AUTOMOTIVE MACSEC INTRODUCTION

2025-04-02
PHILIP LAPCZYNSKI
PRINCIPAL ENGINEER
RENESAS ELECTRONICS CORPORATION

© 2025 Renesas Electronics Corporation. All rights reserved.

MACSEC BASICS

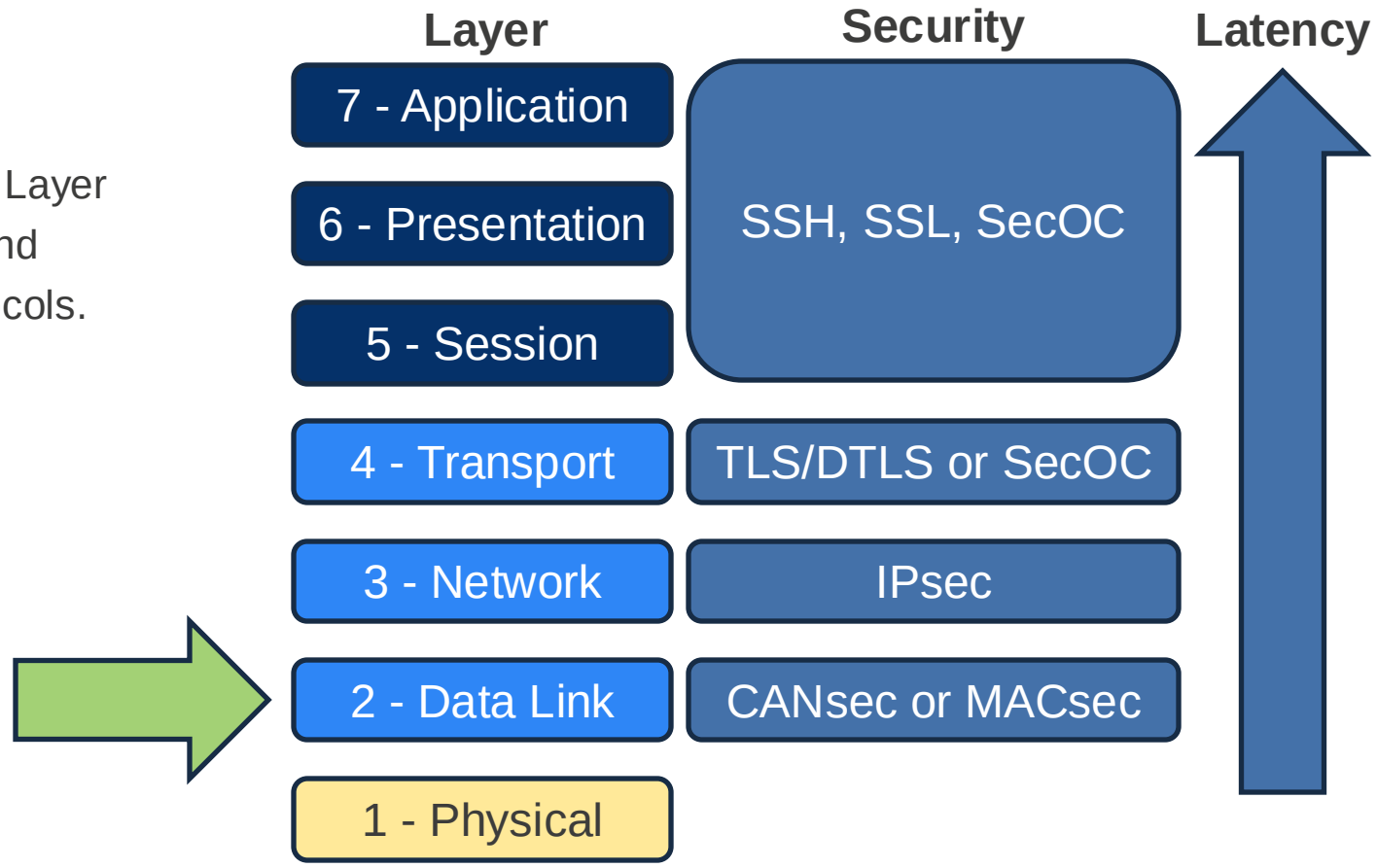
© 2025 Renesas Electronics Corporation. All rights reserved.

WHAT IS MACSEC? MEDIA ACCESS CONTROL SECURITY

- **The MACsec architecture comprises of two components:**

  1. The **IEEE 802.1AE** standard which provides Layer 2 based secure link for data confidentiality and integrity for media access independent protocols.
  2. The MACsec key agreement (MKA) protocol defined in **IEEE 802.1X**

