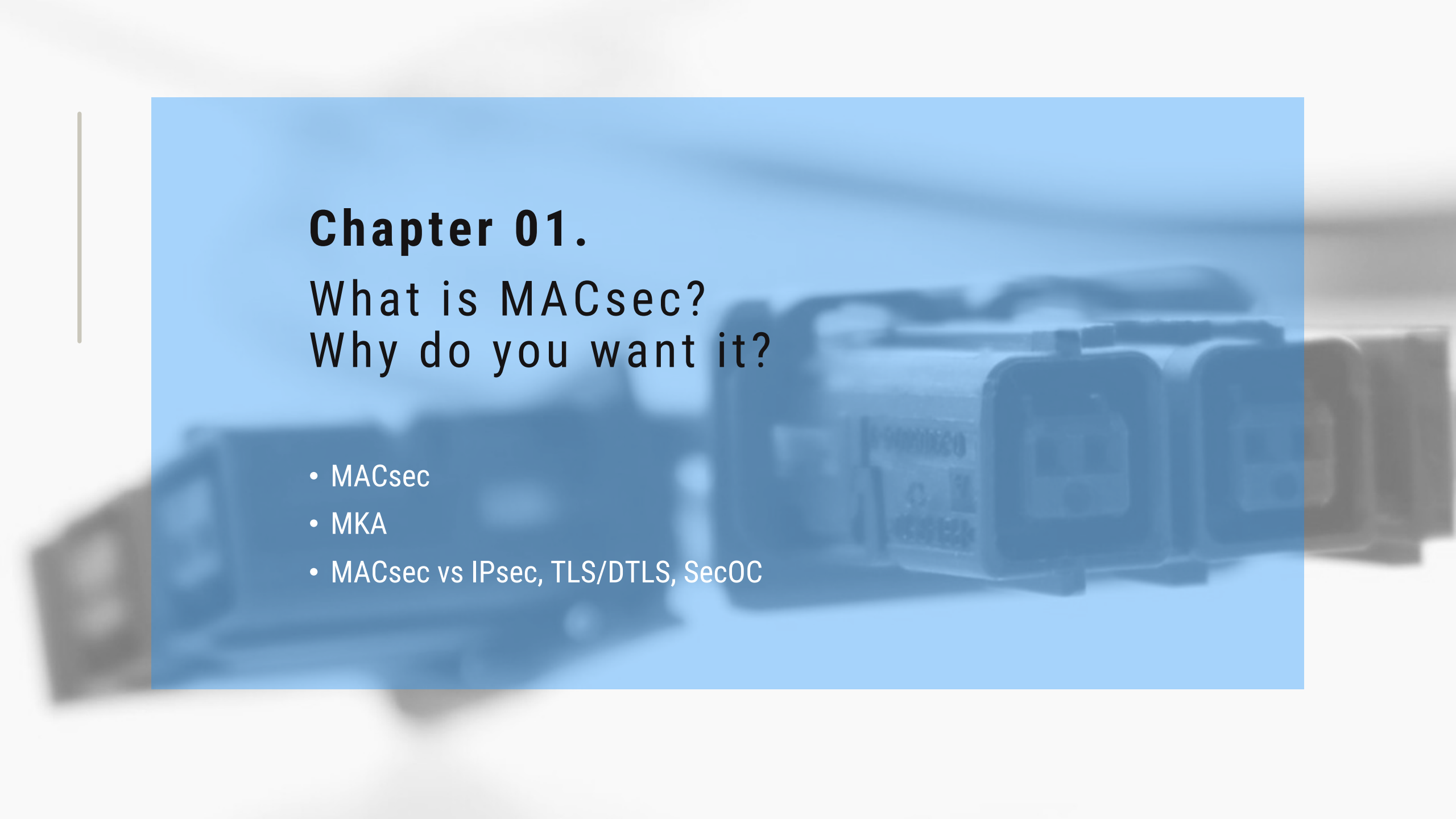
MACsec & Automotive Security

Dr. Lars Völker

CAST Online Workshop Automotive Security

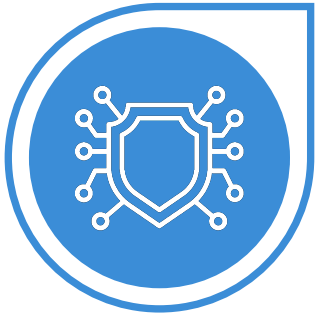


Chapter 01.

