5G 환경의 자율주행과 보안

May 2021

SangGyoo SIM, Ph.D (sgsim@autocrypt.io)
CTO & Co-Founder of AUTOCRYPT
CTO of Penta Security Systems

AUTOCRYPT

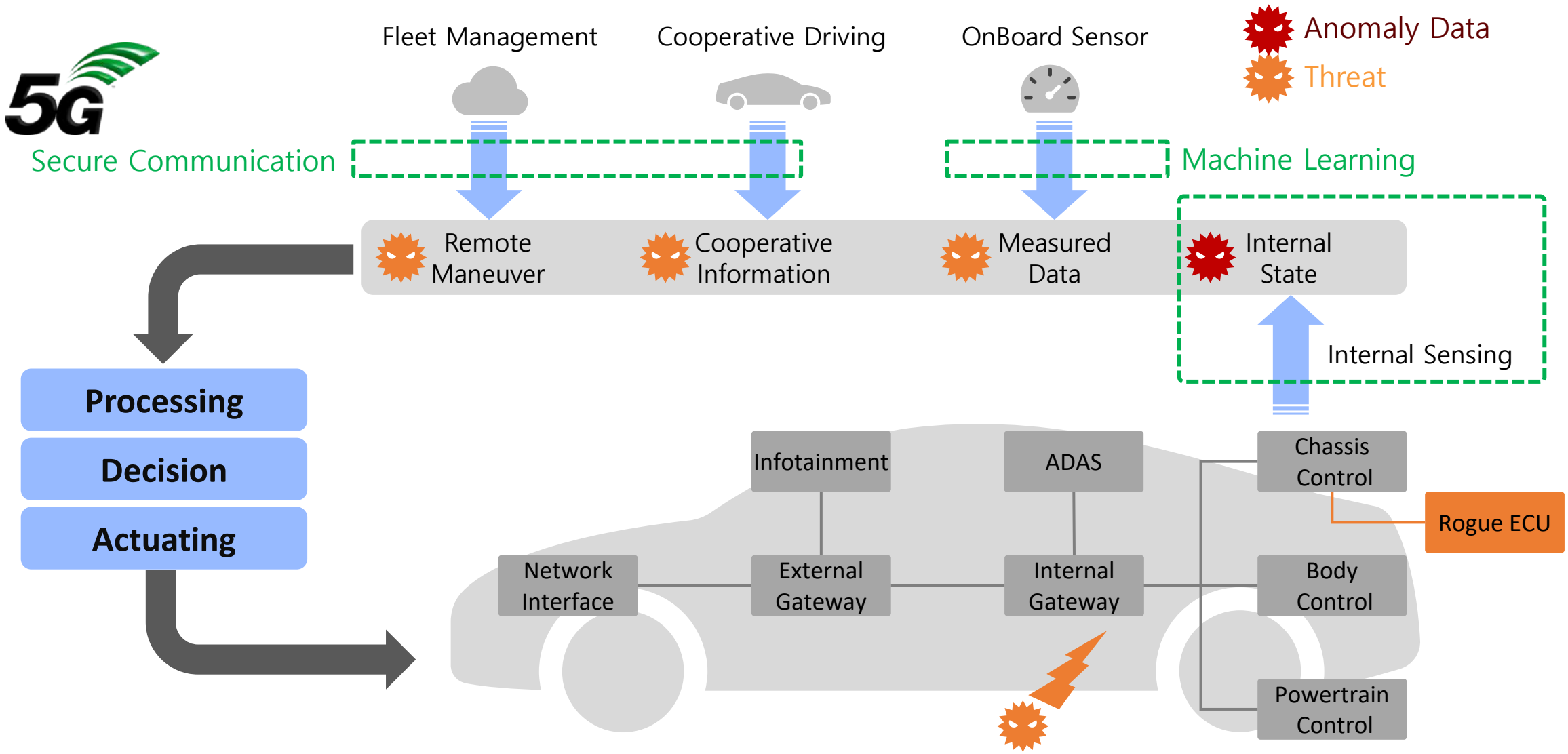
TU-Automotive AWARDS
Best Auto Cybersecurity Product/Service 2019
The Automotive Tech Company of the Year Finalist 2020

CYBER MOBILITY AWARDS
2020 Global Cyber Achievement Award

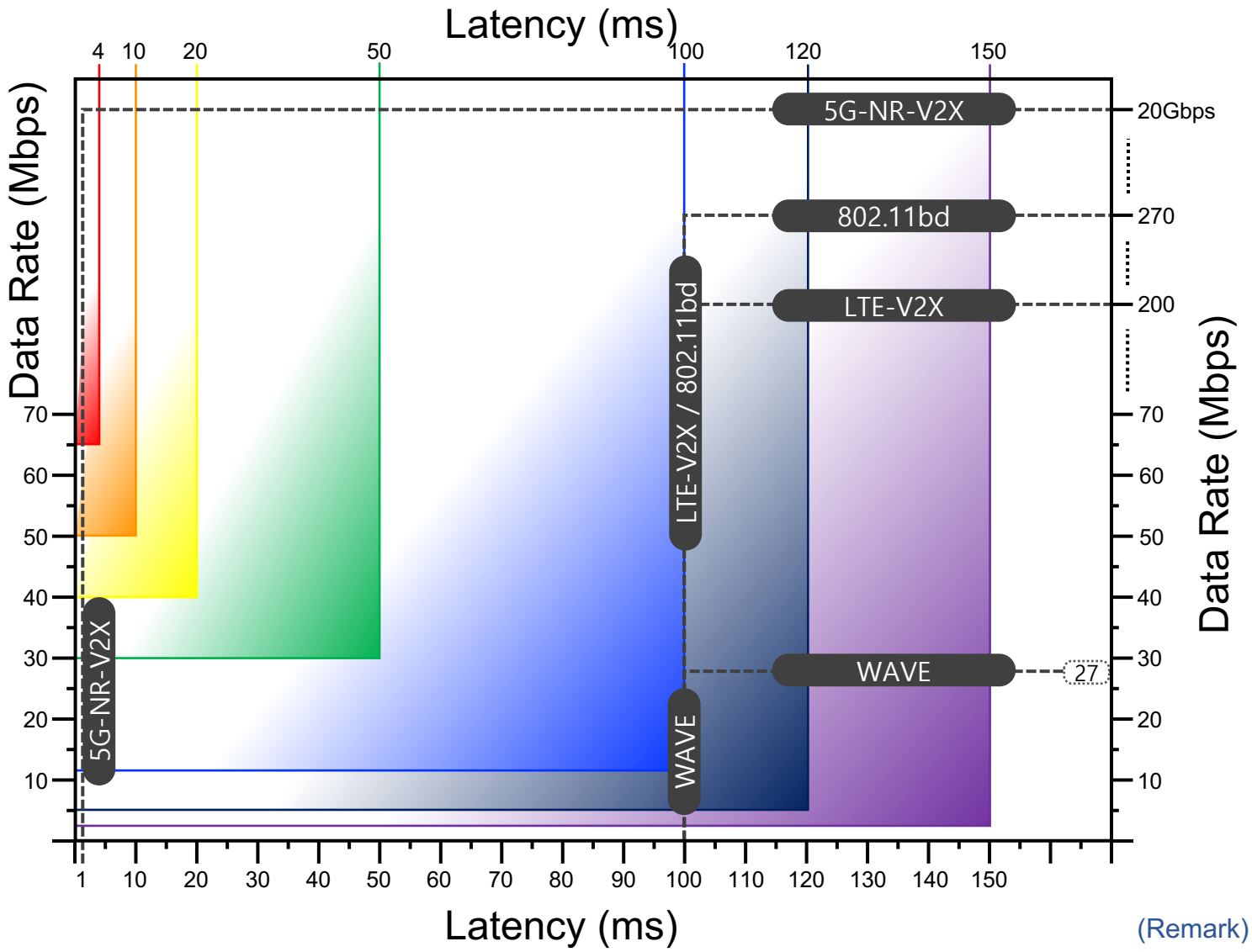
AUTOTECH BREAKTHROUGH AWARDS
2020 Automotive Cybersecurity Company of the Year

AIIA
Artificial Intelligence Industry Association
2020 Emerging AI+X Top 100 Company
Mobility Category

Autonomous Driving



V2X Communications & V2X Usecases



- Cloud-based sensor sharing via V2N
- Latency-critical traffic and road hazard warnings

- High-definition sensor sharing data
- High-density platooning

- Collision risk or potential danger warning
- In-vehicle entertainment contents data
- Automated/Remote valet parking

- ‘See Through’ video streaming data
- Pre-crash sensing warning

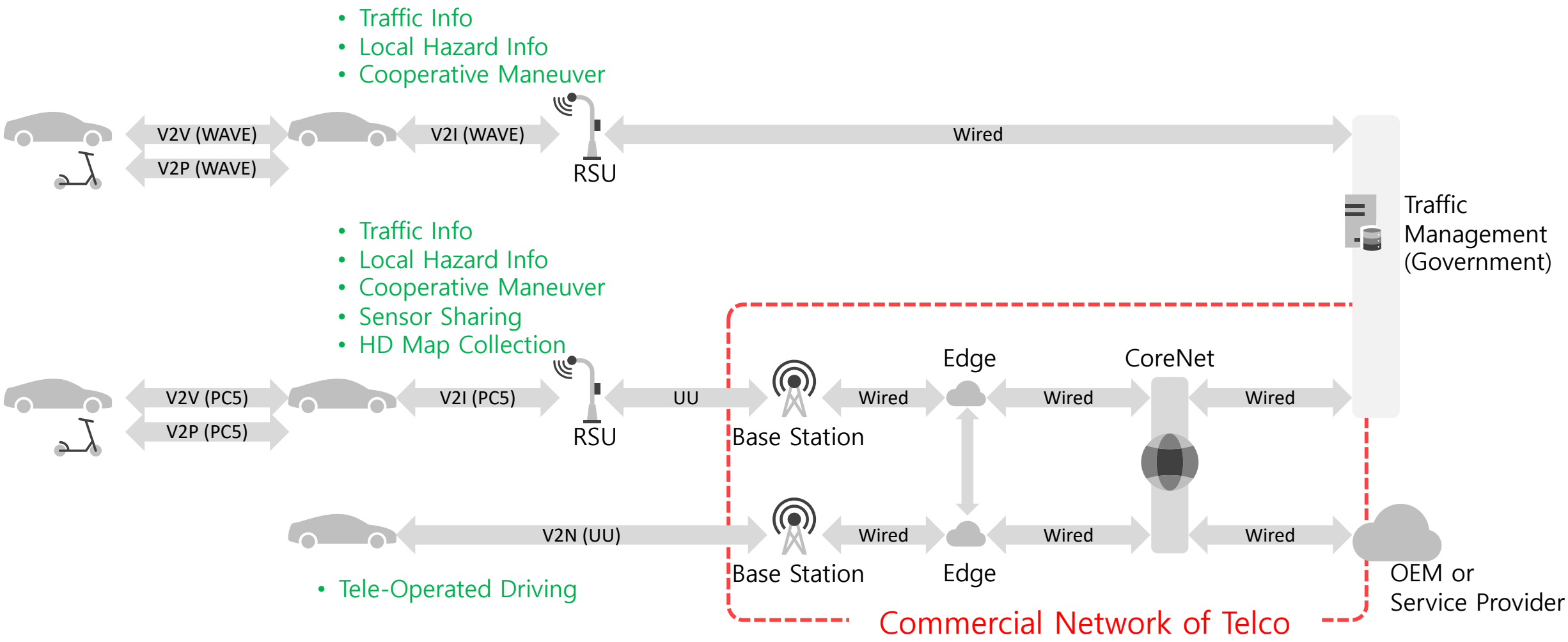
- High-definition map collection and sharing
- Intersection movement assistance
- Abnormal condition warning