MACsec is L2 security deployed in PHYs, switches, and ethernet controllers

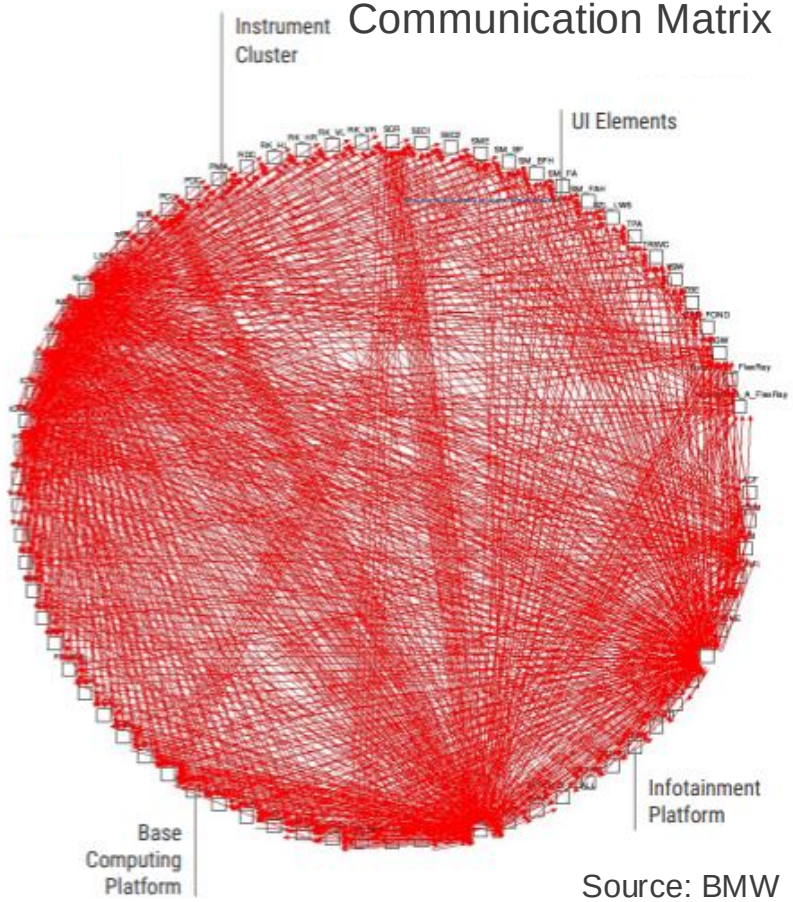


© 2025 Renesas Electronics Corporation. All rights reserved.

WHY DO WE NEED LAYER 2 SECURITY IN AUTOMOTIVE?

- Security is a must in today's vehicle and not a "nice to have" requirement. Everyone knows the spectacular vehicle hacks from the media
  - This could lead to vehicles becoming life-threatening for the passengers as well it could damage the reputation of the car maker and suppliers
  - Recent vehicle theft via an unsecured CAN interface
    - https://kentindell.github.io/2023/04/03/can-injection/

- Classical End-to-End security mechanisms cannot cope with today's communication demand.
  - Since there are thousands of communication links in today's EE architecture
- Therefore, technologies like TLS or IPSec will be considered as not adequate to secure the future in-vehicle network
- But MACsec, when implemented in HW, can cover it since it can protect the data at line-rate



Source: BMW

© 2025 Renesas Electronics Corporation. All rights reserved.

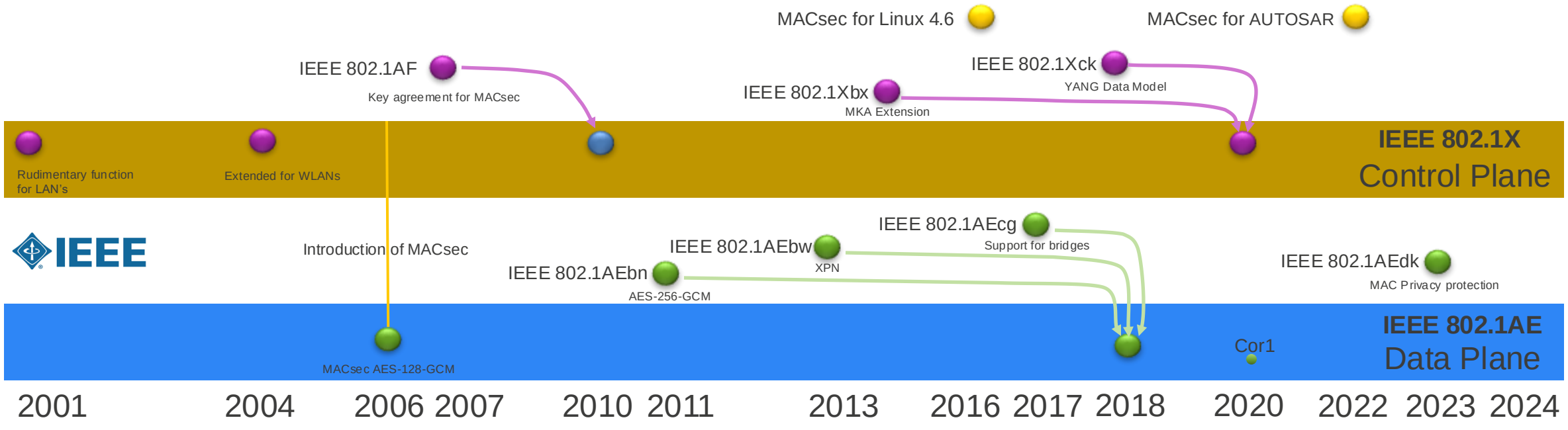
WHY MACSEC?

