technica engineering
Member of KPIT Group

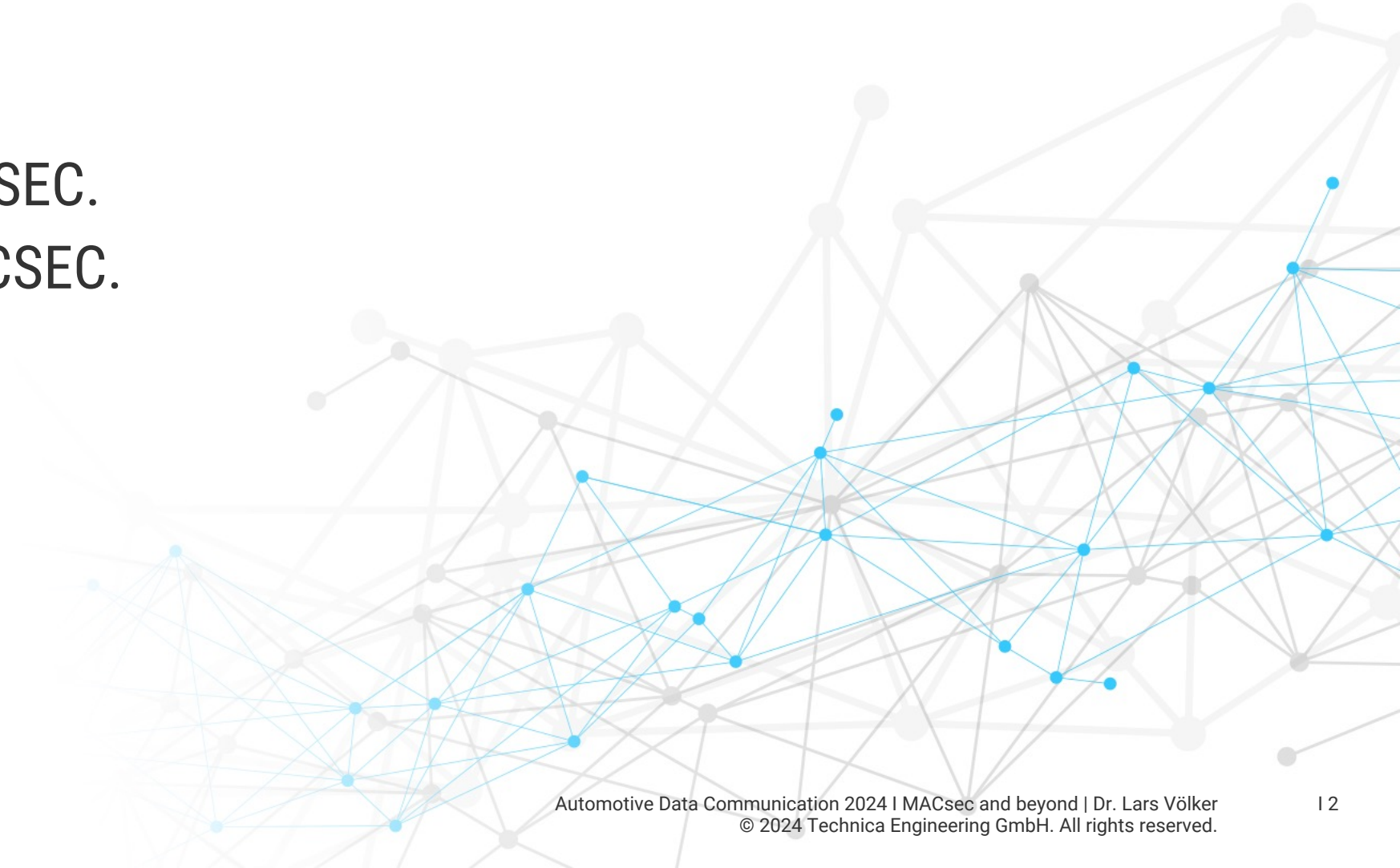
MACSEC AND BEYOND.

THE UPCOMING NETWORK SECURITY STATE OF THE ART.

#OneStepAhead

MACSEC AND BEYOND.

TABLE OF CONTENT.



#1 | MACSEC AND BEYOND.
THE WAY TO MACSEC.

THE WAY TO MACSEC

WHY OTHERS FAILED TO PROTECT AUTOMOTIVE ETHERNET?

technica engineering
Member of KPIT Group

- Ethernet Network Security has been worked on for long [1], [2], [3] et. al.:
  - SecOC can protect only application layer payloads, has no standardized key exchange, introduces a key management nightmare, and is slow.
  - (D)TLS protect only application layer protocols and payloads but only unicast, startup performance is challenging, and AUTOSAR support is incomplete.
  - IPsec protects above IP but only unicast communication and leads to an integration nightmare.
  - And all the above do not scale well, which means resource usage and/or startup.

