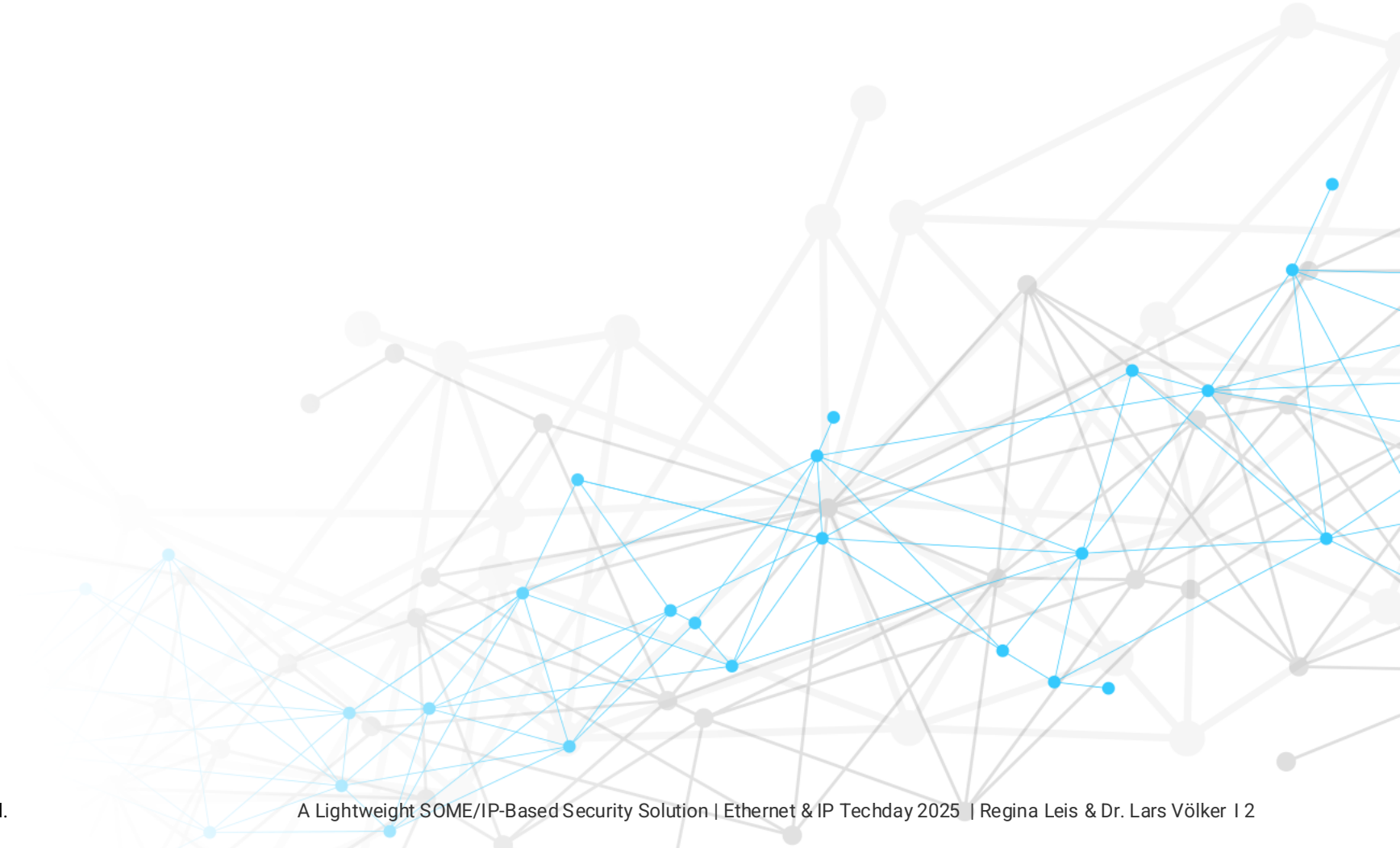
A LIGHTWEIGHT SOME/IP-BASED SECURITY SOLUTION