What is MACsec?
Why do you want it?

- MACsec
- MKA
- MACsec vs IPsec, TLS/DTLS, SecOC

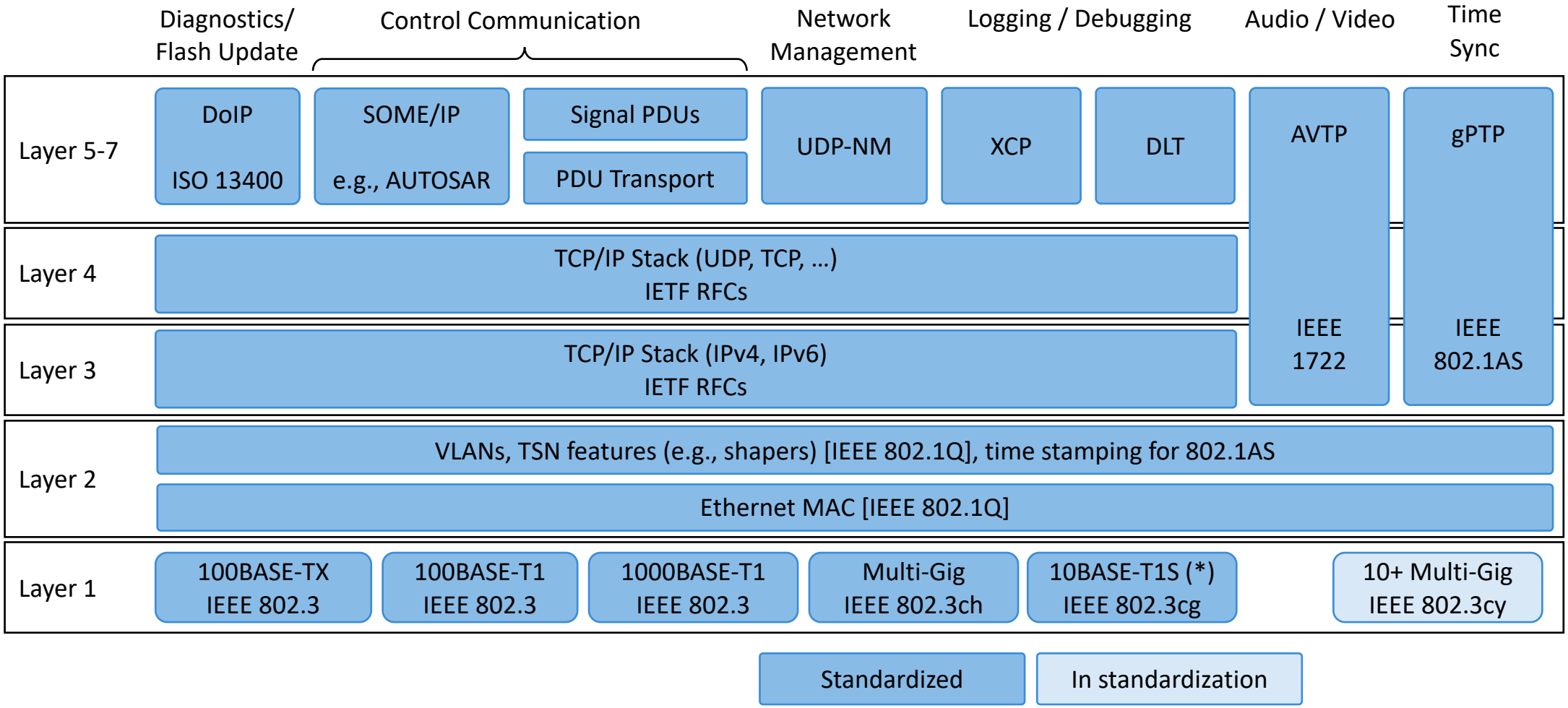
WHAT IS MACSEC?