- Hard braking awareness messages on driving
- Speed harmonization
- Lane change warning
- Traffic condition warning
- Cooperative maneuver

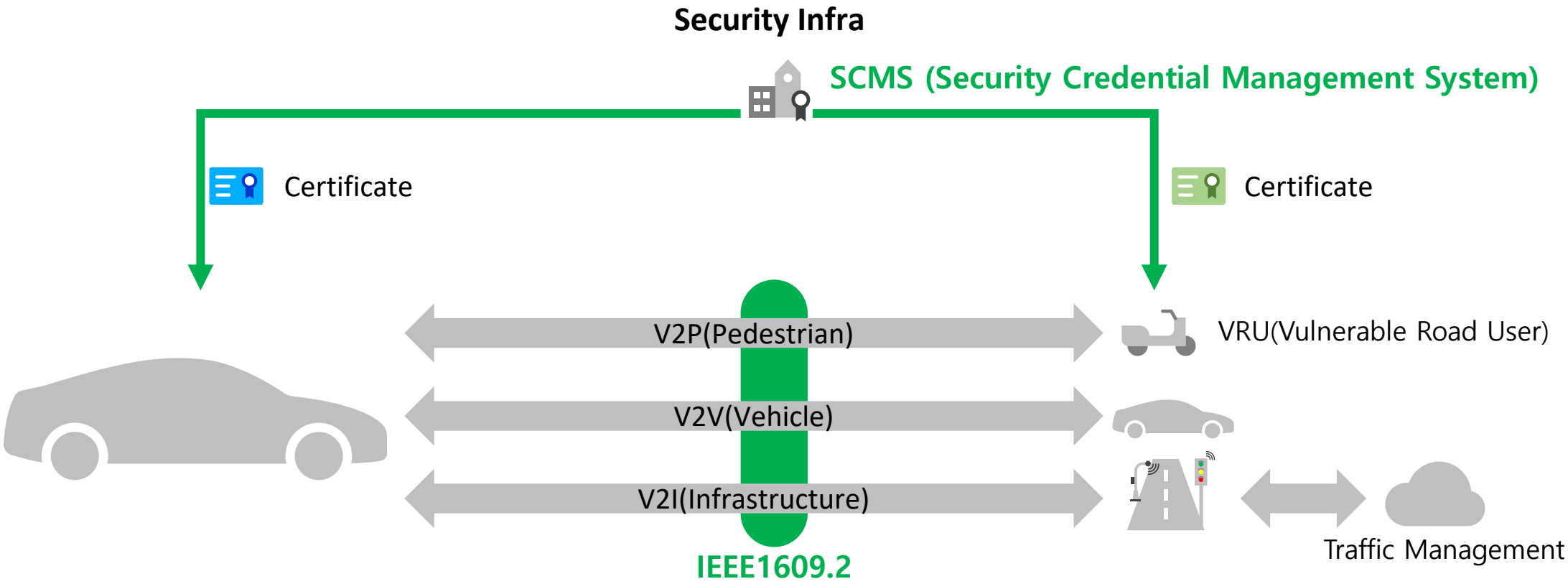
- Route information
- Traffic jam warning(urban/rural/highway)
- Software update
- Remote vehicle health monitoring

(Remark) Special thanks for revising this map to KETI Korea Electronics Technology Institute

