SAND2022-11671C

Current State of OTA

Expensive, difficult to maintain and secure

Sandia National Laboratories

Industry Best Practice:

Cybersecurity Triad/Principles

- **Confidentiality**
  Protect proprietary codes running on Electronic Control Units (ECUs)
- **Integrity**
  Assure that codes are not corrupted or modified
- **Authenticity**
  Only the authorized OEM can update the codes

Centralized Public Key Infrastructure (PKI) – Authentication & Integrity Check

All ECU OEM must agree to comply with Vehicle OEM Certificate Authority

- ECU OEM must purchase digital certificate for every ECU
- Some ECUs may not have enough CPU power to store and process PKI certificate
- ECU must have online connection to verify the certificate

PKI is complex and expensive to maintain, secure

- Digital certificates must be generated and stored on each ECU
- Digital certificates have shorter lifespan than operational lifespan of the vehicles, requires renewal
- PKI under the threat of “quantum supremacy”

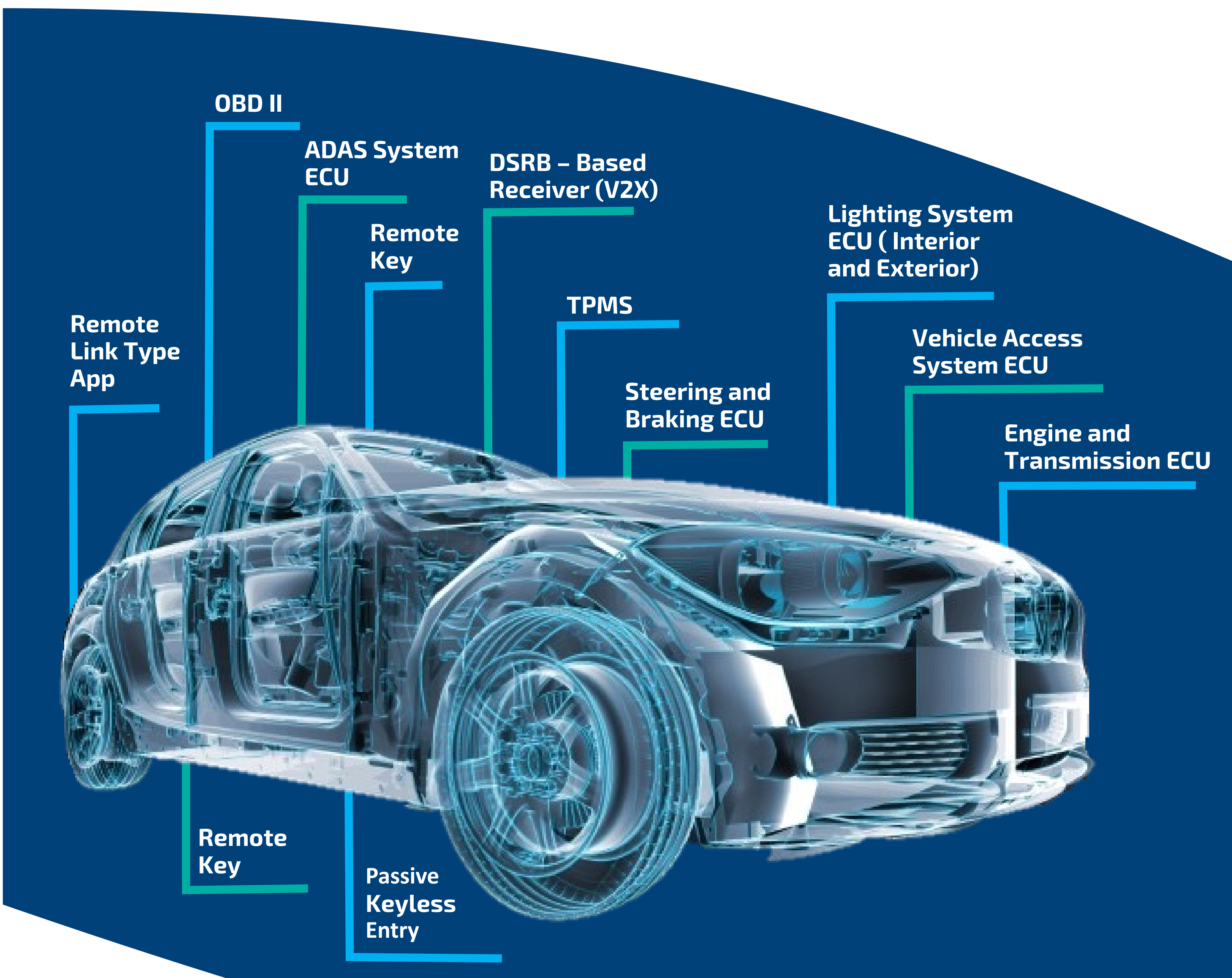
Centralized Key Management Service (KMS) – Confidentiality