Technica Engineering

#OneStepAhead

A LIGHTWEIGHT SOME/IP-BASED SECURITY SOLUTION
TABLE OF CONTENT



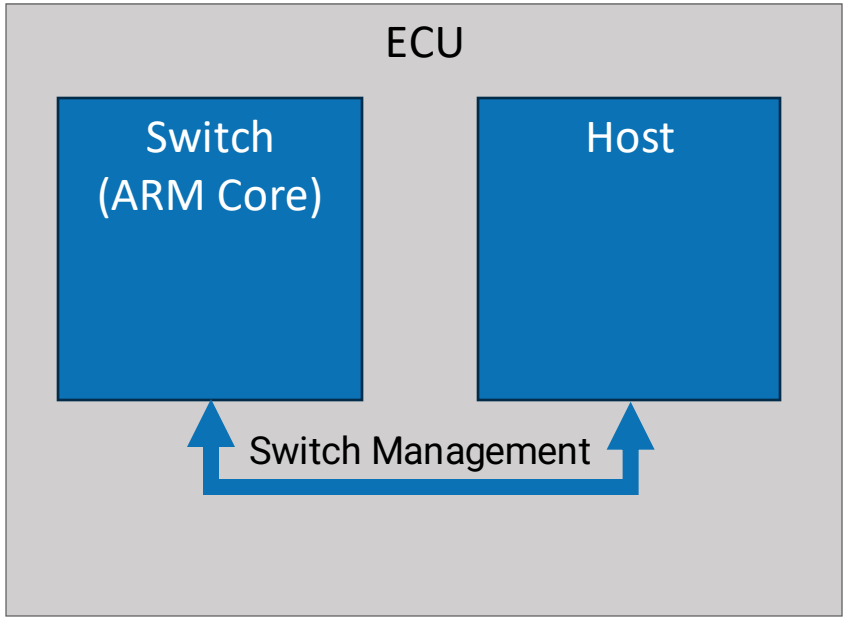
#1 SOME/IP-BASED SECURITY SOLUTION

MOTIVATION

MOTIVATION

GOAL: SWITCH MONITORING/MANAGEMENT

- Management Topics to be covered (examples):
  - Layer 1: PHYs, Cable Diagnostics, Link Up/Down
  - Layer 2: QoS, Switching, Address tables, VLANs
  - Security: MACsec
- Switch Management not standardized yet in Automotive.
  - OPEN TC19 wants to change this [1].
- Goal: Host translates standardized Interface to OEM-specific diagnostic jobs and DTCs.

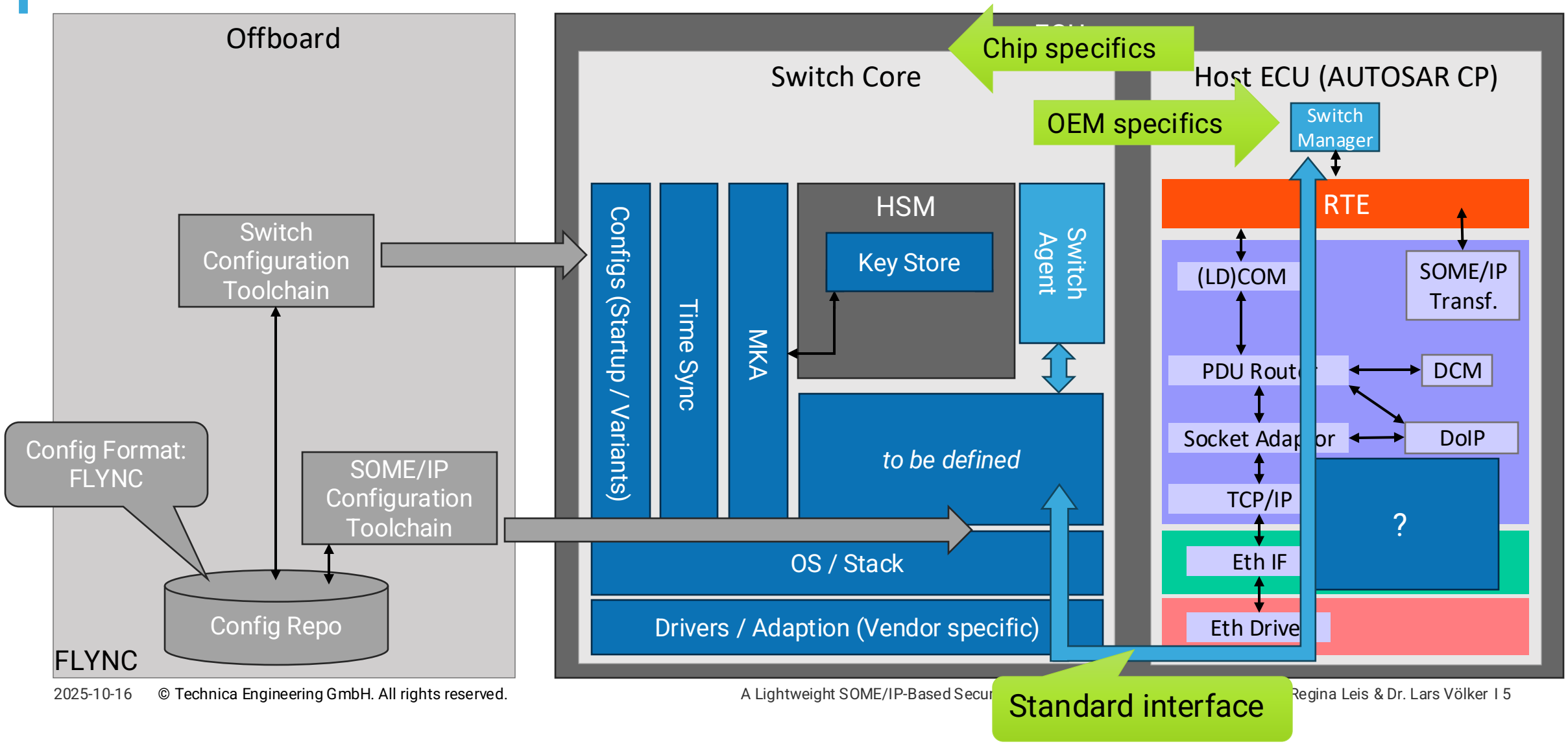


Can be the same or different ECUs

[1] Disclosure: Lars is the chair of OPEN TC19; however, he gives this presentation representing Technica and not OPEN TC19.