- **Scalable**: Can be deployed in different ways across the network and is specifically designed to protect LANs.
- **Protects All Traffic**: MACsec protects all traffic above L2 layer transparently.
- **Fully Hardware Implementable**: MACsec sits at L2 and can be implemented in the PHY or Ethernet controller, freeing up CPU bandwidth.

© 2025 Renesas Electronics Corporation. All rights reserved.

MACSEC STANDARDS

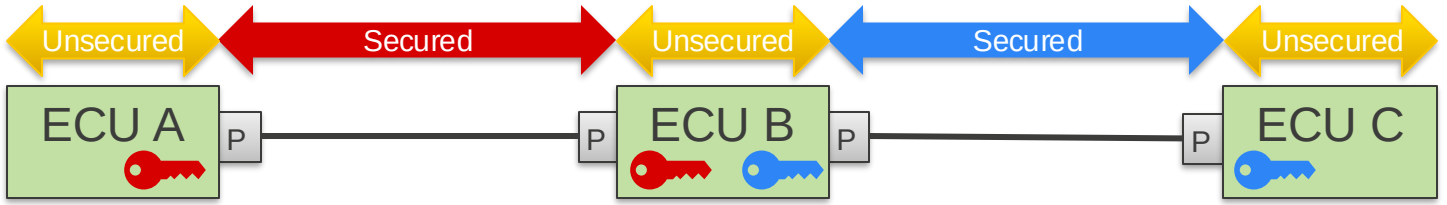
MACsec was developed by the IEEE as 802.1AE to compliment the 802.1X-2004 standard. The 802.1X is developed as Port-Based Network Access Control Layer. The sub standard 802.1AF defines the MACsec Key agreement (MKA) which became part of the 802.1X in 2010. There have been several revisions to the IEEE 802.1AE and 802.1X standard over the years to cover new requirements



© 2025 Renesas Electronics Corporation. All rights reserved.

MACSEC NETWORK

- MACsec was designed as link layer protection
- Due to its location on the link layer, it can cover the entire communication
- And it also allows the interleave of other security standards e.g IPsec over MACsec



- MACsec normally protects communication “hop-by-hop”
- **NOTE:** Cisco introduced an enhancement to MACsec, which allows for End-to-End encryption. Usage is more relevant to enterprise systems and not for automotive networks.

Comparison between multiple encryption standards

Protects . . .	SecOC	(D)TLS	IPsec	MACsec
. . . payload	Yes	Yes	Yes	Yes
. . . of application protocol (above TCP/UDP)	Partially	Yes	Yes	Yes
. . . of TCP and UDP headers	No	No	Yes	Yes
. . . of IP headers	No	No	Partially	Yes
. . . of VLAN-tags	No	No	No	Yes
. . . of Ethernet headers	No	No	No	Yes
. . . of SOME/IP-SD	No	Partially	Partially	Yes
. . . of ARP/NDP	No	No	No	Yes
. . . of ICMP	No	No	Yes	Yes
. . . of IGMP	No	No	No	Yes
. . . of (g)PTP	No	No	No	Yes
. . . of IEEE 1722	No	No	No	Yes
. . . of Unicast messages	Yes	Yes	Yes	Yes
. . . of Multicast messages	Yes	No	(Extension)	Yes
. . . of Broadcast messages	(Yes)	No	No	Yes

© 2025 Renesas Electronics Corporation. All rights reserved.

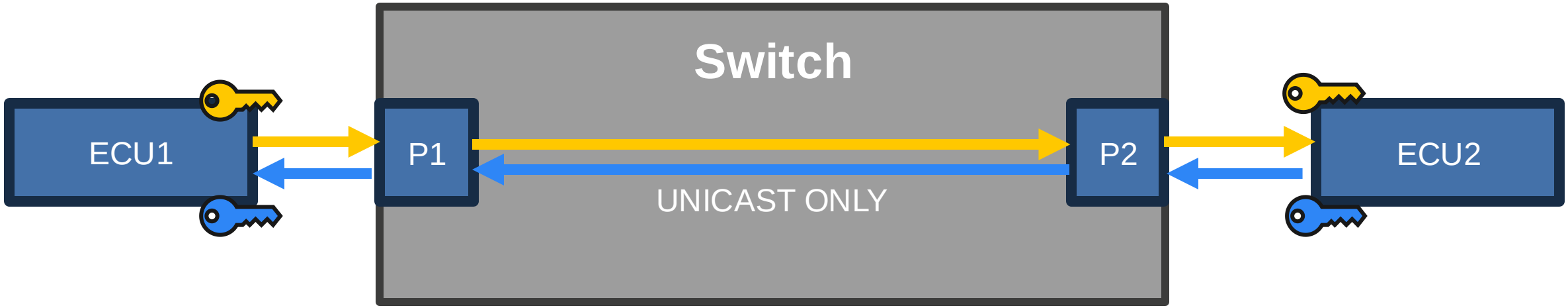
MACSEC - END-TO-END ENHANCEMENT

Advantages

- Offers end-to-end protection
- Reduced switch complexity

Disadvantages

- N-1 associations per ECU
- Can’t protect Multicast and Broadcast messages
- Complex key management



© 2025 Renesas Electronics Corporation. All rights reserved.