- Many know this already as we discussed it for years…

[1] Comparing Automotive Network Security for Different Communication Technologies, L. Völker, BMW, 01/2018, Automotive Ethernet Congress
[2] Security Protocols and Applications – Best Friends or Worst Enemies, A. Gallego, J. Galve, L. Völker, Technica, 11/2022, Ethernet & IP @ Automotive Technology Day
[3] In-Vehicle Network Security – MACsec, the Game Changer, L. Völker, T. Königseder, Technica, 11/2022, 10th ELIV MarketPlace
Find slides here: https://automotive-macsec.com/papers.shtml

THE WAY TO MACSEC.

IS MACSEC BETTER?

- MACsec solves these issues.
  - Automotive Ethernet is a LAN and only MACsec aims to protect LANs.
  - MACsec protects basically all traffic.
  - MACsec is fully hardware accelerated.

- That’s why I was pushing for 8+ years for it.
  - In 2016, we found no majority for MACsec in TC11.

- Why did it take so long?
  - Hardware support needs time and commitment.
  - Some minor issues had to be sorted out…

OPEN TC 11 - Switch Requirements Specification
Draft 2016-01-21

ID-Prefix	ID	Requirement	Value	Revision
		GENERAL		
GEN	01	The switch shall use a non-blocking architecture.		Version 0.1
GEN	02	The switch shall operate as store and forward switch.		Version 0.1
GEN	03	The boot time of the switch without internal PHYs (including configuration via the host processor) from voltage reaches valid range until it't fully operational shall be less than x ms.	50	Version 0.1
GEN	04	The switch shall support the switch-dependent features of rapid spanning tree protocol (RSTP).		Version 0.1
GEN	05	The switch shall support IEEE 802.1X.		Version 0.1
GEN	06	The switch may support IEEE 802.1AE MACsec.		Version 0.1

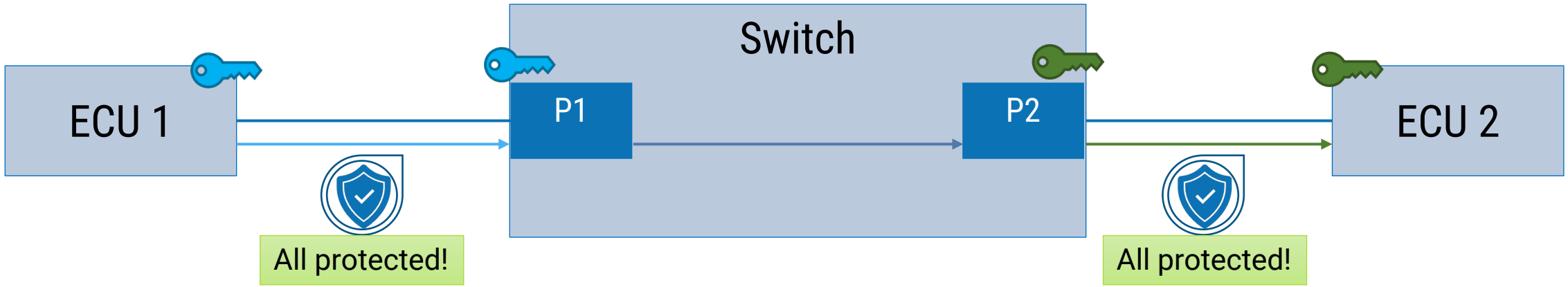
#2| MACSEC AND BEYOND.
AUTOMOTIVE MACSEC.

AUTOMOTIVE MACSEC.

HOP-BY-HOP IS THE KEY TO BEST SECURITY.

- MACsec protects communication “hop-by-hop”.
  - For every link protection with a different keys is done.

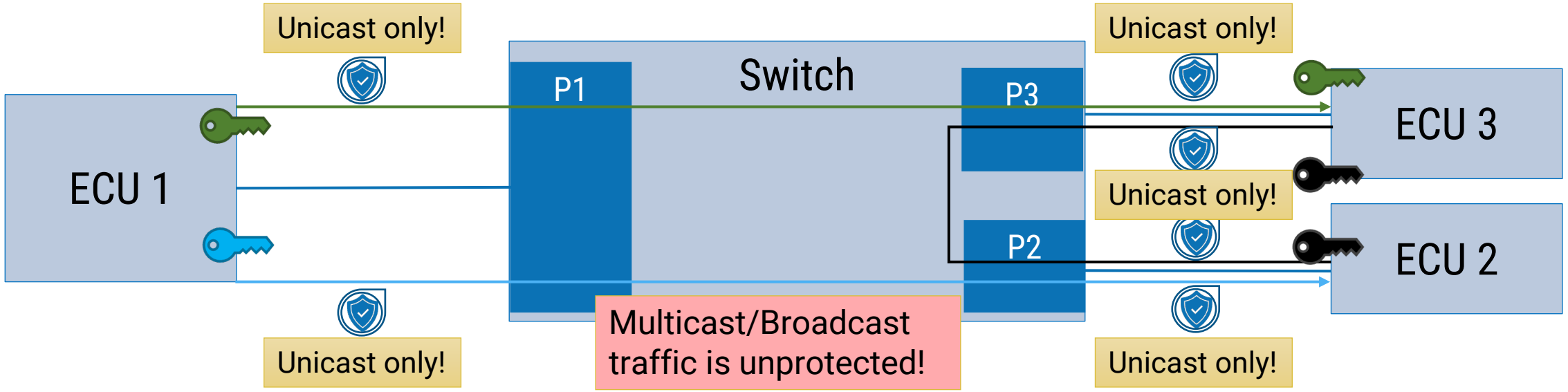
- “Hop-by-hop” Security is the key for MACsec to protect all messages on layer 2!
  - This means every frame going out a port can be protected.
- This also means that frames are unprotected inside switch chip.
  - No serious problem, if Switch Config done right.