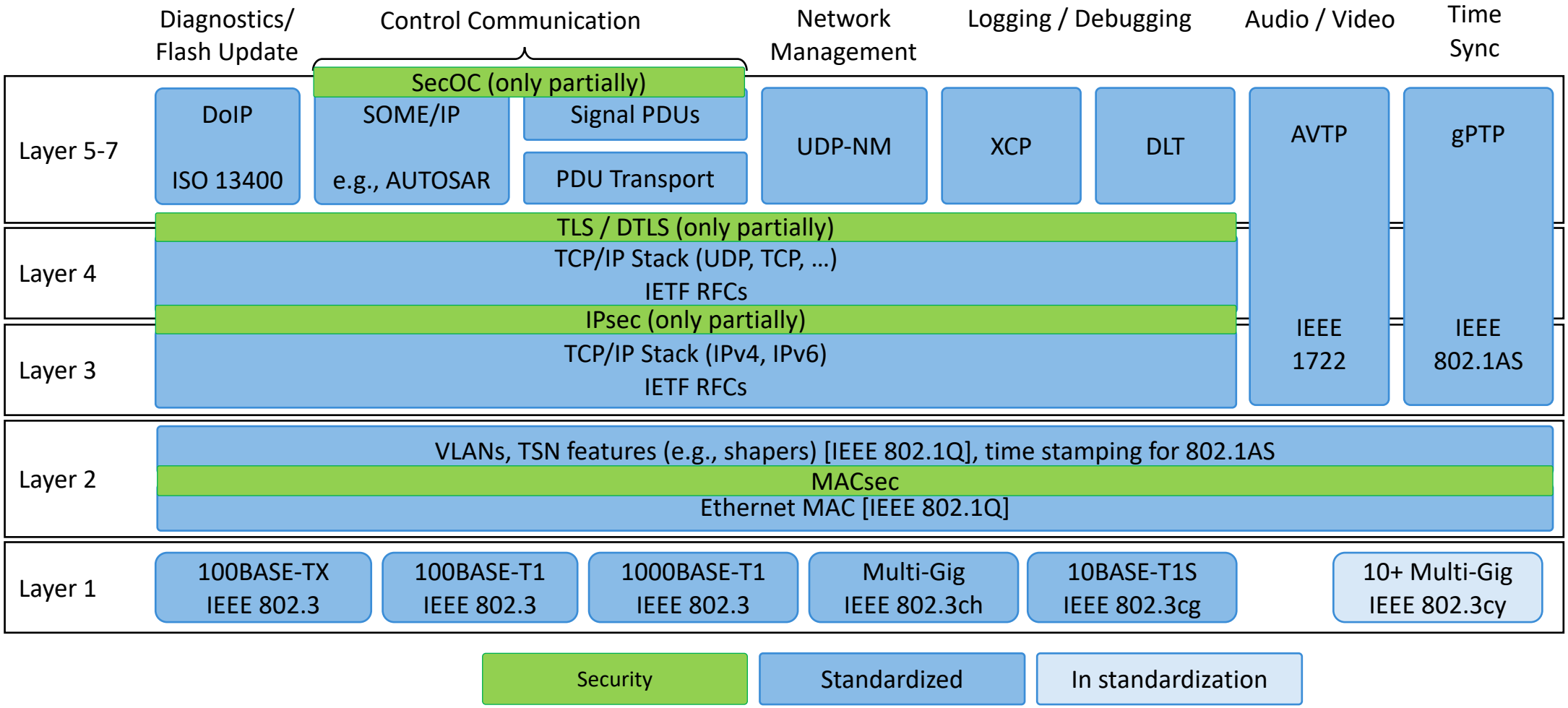
- “Media Access Control (MAC) Security” is the standardized Security solution for the MAC layer by IEEE.
- “MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity”, [1].
- MACsec is typically run in the “hop-by-hop” mode. This means that Ethernet frames are protected on wire but not inside an Ethernet Switch.
- MACsec requires Hardware support.

