

Zero trust for Automotive Ethernet
From MACsec to SDN-managed security

Friedrich Wiemer, Robert Bosch
Florian Wagner, ETAS

October 15th, 2026

Public C-SC0

A Collaboration of BOSCH | ETAS

Vehicle thefts – gone in literally under two minutes

CAN injection





[Toyota RAV4 2021 - stolen in less than two minutes]

[CAN injection @ DEF CON 31]

[CVE-2023-29389]

[CAN injection: keyless car theft @ Ken Tindell's blog]



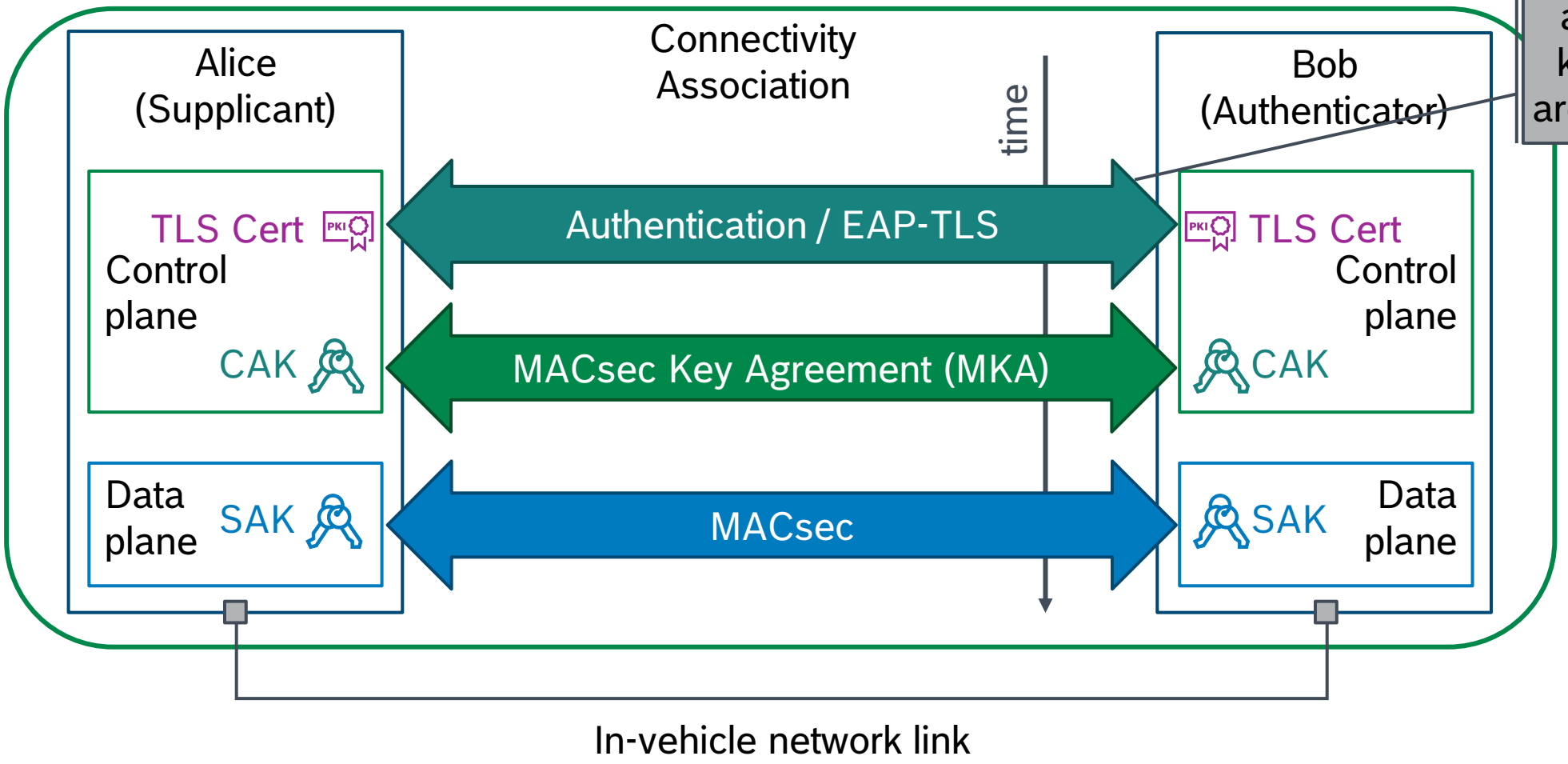
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

TLS: Transport Layer Security
EAP: Extensible Authentication Protocol
CAK: Connectivity Association Key
SAK: Secure Association Key

How to prevent message injection at link level?

MACsec



Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Key management
Kissner’s law



Lea Kissner
@LeaKissner

Crypto is a tool for turning a whole swathe of problems into key management problems. Key management problems are way harder than (virtually all) cryptographers think.

> **Filippo Valsorda @filippo.abyssdomain.exp...** @FiloSott... · Nov 23, 2019
> Quote tweet this with your most controversial cryptography opinion.

5:31 AM · Nov 24, 2019

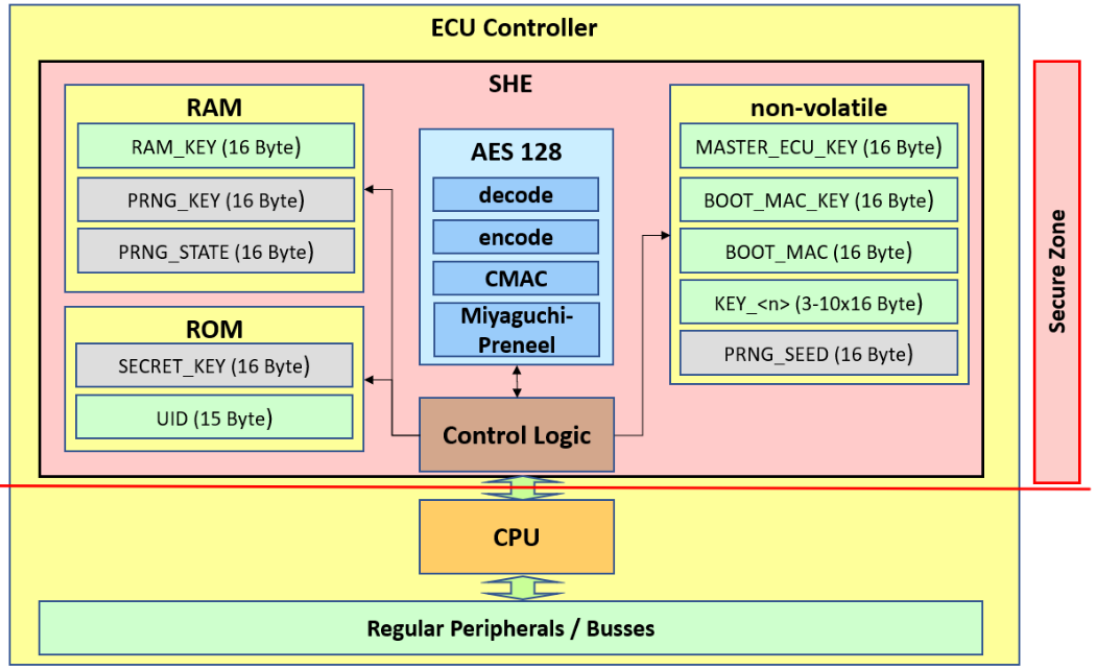
Kissner’s law: cryptography converts ~~many~~ all problems into key management problems, and key management problems are way harder than you think.