AUTOMOTIVE MACSEC.

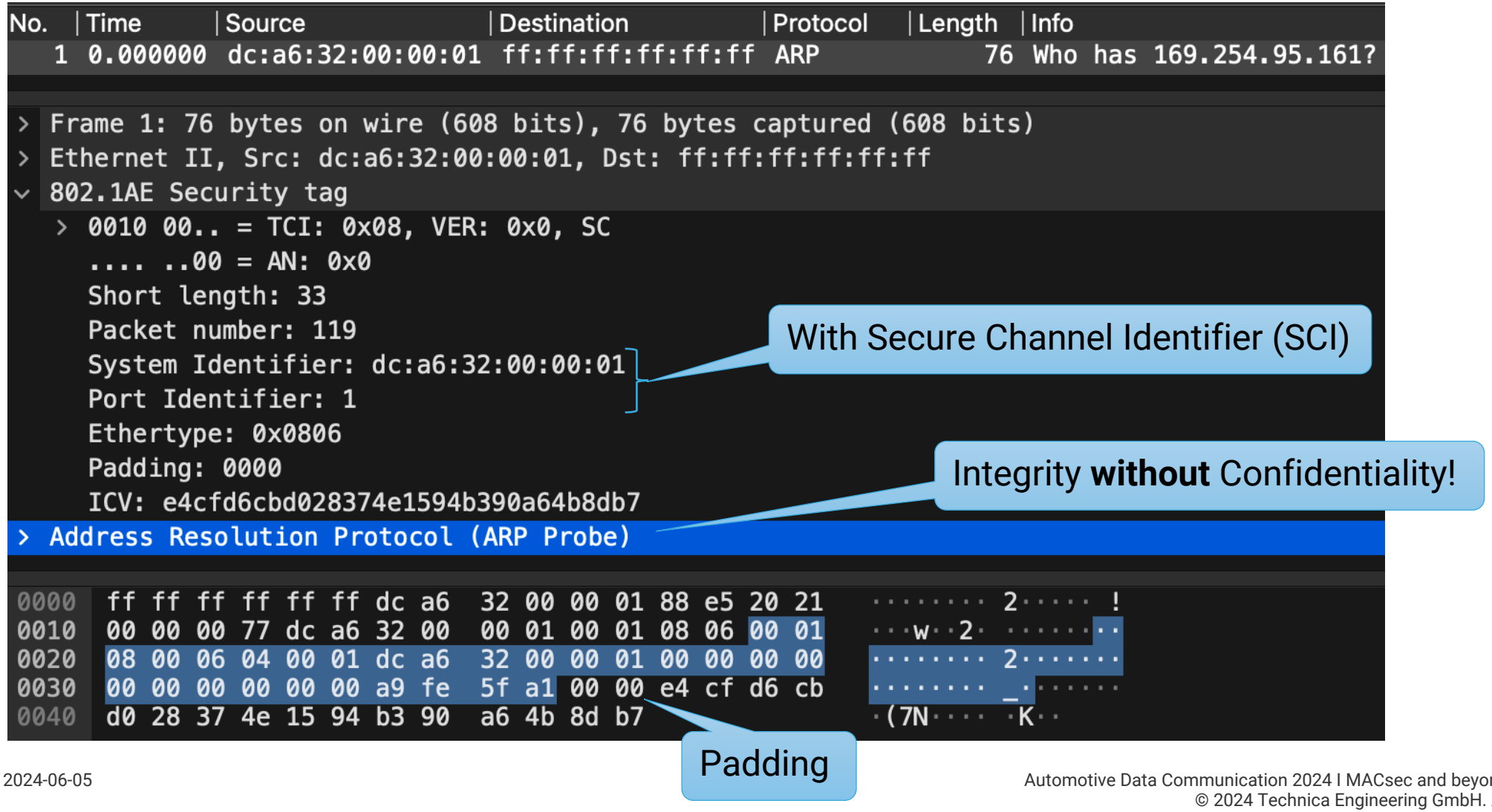
WHY DOES END-TO-END MACSEC NOT WORK FOR AUTOMOTIVE?

- Selected limitations of end-to-end MACsec and others (e.g., IPsec):
  - Massive scalability issues (n-1 associations per ECU).
  - Protection of Multicast and Broadcast traffic not possible anymore (less secure).
  - ECU Integration (when does a link come up) becomes a nightmare (like IPsec).
- In general: end-to-end MACsec is not suitable for in-vehicle communication!



AUTOMOTIVE MACSEC.

MACSEC HEADER.