PROTECTING MANAGEMENT SERVICE

BIG PICTURE: SWITCH MONITORING AND MANAGEMENT



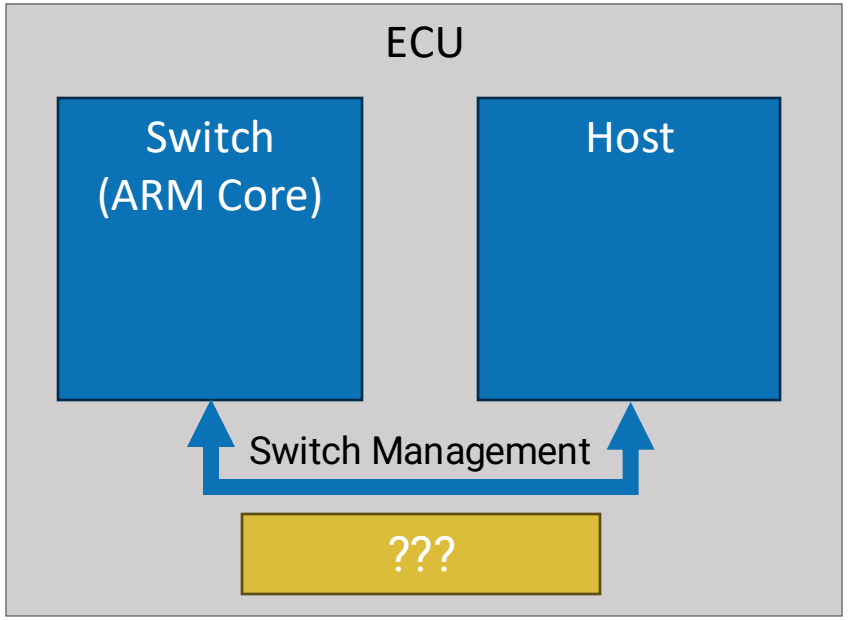
MOTIVATION

GOAL: SWITCH MONITORING/MANAGEMENT (2)

- Introducing a new protocol:
  - Requires new processes and tools (= $$$).
  - Requires know-how at OEM (= $$$).
  - Requires support in the Eco System (= $$$).

- Technica et. al. proposal [2]:
  - Transport this Management Interface via SOME/IP

- Is SOME/IP a better fit?



Can be the same or different ECUs

[2] This has also been proposed by other companies for very similar reasons.

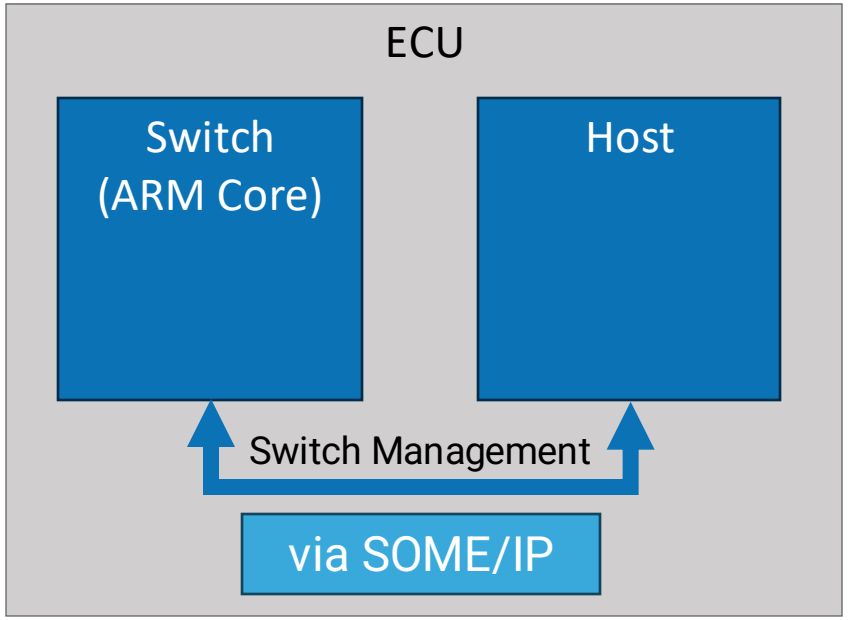
MOTIVATION

IS SOME/IP A GOOD FIT?

- SOME/IP is supported on all major ECU platforms.
- Deployed by most top OEMs worldwide.
- > 10 years in series production.
- Used by > 40 Mio vehicles today (*).

- Supports modern, service-oriented communication.
- Is cost-effective and rolled out today!

- Missing: How to install keys for MACsec/MKA into an ECU.
  - Most (if not all) proposals lack a secure installation of keys too.
  - How to protect the Switch Management communication?