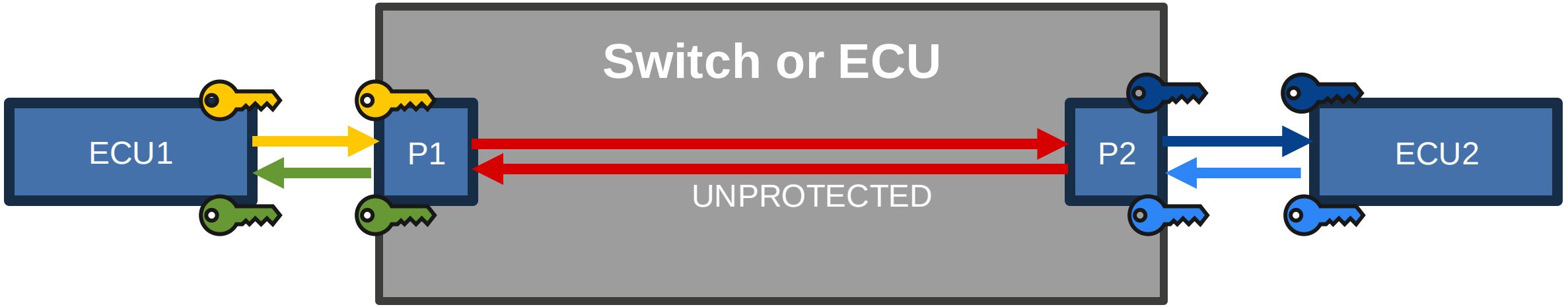
MACSEC - POINT-TO-POINT ("HOP-BY-HOP") SOLUTION

Advantages

- Every frame is protected
- Easier key management
- Don't need to rekey all ECUs when a new ECU comes online

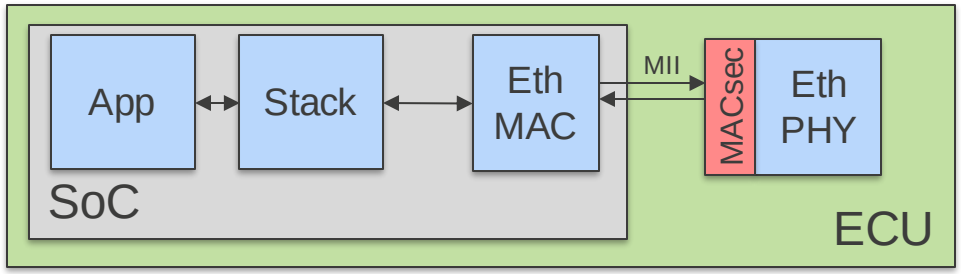
Disadvantages

- Frames unprotected inside switch/ECU

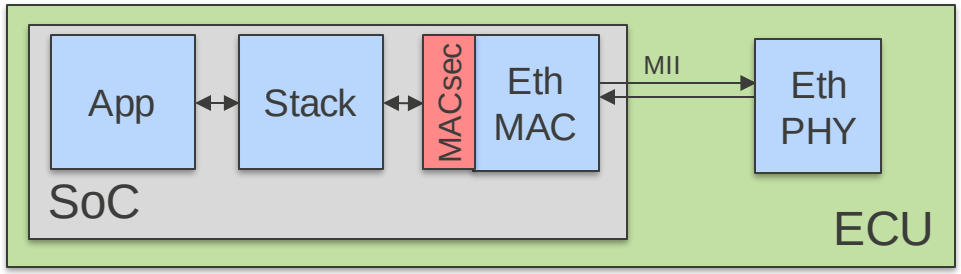


© 2025 Renesas Electronics Corporation. All rights reserved.

MACSEC DEPLOYMENT



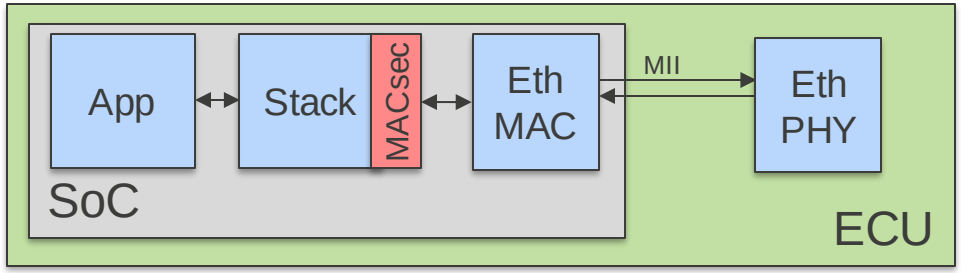
- MACsec in PHY's
  - Available now
  - Access to MII traces may be critical for high security use cases as well slower configuration via MDIO



MACsec in Ethernet MAC

Limited availability, but changing

Best solution and most secure



MACsec in Software

Available (e.g. Linux)

Cost effective solution with hardware crypto. Performance of hardware crypto very critical. Lower speed grades only

© 2025 Renesas Electronics Corporation. All rights reserved.

SECURITY FEATURES OF MACSEC

Confidentiality (optional)

MACsec provides the option to encrypt the data payload of Ethernet frames, safeguarding sensitive information from unauthorized access and ensuring privacy.

Integrity

MACsec safeguards the integrity of the data payload within Ethernet frames, defeat unauthorized manipulation or injection of new frames into the network.