AUTOMOTIVE MACSEC.

PROTOCOL OVERVIEW WITH EAP.

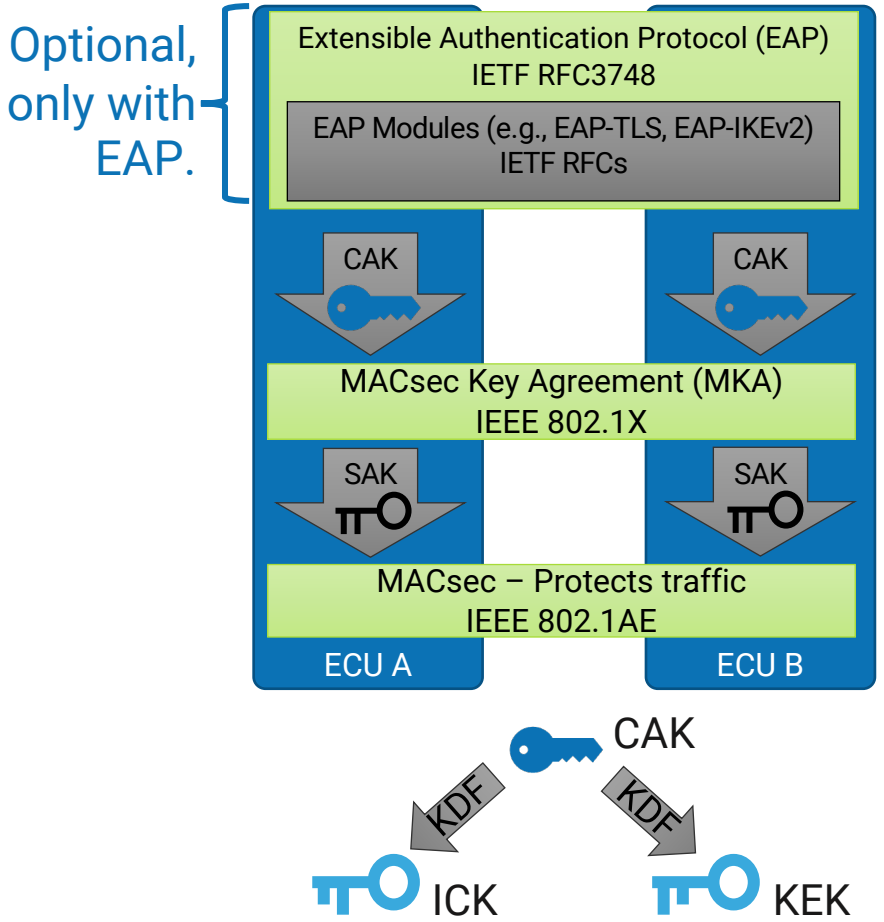
technica engineering
Member of KPIT Group

MACsec startup sequence (with EAP):

1. Port-based Authentication with EAP:
   - Authenticate the Port with EAP module.
   - Generate key material (CAK/CKN) for the next steps at both peers.
2. MACsec Key Agreement Protocol (MKA):
   - Discover MACsec peer(s).
   - Negotiating and distributing MACsec keys (SAK).

Example for EAP module:

- EAP-TLS using TLS with X.509 certificates.



CAK	Secure Connectivity Association Key
CKN	Secure Connectivity Association Key Name
ICK	ICV Key
ICV	Integrity Check Value
KDF	Key Derivation Function
KEK	Key Encrypting Key
SAK	Secure Association Key

AUTOMOTIVE MACSEC.

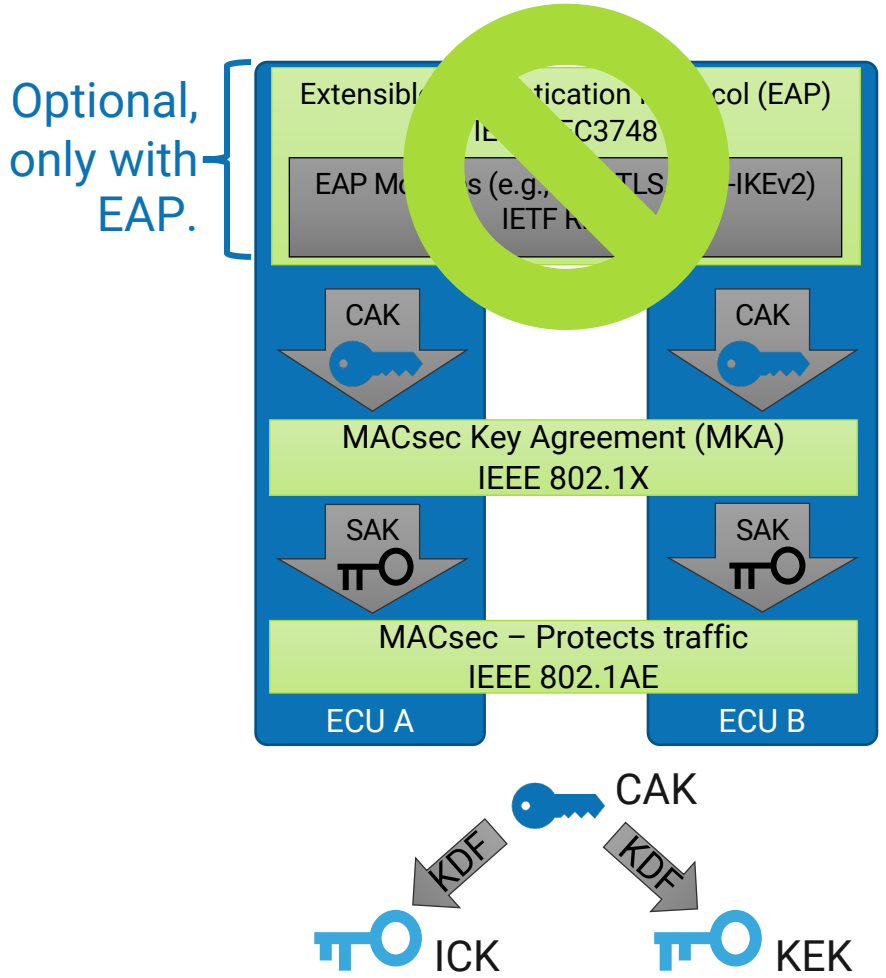
PROTOCOL OVERVIEW WITHOUT EAP.