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

OEM: Original Equipment Manufacturer
SHE: Secure Hardware Extension



Key management
Current concepts



AUTOSAR Secure Hardware Extension (SHE): Sect. 4.9 Memory update protocol

- SHE offers standardized interface
  - CMD_LOAD_KEY(M1, M2, M3, M4, M5)

    Inputs Outputs
  - CMD_EXPORT_FROM_RAM_KEY outputs M1, ..., M5

Alternatives to SHE: OEM proprietary solutions
- OEM 1: based on asymmetric crypto
- OEM 2: based on symmetric crypto
- ...

Proprietary solutions = “build your own crypto” – can go right but can also go wrong; see e.g. SMEP attack!

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
A Collaboration of BOSCH | ETAS

YANG-based key management

Public C-SC0

HSM: Hardware Security Module
JTAG: Joint Test Action Group
CAK: Connectivity Association Key
SecOC: Secure Onboard Communication

YANG-based key management

Automotive key lifecycle and management

2 System level keys

CAKs
SecOC keys





Securely update / replace keys

3



CAKs
SecOC keys

Vehicle lifecycle

Dynamic key mgmt. at runtime required!

Requirements:

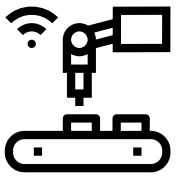
Confidentiality
Integrity
Authenticity

Handle “pre-configured”
Standardized

1 Device specific



via JTAG or generated in HSM

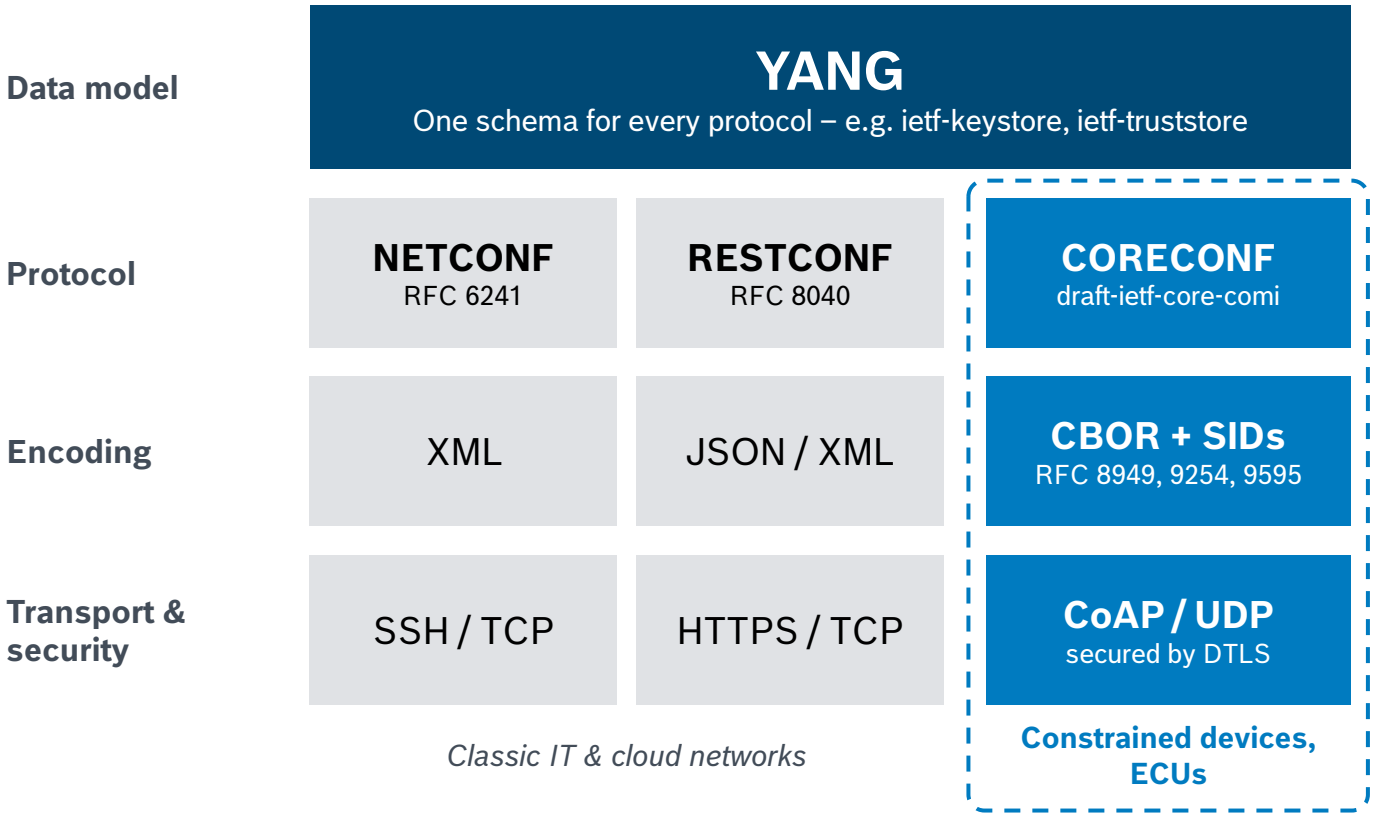


Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

CoAP: Constrained Application Protocol
SID: YANG Schema Item iDentifier
DTLS: Datagram Transport Layer Security
RFC: Request For Comments

YANG-based key management
Primer: YANG, CORECONF and CBOR



In a nutshell

YANG data modelling language (RFC 7950)

- Describes configuration and state data as a typed tree of containers, lists and leaves
- Standard models are reused as-is and extended via augment

CBOR Concise Binary Object Representation

- Binary, JSON-like encoding: compact on the wire, tiny parsers on microcontrollers
- YANG-CBOR turns schema names into numeric SIDs; keys travel as raw bytes – no Base64

