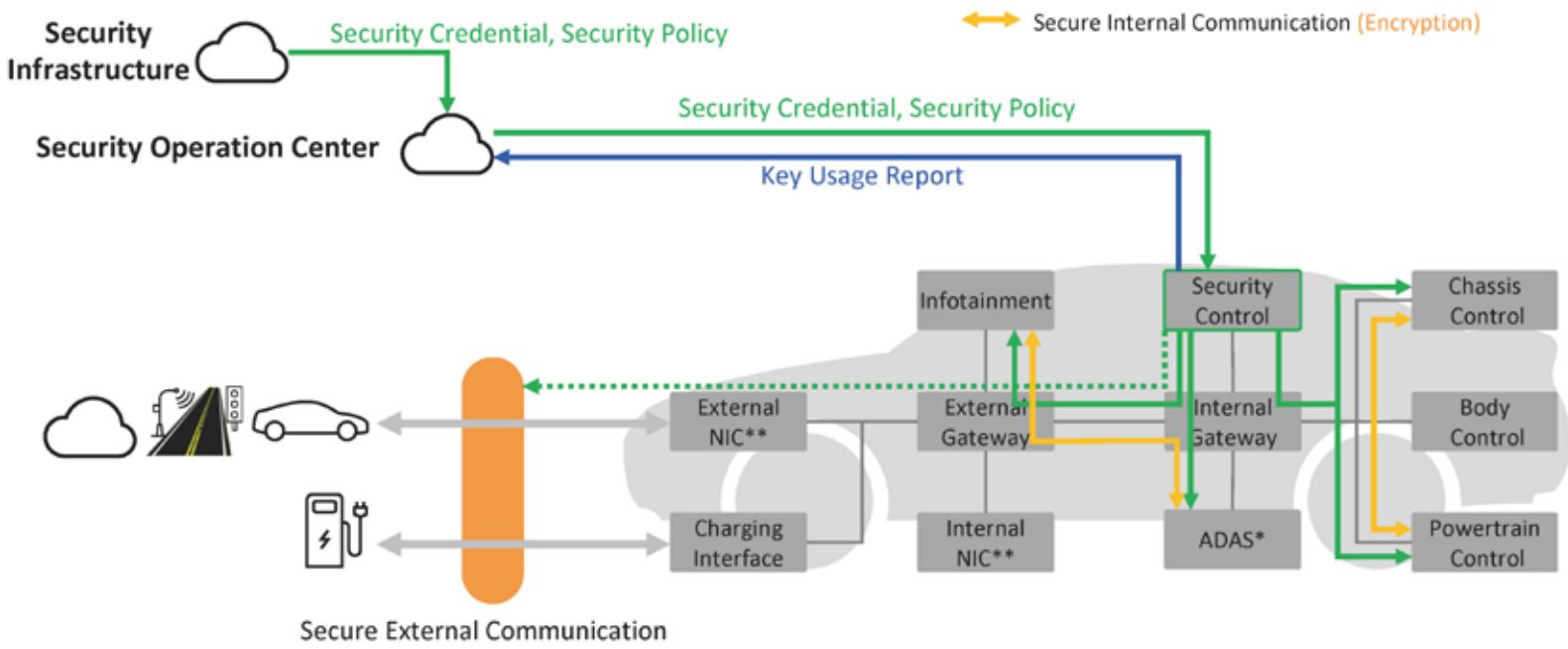
S2. Secure Gateway – Data Security & Privacy Preserving