Optimization for faster startup:

- Usage of EAP is optional.
- Do not use EAP.

- What must be done?
  - Install CAK into ECUs during production/service.
  - Run MKA with pre-shared keys.

- Benefits: Faster startup, less complexity!



CAK	Secure Connectivity Association Key
CKN	Secure Connectivity Association Key Name
ICK	ICV Key
ICV	Integrity Check Value
KDF	Key Derivation Function
KEK	Key Encrypting Key
SAK	Secure Association Key

AUTOMOTIVE MACSEC.

FROM MKA TO AUTOMOTIVE MKA.

- Regular MKA is too slow for Automotive: 3-8s to start MACsec.

- Protocol tuning required to get to ~9ms [4], [5].
  - Faster Key Server Election – hard-code role.
  - Optimized Protocol Timings – answer immediately instead of waiting for timeout.
  - And more optimizations.
  - Linux version available online to understand optimizations:
    - https://github.com/Technica-Engineering/MKAdaemon

- OPEN Alliance TC17 plan: release **Automotive MKA** standard this year.
  - Switched Ethernet only.

[4] **Starting up MACsec for Automotive Ethernet**, L. Völker, Technica, 06/2021, 7th International VDI Conference – Cyber Security for Vehicles.
[5] **Automotive MACsec (Demo)**, L. Völker, 05/2022, Technica Demo on YouTube.
Find slides and videos here: https://automotive-macsec.com/papers.shtml

AUTOMOTIVE MACSEC.

EXTENDED PACKET NUMBERS (XPN).

- The faster Ethernet gets, the more often you need to rekey.
  - Frequent rekeying should be avoided in Automotive.

Speed in bit/s	10G	5G	2.5G	1G	100M	10M
Lifetime Worst Case *	~5mins	~10mins	~20mins	~50mins	~8.4 hours	~3.5 days

- XPN changes in MACsec are minor:
  - Increases packet numbers from 32 to 64 bit.
  - Only lower 32 bit are transported (header stays the same).
  - Small adaption of IV calculation.
  - MACsec implementation needs to handle the ”overflow” of PN counter in RX frames
    - Based on 64bit shadow counter.
- XPN changes in MKA also very small.
- Recommendation and current trend: XPN turned on everywhere.

* Rekeying starts at reaching 80% of that time.

AUTOMOTIVE MACSEC.

CHECK LIST.

- ❑ MACsec and MKA but not EAP.
- ❑ Hop-by-hop MACsec and not End-to-End MACsec.
- ❑ Integrity only MACsec or Integrity + Confidentiality?
- ❑ Activate XPN.
- ❑ Automotive MKA tuning.

- Use MACsec to create a proactive security strategy!
  - Do not wait for threat analysis.
  - Use MACsec for everything and add only more, when needed.

#3| MACSEC AND BEYOND.
BEYOND MACSEC.