ECU OEMs’ best interest to encrypt their intellectual property (i.e., software/firmware)

- Competitive edge
- Less opportunity for hackers to find vulnerabilities
- Using KMS has “cost”

KMS is complex and expensive to maintain, secure

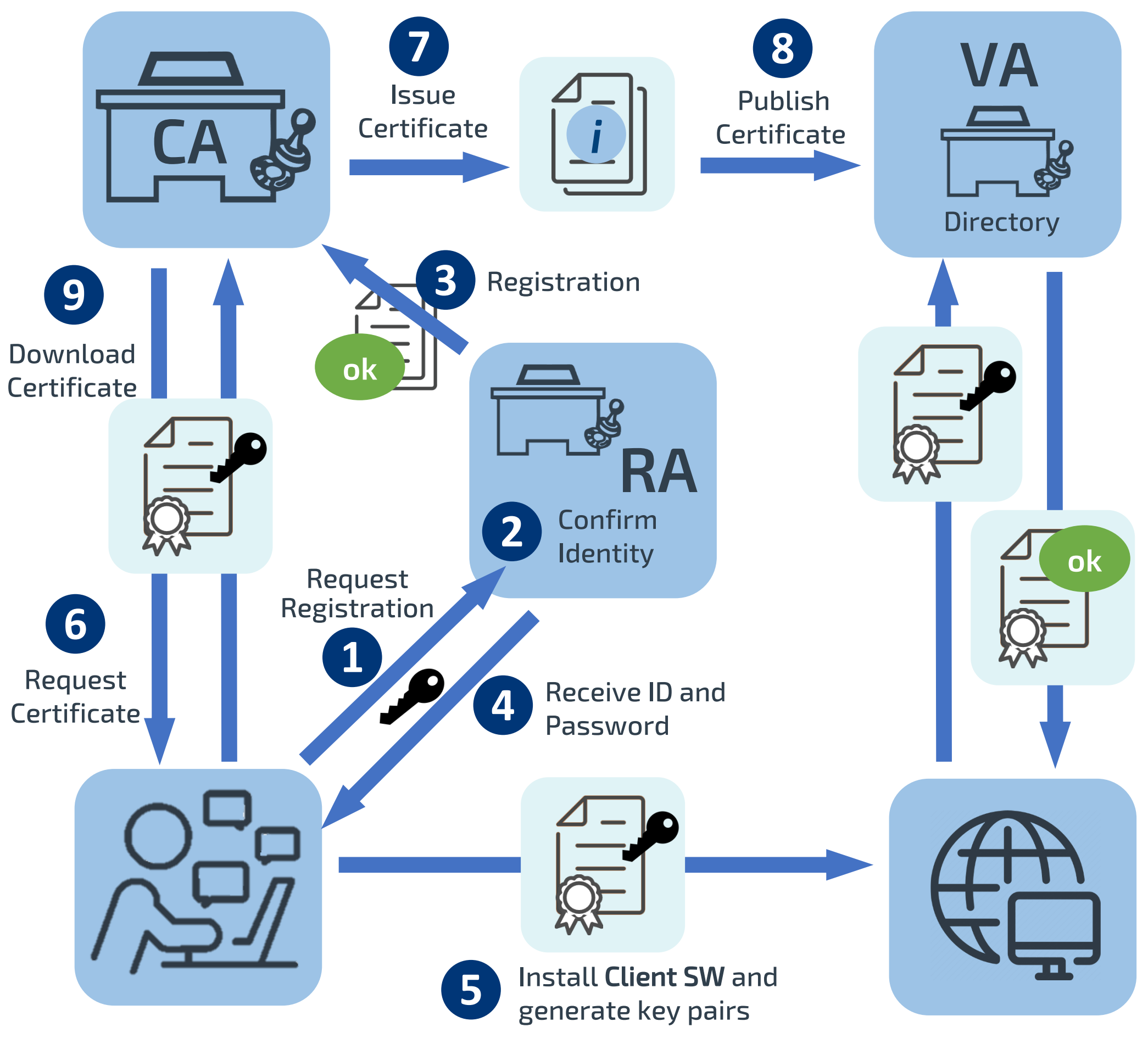
- Key generation, distribution, expiration, & access privileges must be planned and agreed upon by all ECU OEMs (to enable OTA, ECU OEMs must relinquish the encryption keys to vehicle OEM)
- Digital certificates (PKI) are the default technology for linking access privileges to encryption/decryption keys
- Compromising KMS has much lower threshold vs conducting full scale cryptographic analysis (e.g., Quantum Computer)
- When encryption keys do get compromised, who will be held liable?