Can be the same or different ECUs

(*) Conservative estimation based on publicly announced SOPs of a few OEMs using SOME/IP.

#2 SOME/IP-BASED SECURITY SOLUTION

DESIGN

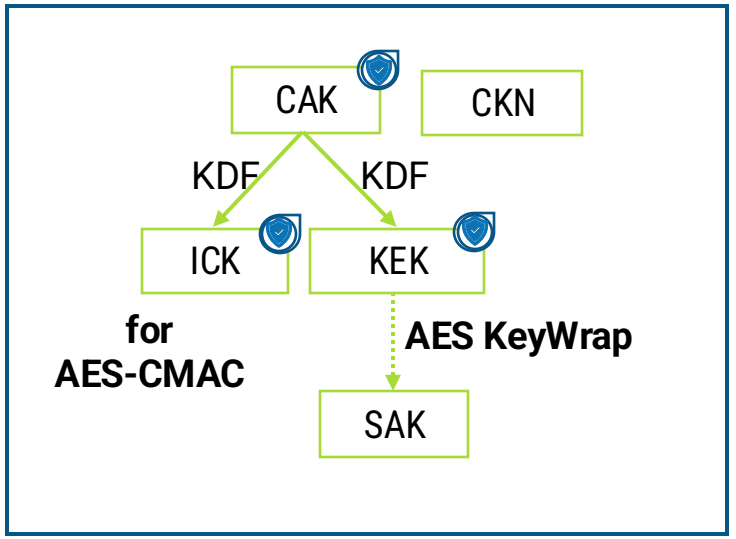
SECURITY SOLUTION DESIGN

HIGH LEVEL REQUIREMENTS

- Securely install CAKs (AES keys) into the Switch.
  - Limited trust in Host and Switch.
  - Should be able to run in HSMs.
  - Transport security (e.g., TLS or SSH) is not secure enough!

- Efficient and cost-effective solution.
  - Minimize the required crypto algorithms.
  - For MKA already crypto present:
    - AES-CMAC
    - AES KeyWrap
  - Try to reuse MKA crypto!

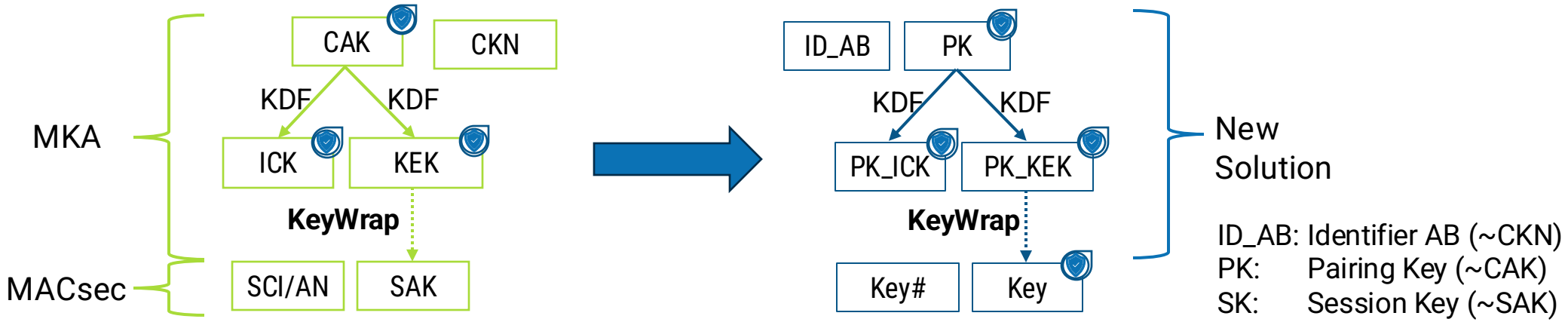
MKA (Pre-shared Key)



CAK: Connectivity Association Key
CKN: Connectivity Association Key Name
ICK: Integrity Check Key
KEK: Key Encryption Key
SAK: Secure Association Key
MKA: MACsec Key Agreement