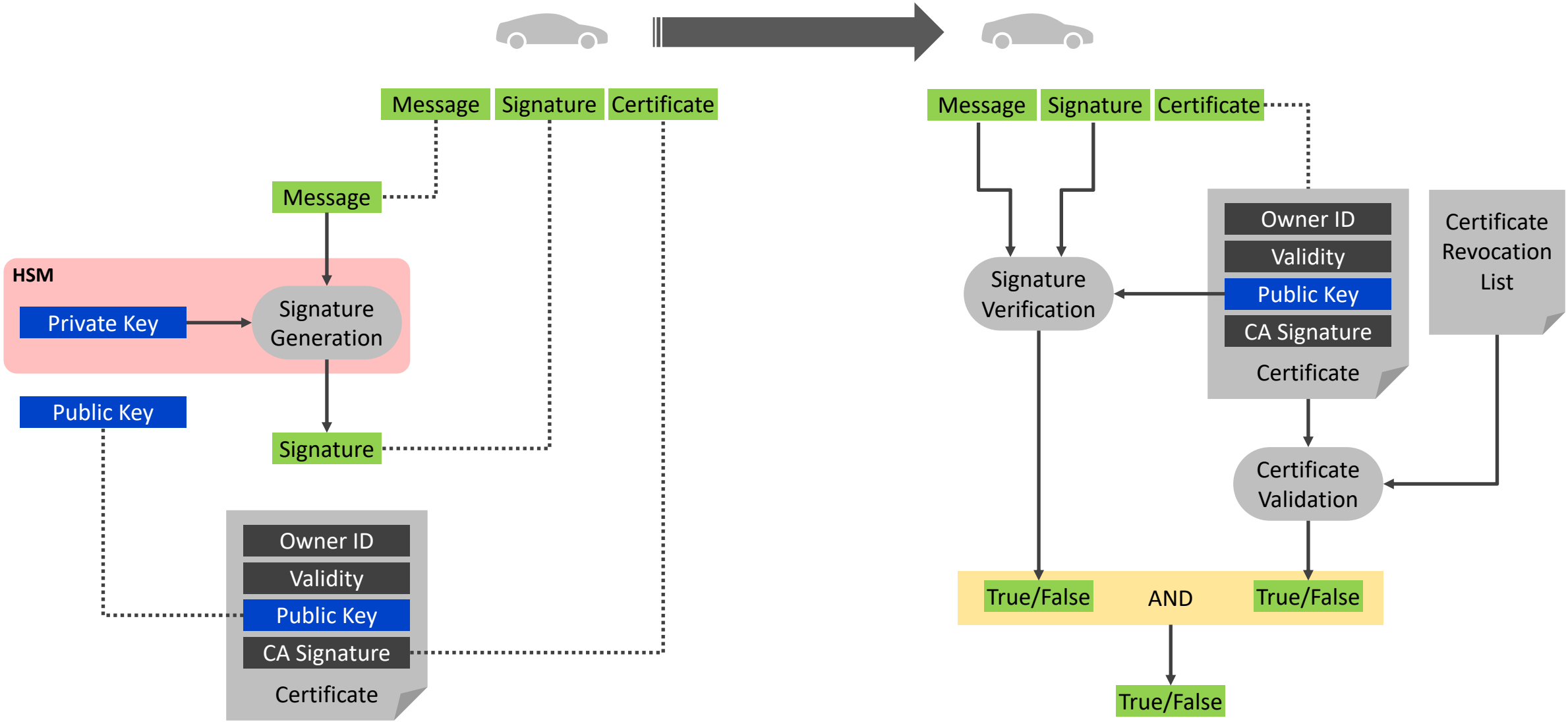
C-ITS : WAVE & Cellular



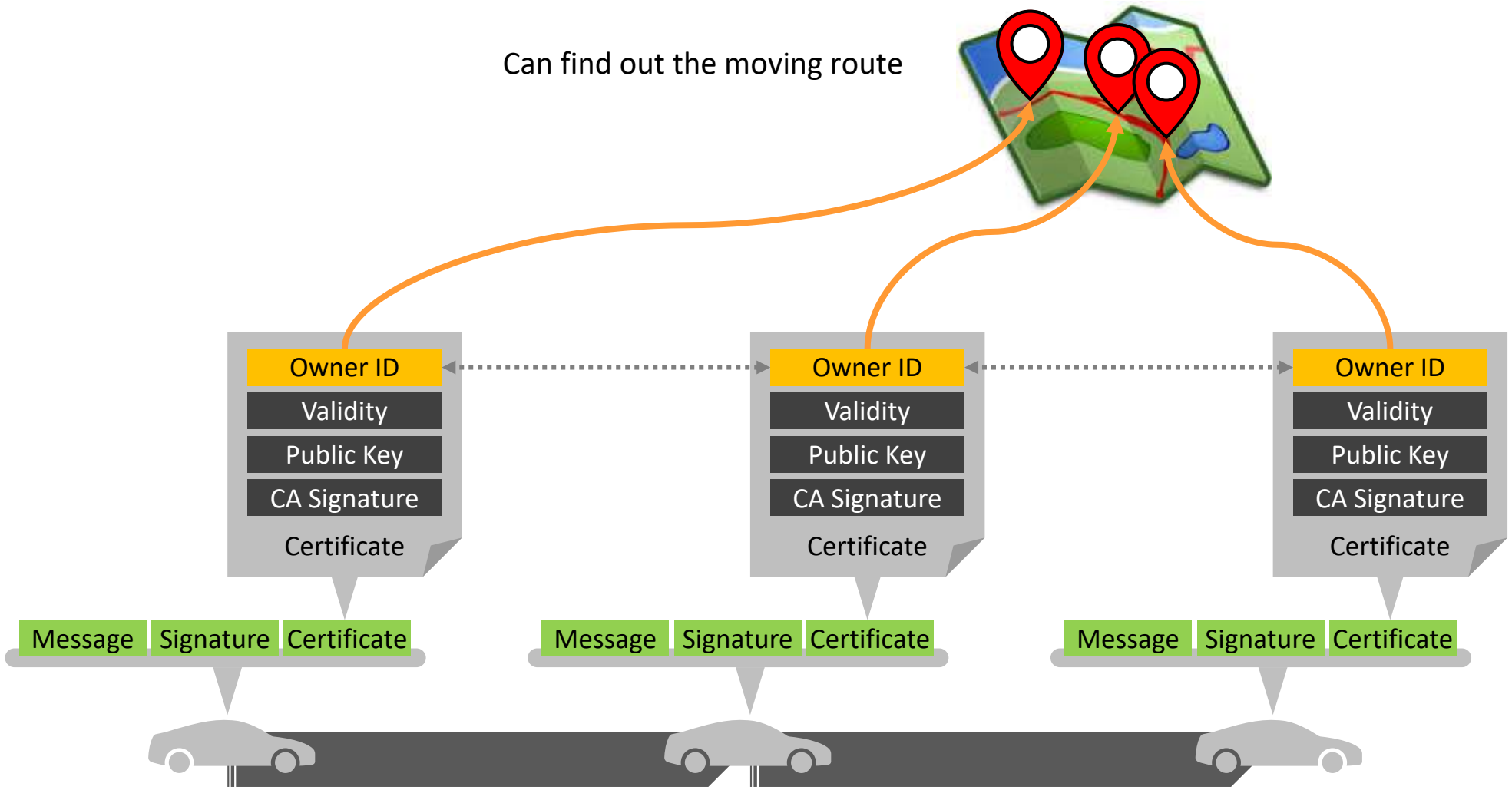
C-ITS : Security Structure



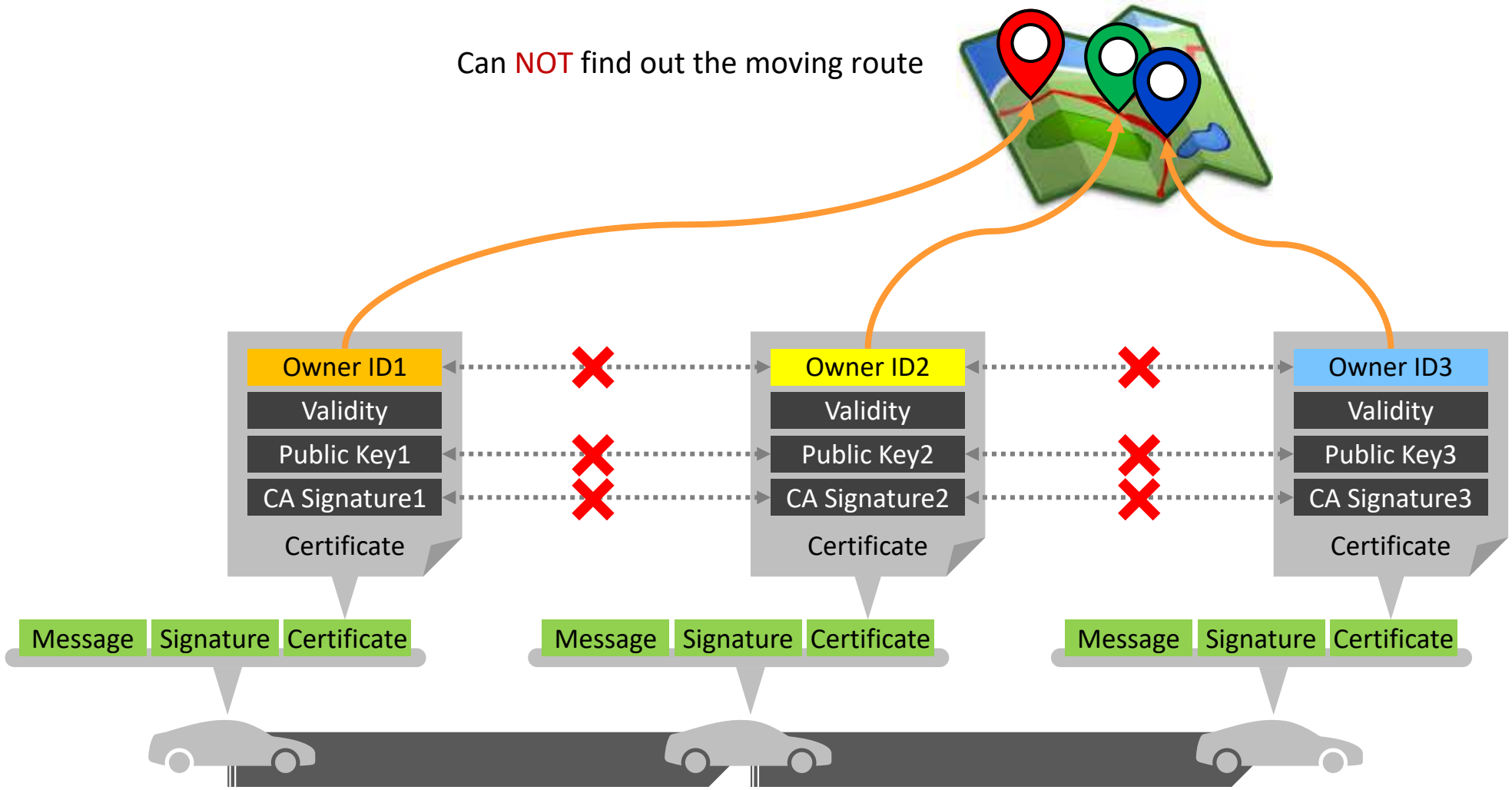
C-ITS : Signature Generation & Verification