- Relevant Standards:
  - [1] “Media Access Control (MAC) Security”, IEEE Std 802.1AE, 2018.

EXAMPLE PROTOCOL STACK.



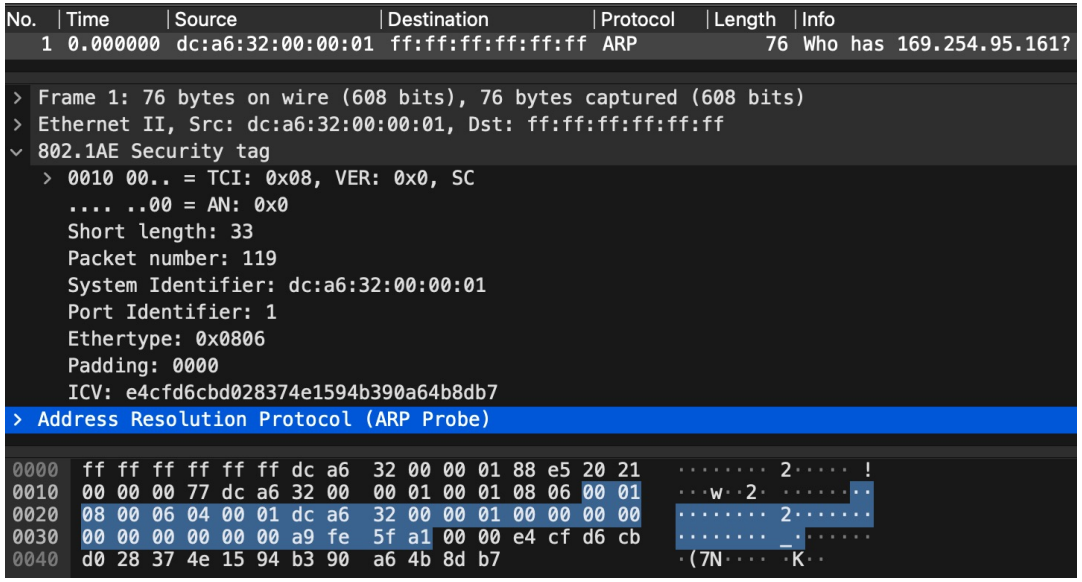
EXAMPLE PROTOCOL STACK.



HOW DOES MACSEC WORK?

MACsec:

- “Authentication only” or “Encryption + Auth”.
- Hop-by-hop mode 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?

MACSEC KEY AGREEMENT.

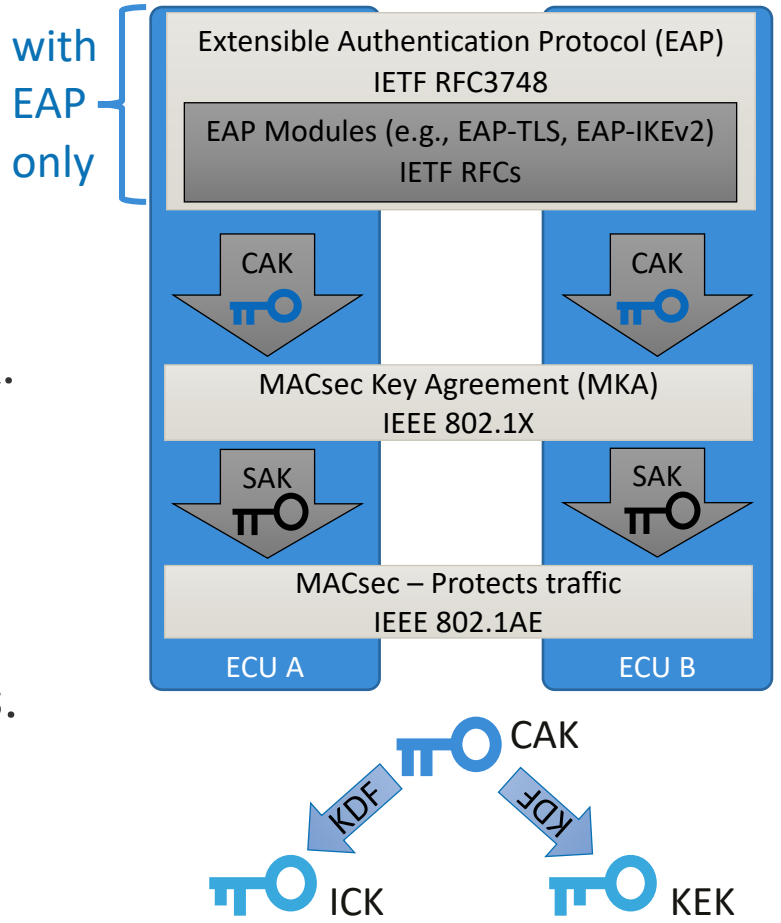
MACsec Key Agreement (MKA):