Endpoint Authenticity

By verifying the identity of authorized hosts entering into a secure communication on the network, MACsec ensures the authenticity of endpoints, mitigating the risk of unauthorized entities gaining access.

Replay Prevention

MACsec implements measures to prevent unauthorized actors from attempting to duplicate and transmit Ethernet frames originating from valid hosts. This feature enhances network security by mitigating the risk of replay attacks.

© 2025 Renesas Electronics Corporation. All rights reserved.

TYPICAL MACSEC ATTACK SCENARIOS

Eavesdropping / Sniffing

MACsec offers optional confidentiality through encryption, which protects the data payload of Ethernet frames. This prevents unauthorized parties from eavesdropping on sensitive information being transmitted over the network.

Data Manipulation

MACsec ensures integrity by protecting the data payload within Ethernet frames. This prevents unauthorized actors from tampering with or manipulating the contents of the frames during transmission.

Identity Spoofing

Endpoint authenticity is established through MACsec, which verifies the identity of authorized hosts entering into a secure relationship on the network. This prevents attackers from spoofing the identity of valid hosts.

Replay Attacks

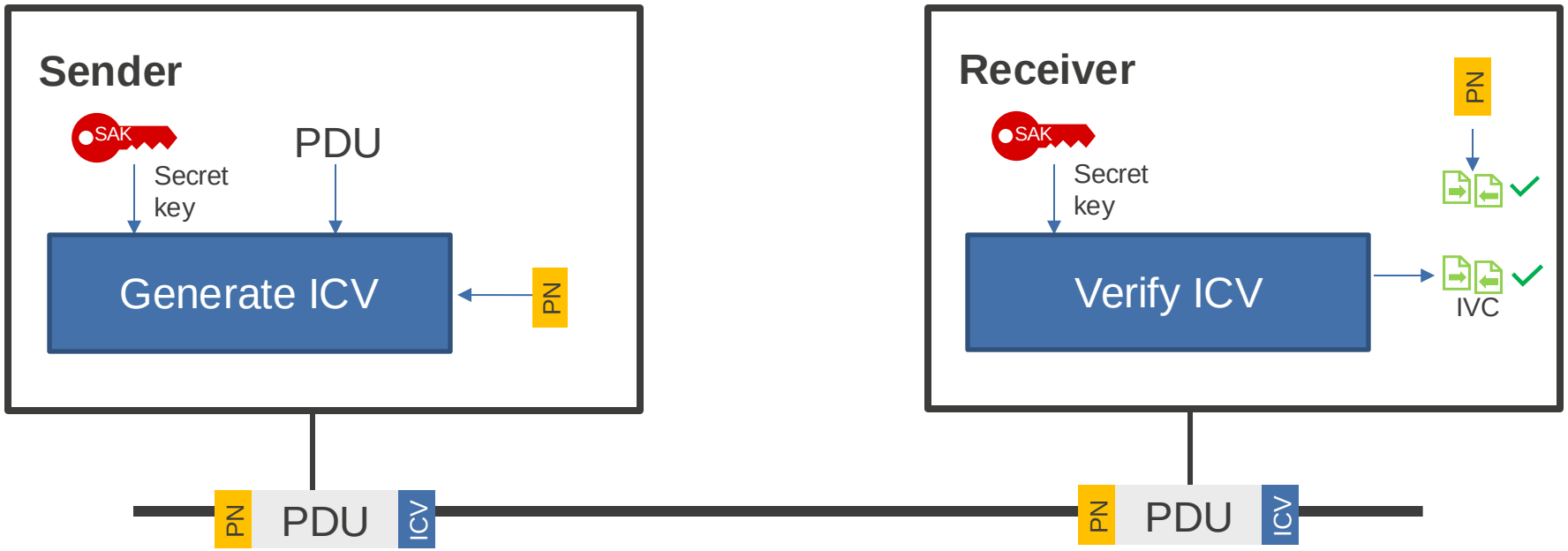
MACsec incorporates mechanisms for replay prevention. It ensures that unauthorized actors cannot duplicate and retransmit Ethernet frames originating from valid hosts, thereby preventing replay attacks.

Adversary-in-the-Middle Attacks

By verifying the authenticity of endpoints, MACsec mitigates the risk of adversary-in-the-middle attacks where an unauthorized entity intercepts and potentially alters communication between two parties. The combination of confidentiality, integrity, and endpoint authenticity features collectively defends against this type of attack.

© 2025 Renesas Electronics Corporation. All rights reserved.