C-ITS : Issue of Location Privacy

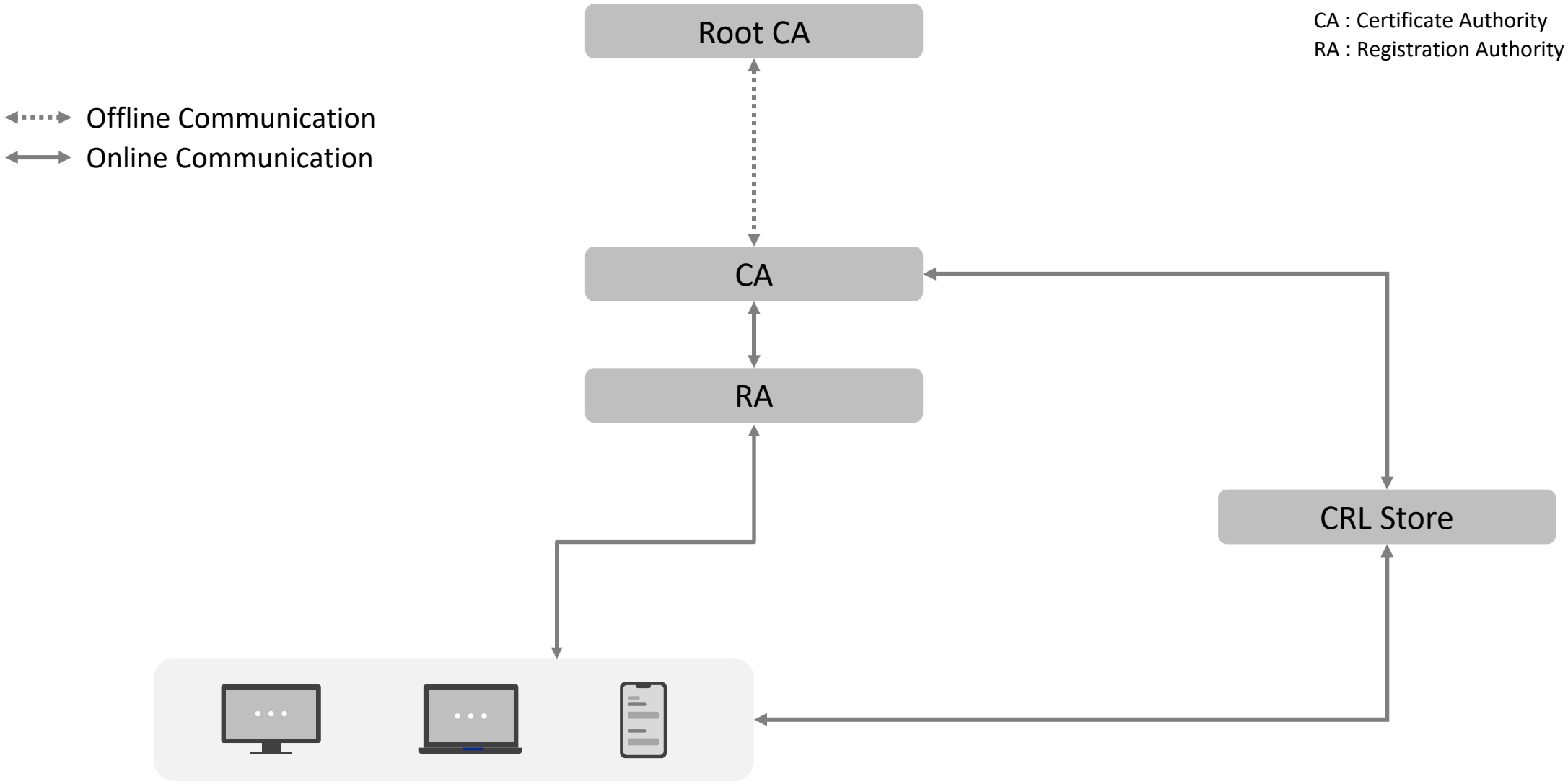


C-ITS : Privacy Preserving Technologies

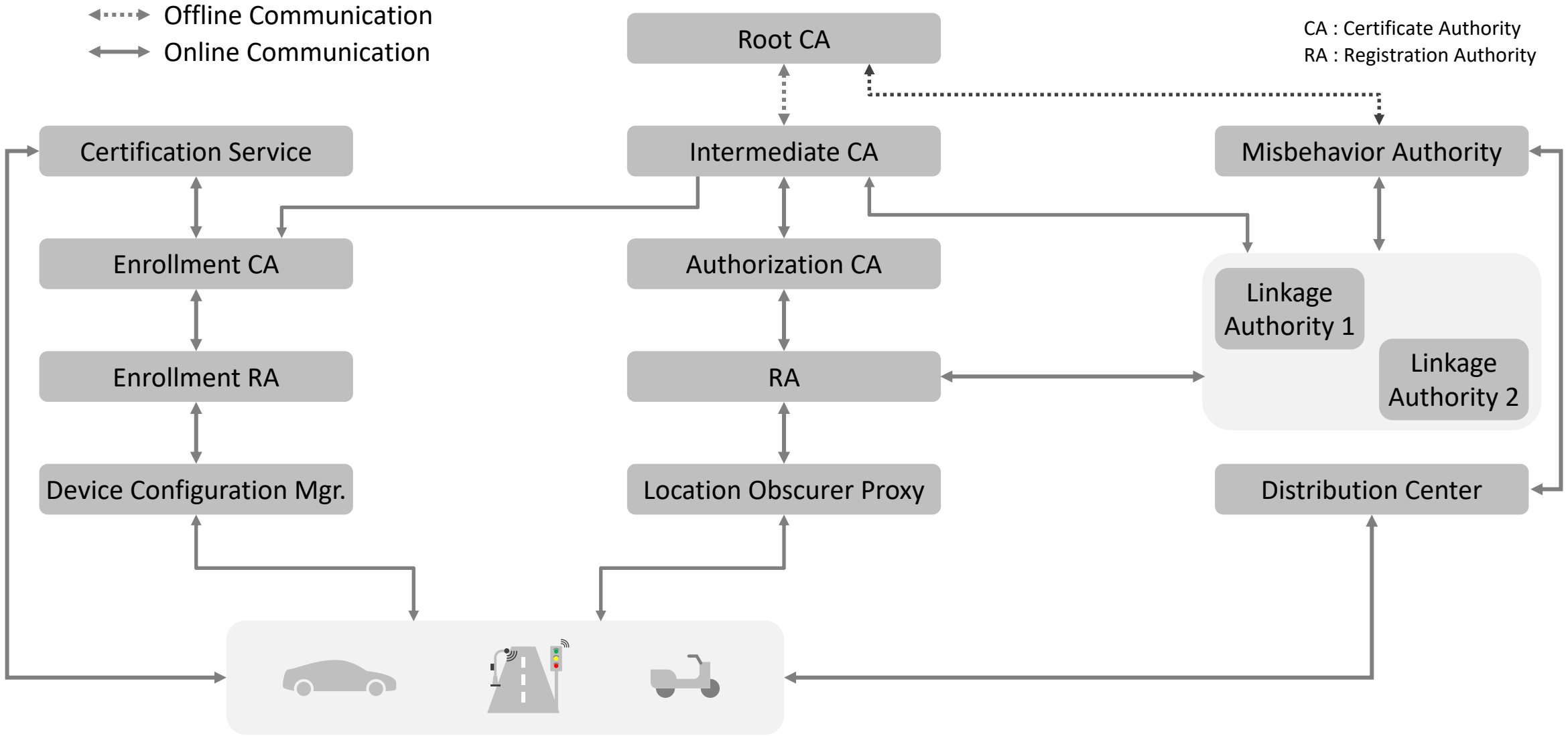


C-ITS : PKI(Public Key Infrastructure) for General IT

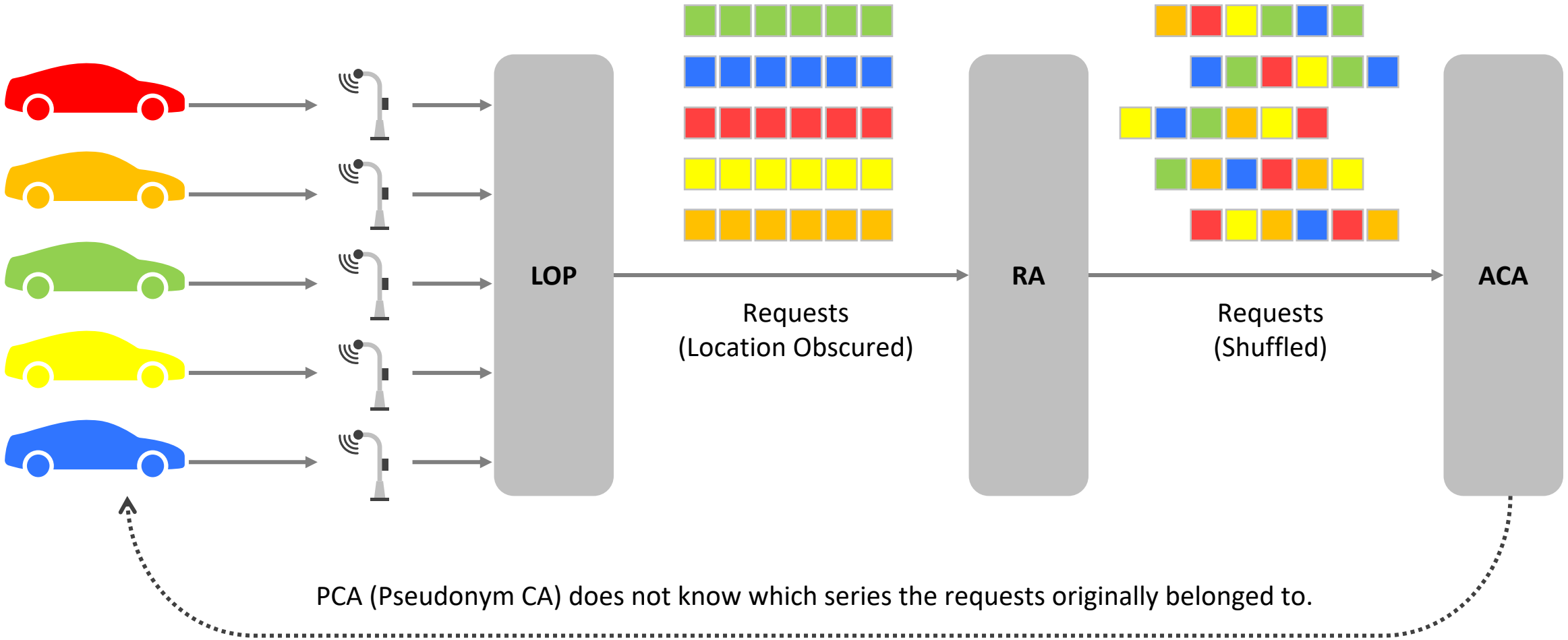
CA : Certificate Authority
RA : Registration Authority



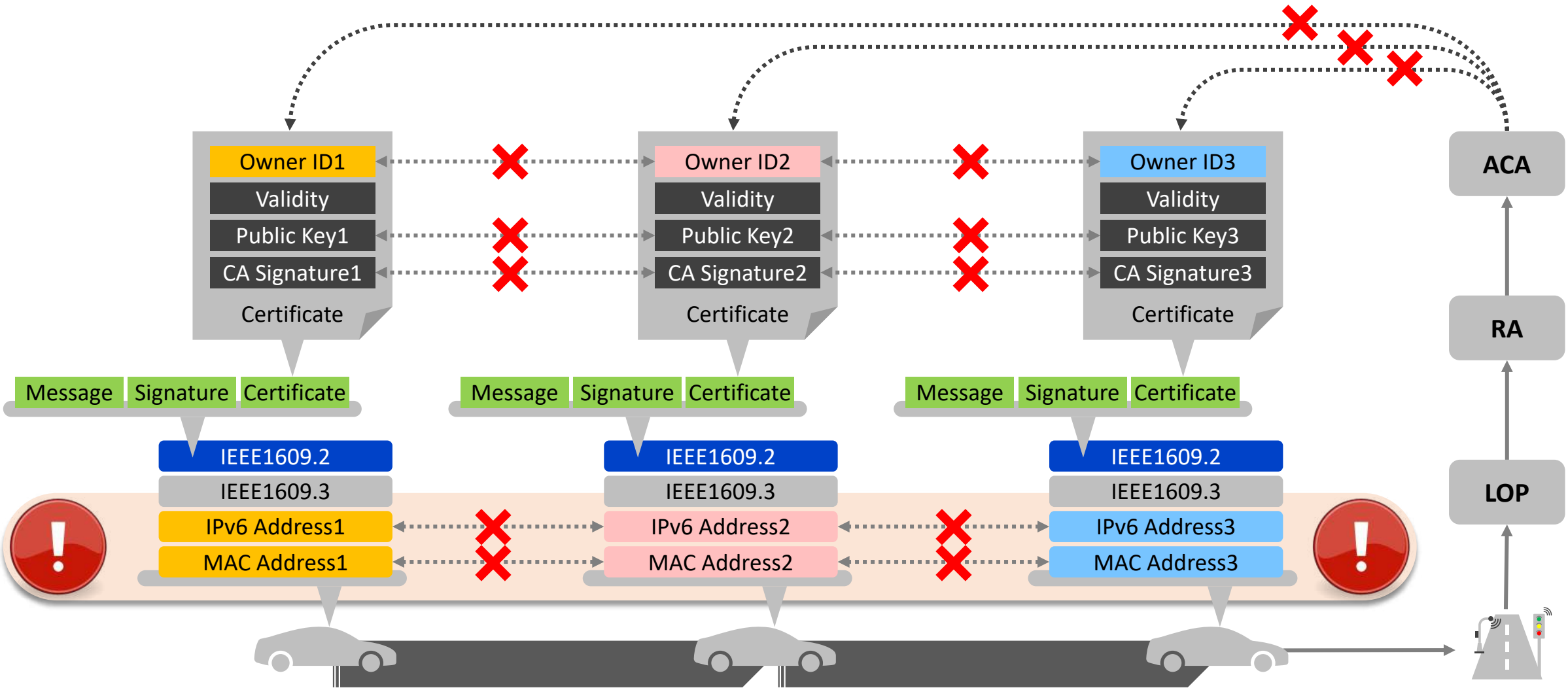
C-ITS : PKI(Public Key Infrastructure) for C-ITS



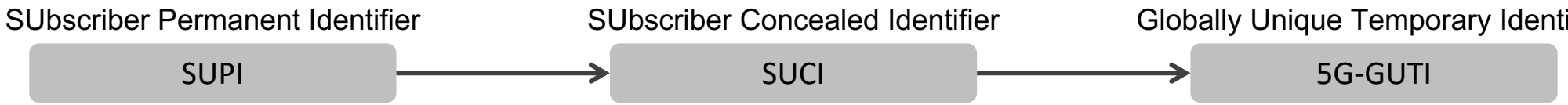
C-ITS : LOP(Location Obscurer Proxy) & Request Shuffling

