



WHY DO FUTURE E/E ARCHITECTURES REQUIRE MACSEC?

Dr. Lars Völker, Technical Fellow

4th Automotive E/E Architecture Technology Innovation Conference



Chapter 01. Motivation.

E/E Architecture Trends.
Technology.



E/E ARCHITECTURE TRENDS...

Trend 1: "Expecting always fresh":

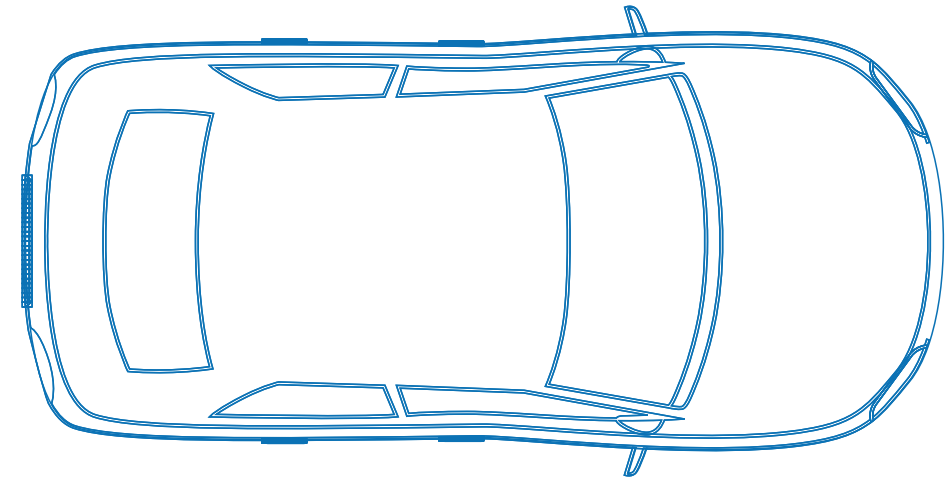
Software updates expected, like on smartphones.
Faster time to market required to stay competitive.

Trend 2: "More in-vehicle communication":

In-vehicle data volume increases.
Multi-gigabit is the next backbone.

Trend 3: "Security is required":

Attackers are more focused on vehicles.
Regulation and type approval are getting serious.



... REQUIRE STRATEGIC THINKING!

Solution: A secure, scalable high-performance communication platform:

Create a scalable, secure platform to deploy features faster.

Convergence and standards give you freedom to deploy more innovations.

Solid standard technology improves time to market and quality.

Scalable technology means future-proof.

Best in class technology: Ethernet and MACsec.



WHY AUTOMOTIVE ETHERNET?

Ethernet is a strong technology base:

Ethernet delivers for 40+ years increasing speeds and innovations.

Ethernet dominates most markets for good reasons.

Automotive Ethernet is the in-vehicle communication platform:

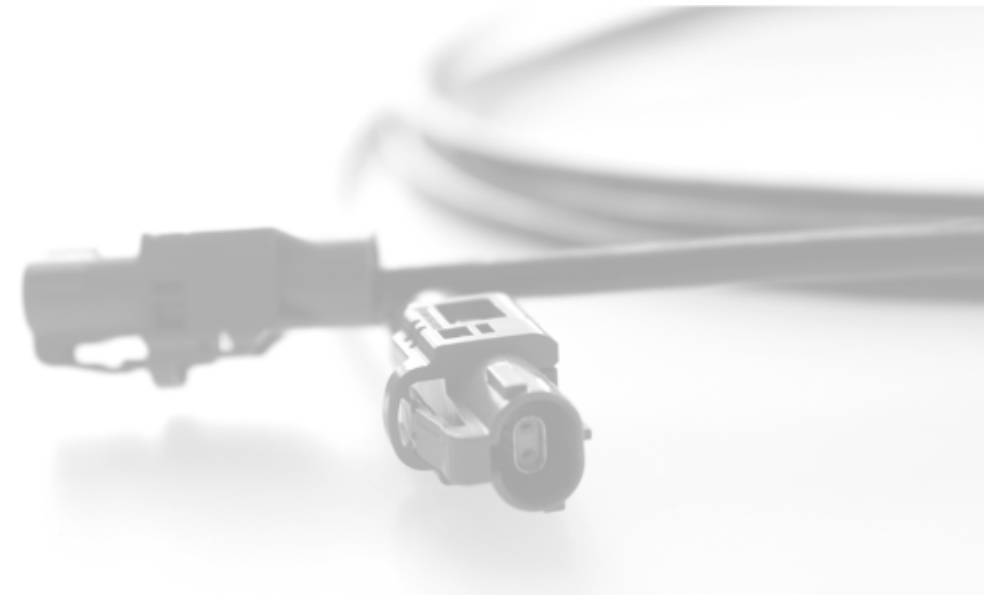
Automotive Ethernet is the only technology with forward compatibility.