OBD II
ADAS System ECU
DSRB – Based Receiver (V2X)
Remote Key
Remote Link Type App
TPMS
Lighting System ECU (Interior and Exterior)
Vehicle Access System ECU
Steering and Braking ECU
Engine and Transmission ECU
Remote Key
Passive Keyless Entry

Over-the-Air (OTA) Environment

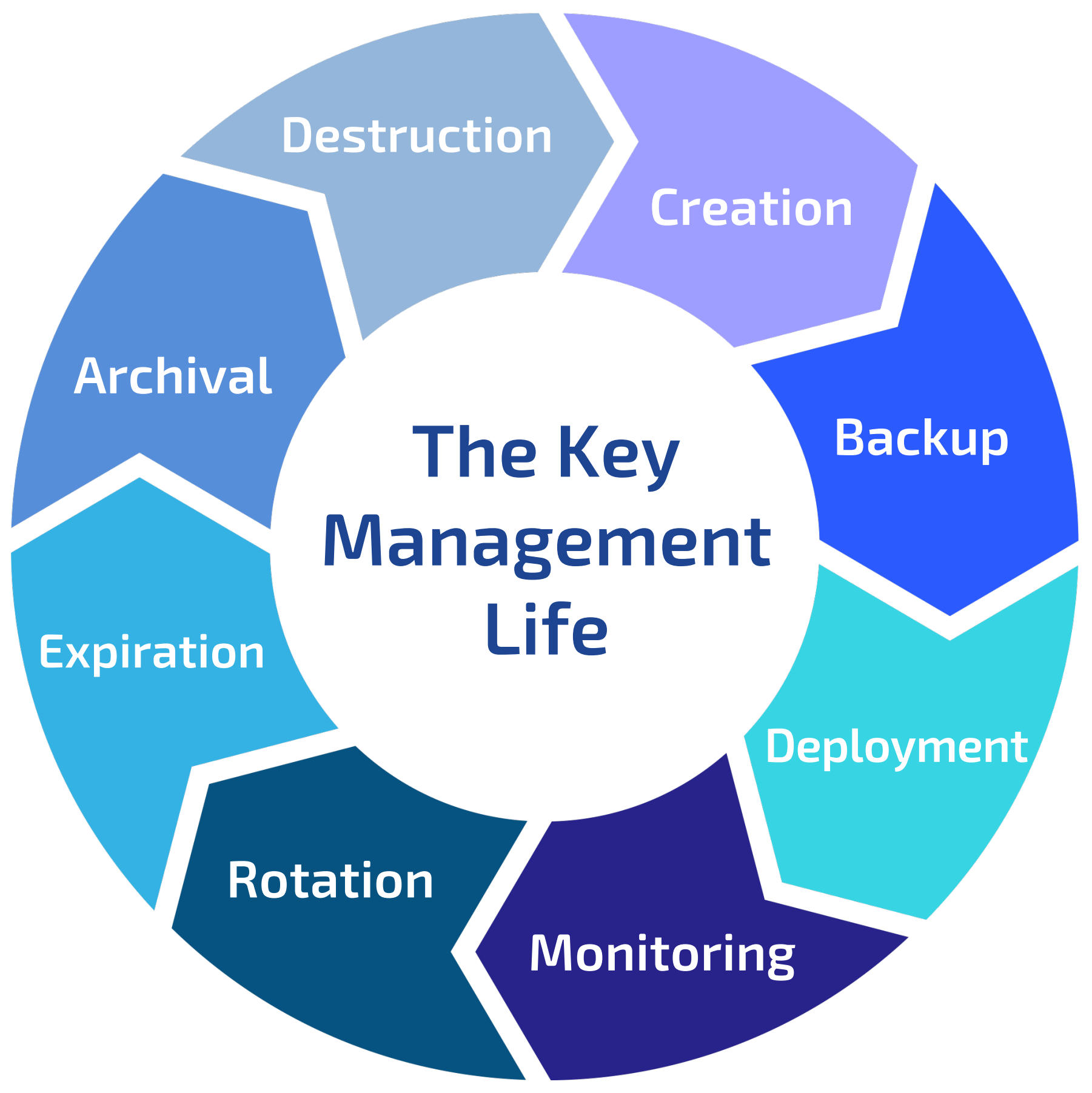
Potential Attack Surfaces

Public Key Infrastructure (PKI)



+

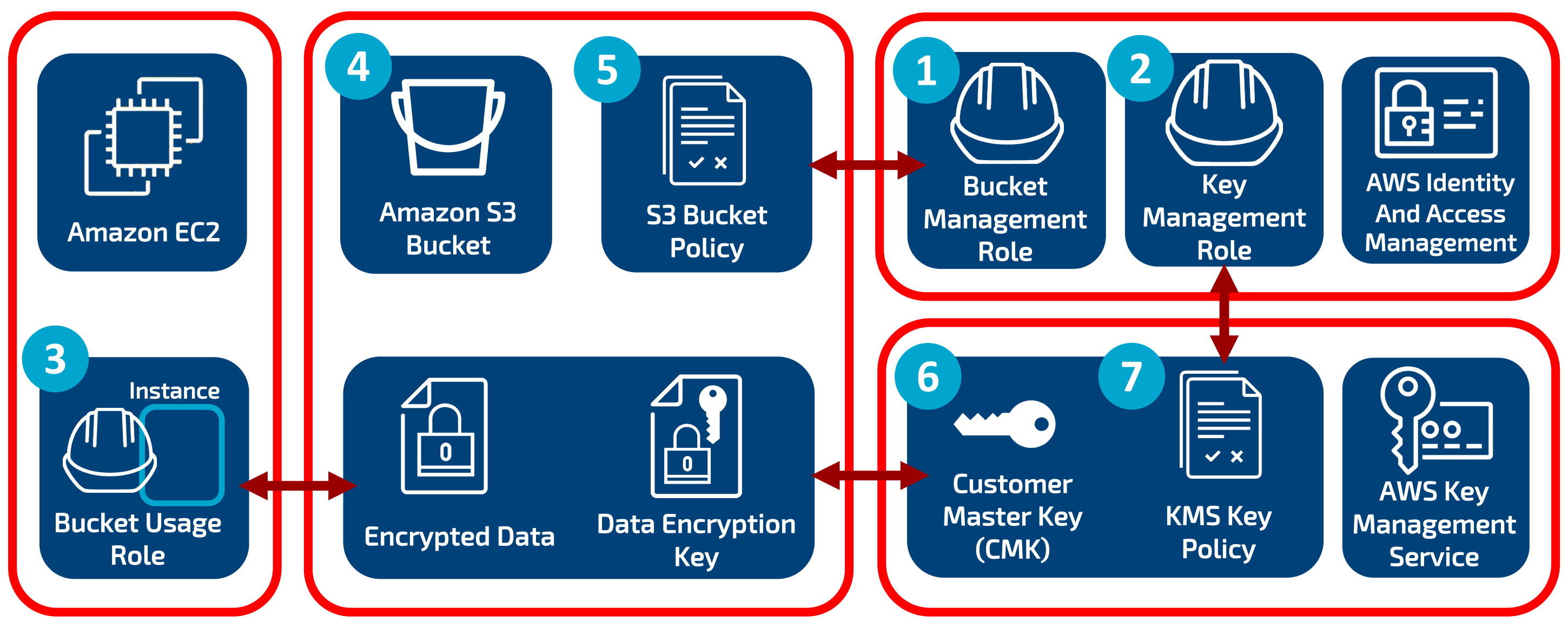
Centralized Key Management Service (KMS)