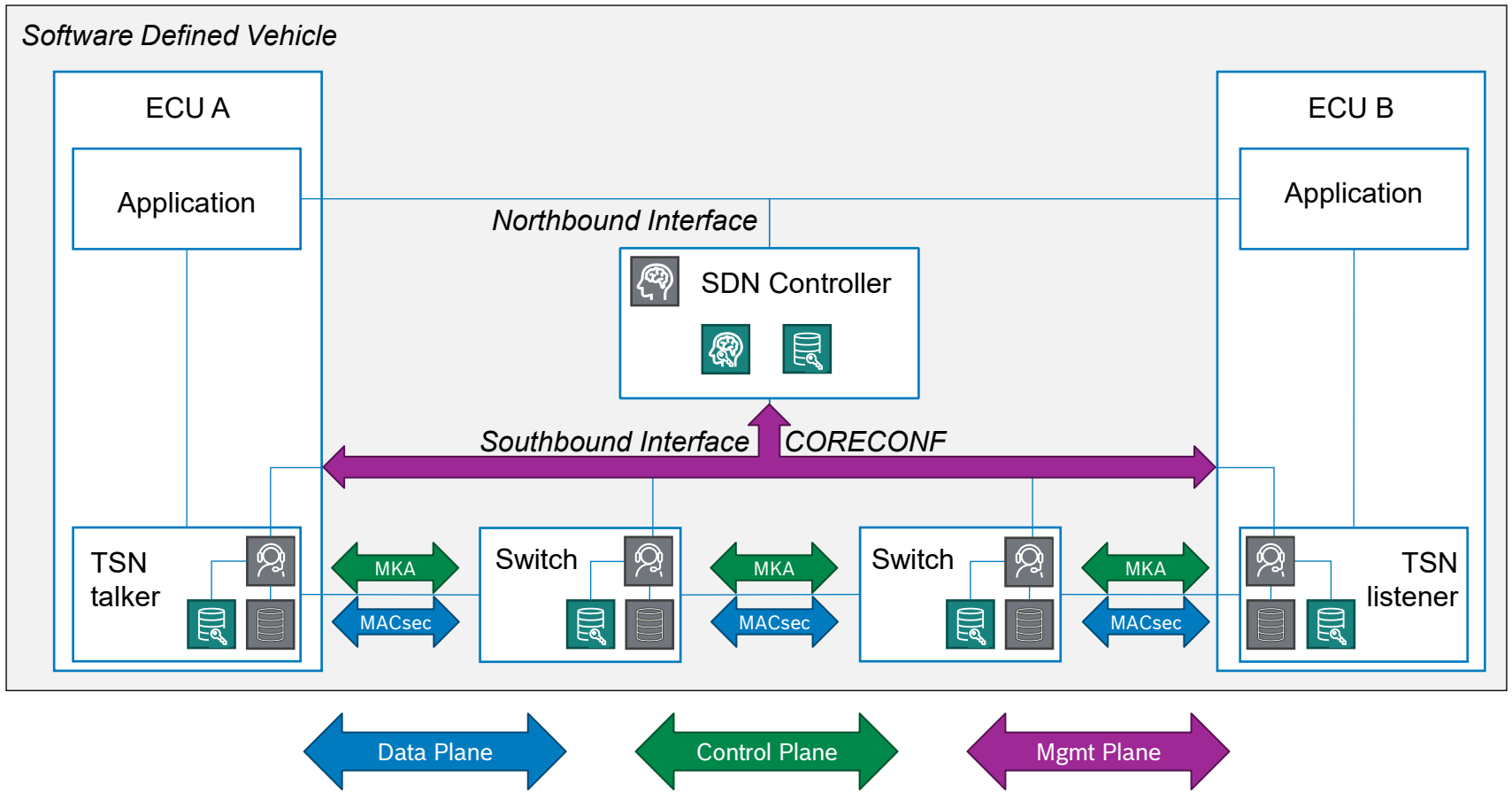
CORECONF CoAP Management Interface

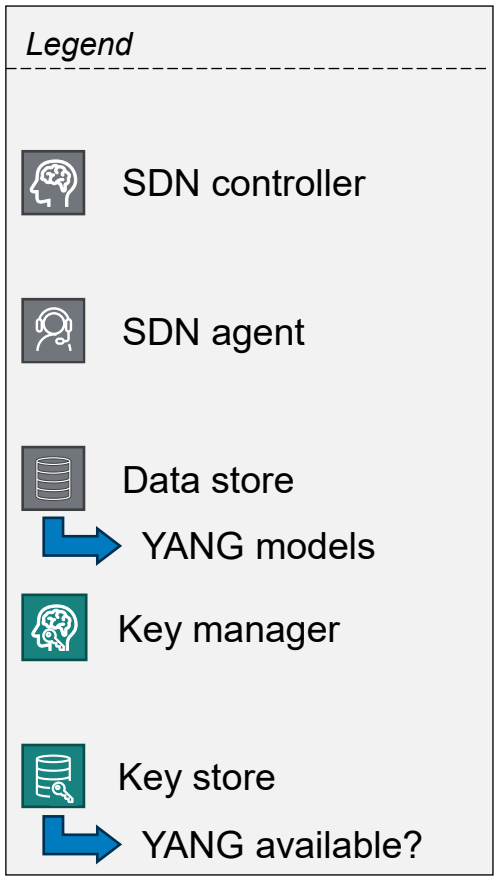
- RESTCONF-style access to YANG datastores over CoAP
- GET, FETCH, iPATCH, POST

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
A Collaboration of BOSCH | ETAS

TSN: Time-Sensitive Networking
ECU: Electronic Control Unit
YANG: Data Modelling Language
MKA: MACsec Key Agreement

YANG-based network management
Integrated in Software-Defined Networking (SDN)





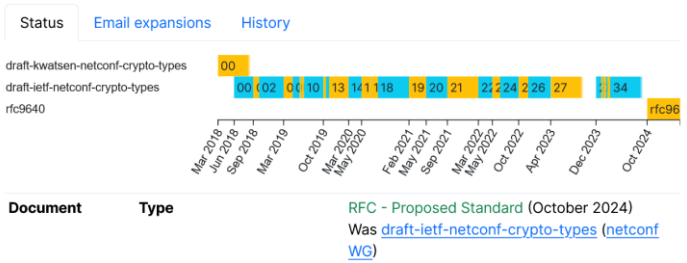
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

RFC: Request For Comments
YANG: Data Modelling Language

YANG-based key management
Existing YANG-models for key management

YANG Data Types and Groupings for Cryptography
RFC 9640



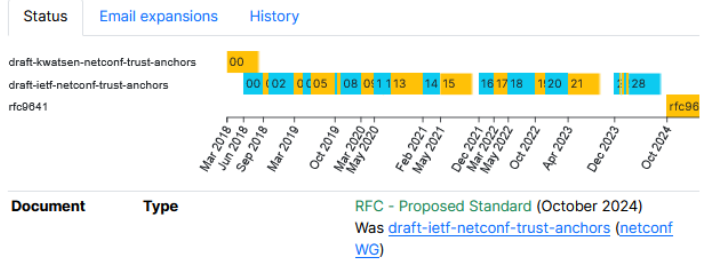
- Defines (symmetric) keys:
  - Hidden – non-readable via mgmt. interface
  - Encrypted – wrapped by another key
- Further types for asymmetric keys, certificates,…

A YANG Data Model for a Keystore
RFC 9642



- Defines keystore semantics on top of crypto types
- Supports
  - built-in keys (set during manufacturing) --> hidden
  - Key Encryption Keys (KEK) for encrypted keys

A YANG Data Model for a Truststore
RFC 9641



- Defines trust store model
- Management of
  - Certificates
  - Public-keys

➔ Whom to trust?