SECURITY SOLUTION DESIGN

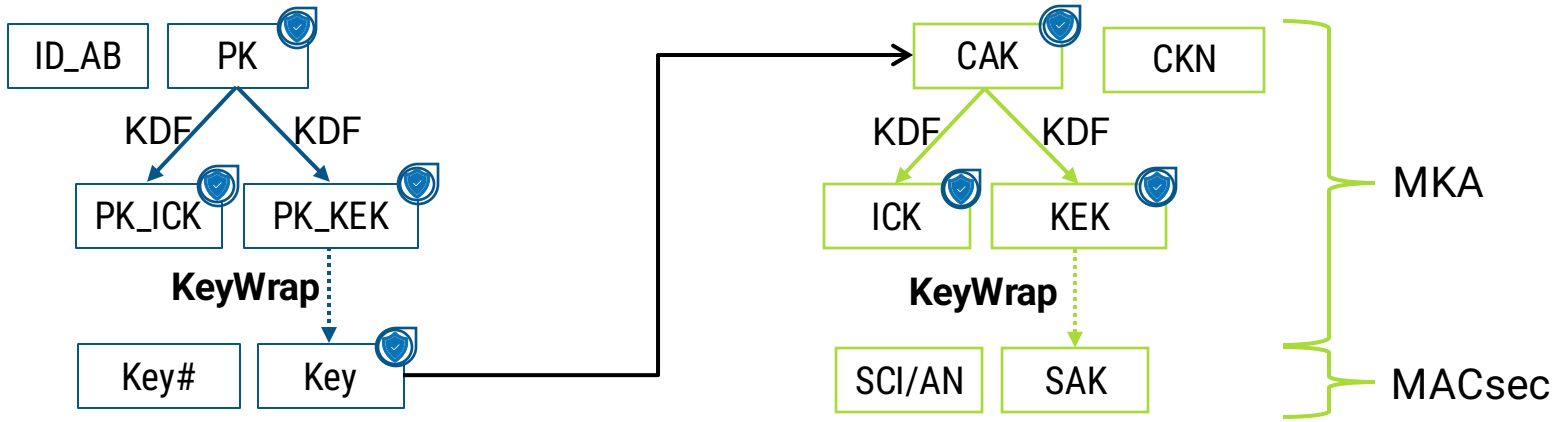
REUSING MKA KEY HIERARCHY PRINCIPLE



- Pairing Key (PK) and static identity of PK (ID_AB) are permanent.
  - PK could be installed/generated during ECU production into/in Switch and Host.
  - ID_AB is compiled into software.
- Key Hierarchy and usage is basically like MKA.
- But what can we do with the “Key” now?

SECURITY SOLUTION DESIGN

SECURE CAK INSTALLATION



- This allows installation of CAKs.
  - Typically, 1 CAK per Switch with MACsec required.
  - CAKs need unique Key#.

- Host pushes the keys into the Switch (details later).

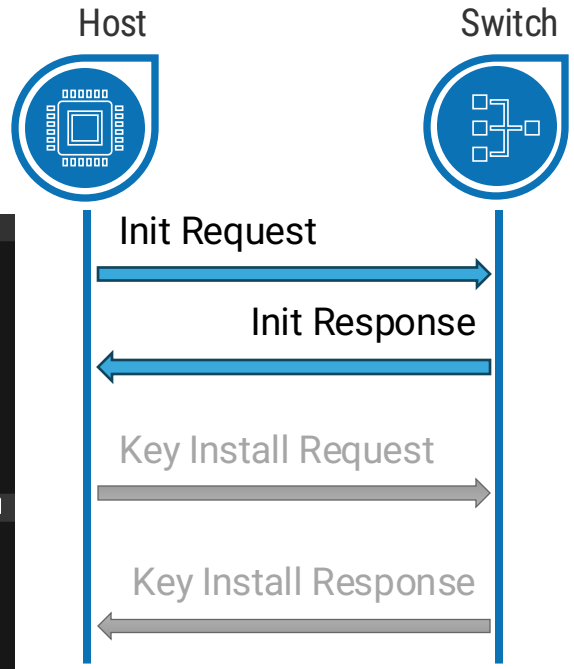
SECURITY SOLUTION DESIGN

SOME/IP-KEYEX: MESSAGE FLOW AND FORMAT (1)

Init Request

```
SOME/IP Protocol (Service ID: 0xff00, Method ID: 0x0001, Length: 38)
   Service ID: 0xff00 (SwitchManagement_KeyEx)
   Method ID: 0x0001 (Init)
   Length: 38
   Client ID: 0x0000
   Session ID: 0x0000
   SOME/IP Version: 0x01
   Interface Version: 0x01
 > Message Type: 0x00 (Request)
   Return Code: 0x00 (Ok)
 v Payload: 1337133707d49e940000000100007c481a59d4c86c60abee0427ad38d6ad
      ID [uint32]: 322376503
      Nonce_i [uint32]: 131374740
      Sequence_Number_i [uint32]: 1
      Status [uint8]: 0 (OK)
      Reserved [uint8]: 0
    > array ICV (elements limit: 16)
```

My Nonce, my Seq#!



Init Response

```
SOME/IP Protocol (Service ID: 0xff00, Method ID: 0x0001, Length: 46)
   Service ID: 0xff00 (SwitchManagement_KeyEx)
   Method ID: 0x0001 (Init)
   Length: 46
   Client ID: 0x0000
   Session ID: 0x0000
   SOME/IP Version: 0x01
   Interface Version: 0x01
 > Message Type: 0x80 (Response)
   Return Code: 0x00 (Ok)
 v Payload: 1337133707d49e9472e3d3bd0000000100000001000000010000b8ad86ad1e6ca66
      ID [uint32]: 322376503
      Nonce_i [uint32]: 131374740
      Nonce_r [uint32]: 1927533501
      Sequence_Number_i [uint32]: 1
      Sequence_Number_r [uint32]: 1
      Status [uint8]: 0 (OK)
      Reserved [uint8]: 0
    > array ICV (elements limit: 16)
```

Your Nonce, your Seq#, and mine too!