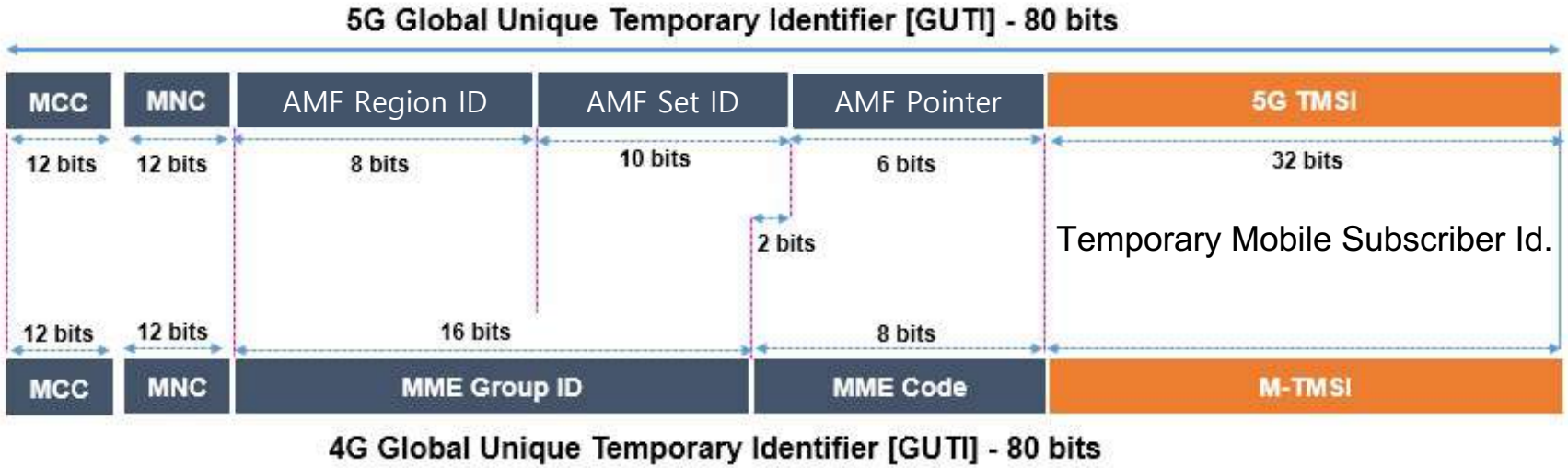


C-ITS : Privacy Preserving Technologies



Identifiers of 5G





5.5 Requirements on the AMF

5.5.3 Subscriber privacy [3GPP TS 33.501 V17.1.0 (2021-03) “Security architecture and procedures”]

The AMF shall support to trigger primary authentication using the SUCI.

The AMF shall support assigning 5G-GUTI to the UE.

The AMF shall support reallocating 5G-GUTI to UE.

6.12 Subscription identifier privacy [3GPP TS 33.501 V17.1.0 (2021-03)]

6.12.3 Subscription temporary identifier

A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003.

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the N1 NAS signalling connection is suspended.

Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM- IDLE mode with suspend indication in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the suspension of the N1 NAS signalling connection.

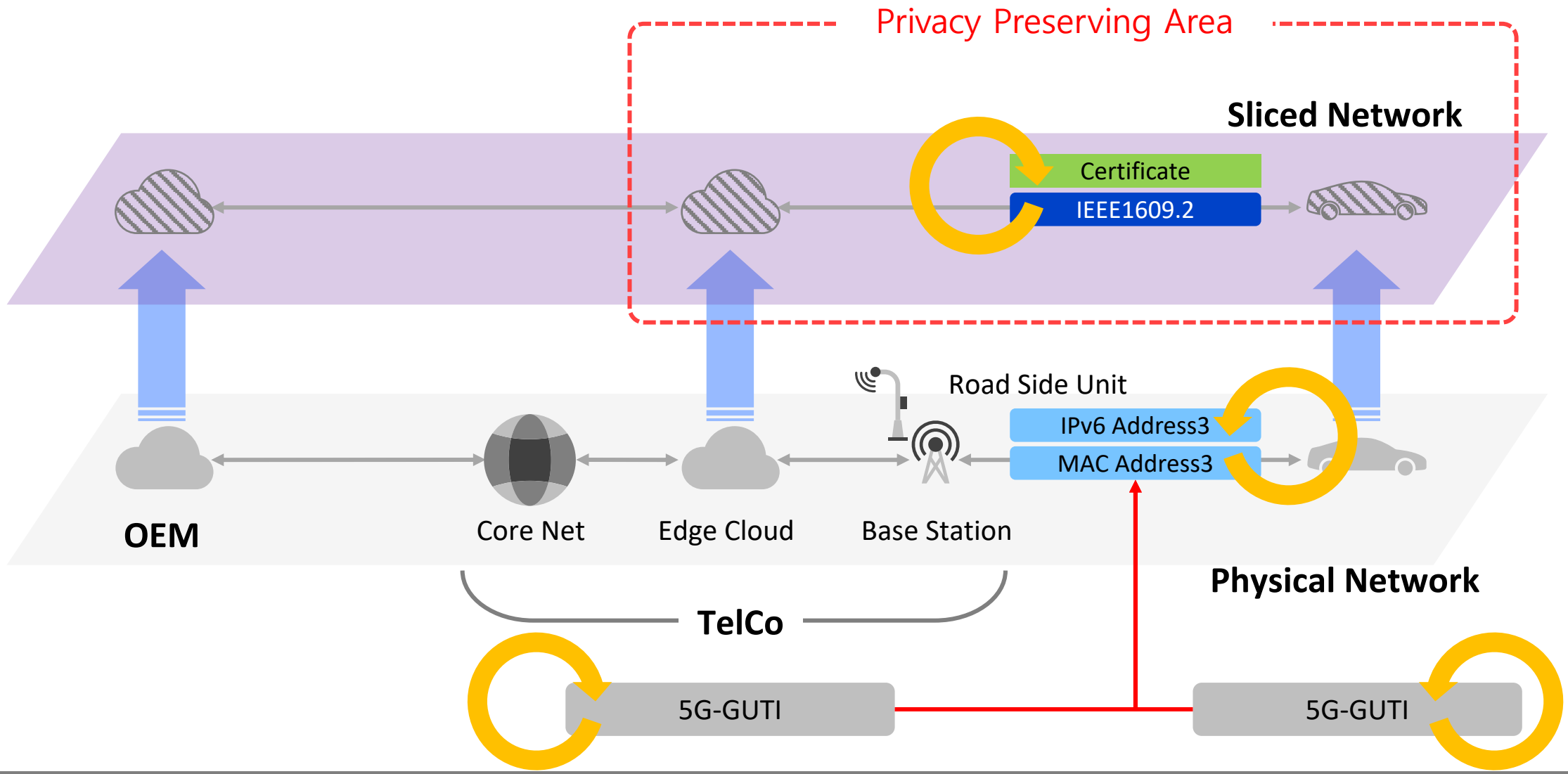
NOTE1: It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above, for example after a Service Request message from the UE not triggered by the network.

NOTE2: It is left to implementation to generate 5G-GUTI containing 5G-TMSI that uniquely identifies the UE within the AMF.

5G-TMSI generation should be following the best practices of unpredictable identifier generation. A new I-RNTI shall be sent to a UE only after a successful activation of AS security.

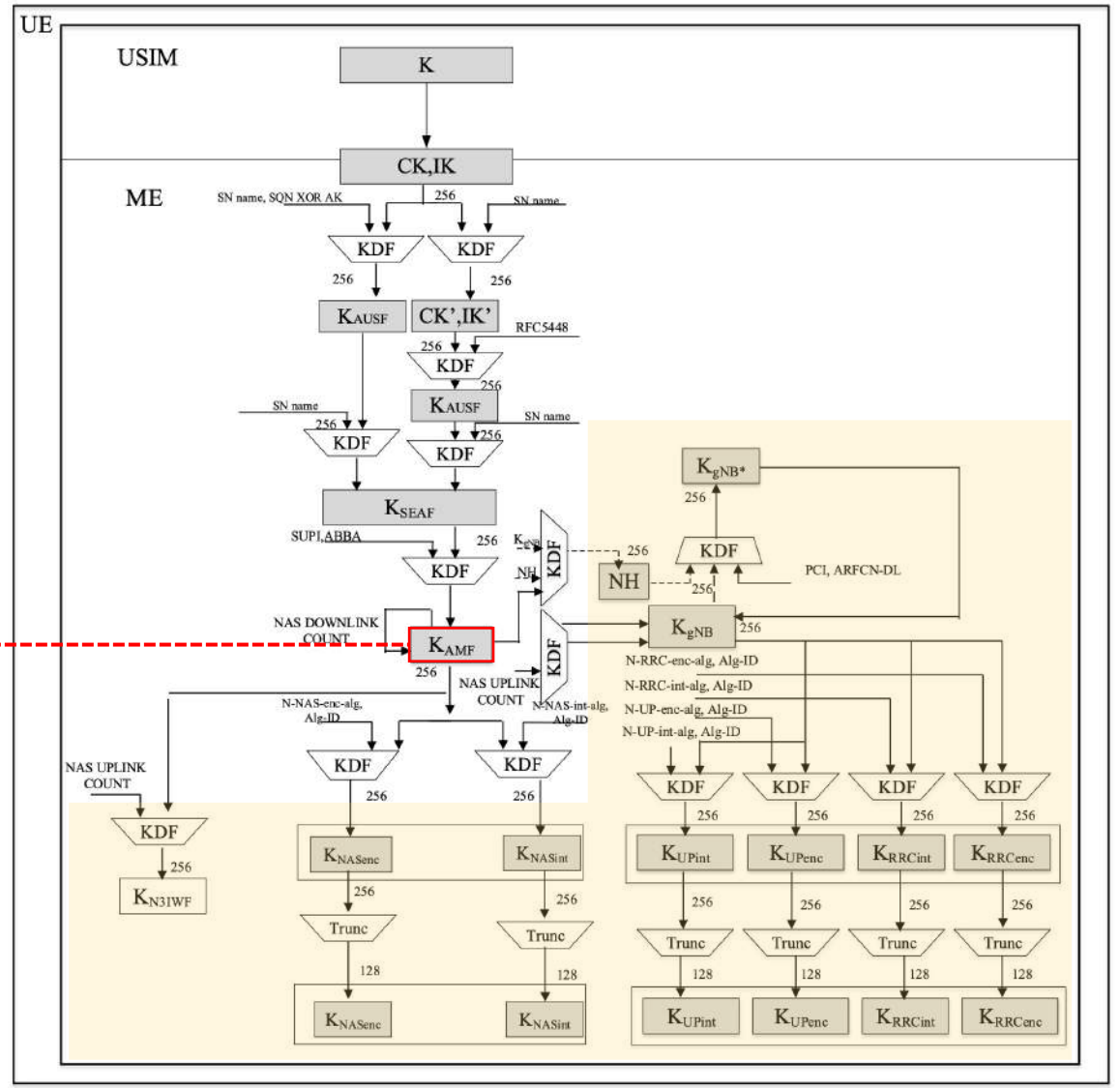
On transition of UE to RRC INACTIVE state requested by gNB during RRC Resume procedure or RNAU procedure, the gNB shall assign a new I-RNTI to the UE.