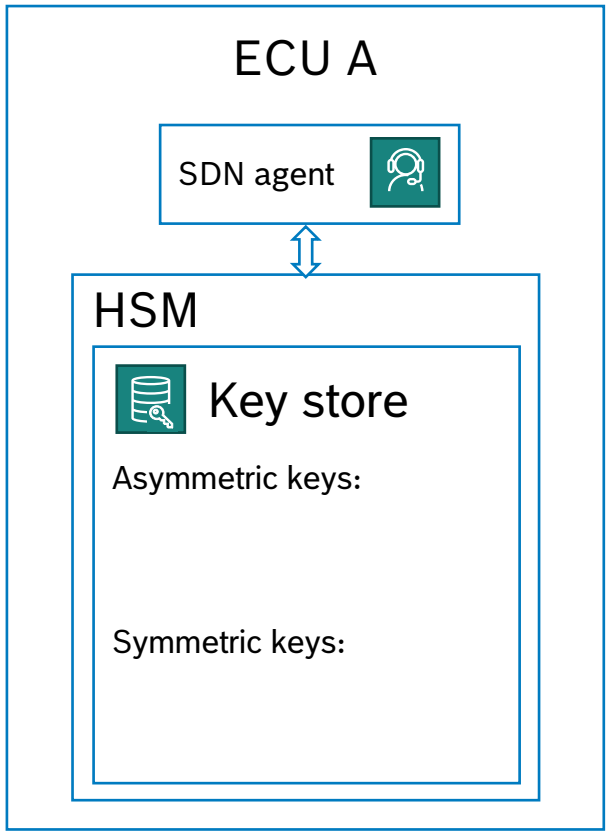
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

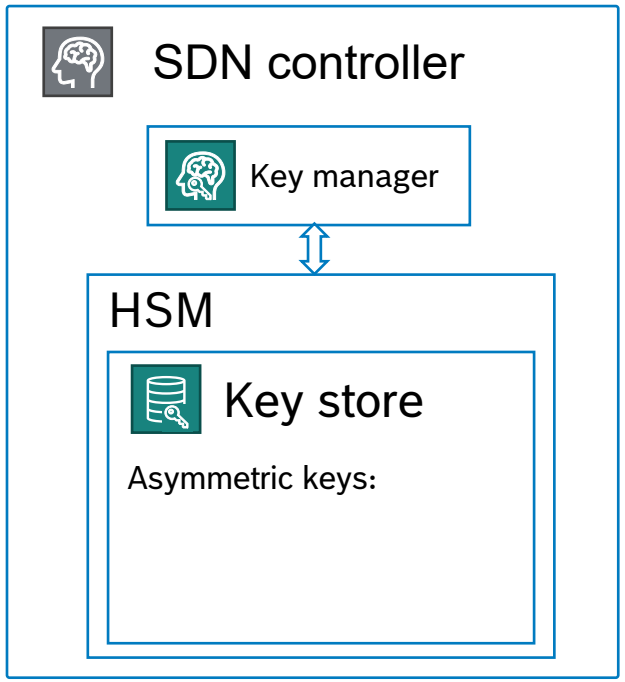
A Collaboration of BOSCH | ETAS

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module

YANG-based key management

Walkthrough: securely installing a CAK into an ECU





Key management steps

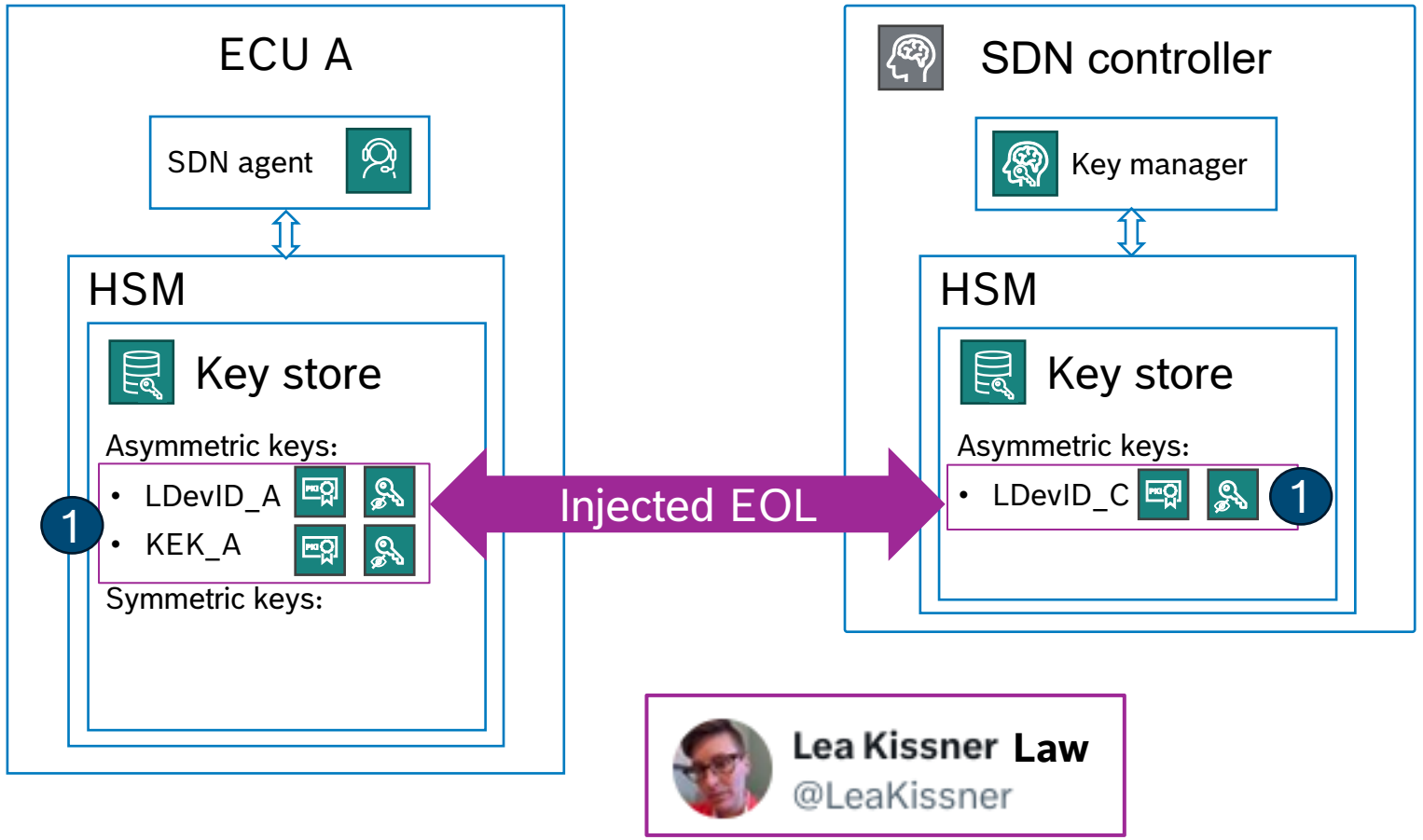
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module
EOL: End-of-line