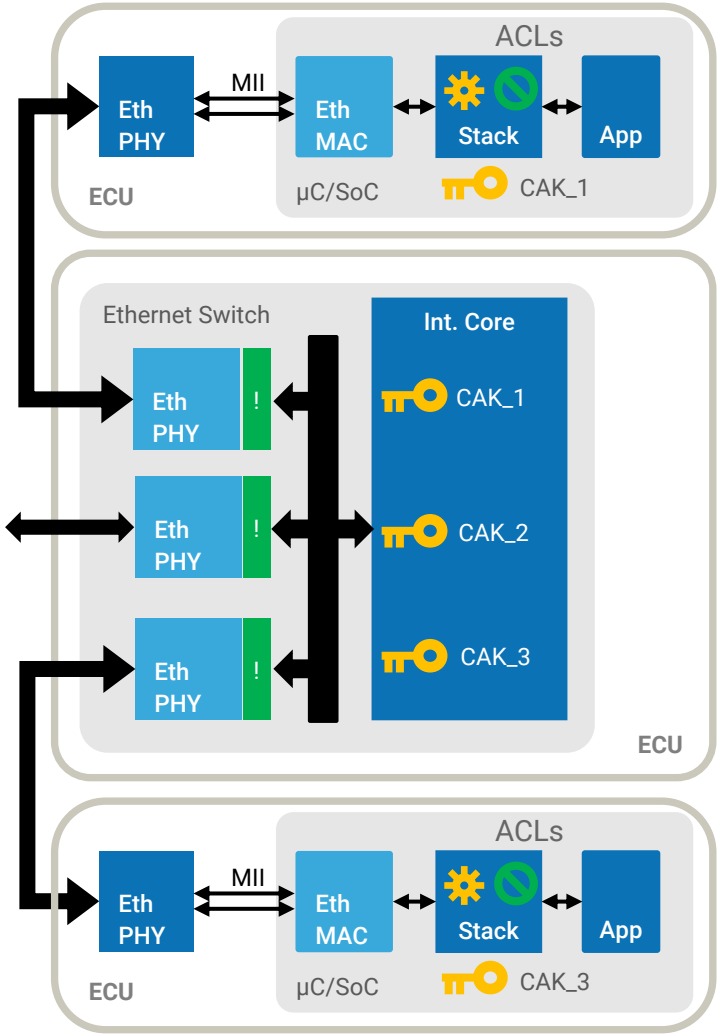
BEYOND MACSEC.

MECHANISMS COMPLEMENTING MACSEC.

- Authenticated Switch Ports allow Address Filtering:
  - This can stop address spoofing.
  - Similar peer authentication as with TLS or IPsec possible.
  - In addition, dynamic enforcement of VLANs.

- Without address spoofing, ACLs become easy!
  - A simple list of endpoints instead of complex protocols.

- Keep another security protocol for critical use cases:
  - Car Immobilizer, Mileage, Component Theft, etc.
  - Think: Defense in Depth.



BEYOND MACSEC.

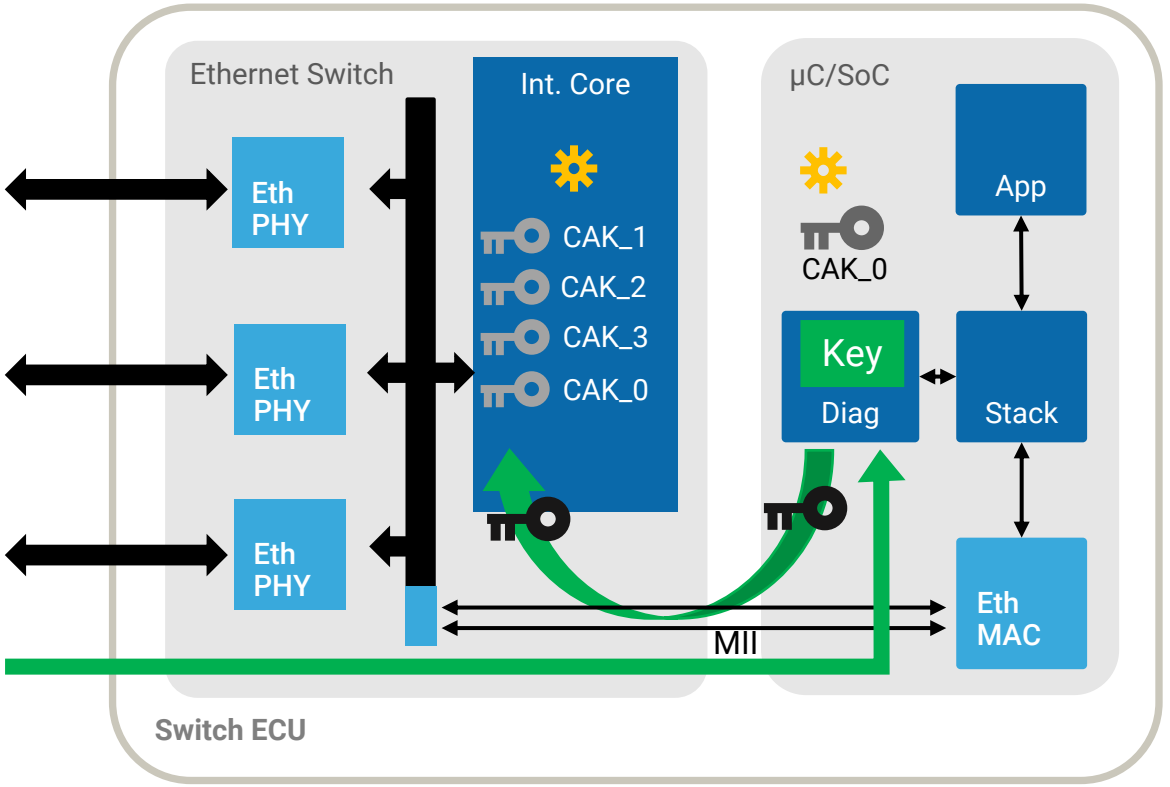
WHAT IS NEEDED? KEY MANAGEMENT!