- 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.



CAK: Connectivity Association Key (symmetric long-term secret)

SAK: Secure Association Key (symmetric session key)

MACSEC VS IPSEC, TLS, SECOC.

MACsec can cover more communication:

- More protocols.
- Multicast + Broadcast too!

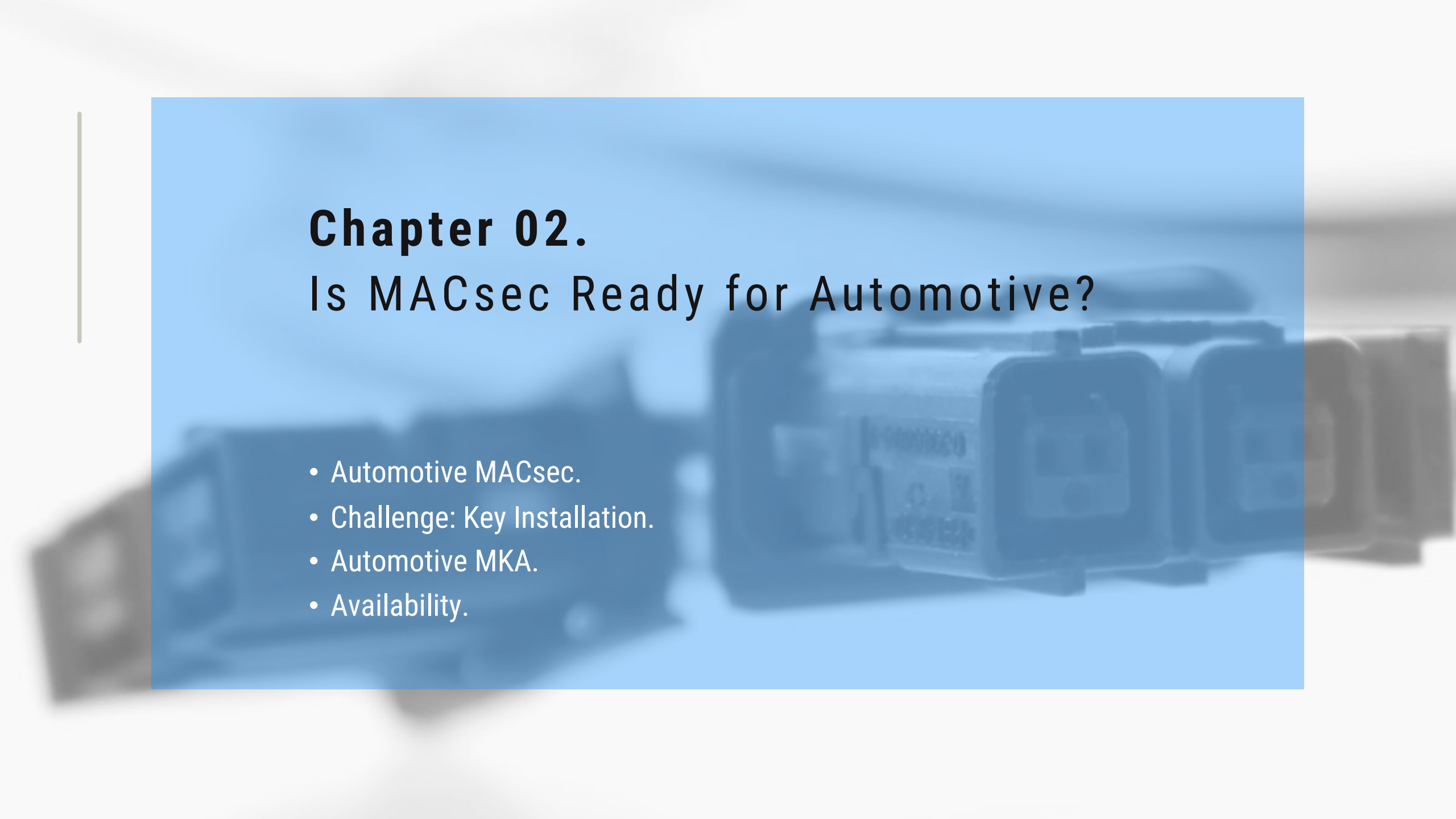
MACsec is secure:

- MACsec, IPsec, TLS/DTLS can exchange fresh keys.
- SecOC typically does not a have strong key exchange.

MACsec is faster on startup (Key Exchange):

- MACsec one per Link
- IPsec one per ECU
- TLS/DTLS one per “application connection” * “ECU using it”

→ MACsec protects more, is secure, and faster.

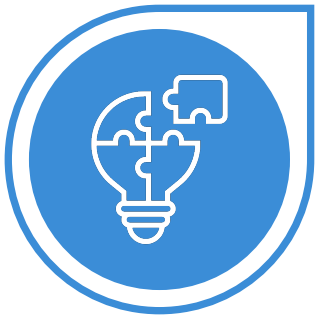


Chapter 02.

Is MACsec Ready for Automotive?

- Automotive MACsec.
- Challenge: Key Installation.
- Automotive MKA.
- Availability.

AUTOMOTIVE MACSEC.



Algorithm Choices:

- GCM-AES-128 or GCM-AES-256 depending on HW support.
- Typically, in “Authentication Only” for better testability.
- “Encryption + Authentication” requires more support:
  - Generate special CAKs for development vehicles.
  - Ensure that encrypted SAKs can be recorded by test equipment.

Rekeying:

- Goal is one key exchange per power cycle.
- Extended Packet Number (XPN) allows that.

CHALLENGE: KEY INSTALLATION.

Challenge: Key installation (in plant and service):

- How to install keys for MACsec, if communication is not present yet?

Option 1 – deactivate security for key installation.

- Simple solution but requires trust in service.
- OEM may not trust 3rd party service in all regions.

Option 2 – bypassing MACsec.

- Current MACsec chips allow selected traffic to bypass MACsec (e.g., MKA).
- Best practice: create bypass for key installation, diagnostics, and update.
  - Securing the unprotected communication is critical (typically, DoIP).

AUTOMOTIVE MKA.

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

See: Dr. Lars Völker, “Starting up MACsec for Automotive Ethernet”, VDI Conference Cyber Security for Vehicles, Jun 2021.

Automotive Hardware: Technica Automotive MKA implementation:

Our Automotive demos takes from PHY linkup to MACsec ready:

- ~18ms including configuration of MACsec hardware.

AVAILABILITY.

Semiconductors:

- We have shown MACsec running on samples of two different vendors.
- Multiple vendors and chips for different speeds announced.