Automotive Ethernet allows convergence like no other technology.

Automotive Ethernet has a solid, competitive multi-vendor market.

Automotive Ethernet delivers the best-in-class feature portfolio.

Automotive Ethernet is adopted by most OEMs already.



WHY MACSEC?

Coverage, Coverage, Coverage:

MACsec can secure unicast, multicast, and broadcast communication.

MACsec can protect almost all packets transported (layer 2 and up).

MACsec secures the communication of upcoming features today.

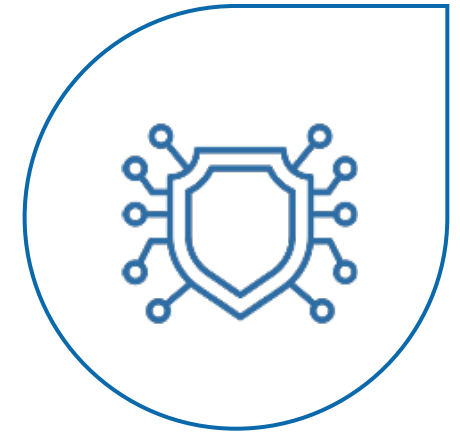
Fast and easy to use:

MACsec is currently the only available security solution for high-speed.

MACsec scales with high speed and increasing number of Ethernet nodes.

MACsec is based on the Ethernet interface – a perfect abstraction for ECUs.

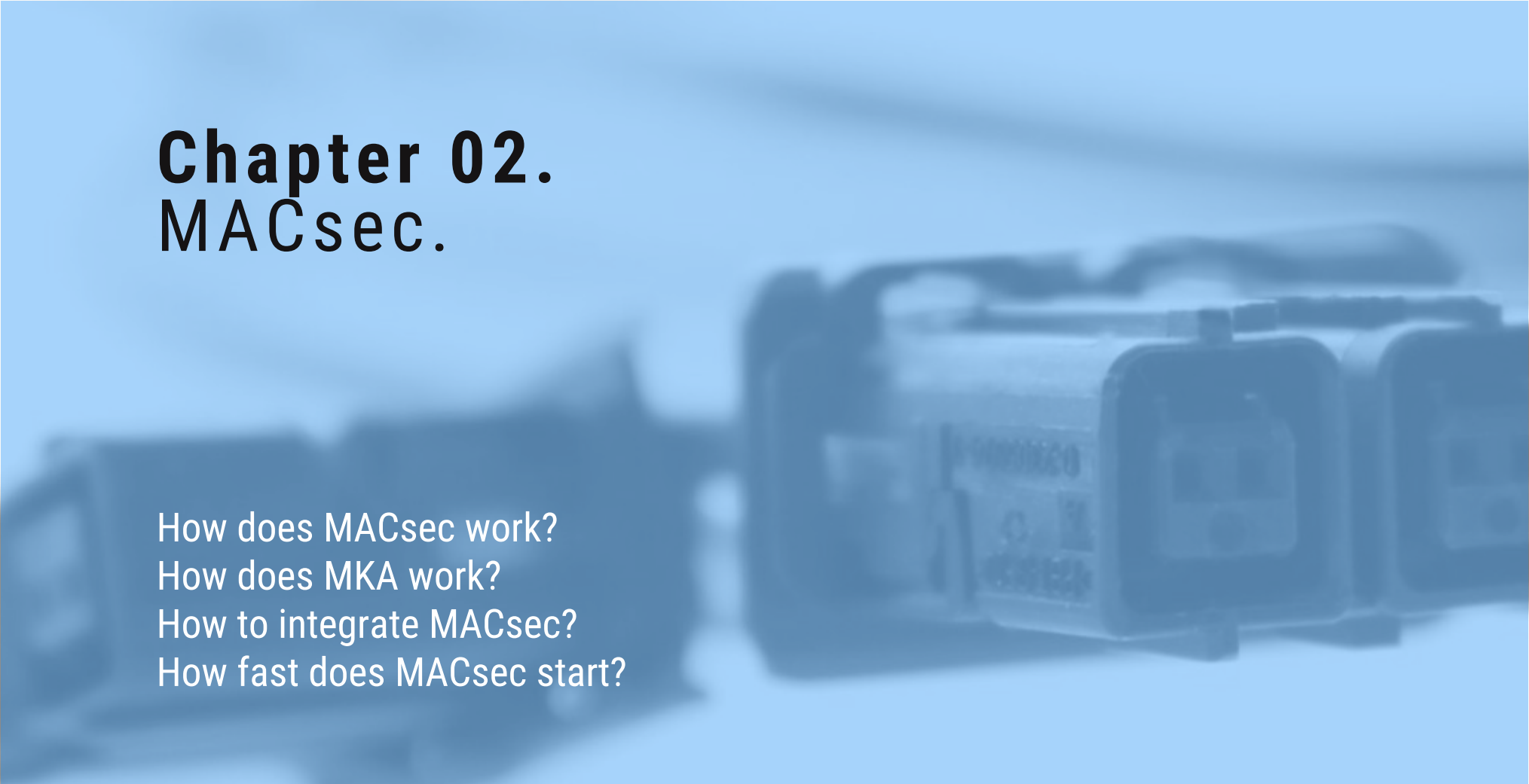
Leading premium OEMs are already working on MACsec for their next architecture.