- Synchronizing Nonces and Sequence Numbers.
- Alive Check.

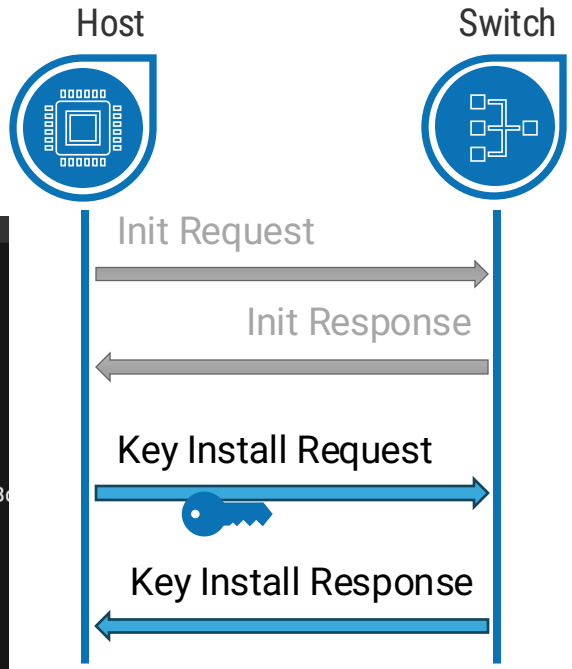
SECURITY SOLUTION DESIGN

SOME/IP-KEYEX: MESSAGE FLOW AND FORMAT (2)

technica engineering
Member of KPIT Group

Key Install Request

```
SOME/IP Protocol (Service ID: 0xff00, Method ID: 0x0002, Length: 92)
   Service ID: 0xff00 (SwitchManagement_KeyEx)
   Method ID: 0x0002 (InstallKey)
   Length: 92
   Client ID: 0x0000
   Session ID: 0x0000
   SOME/IP Version: 0x01
   Interface Version: 0x01
 > Message Type: 0x00 (Request)
   Return Code: 0x00 (Ok)
 v Payload: 1337133707d49e9472e3d3bd0000000200000001000000 2c00010128278
     ID [uint32]: 322376503
     Nonce_i [uint32]: 131374740
     Nonce_r [uint32]: 1927533501
     Sequence_Number_i [uint32]: 2
     Sequence_Number_r [uint32]: 1
     Status [uint8]: 0 (OK)
     Reserved [uint8]: 0
   v array Key_Array (elements limit: 0-0)
     v struct Payload [Key_Struct]
         Key_Number [uint16]: 1
         Keywrap_Type [uint8]: 1 (RFC3394-256-256)
       > array Key_Wrap (elements limit: 0-0)
   > array ICV (elements limit: 16)
```