=

PKI & KMS Implementation

Every entity in this diagram is digitally susceptible



U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2022-1618120

Sandia National Laboratories

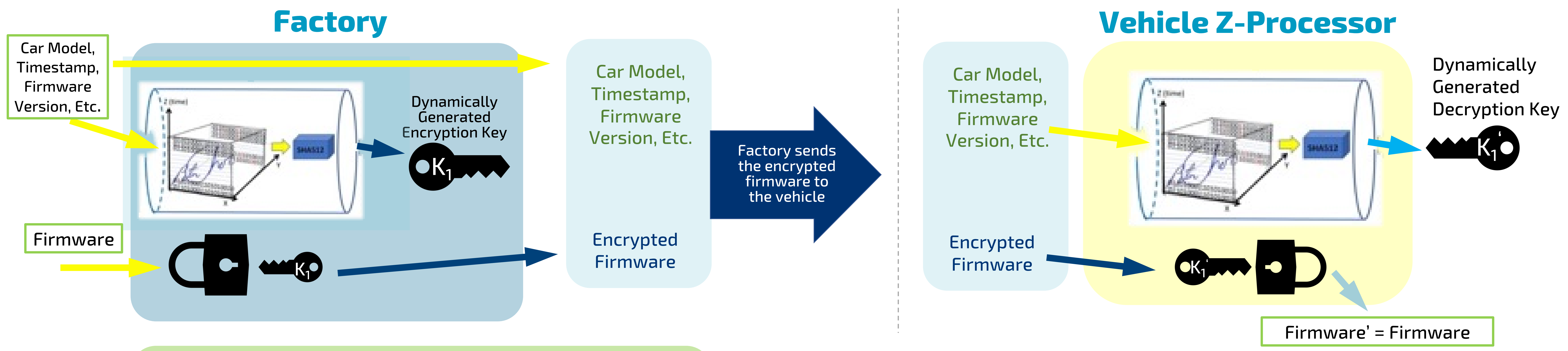
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Secure OTA

Enabling an efficient and secure future

Sandia National Laboratories

Secure OTA Firmware Update Data Flow Diagram



Factory
Car Model, Timestamp, Firmware Version, Etc.
Dynamically Generated Encryption Key
K_1
Firmware
K_1
Car Model, Timestamp, Firmware Version, Etc.
Encrypted Firmware
Factory sends the encrypted firmware to the vehicle
Vehicle Z-Processor
Car Model, Timestamp, Firmware Version, Etc.
Encrypted Firmware
Dynamically Generated Decryption Key
K_1'
K_1'
Firmware' = Firmware

If vehicle successfully decrypts, then identical decryption key was generated by Vehicle Z-Processor.

K1=K1'

Z-Processor dynamically generates the decryption keys that are automatically matched to the encrypted file, as well as providing **INTEGRITY** and **AUTHENTICITY** checks on the received message.
Z = Zero Trust Cryptographic Engine

US Patent #11,070,532 B1: Methods for Communicating Data Utilizing Sessionless Dynamic Encryption