Chapter 02. **MACsec.**

How does MACsec work?
How does MKA work?
How to integrate MACsec?
How fast does MACsec start?



HOW DOES MACSEC WORK?

MACsec:

“Authentication only” or “Encryption + Authentication”.

Hop-by-hop mode supported for link-based protection.

Security Tag including Integrity Check Value (ICV).

Based on Secure Association Key (SAK).

Typically: GCM-AES-128 or GCM-AES-256.

Optional: Extended Packet Number (XPN).

But where to get the SAK from?

```

No. | Time      | Source           | Destination           | Protocol | Length | Info
---|---|---|---|---|---|---
1  | 0.000000 | dc:a6:32:00:00:01 | ff:ff:ff:ff:ff:ff | ARP      | 76     | Who has 169.254.95.161? (ARP Probe)

> Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: dc:a6:32:00:00:01, Dst: ff:ff:ff:ff:ff:ff
< 802.1AE Security tag
  > 0010 00.. = TCI: 0x08, VER: 0x0, SC
    .... ..00 = AN: 0x0
    Short length: 33
    Packet number: 119
    System Identifier: dc:a6:32:00:00:01
    Port Identifier: 1
    Ethertype: 0x0806
    Padding: 0000
    ICV: e4cfd6cbd028374e1594b390a64b8db7
> Address Resolution Protocol (ARP Probe)

0000  ff ff ff ff ff ff dc a6 32 00 00 01 88 e5 20 21  ..... 2..... !
0010  00 00 00 77 dc a6 32 00 00 01 00 01 08 06 00 01  ..w..2. .... ..
0020  08 00 06 04 00 01 dc a6 32 00 00 01 00 00 00 00  ..... 2.....
0030  00 00 00 00 00 00 a9 fe 5f a1 00 00 e4 cf d6 cb  ..... -.....
0040  d0 28 37 4e 15 94 b3 90 a6 4b 8d b7  ..... (7N... ·K..
  
```


HOW DOES MKA WORK?

MACsec Key Agreement (MKA):

MKA allows to generate fresh SAKs for MACsec.

- a) based on pre-shared Connectivity Association Key (CAK).
- b) based on EAP generated CAK (e.g., based on EAP-TLS).