YANG-based key management

Walkthrough: securely installing a CAK into an ECU



Key management steps

1 End-of-line key-injection

Certificate

Hidden key

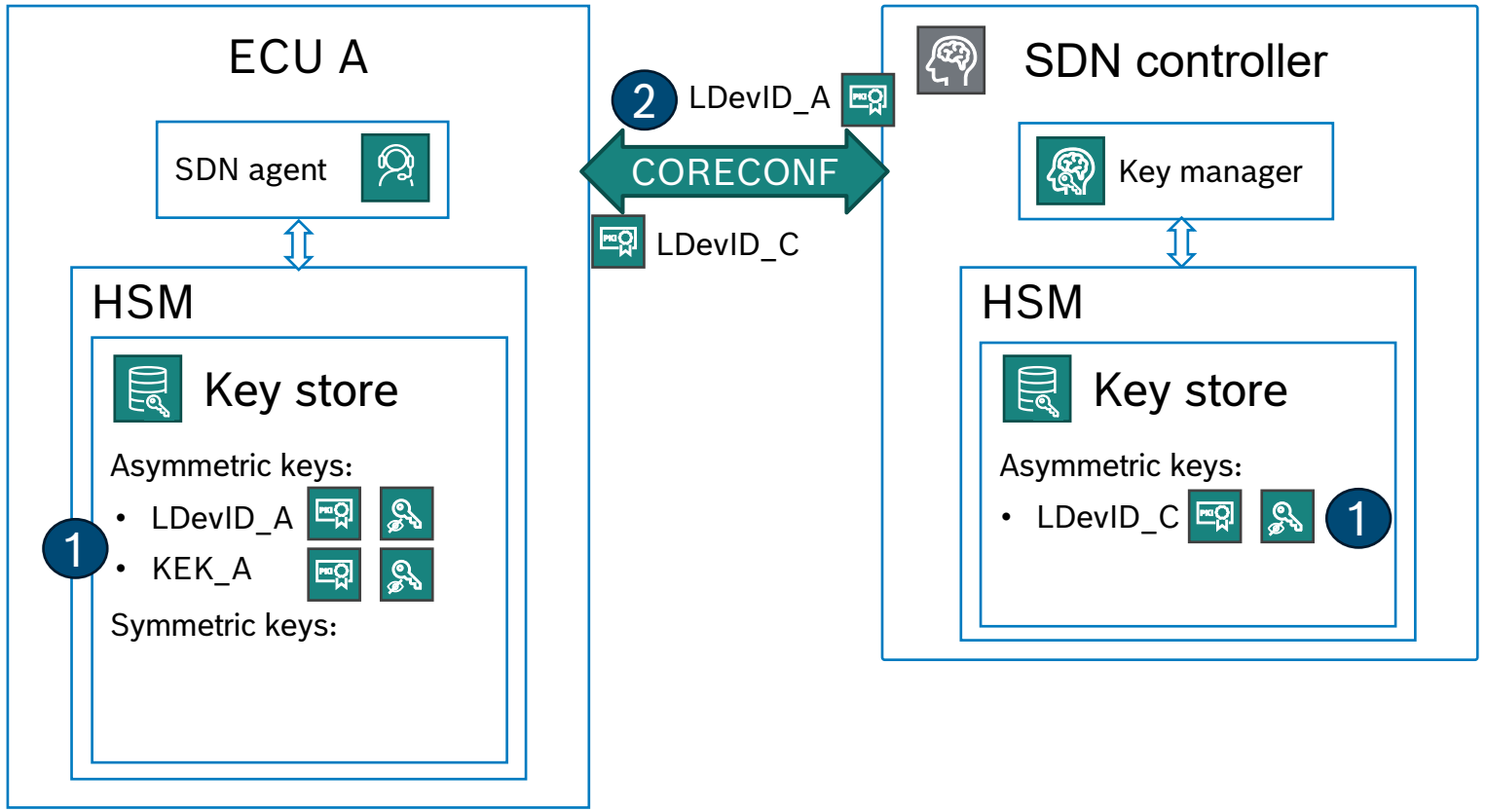
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module
DTLS: Datagram Transport Layer Security

YANG-based key management

Walkthrough: securely installing a CAK into an ECU



Key management steps

1. End-of-line key-injection
2. Authentication (DTLS)

Certificate

Hidden key

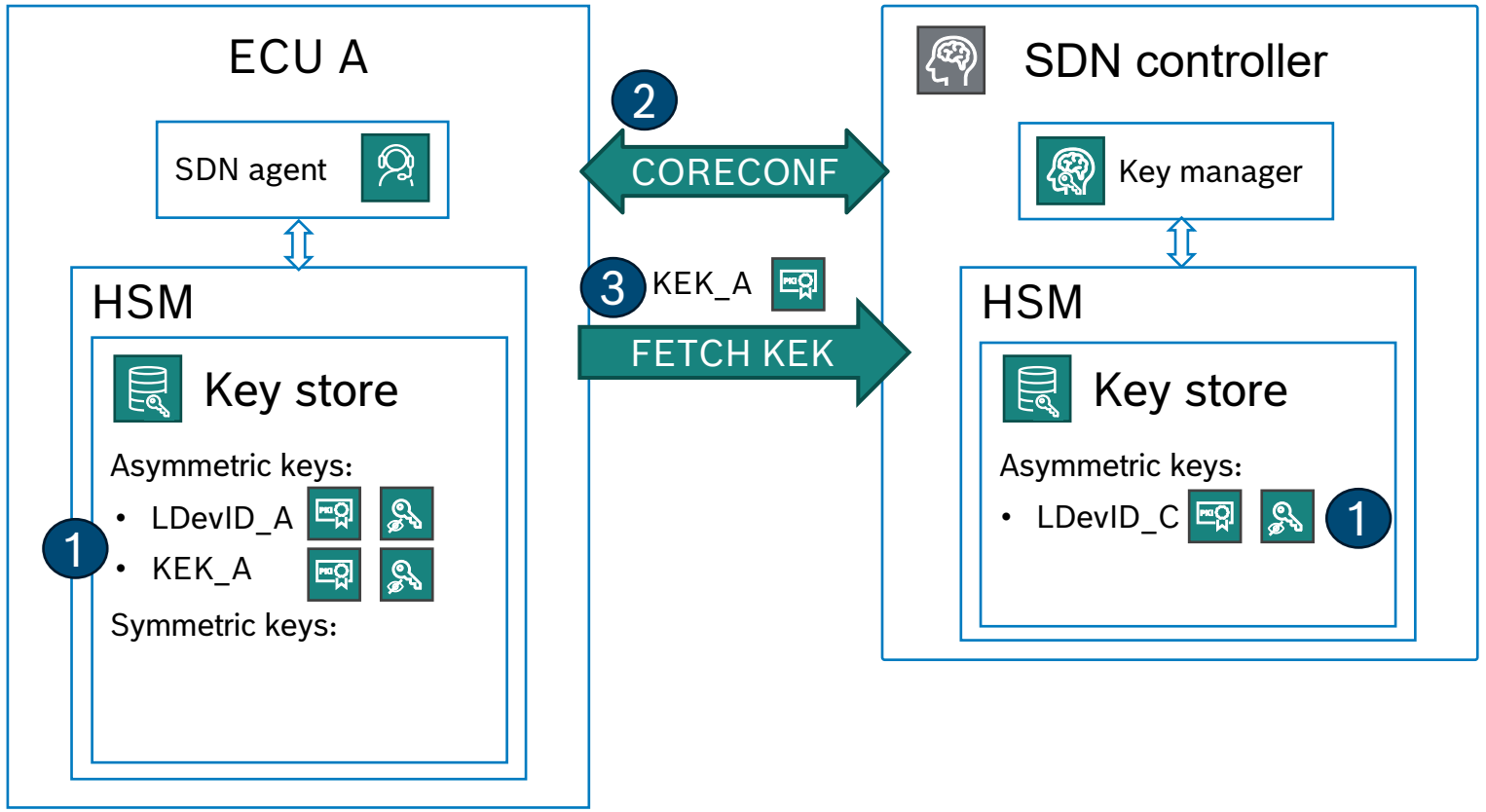
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module
DTLS: Datagram Transport Layer Security
KEK: Key-Encryption-Key