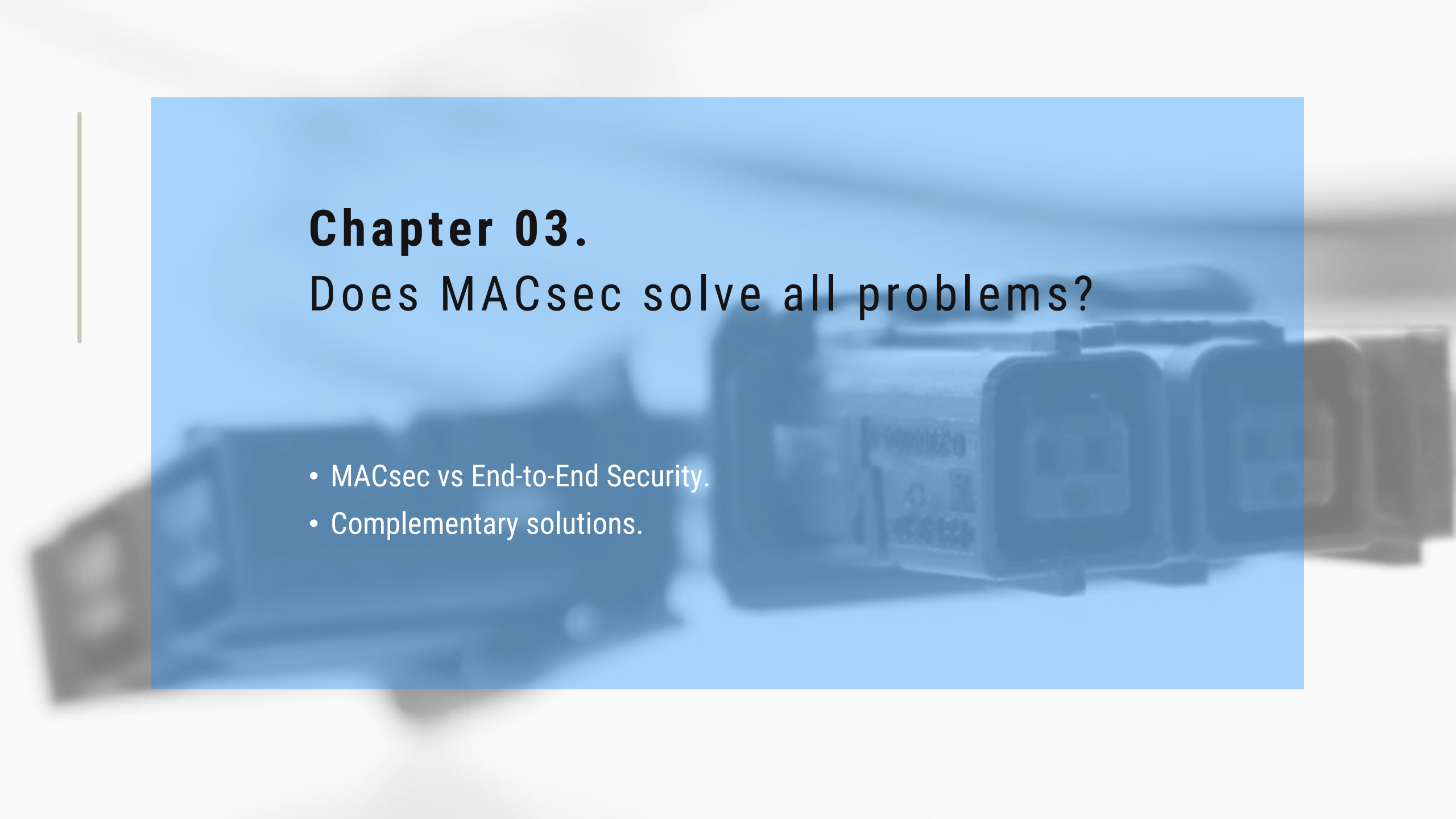
Software:

- MACsec supported by Linux. You just need an “Automotive MKA” and a driver.
- We have created Automotive MKA code.
- AUTOSAR is working on MACsec integration for AUTOSAR Classic.

Tools:

- We are working on Tools, Test Suites, etc.

Estimation: First SOPs in 2024 – 2026 probable.