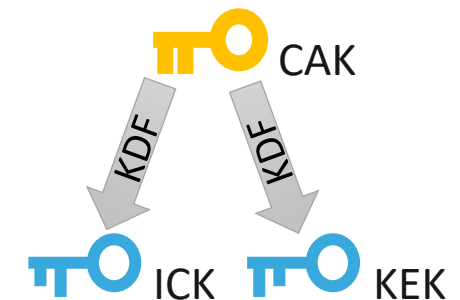
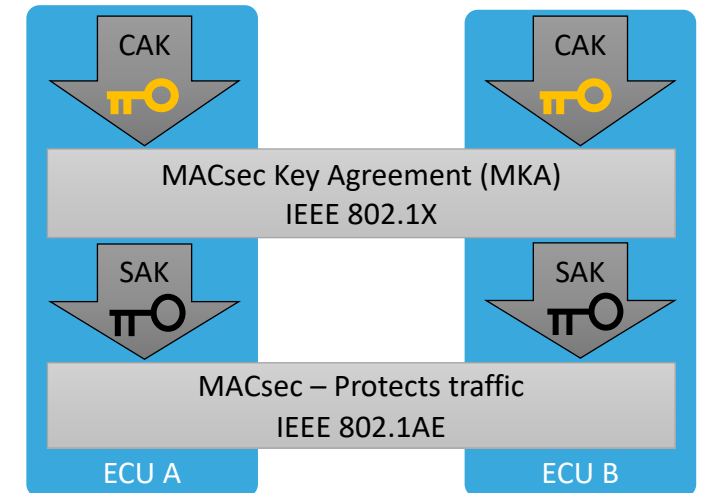
Key Server is elected, and Key Server distributes encrypted SAK.

MKA generates additional keys out of CAK:

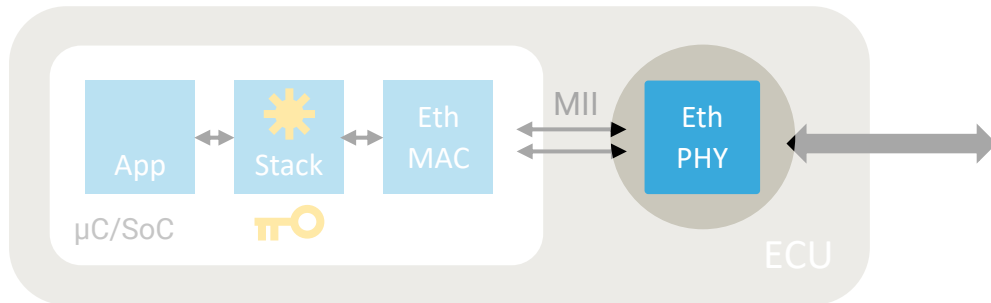
ICV Key (ICK): MKA message integrity protection.

Key Encryption Key (KEK): encryption of keys in MKA messages.

Recommendation: Use pre-shared CAKs for fastest startup.



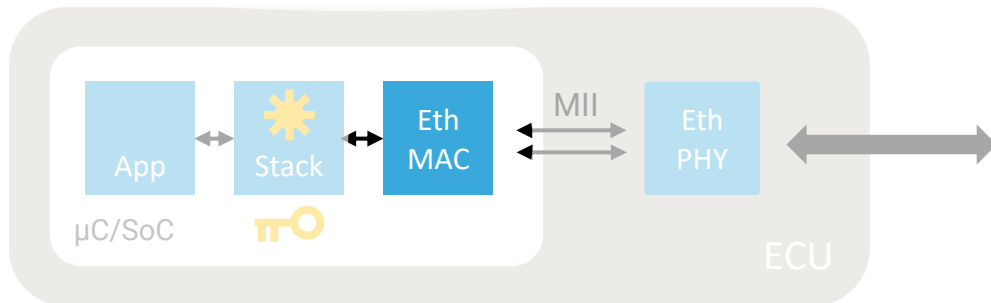
HOW TO INTEGRATE MACSEC?



Option “MACsec in the Ethernet PHY”:

Available now.

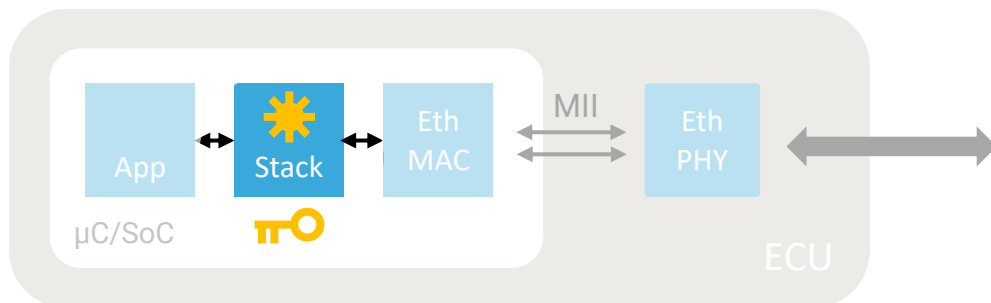
Access to MII traces may be critical for high security use cases.



Option “MACsec in the Ethernet MAC”:

Best solution for ease and security.

Long adoption time for all μC/SoCs.