GENERAL MACSEC CONCEPT

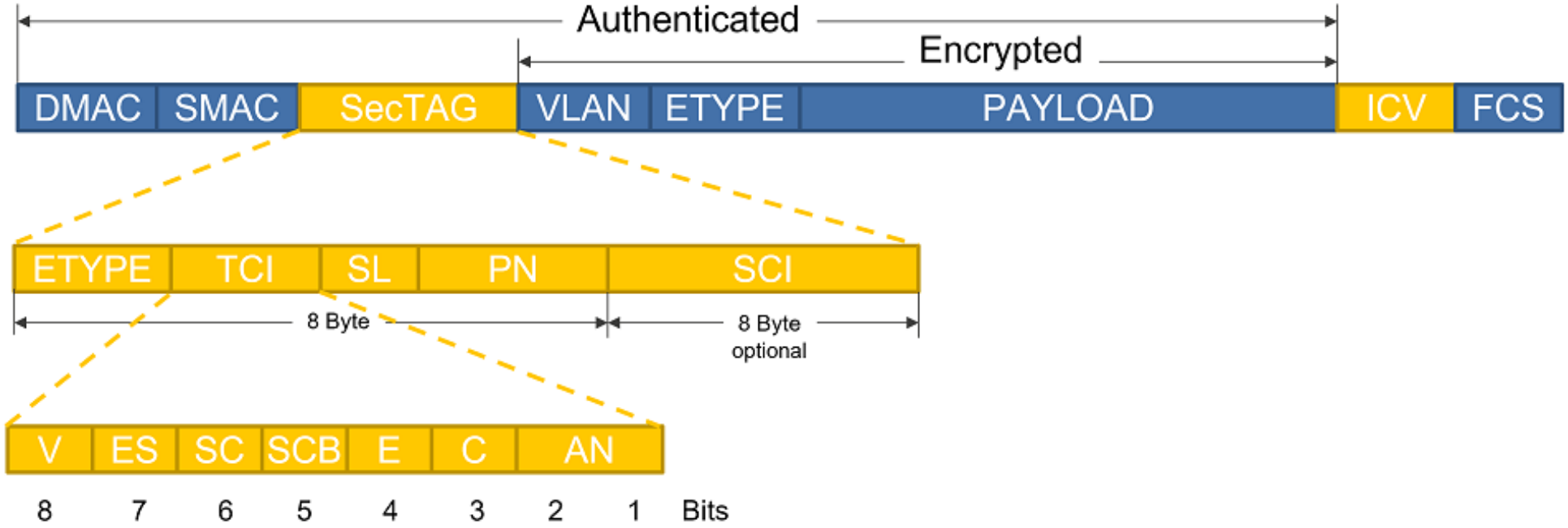


The sender uses the symmetric **Secure Association Key (SAK)** to generate the **Integrity Check Value (ICV)**. On the receiving end, the SAK is used to verify the received ICV. The receiver also checks the packet number to ensure data freshness.

© 2025 Renesas Electronics Corporation. All rights reserved.

MACSEC FRAME FORMAT

A MACsec packet is formed with an Ethernet frame by adding a Security TAG (SecTAG) and an Integrity Check Value (ICV).



- **ETYPE** – **MACsec** has a fixed value of **0x88e5**
  TCI –**Tag Control Information (TCI)** contains:
  - **Version number (V), End Station (ES), SCI present (SC), Single Copy Broadcast (SCB), Encrypted payload (E), Changed Text (C), and Association Number (AN)**
- **SL** – **Short Length** frame; the field is 6 bits long and indicates the bytes between the last byte of the SecTAG and the first byte of the ICV
- **PN** – **Packet Number** protects against replay attacks. The PN is also used as Initial Value (IV) for the Cipher Suite.
- **SCI** – **Secure Channel Identifier** used to identify the security association the traffic belongs.
- **ICV** – **Integrity Check Value** ensures the integrity of data.

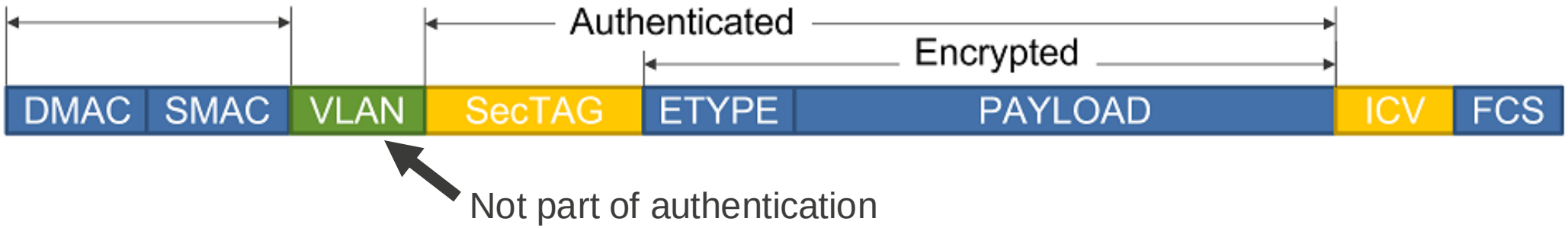
© 2025 Renesas Electronics Corporation. All rights reserved.

MACSEC VLAN AWARE FRAMES

To support end-to-end applications using VLAN (802.1Q), the MACsec frame can optionally support the VLAN tag bypassing the MACsec encryption.

Normal MACsec frame

Optional VLAN aware MACsec frame



© 2025 Renesas Electronics Corporation. All rights reserved.

KEY AGREEMENT IN AUTOMOTIVE

© 2025 Renesas Electronics Corporation. All rights reserved.