Chapter 03.
Does MACsec solve all problems?

- MACsec vs End-to-End Security.
- Complementary solutions.

MACSEC VS. END-TO-END SECURITY.

Unprotected in Ethernet Switches?

- Inside the Ethernet Switch communication is unprotected.
- As before: Secure configuration of Ethernet Switches is a must!
- Attacking the Switch itself seems unfeasible since all silicon.

No “End-to-End Security” with MACsec?

- “But MACsec cannot protect until the application”.
  - IPsec, TLS, SecOC do not either, if you examine implementations!
- “But MACsec does not protect the “host identity”.
  - MACsec need to combined with complementary solutions!

COMPLEMENTARY SOLUTIONS (1).

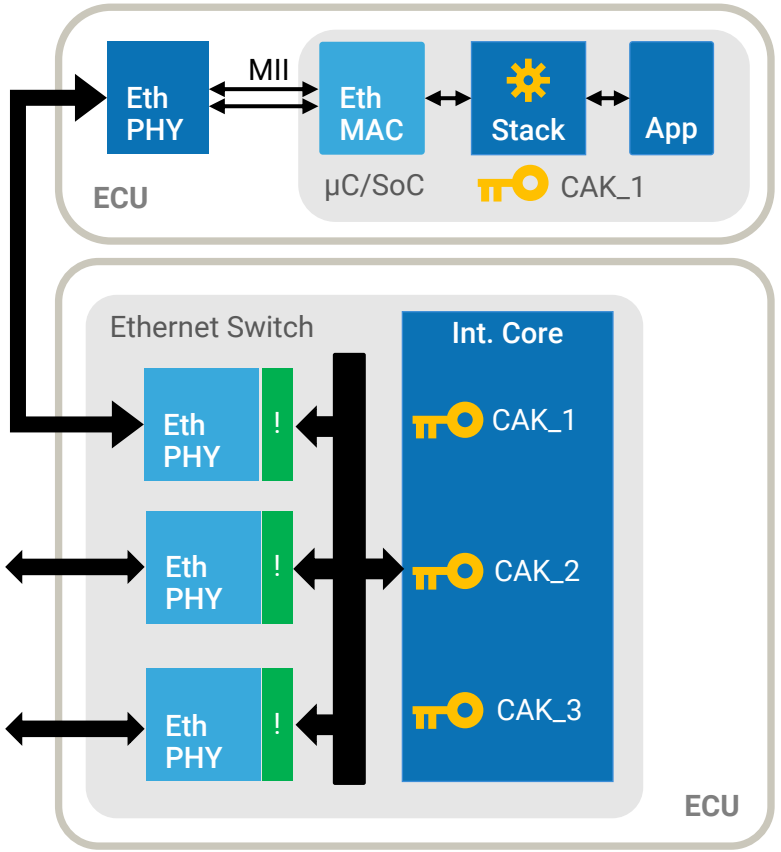
Address Filtering on Switches

- 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.

→ **Similar security as with IPsec and TLS/DTLS is achieved.**

In addition, Security on Ethernet Switches in greatly improved:

- Ports are blocked until MKA authentication successful.
- Ports only accept protected traffic.
- Port filters can be more specific (think ECU options).



COMPLEMENTARY SOLUTIONS (2).

Packet Filters and ACLs:

- Without spoofing many solution get easier.
- Packet filters can trust that a source IP is not modified.
  - Stronger filtering on ECUs possible.
  - With multiple IPs (e.g., virtualization), ECUs need to also filter outgoing.
- Simple ACLs can now achieve high Security for SOME/IP.
  - No need for “costly” application protocol specific security.
  - Updating and managing ACL policy needs to be solved.

Don’t forget: Use VLANs for segmentation!

SUMMARY.

Maximum Protection:

- MACsec allows protection of basically all Ethernet frames.

Ready:

- MACsec and MKA can be made ”Automotive”.
- Chips, Software, Tools, and Testing are worked on.

Thank you for your attention!

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/