Option “MACsec in Software”:

Cost effective solution with hardware crypto.

Performance of hardware crypto very critical.

Lower speed grades only.

HOW FAST DOES MACSEC START?

Raspberry Pi: Regular MACsec Key Agreement (MKA) up to 8s (here 3s):


No.	Time	Time Delta	Source	Destination	Protocol	Length	Info
1	0.000000000	0.000000000	aa:ea:c4:e5:42:cc	01:80:c2:00:00:03	EAPOL-MKA	98	Key Server
2	0.986986779	0.986986779	ce:e9:55:df:c2:5e	01:80:c2:00:00:03	EAPOL-MKA	98	Key Server
3	2.001422945	1.014436166	aa:ea:c4:e5:42:cc	01:80:c2:00:00:03	EAPOL-MKA	118	Key Server, Potential Peer List
4	2.988365546	0.986942601	ce:e9:55:df:c2:5e	01:80:c2:00:00:03	EAPOL-MKA	150	Key Server, Live Peer List, Distributed SAK
5	2.995237588	0.006872042	ce:e9:55:df:c2:5e	01:80:c2:00:00:03	EAPOL-MKA	194	Key Server, Live Peer List, MACsec SAK Use, Distributed SAK
6	2.995736763	0.000499175	aa:ea:c4:e5:42:cc	01:80:c2:00:00:03	EAPOL-MKA	162	Live Peer List, MACsec SAK Use
7	2.996580117	0.000843354	aa:ea:c4:e5:42:cc	01:80:c2:00:00:03	EAPOL-MKA	162	Live Peer List, MACsec SAK Use

Raspberry Pi: Extensive tuning work <30ms but sometimes much longer:

No.	Time	Time Delta	Source	Destination	Protocol	Length	Info
1	0.000000000	0.000000000	52:54:00:5c:f9:b1	01:80:c2:00:00:03	EAPOL-MKA	82	Key Server
2	0.006542060	0.006542060	52:54:00:aa:62:b6	01:80:c2:00:00:03	EAPOL-MKA	82	
3	0.006907319	0.000365259	52:54:00:5c:f9:b1	01:80:c2:00:00:03	EAPOL-MKA	102	Key Server, Potential Peer List
4	0.009524439	0.002617120	52:54:00:aa:62:b6	01:80:c2:00:00:03	EAPOL-MKA	102	Potential Peer List
5	0.010436494	0.000912055	52:54:00:5c:f9:b1	01:80:c2:00:00:03	EAPOL-MKA	134	Key Server, Live Peer List, Distributed SAK
6	0.011732499	0.001296005	52:54:00:5c:f9:b1	01:80:c2:00:00:03	EAPOL-MKA	178	Key Server, Live Peer List, MACsec SAK Use, Distributed SAK
7	0.017284492	0.005551993	52:54:00:aa:62:b6	01:80:c2:00:00:03	EAPOL-MKA	146	Live Peer List, MACsec SAK Use
8	0.023570478	0.006285986	52:54:00:aa:62:b6	01:80:c2:00:00:03	EAPOL-MKA	146	Live Peer List, MACsec SAK Use
9	0.025617745	0.002047267	52:54:00:aa:62:b6	01:80:c2:00:00:03	EAPOL-MKA	146	Live Peer List, MACsec SAK Use

Automotive Hardware: Technica Automotive MKA implementation:

* demo time *



Chapter 03. Additional Aspects.

Complementary Solutions
Testing and Integration



ADDITIONS.

Important complementary solutions

! Address Filtering on Switches

Since switch ports are authenticated, strong address and VLAN filtering (layer 2 and 3) is possible and highly recommended. This stops address spoofing and unauthorized VLAN access.