5G-V2X Privacy

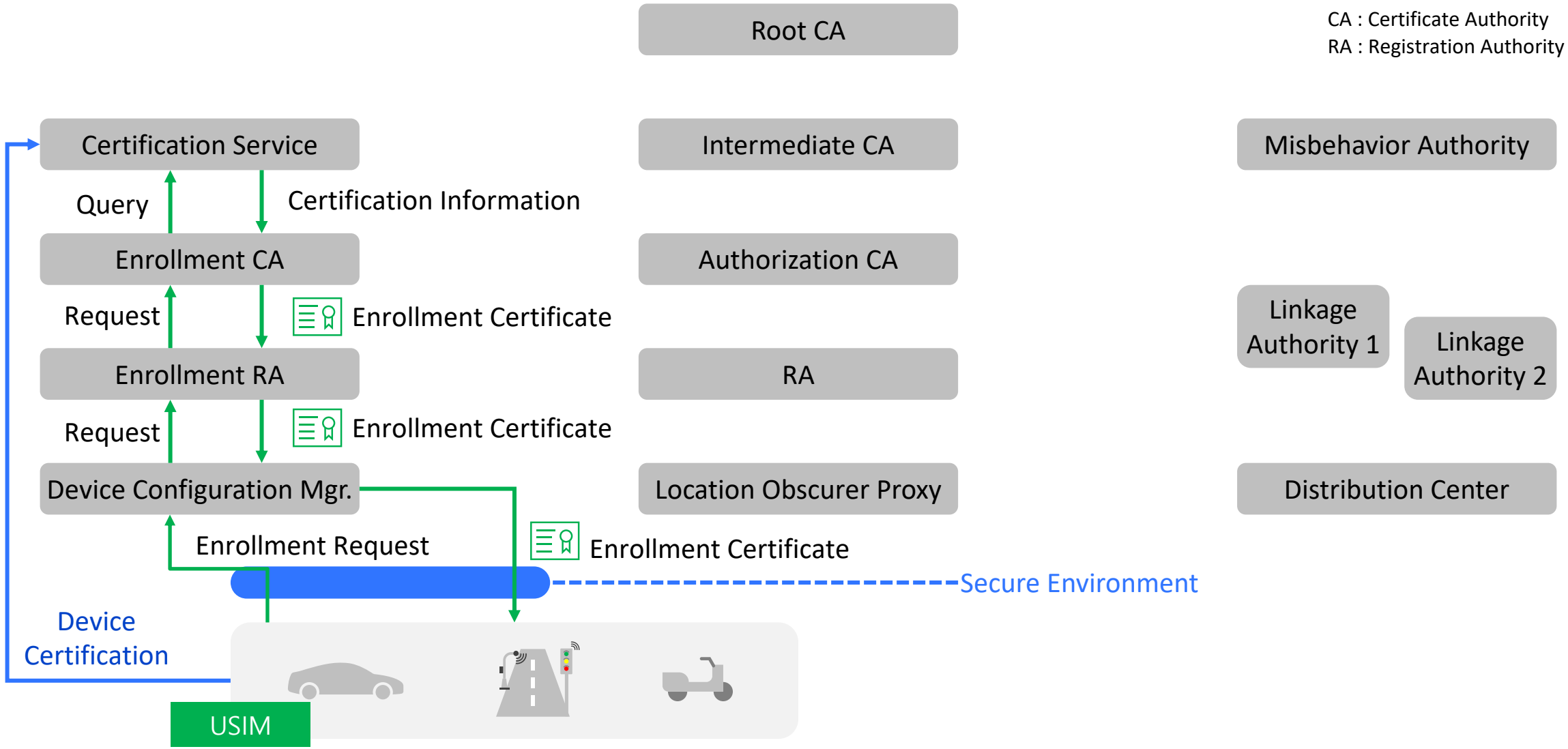


Updating GUTI & Keys

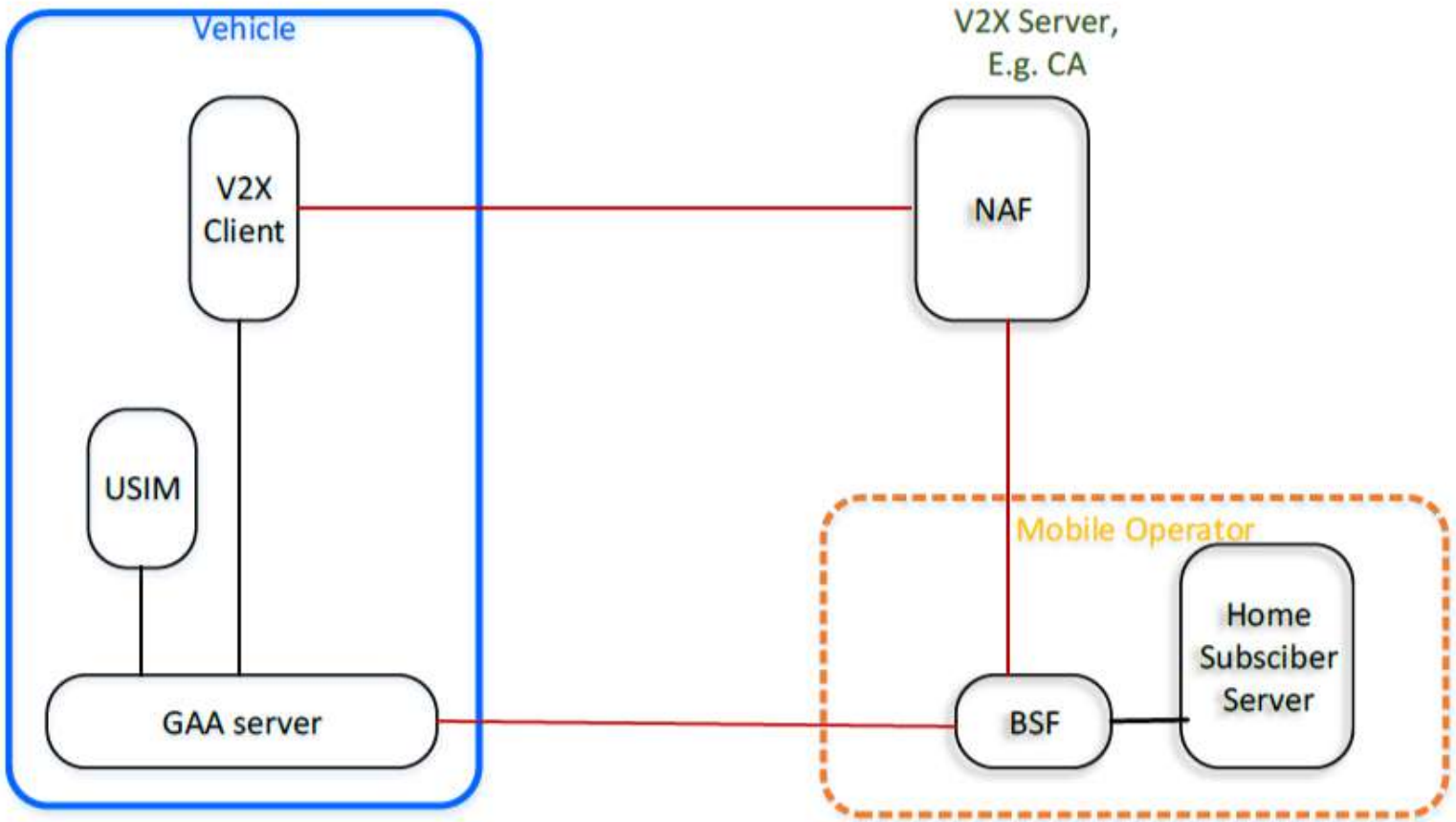
5G-GUTI



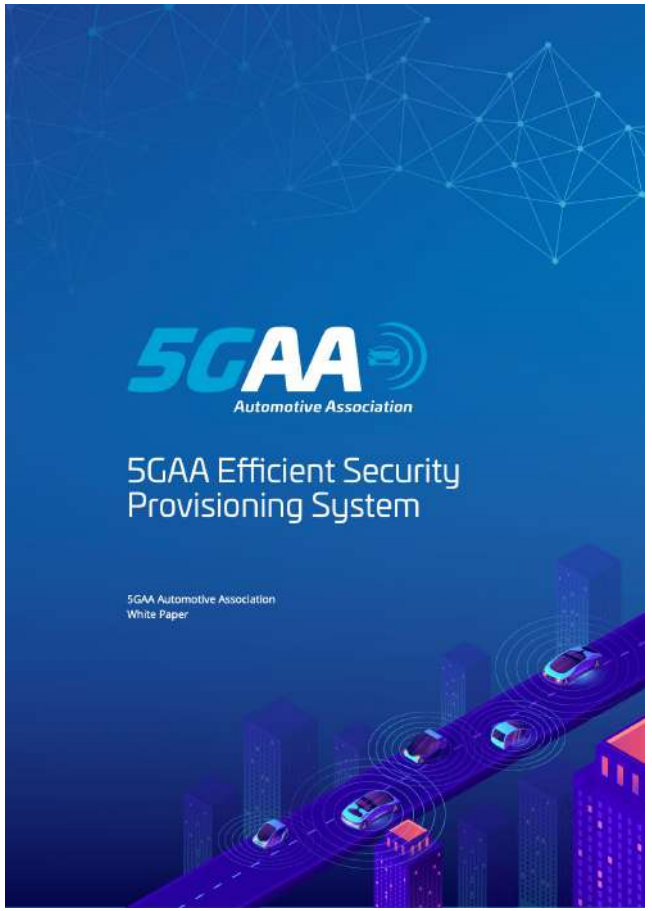
PKI(Public Key Infrastructure) for C-ITS : Provisioning & Bootstrapping