YANG-based key management

Walkthrough: securely installing a CAK into an ECU



Key Management Steps

1. End-of-line key-injection
2. Authentication (DTLS)
3. SDN controller fetches KEK certificate

Certificate

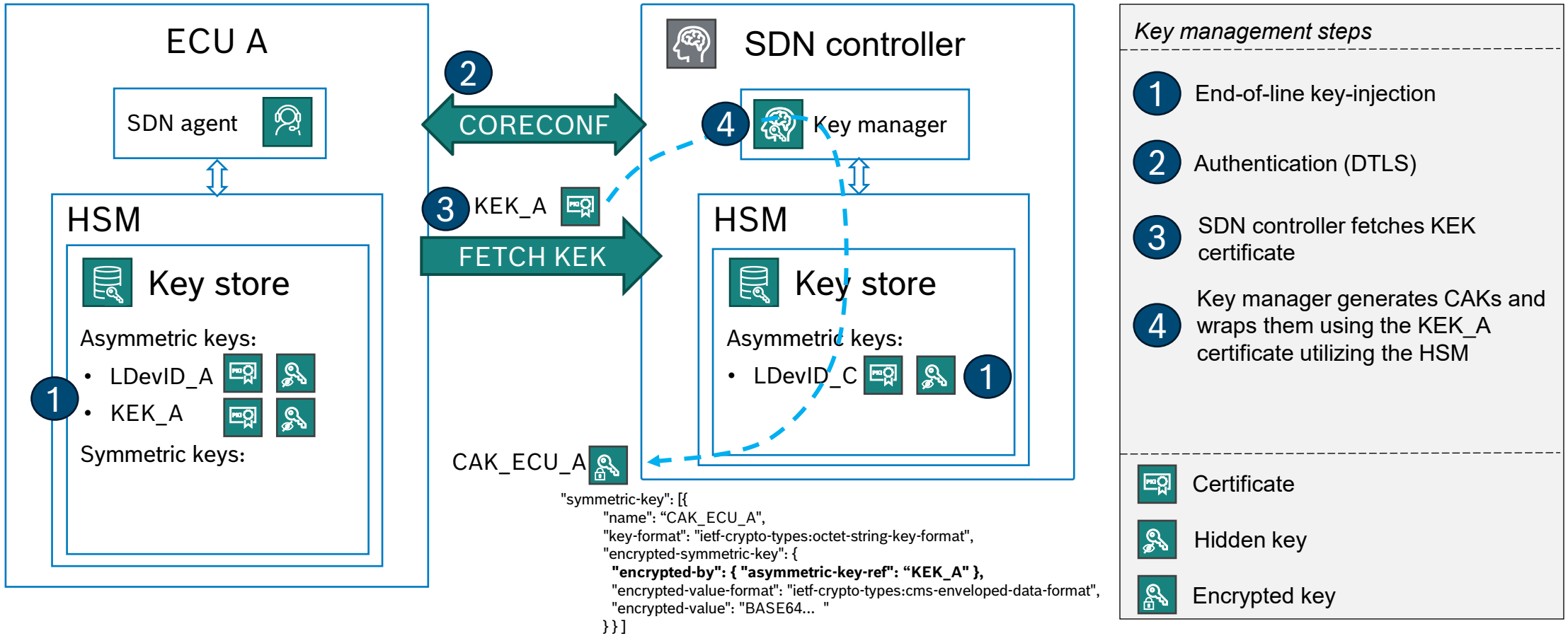
Hidden key

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module
DTLS: Datagram Transport Layer Security
KEK: Key-Encryption-Key
CAK: Connection Association Key

YANG-based key management
Walkthrough: securely installing a CAK into an ECU



Key management steps

1. End-of-line key-injection
2. Authentication (DTLS)
3. SDN controller fetches KEK certificate
4. Key manager generates CAKs and wraps them using the KEK_A certificate utilizing the HSM

Certificate
Hidden key
Encrypted key

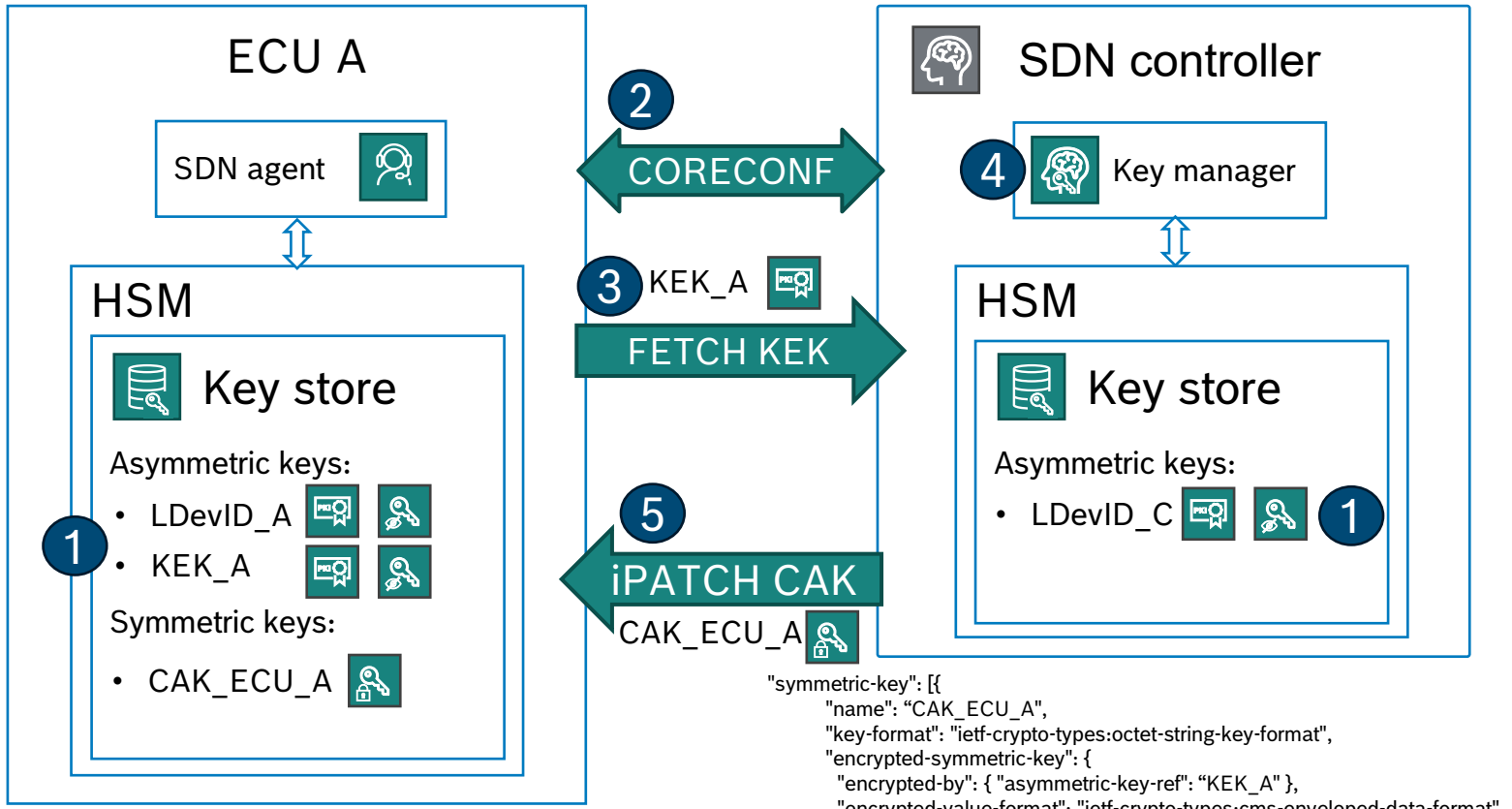
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