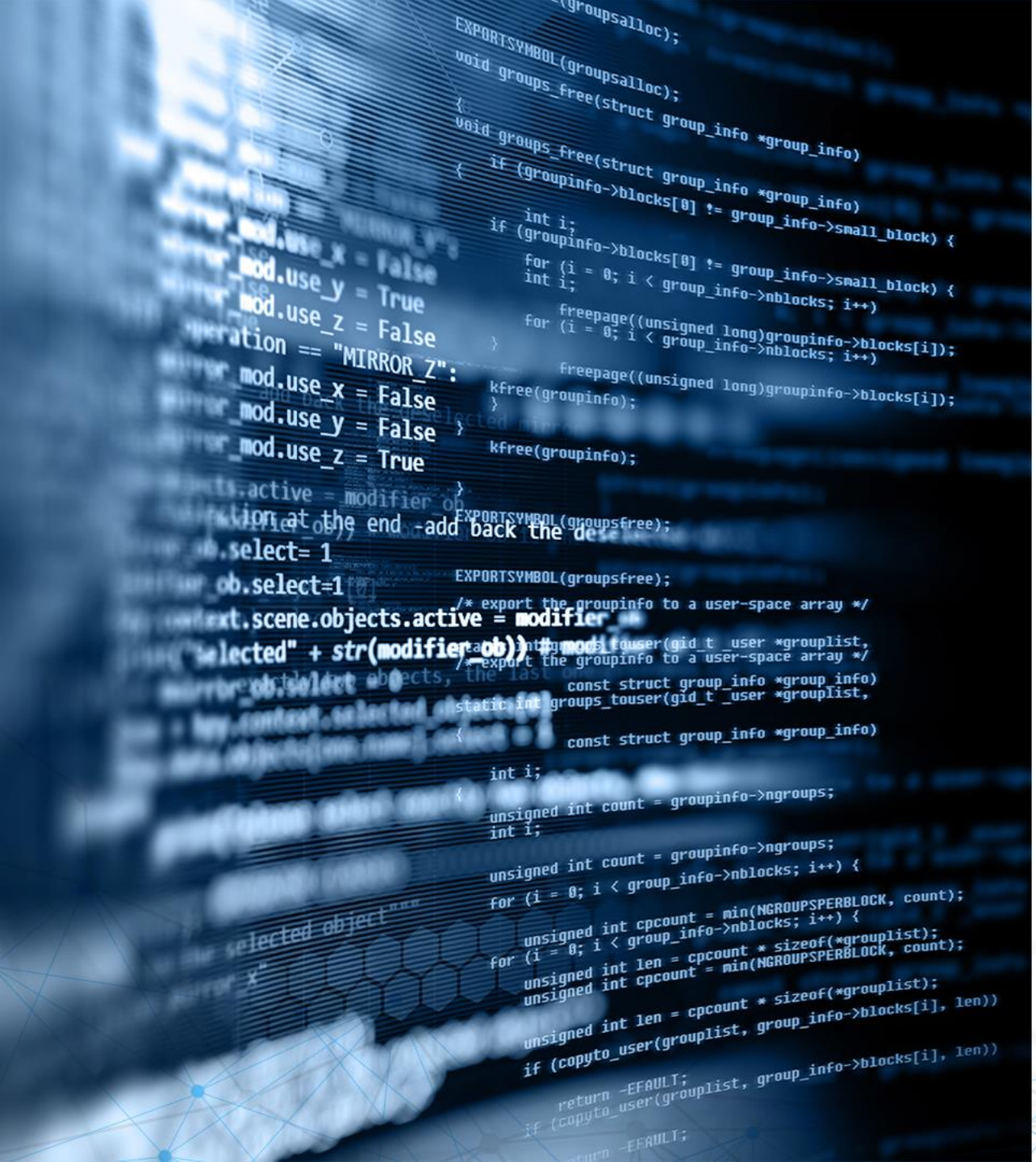


Key Install Response

```
SOME/IP Protocol (Service ID: 0xff00, Method ID: 0x0002, Length: 52)
   Service ID: 0xff00 (SwitchManagement_KeyEx)
   Method ID: 0x0002 (InstallKey)
   Length: 52
   Client ID: 0x0000
   Session ID: 0x0000
   SOME/IP Version: 0x01
   Interface Version: 0x01
 > Message Type: 0x80 (Response)
   Return Code: 0x00 (Ok)
 v Payload: 1337133707d49e9472e3d3bd0000000200000002000000040001000025c5
     ID [uint32]: 322376503
     Nonce_i [uint32]: 131374740
     Nonce_r [uint32]: 1927533501
     Sequence_Number_i [uint32]: 2
     Sequence_Number_r [uint32]: 2
     Status [uint8]: 0 (OK)
     Reserved [uint8]: 0
   v array Key_Status_Array (elements limit: 0-0)
     v struct KeyStatusArray [Key_Status]
         Key_Number [uint16]: 1
         Reserved [uint8]: 0
         Status [uint8]: 0
   > array ICV (elements limit: 16)
```

OK!

- Installation one or multiple keys.

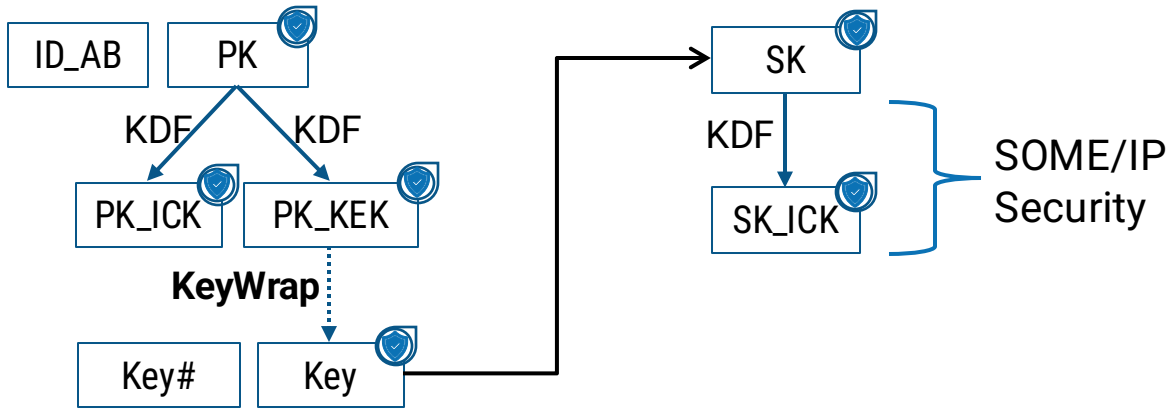


#3 SOME/IP-BASED SECURITY SOLUTION

PROTECTION

PROTECTING MANAGEMENT SERVICE

SOME/IP-SEC



- We protect SOME/IP communication too.
- Think “SecOC” for SOME/IP.