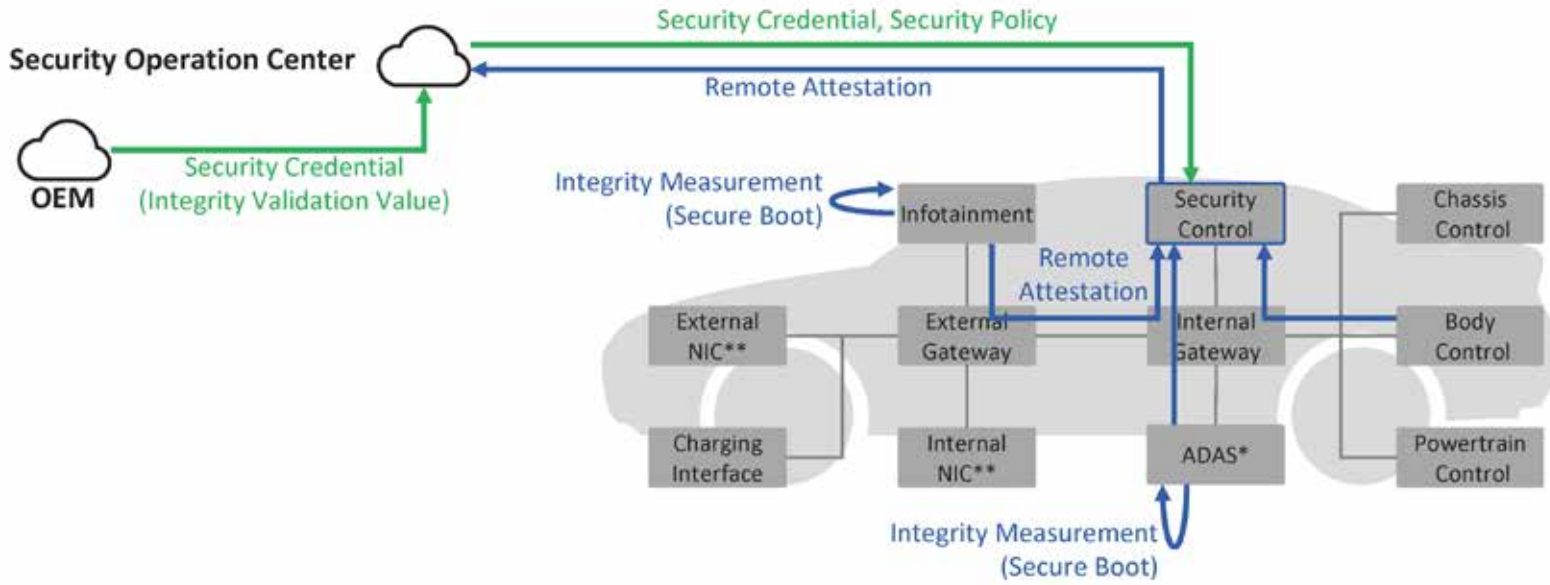
S2. Secure Gateway – "Defense-in-Depth"



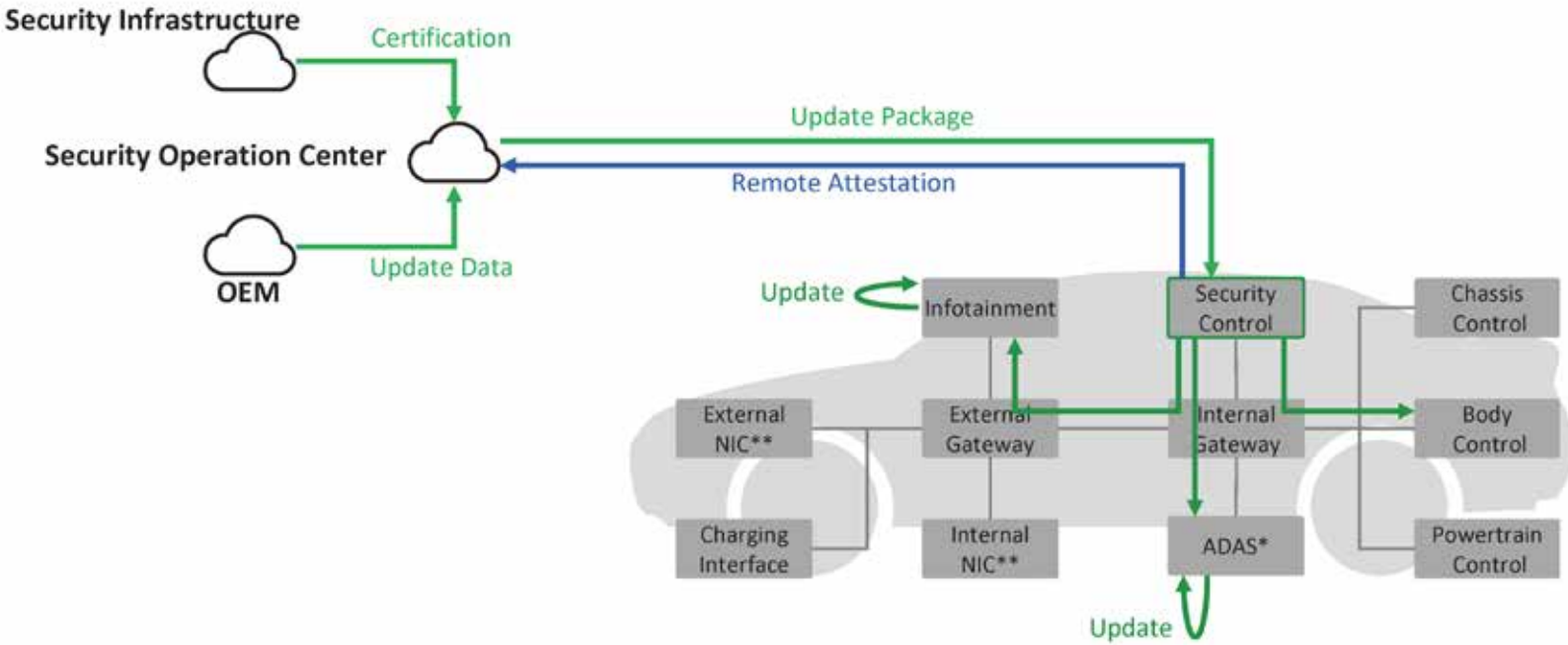
S3. Secure Internal Communication – Key Management