TRADITIONAL MACSEC KEY AGREEMENT USING EAP

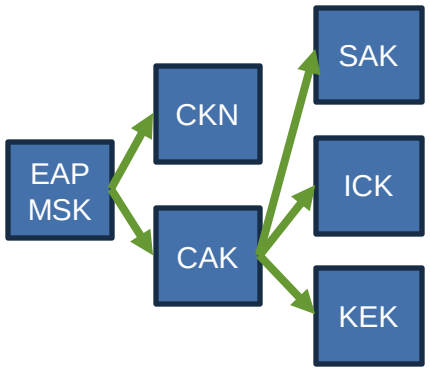
Step 1: MACsec startup using EAP

- Authenticate port using EAP
- Generate key material (CAK/CKN) for next steps

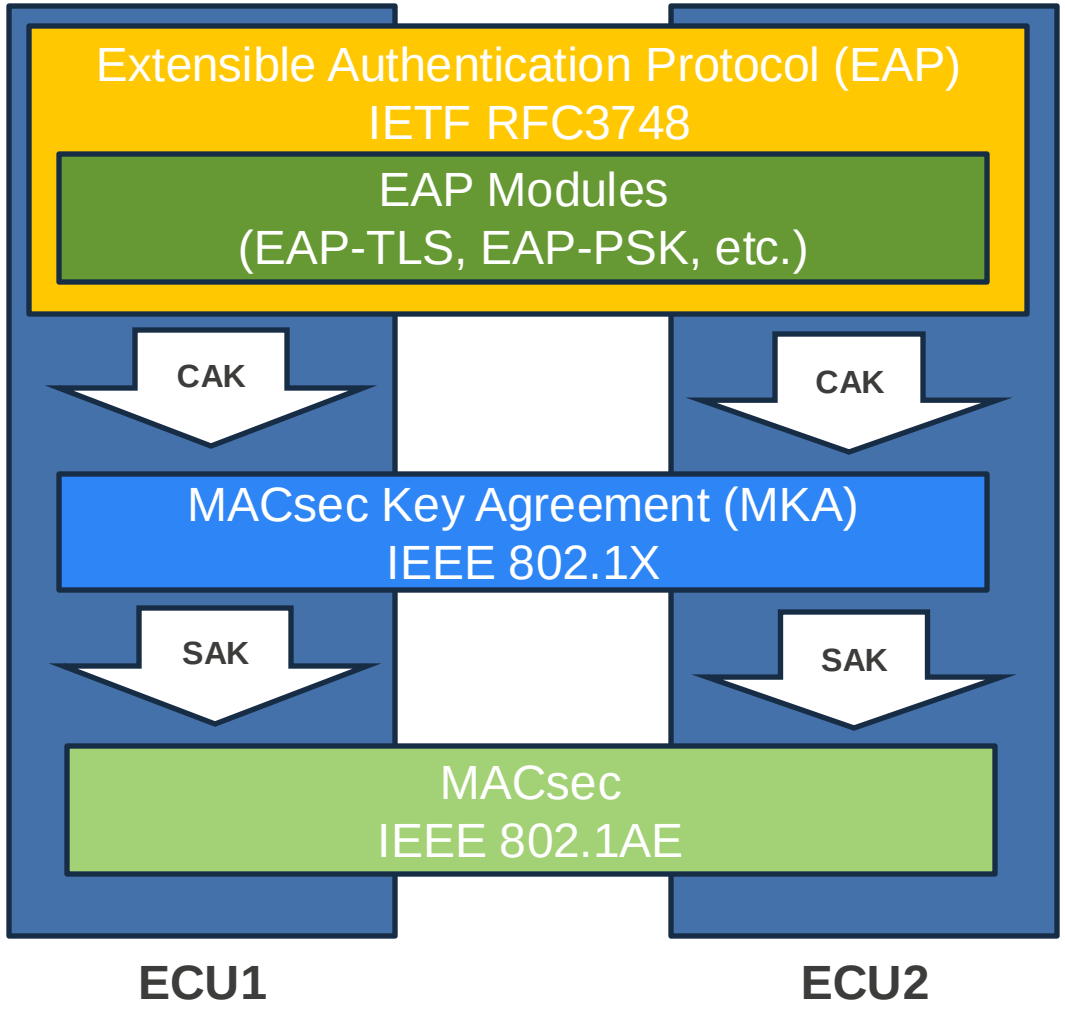
Step 2: MACsec Key Agreement Protocol (MKA)

- Discover MACsec peers
- Negotiate and distribute secure association keys

Dynamic key management and rotation but slow startup! MKA could take 3~8 seconds



MSK – Master Session Key
CKN – Connectivity Association Key Name
CAK – Connectivity Association Key
SAK – Secure Association Key
ICK – Integrity Check Key
KEK – Key Encryption Key



© 2025 Renesas Electronics Corporation. All rights reserved.

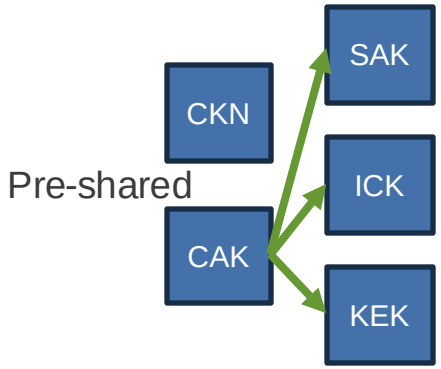
AUTOMOTIVE MACSEC USING PRE-SHARED KEYS

EAP not required by MACsec!