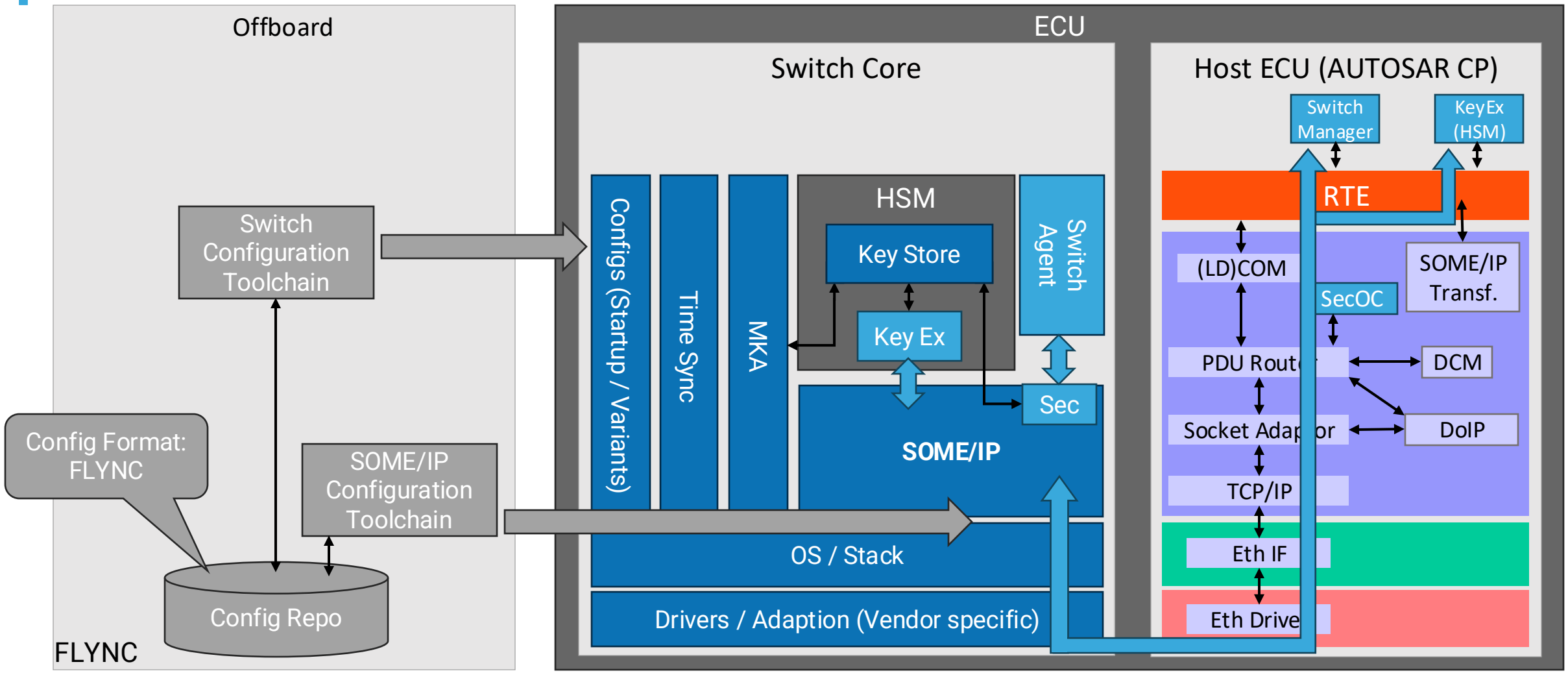
- Integration into AUTOSAR CP et. al. straight-forward.

Service ID 16 bit		Method ID 16 bit	
Length 32 bit			
Client ID 16 bit		Session ID 16 bit	
Protocol Version 8 bit	Interface Version 8 bit	Message Type 8 bit	Return Code 8 bit
Payload 0 bytes or more			
ID 16 bit		KeyNumber 8 bit	Dir / Res. 1 + 7 bit
Sequence Number 32bit			
ICV 128bit			

Layout of SOME/IP-SEC protection.

PROTECTING MANAGEMENT SERVICE

BIG PICTURE: SWITCH MONITORING AND MANAGEMENT

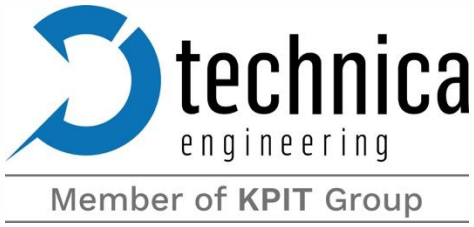


#4 SOME/IP-BASED SECURITY SOLUTION

SUMMARY

A LIGHTWEIGHT SOME/IP-BASED SECURITY SOLUTION
SUMMARY

- Motivation: “Manage Switch via SOME/IP”
  - Most efficient and cost-effective solution identified.
- Add Security to SOME/IP:
  - SOME/IP-KeyEx as lightweight Key Management solution.
  - SOME/IP-Sec as ”SecOC”-like protection of SOME/IP messages.
- Key advantages:
  - Crypto of MKA already present and being reused.
  - Keys can be securely deployed into HSMs!
- One more thing



Technica Engineering GmbH

Leopoldstraße 236
80807 Munich
Germany

REGINA LEIS
System Engineer
regina.leis@technica-engineering.de

DR. LARS VÖLKER
Technical Fellow
lars.voelker@technica-engineering.de