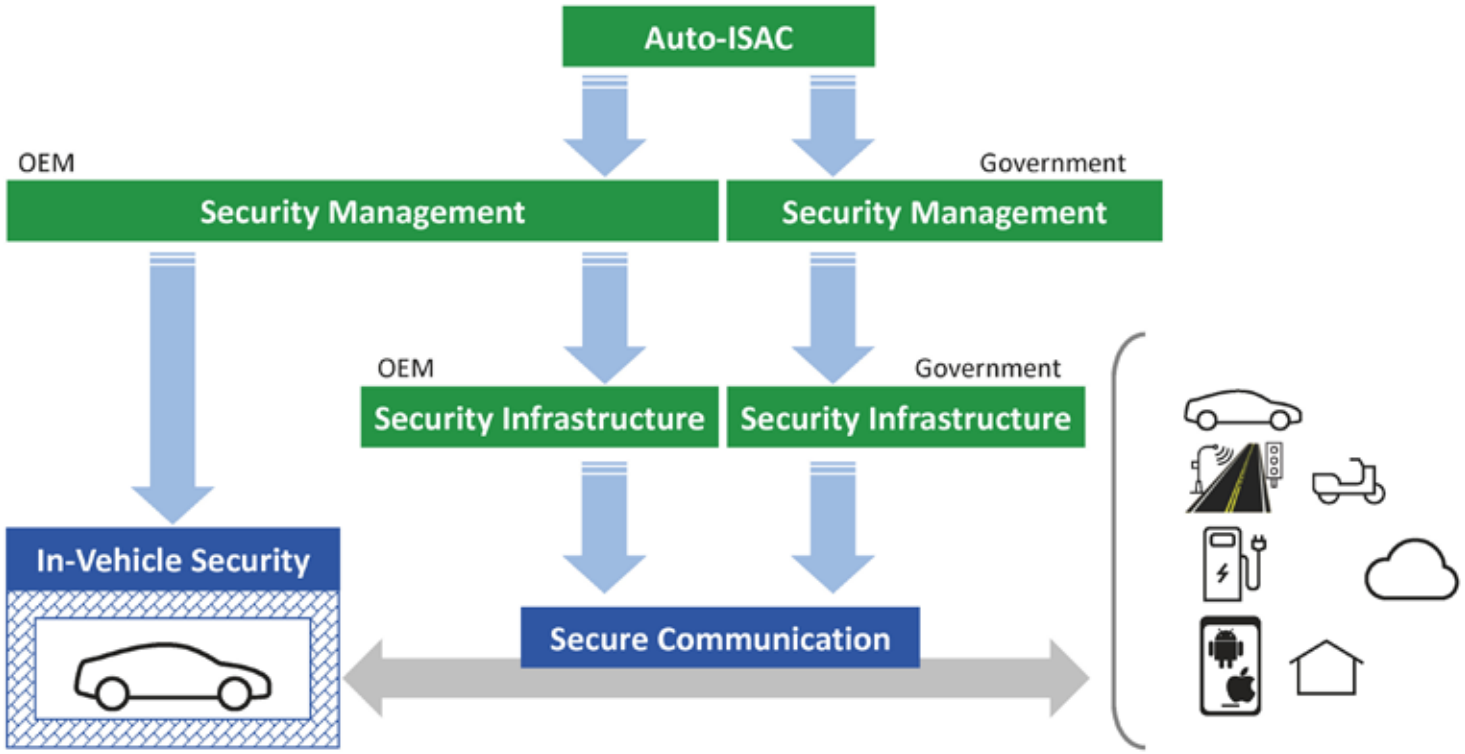
S4. Secure Platform – Secure Boot & Remote Attestation