Bootstrapping



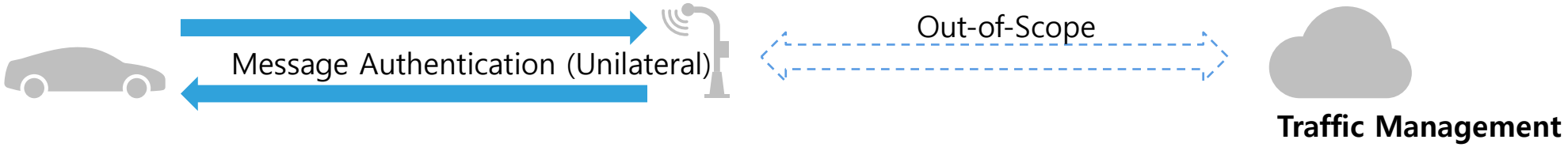
Generic Bootstrapping Architecture



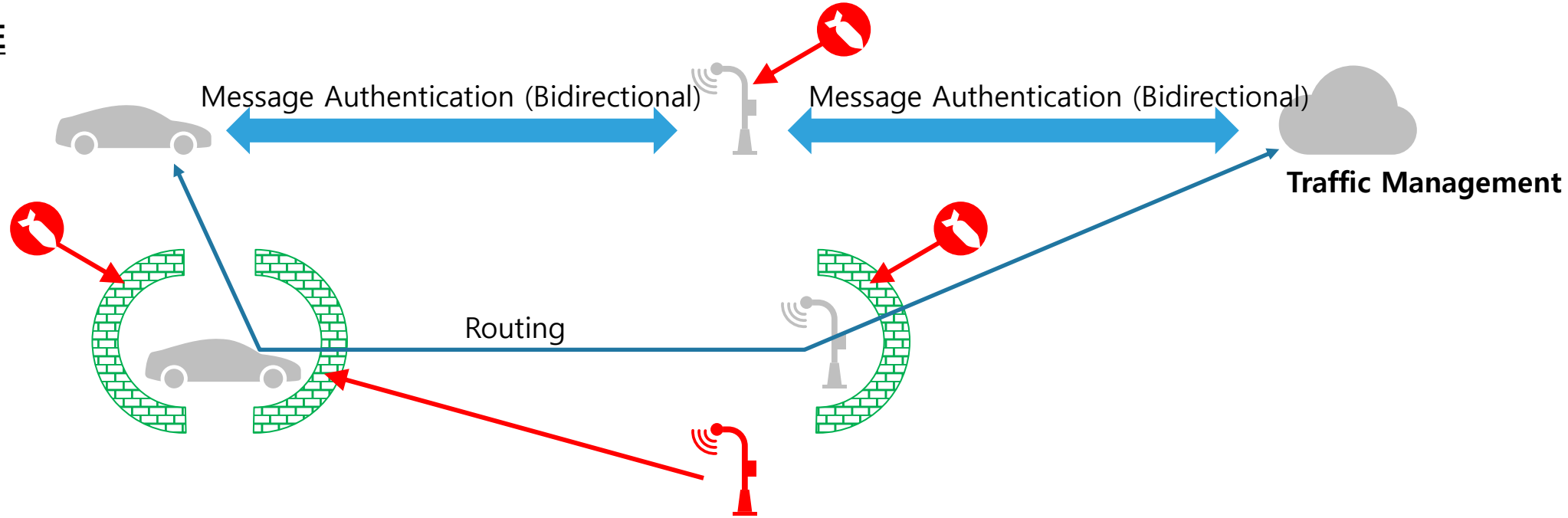
2020.05

C-ITS (Cooperative Intelligent Transportation System)

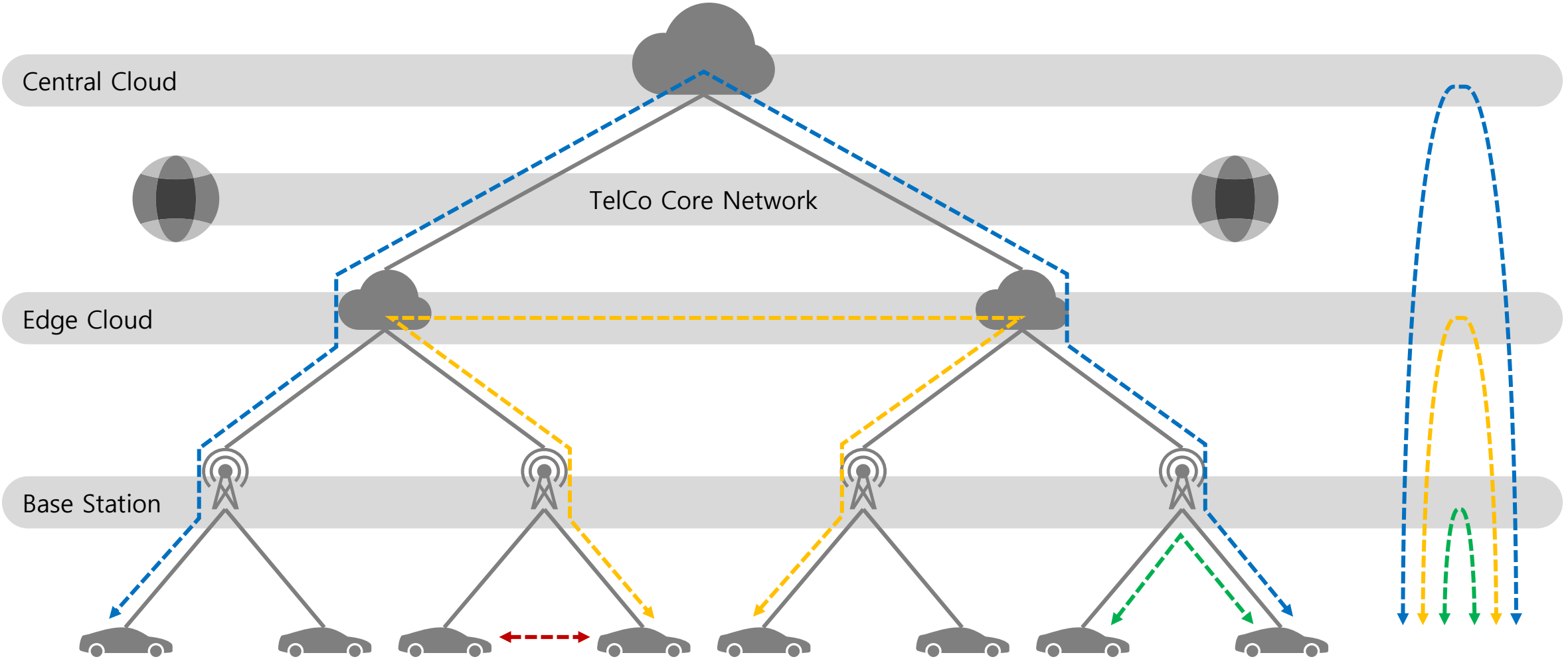
AS-IS



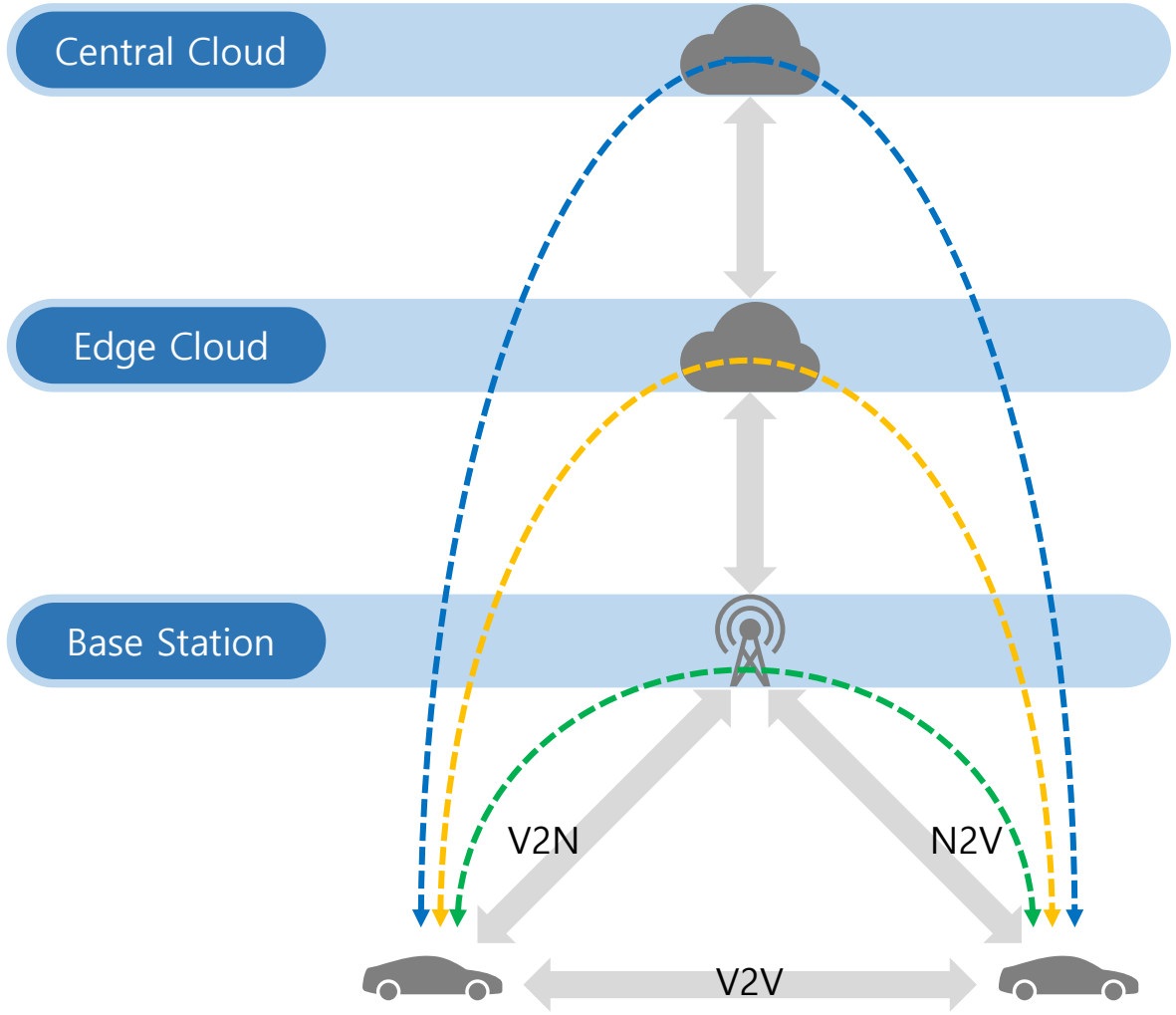
TO-BE



5G-V2X with Edge Cloud



V2N2V Service Structure for LDM(Local Dynamic Map)