YANG-based key management

Walkthrough: securely installing a CAK into an ECU

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module
DTLS: Datagram Transport Layer Security
KEK: Key-Encryption-Key
CAK: Connection Association Key




```
"symmetric-key": [{
      "name": “CAK_ECU_A",
      "key-format": "ietf-crypto-types:octet-string-key-format",
      "encrypted-symmetric-key": {
        "encrypted-by": { "asymmetric-key-ref": “KEK_A" },
        "encrypted-value-format": "ietf-crypto-types:cms-enveloped-data-format",
        "encrypted-value": "BASE64...  "
      }}]
```

Key management steps

1. EOL key-injection
2. Authentication (DTLS)
3. SDN controller fetches KEK certificate
4. Key manager generates CAKs and wraps them using the KEK_A certificate utilizing the HSM
5. Key manager sends CAK as wrapped key to ECU A

Certificate
Hidden key
Encrypted key

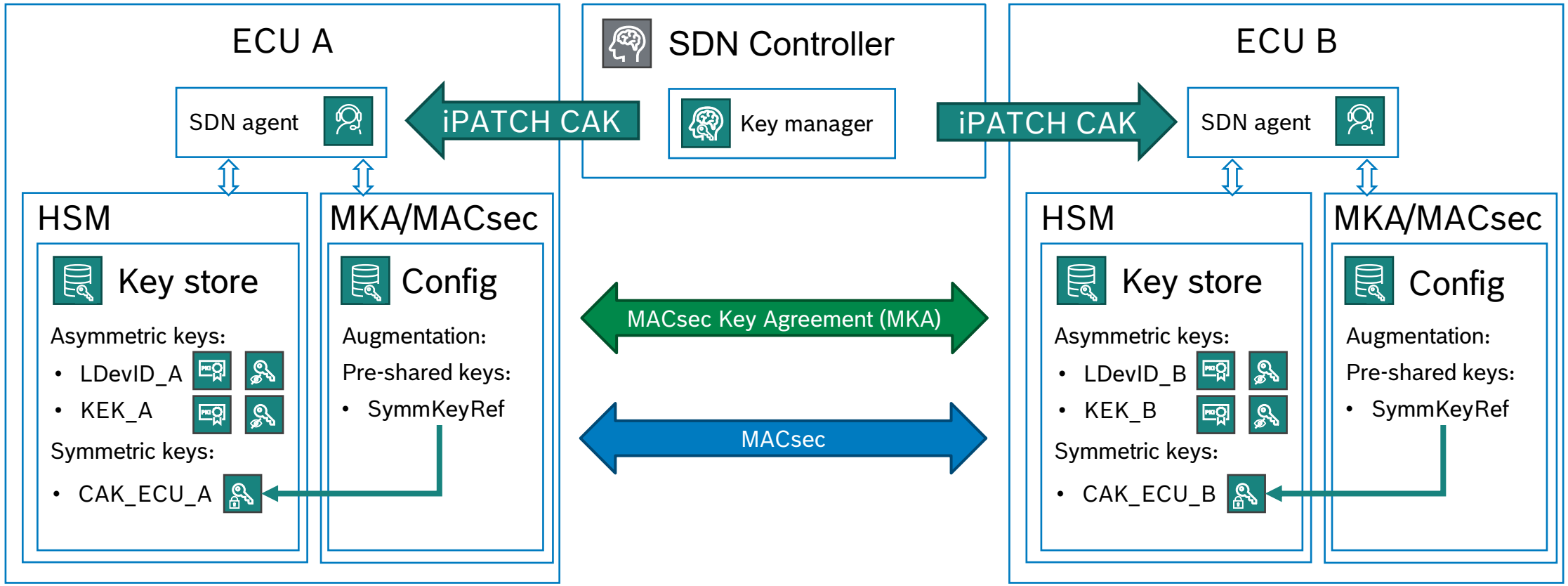
Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

SDN: Software-Defined Networking
ECU: Electronic Control Unit
HSM: Hardware Security Module
MKA: MACsec Key Agreement
KEK: Key-Encryption-Key
CAK: Connection Association Key