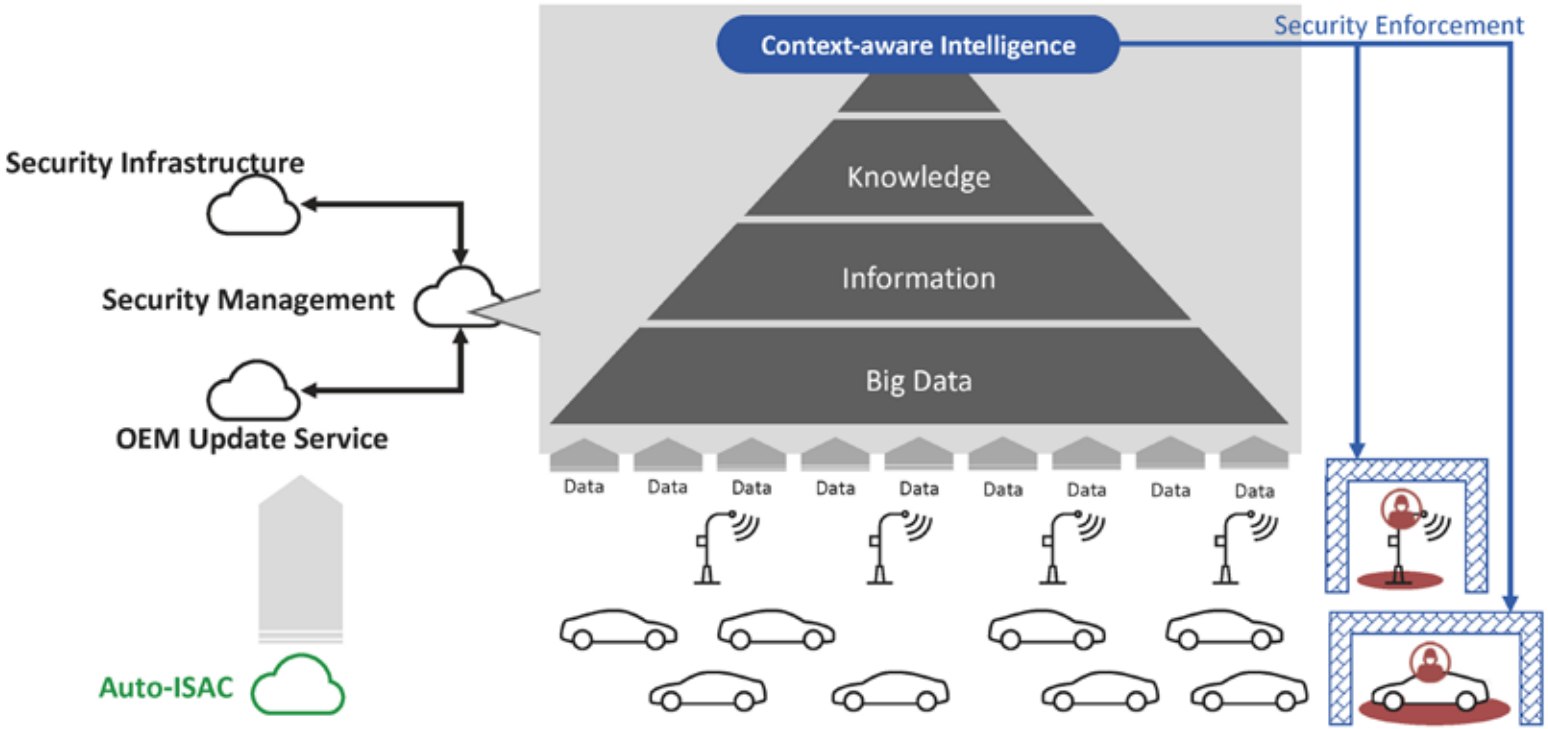
S4. Secure Platform – Secure Update



Security Management



Security Management – "Adaptive Security Architecture" (Gartner)