Secure OTA without PKI or KMS

1 Z_1 sends V_1's ECU firmware status

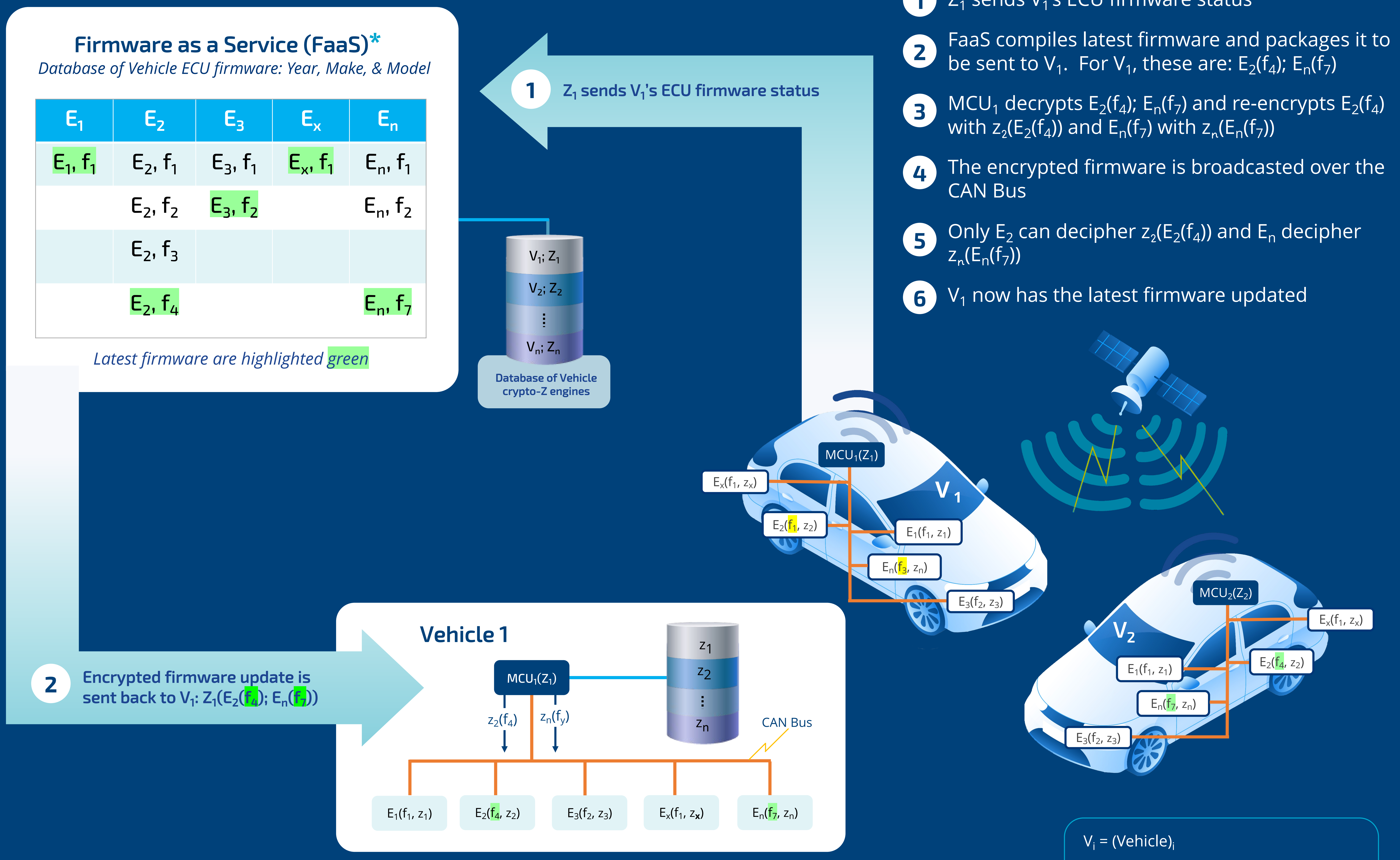
2 FaaS compiles latest firmware and packages it to be sent to V_1. For V_1, these are: $E_2(f_4)$; $E_n(f_7)$

3 MCU_1 decrypts $E_2(f_4)$; $E_n(f_7)$ and re-encrypts $E_2(f_4)$ with $z_2(E_2(f_4))$ and $E_n(f_7)$ with $z_n(E_n(f_7))$

4 The encrypted firmware is broadcasted over the CAN Bus

5 Only E_2 can decipher $z_2(E_2(f_4))$ and E_n decipher $z_n(E_n(f_7))$

6 V_1 now has the latest firmware updated



Firmware as a Service (FaaS)*

Database of Vehicle ECU firmware: Year, Make, & Model

E_1	E_2	E_3	E_x	E_n
E_1, f_1	E_2, f_1	E_3, f_1	E_x, f_1	E_n, f_1
	E_2, f_2	E_3, f_2		E_n, f_2
	E_2, f_3			
	E_2, f_4			E_n, f_7

Latest firmware are highlighted green

1 Z_1 sends V_1's ECU firmware status

2 Encrypted firmware update is sent back to V_1: $Z_1(E_2(f_4); E_n(f_7))$

V_i = (Vehicle)$_i$
Z_i = (Zero trust cryptographic engine)$_i$
f_i = (firmware version)$_i$
z_i = (ECU$_i$ zero trust crypto engine)$_i$
E_i = (Electronic Control Unit)$_i$
MCU_i =(Master Control Unit)$_i$*
FaaS = Firmware as a Service*

Principal Investigator

Peter Choi
schoi@sandia.gov
(505) 263-2653

Sandia National Laboratories
NNSA National Nuclear Security Administration
U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND SAND2022-1618120

*Patent Pending