Key

- Key Management is an important security mechanism:
  - Key Management for installing CAKs for MKA.
    - And optionally CKNs.

- MKA can use X.509 certificates alternatively:
  - Avoid this as certificate path validation is hard and takes time.
  - If you can install X.509 certificates, adding symmetric key support is typically easy.

- And make sure that CAKs are stored in HSMs.



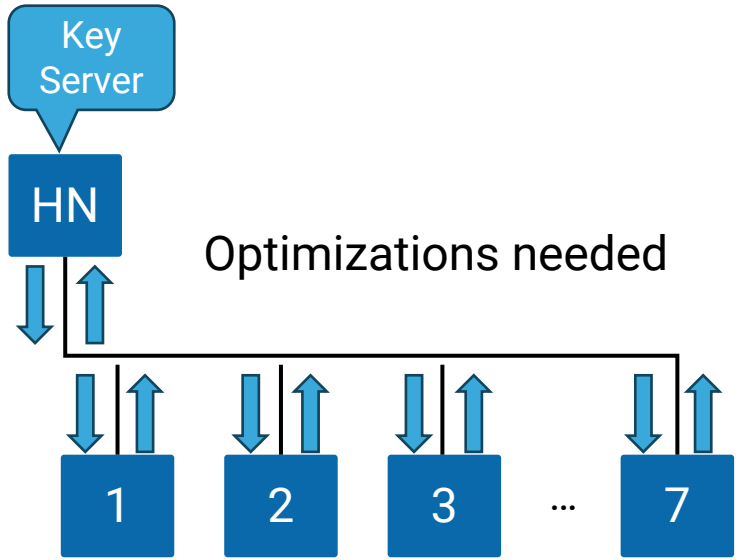
BEYOND MACSEC.

AUTOMOTIVE ETHERNET BUSSES.

- Automotive MACsec starts with switched Ethernet.
  - MKA support busses but with up to 8s startup!

- Automotive MKA needs update for busses:
  - Different optimizations for busses are required.
  - How many Security Zones on busses are required?
  - Which ECUs can be mixed in a security zone?
  - Can busses only achieve weaker security?

- OPEN TC17 has busses on the roadmap.
  - Concepts and ideas welcome!
  - For OPEN membership, see https://opensig.org

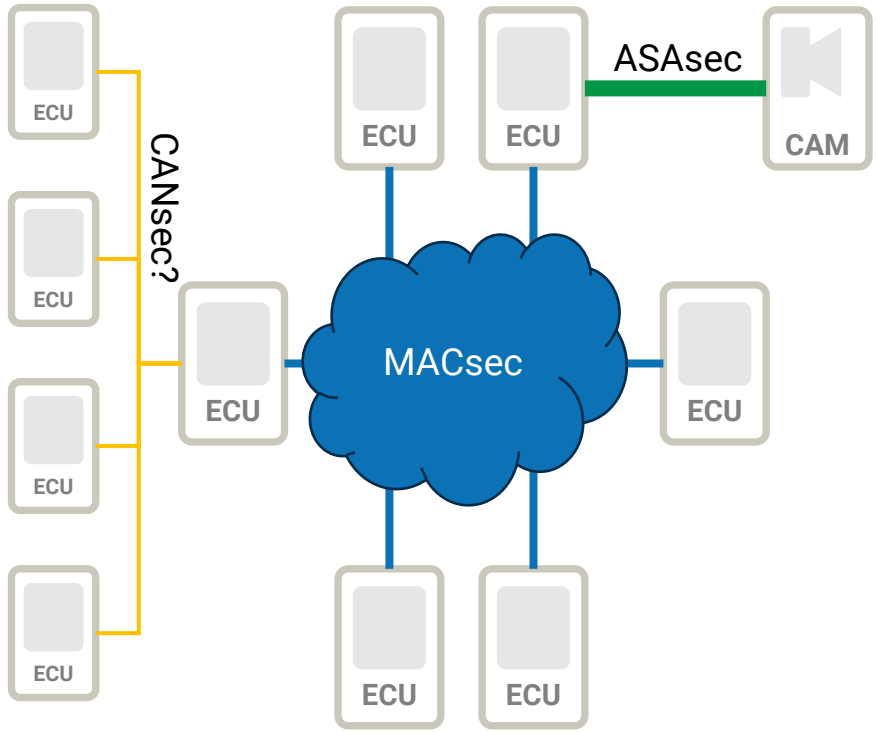


BEYOND MACSEC.

OTHERS.

- SerDes:
  - Most solutions on the market have no strong security.
  - ASA a MACsec-like security solution ASAsec [6], [7].
    - Different key exchange protocol.
    - Includes custom key management protocol.