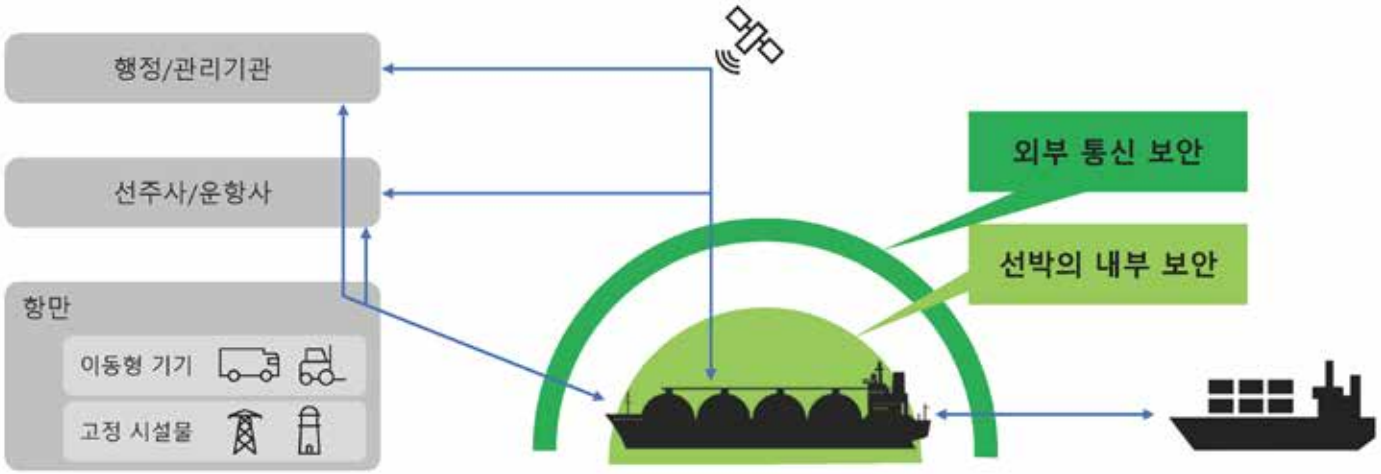


Autonomous Trasport

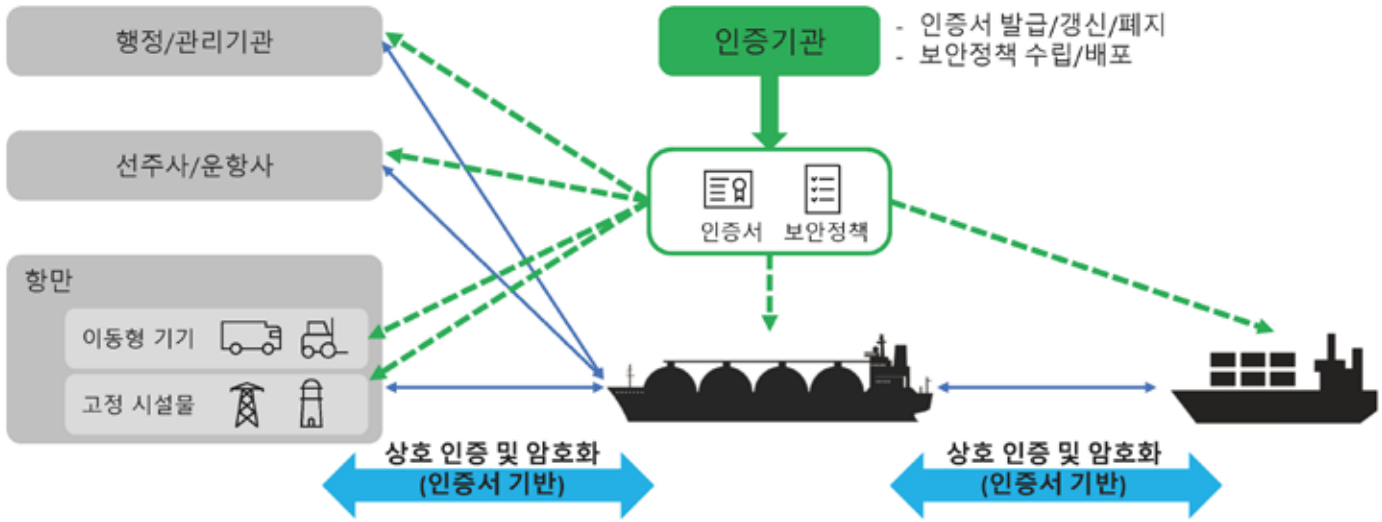
자율주행열차 보안

자율운항선박 보안

CyberSecurity for Maritime



Secure Communication and Authentication Infrastructure



SEOUL · SEJONG · SHANGHAI · WUXI

www.autocrypt.io