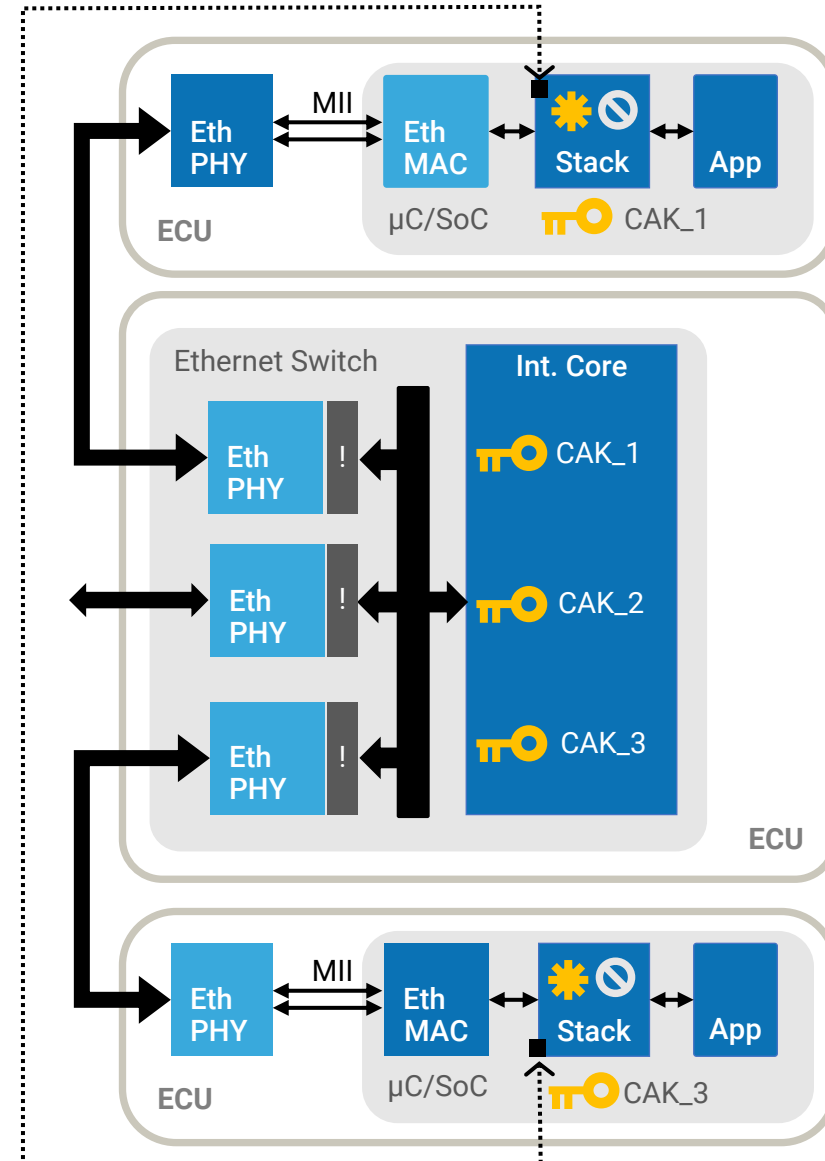
⊘ Access Control Lists (ACLs) on ECUs

Without address spoofing, access control can be based on addresses.

For example, SOME/IP ACLs or regular packet filters in ECUs.

→ SecOC or similar for selected communication

Legacy to Ethernet, Secure Element to Application, etc.
Highly critical use cases (e.g., vehicle immobilizer).



TESTING AND INTEGRATION.

Aspect 1: “Prototypes / A-samples”:

Proof that MACsec fits your requirements!

Aspect 2: “Testing MACsec”:

Test cases and test suites for MKA.

Test cases and test suites for MACsec.

Hardware tools to enable MACsec testing.

Aspect 3: “Trace analysis vs. MACsec”:

Solution: “Authentication only MACsec”.

Hardware tools to record communication.

Wireshark support since Wireshark 3.4.



<https://automotive-macsec.com>



Chapter 04. Summary.



SUMMARY.

WHY DO FUTURE E/E ARCHITECTURES REQUIRE MACSEC?

Automotive Ethernet and MACsec are the future:

- Ethernet allows the best communication platform for convergence and extensibility.
- MACsec can easily protect Ethernet communication and allows for secure platform.
- Ethernet + MACsec are great foundations for future E/E architectures.

- Bring up of MACsec can be engineered to be secure, fast, and robust.
- Automotive MACsec requires optimized MKA!
 - Find details of automotive MKA and more here: <https://automotive-macsec.com>
- Also important: Consulting, prototyping, testing, and tooling.





Shiqiu Chen

CEO

shiqiu.chen@sigent.cn

+86-1381-002-6761

Sigent Technology ICP
No. 299, Changping Road, Shahe Town
Changping District, Beijing

<https://www.sigent.cn>



Dr. Lars Völker

Technical Fellow

Lars.Voelker@technica-engineering.de

+49-175-1140982

Technica Engineering GmbH
Leopoldstraße 236
80807 Munich
Germany

<https://www.linkedin.com/in/lars-voelker/>

Local partner of Technica Engineering.