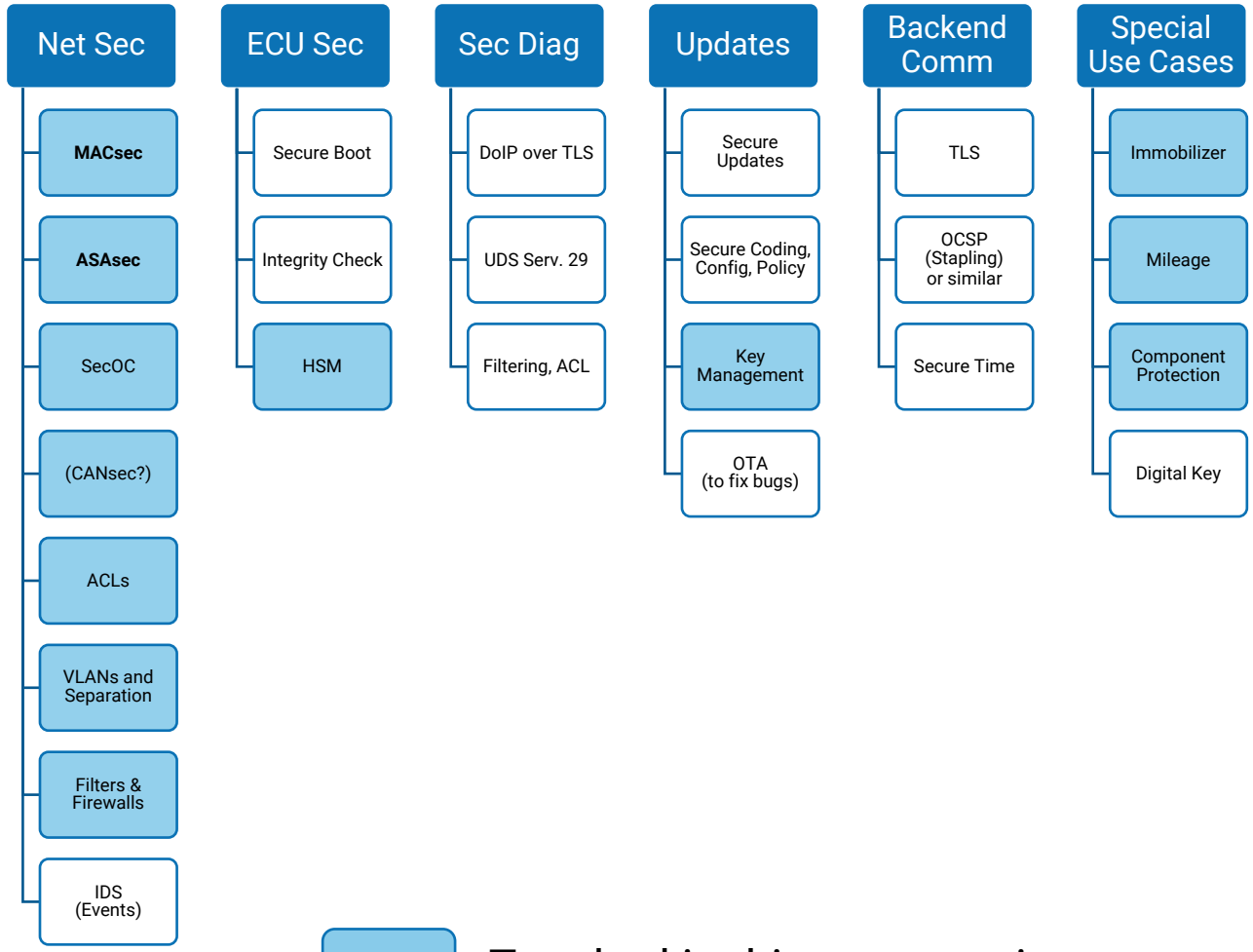
- Legacy busses have no similar security solutions:
  - In general, SecOC might be good enough.
  - For CAN-XL a MACsec-like solution was proposed: CANsec.
    - This might be needed, if Ethernet tunneling is required!?



[6] **Automotive Security Challenges and the Automotive SerDes Alliance Solution**, S. Lachner and L. Völker, Technica, 10/2020, Automotive SerDes Conference
[7] **Automotive MACsec (Demo),** L. Völker, Technica, 05/2022, Technica Demo on YouTube.
Find slides and videos here: https://automotive-network-security.com/papers.shtml

BEYOND MACSEC.

SELECTED ELEMENTS OF OUR SECURITY STATE OF THE ART PREDICTION.



Touched in this presentation.

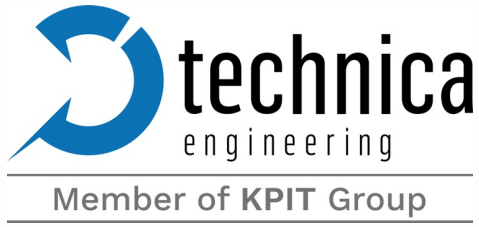
Next steps:

- Automotive MKA for busses.

Up for discussion:

- CANsec needed?
- SecOC key exchange standard?
- Standardized Key Management?

#4| MACSEC AND BEYOND.
CONTACT.



Technica Engineering GmbH

Leopoldstraße 236
80807 Munich
Germany

DR. LARS VÖLKER
Technical Fellow
lars.voelker@technica-engineering.de
+49 175 11 40 982