YANG-based key management

Suggestion: MKA config augmentation for PSKs



Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

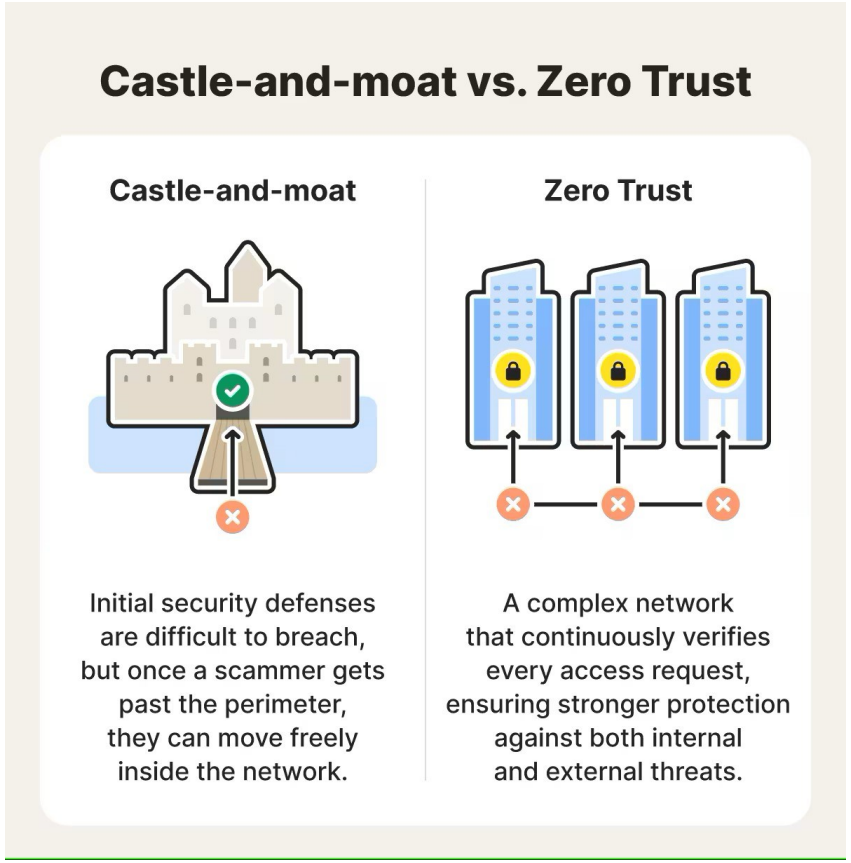
Advanced security features enabled by SDN

Public C-SC0

NIST: National Institute of Standards and Technology
NIST SP: NIST Special Publication
ECU: Electronic Control Unit
IVN: In-Vehicle Network

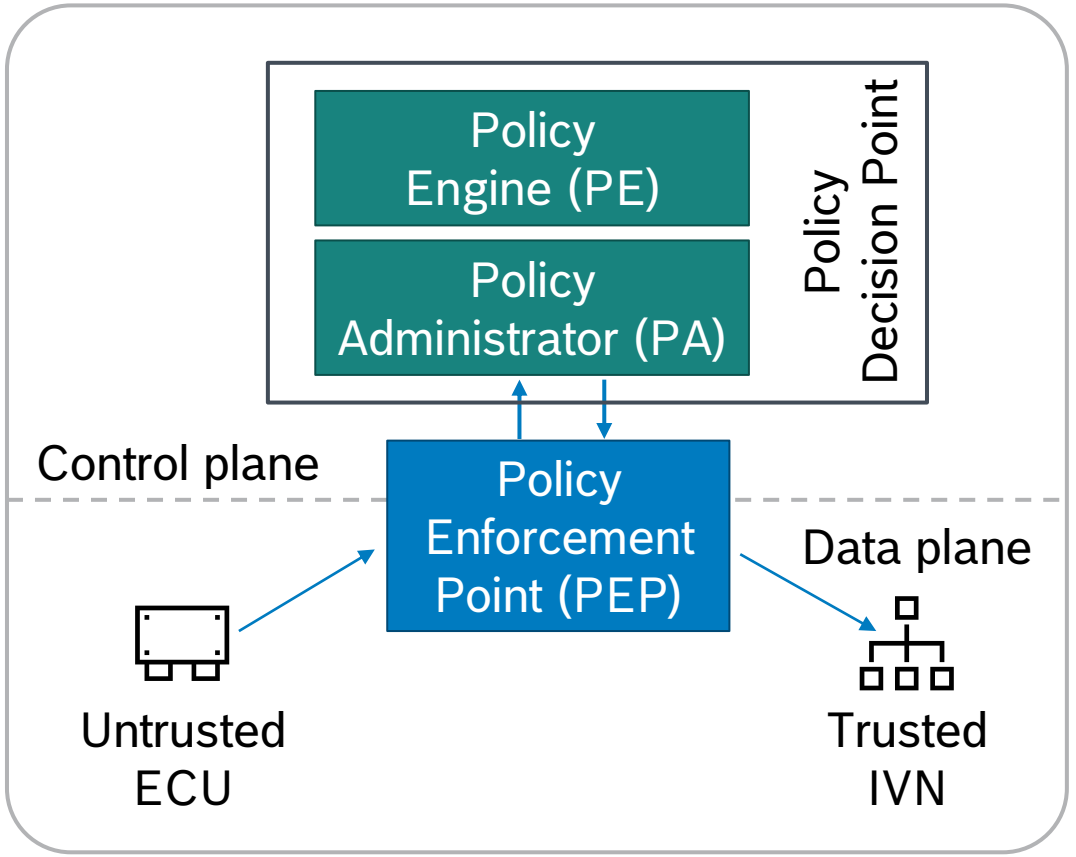
Advanced security features enabled by SDN

Zero trust architecture



https://us.norton.com/blog/security-tips/zero-trust

NIST SP 800-207 zero trust architecture



© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

SDN: Software-Defined Networking
CAK: Connection Association Key
ACL: Access Control List
DTLS: Datagram Transport Layer Security

SDN-based zero trust architecture

Recap: what we built so far

Layer	What we have	Source
Central orchestration point	SDN Controller on vehicle computer	Given by SDN architecture
Data plane protection	MACsec protects all traffic (line rate)	Layer 2 security protocol
Authenticated SDN mgmt.	CORECONF/DTLS	Given by SDN architecture
Centralized key distribution	YANG-based key provisioning (CAK)	**Integrate in SDN**
Network access control	Policy mgmt. / ACLs in SDN controller	**Integrate in SDN**

… and what we get with that

Verify explicitly

ECUs mutually authenticate with the SDN controller (DTLS); MACsec authenticates every frame

Least-privilege access

The controller distributes per-link CAKs and ACLs – each ECU gets only what it needs

Assume breach

In-vehicle traffic is always protected; a compromised ECU is isolated by SDN reconfiguration

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

SDN-based zero trust architecture
Summary

A YANG-based / CORECONF-managed SDN enables us to…

YANG-based key management

- Integrate key lifecycle into SDN config
- Reuse RFCs 9640, 9641, 9642 as standardized data model
- Replace proprietary per-OEM key management

Lightweight 802.1X NAC

- Reuse DTLS for mutual authentication
- Instead of an EAP-TLS/RADIUS stack: reuse what SDN management already provides

Lightweight zero trust

- SDN Controller takes over PE + PA role
- SDN Agents act as PEP
- Use YANG as policy modeling language
- Restrict blast radius by SDN reconfiguration

… at the cost of already “existing” infrastructure.

DTLS: Datagram Transport Layer Security
EAP: Extensible Authentication Protocol
NAC: Network Access Control

SDN: Software-Defined Networking
OEM: Original Equipment Manufacturer
RFC: Request For Comments
YANG: Data Modelling Language

PE: Policy Engine
PA: Policy Administrator
PEP: Policy Enforcement Point

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

A Collaboration of BOSCH | ETAS

Wrap up
Questions? Feedback?



“Secure, or not secure, that is the question”

—freely adapted from Hamlet

Public C-SC0 | Robert Bosch GmbH | ETAS GmbH | 2026-12-1
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.