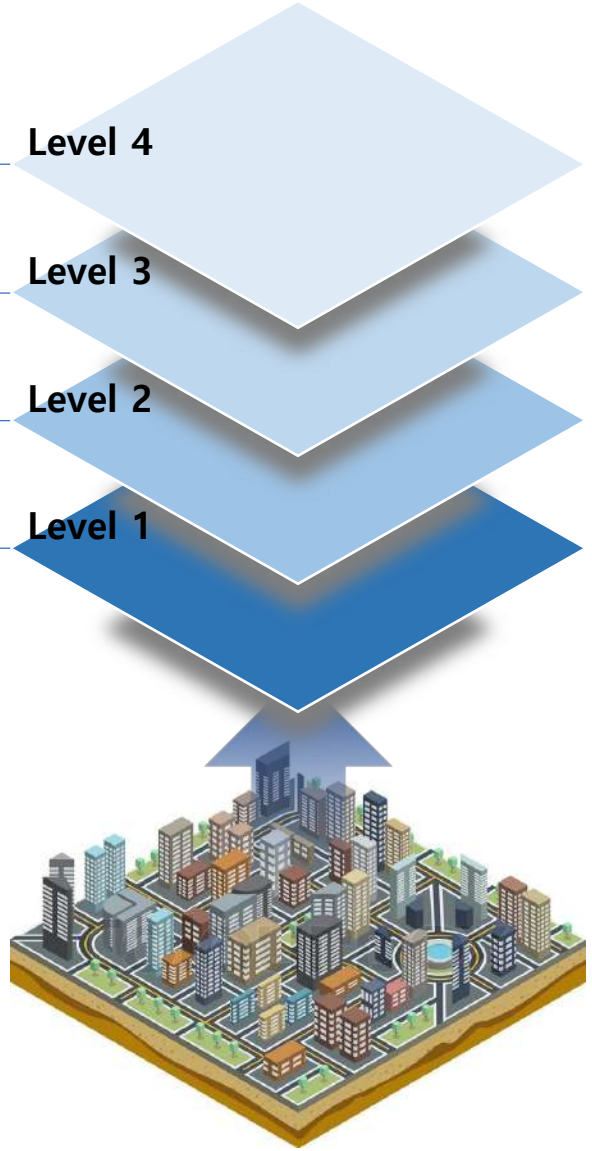


Highly dynamic data — **Level 4**
vehicle, pedestrian

Transient dynamic data — **Level 3**
congestion, signal phase

Transient static data — **Level 2**
roadside infra

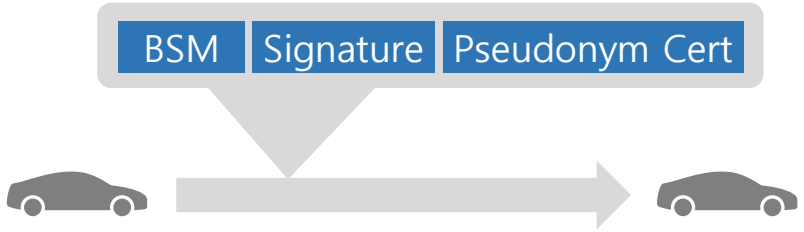
Static data — **Level 1**
map



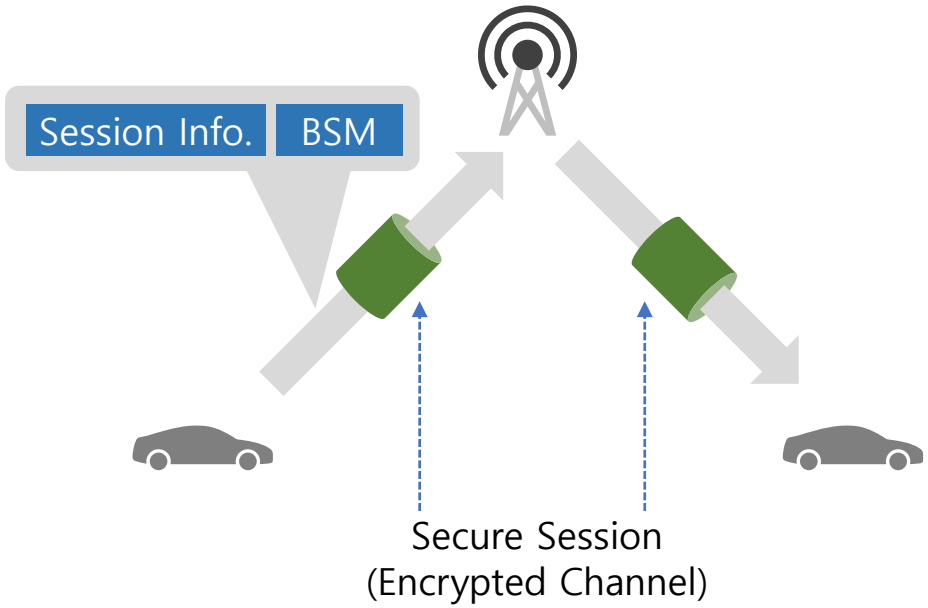
Local Dynamic Map

V2V Security vs. V2N2V Security

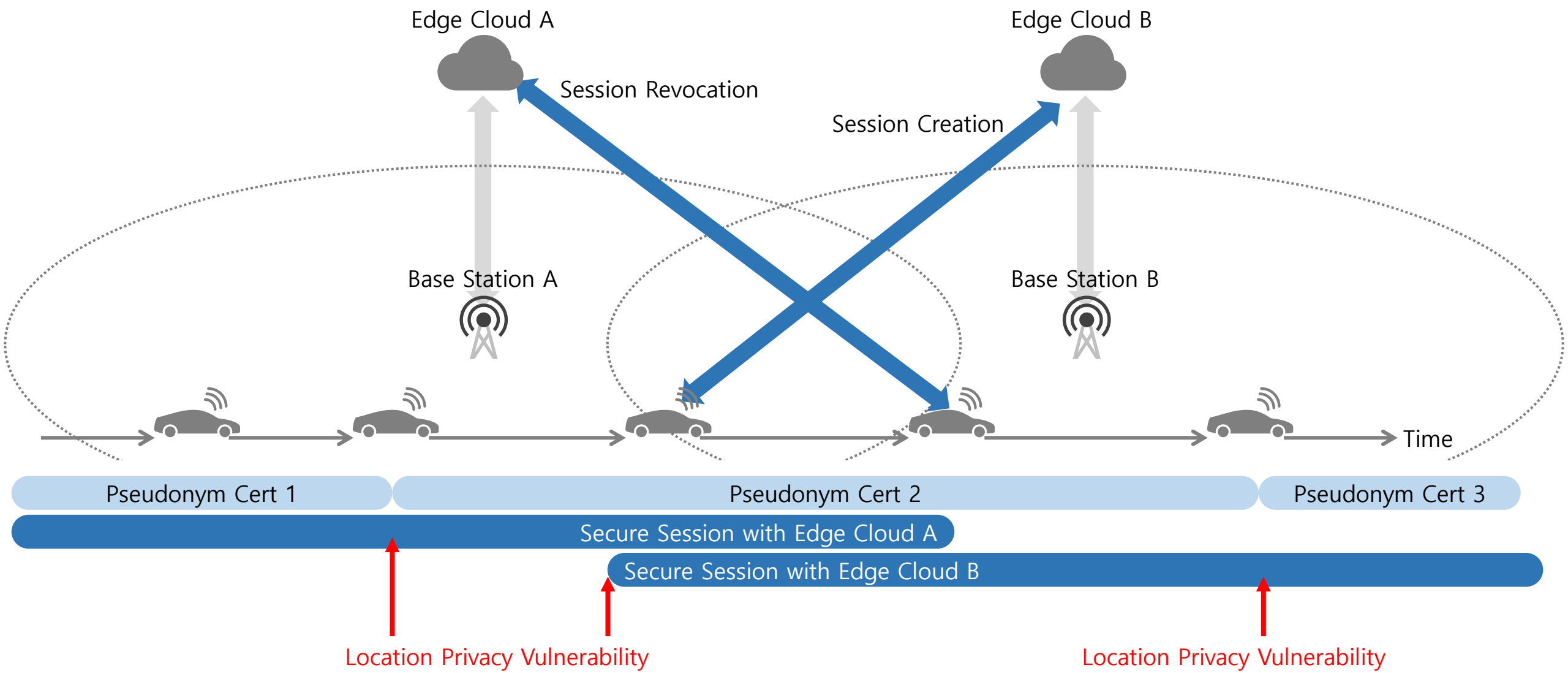
AS-IS



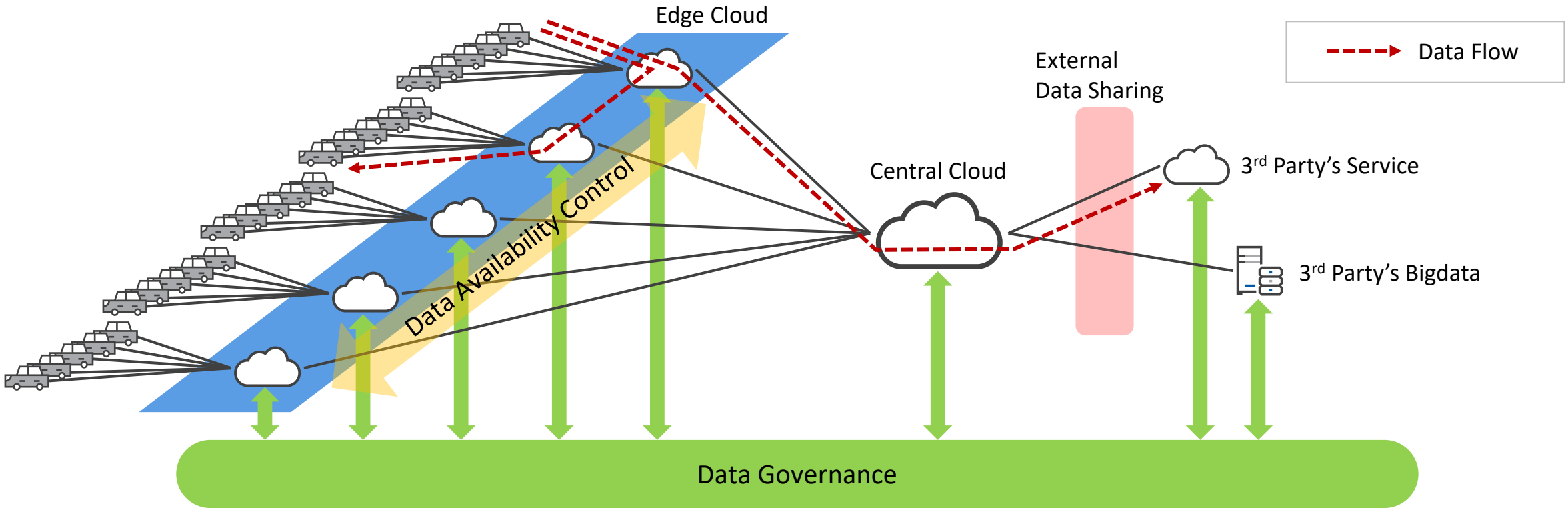
TO-BE



Privacy Issue on V2N2V Security



Data Governance & Edge Network



SEOUL · SEJONG · SHANGHAI · WUXI · TOKYO · TORONTO

www.autocrypt.io