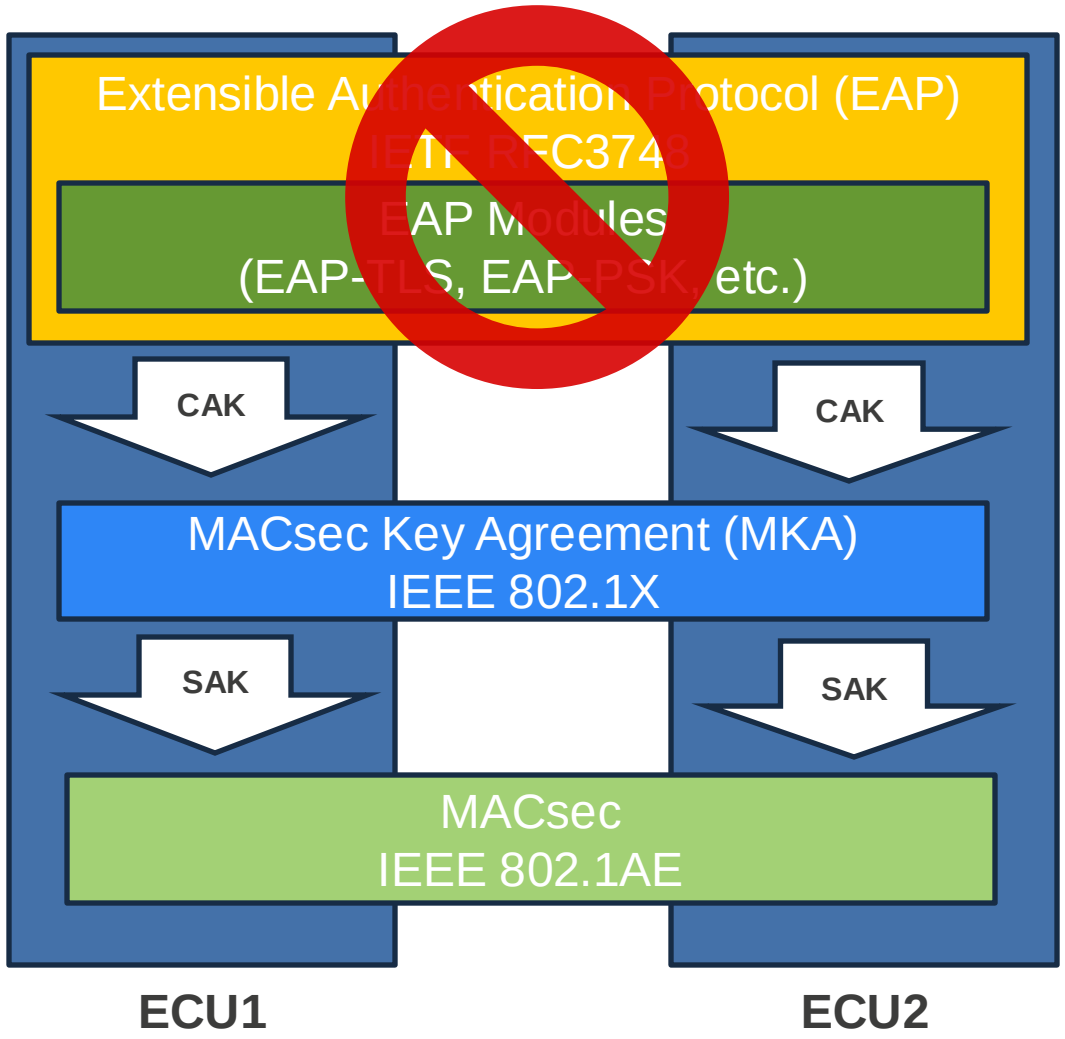
- Skip EAP step and use pre-shared CAK/CKN

CAK provisioned into ECUs during production/service

Faster Startup, less complexity!



MSK – Master Session Key
CKN – Connectivity Association Key Name
CAK – Connectivity Association Key
SAK – Secure Association Key
ICK – Integrity Check Key
KEK – Key Encryption Key



© 2025 Renesas Electronics Corporation. All rights reserved.

OPEN ALLIANCE TC17 – MACSEC AUTOMOTIVE PROFILE

Goal: Define a MACsec profile optimized for automotive use case

- **Initial profile to focus on:**
  - Switched ethernet
  - Point-to-point MACsec only
  - “Integrity without confidentiality” and “integrity + confidentiality” modes
  - Pre-shared CAK
  - Optimized tuning requirements to achieve <10ms MKA

Status:

- Automotive MACsec Profile draft complete now

Next Steps:

- Formal Release upcoming

© 2025 Renesas Electronics Corporation. All rights reserved.

CHALLENGES AND NEXT STEPS

- Key management for installing CAKs and CKNs
- Where to store keys in ECUs? (Hint: Use an HSM!)
- Support shared media (bussed ethernet) (On the TC17 roadmap)

© 2025 Renesas Electronics Corporation. All rights reserved.

© 2025 Renesas Electronics Corporation. All rights reserved.