Technical White Paper

Enhancing the Confidentiality and Integrity of Automotive Ethernet Data Using MACsec

Avtar Dhaliwal

ABSTRACT

As modern vehicles increasingly rely on Ethernet for critical communication, making sure data security against unauthorized access and tampering is imperative. The automotive industry is evolving to meet the growing cybersecurity demands driven by advanced electronic systems and connectivity features. MACsec (Media Access Control Security) provides robust security through encryption and integrity checks, protecting data transmitted over automotive Ethernet networks.

As data transmission speeds and bandwidth requirements in vehicles increase, traditional security measures become insufficient. MACsec addresses these challenges by preventing eavesdropping, replay attacks, and unauthorized device access, thereby enhancing vehicular communication security and contributing to a safer driving experience.

Table of Contents

List of Figures

List of Tables

Trademarks

All trademarks are the property of their respective owners.

1 Introduction to MACsec

Media Access Control Security (MACsec) makes sure the protection of data exchanged between Ethernet-connected devices. Defined by the IEEE standard 802.1AE, MACsec allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.

MACsec operates at layer 2 of the OSI model, the data link layer. Data gets packaged from the previously unstructured data into frames and at the data link layer the format of the data is defined.

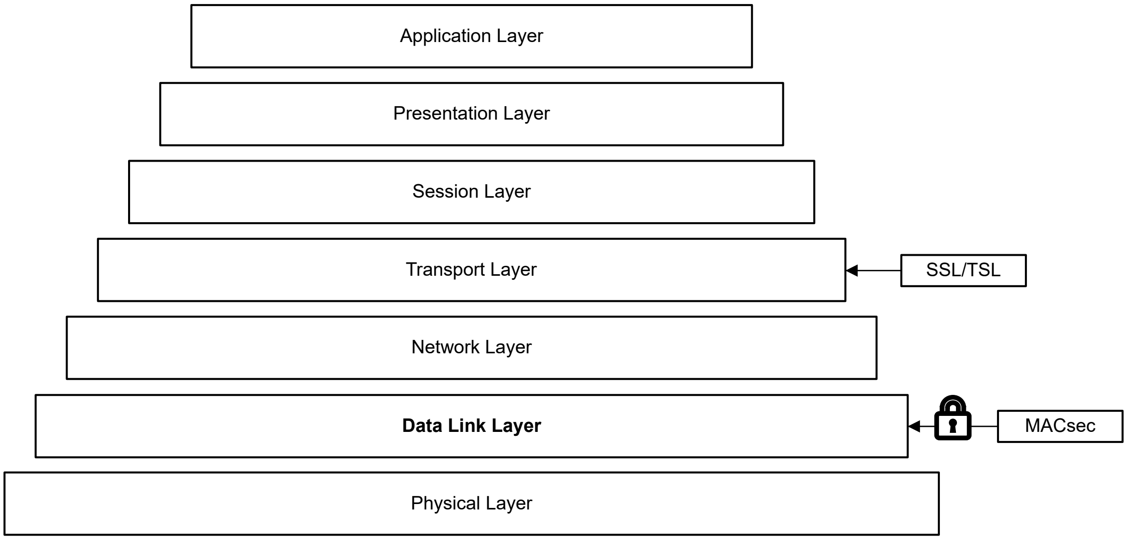

Figure 1-1. OSI Networking Stack

Before MACsec, security protocols like SSL and TLS were widely used, but they operated at the software layer, creating challenges. These protocols required significant CPU and memory resources from the SoC, potentially slowing down performance.

When MACsec is enabled, a bi-directional secure link is established after an exchange and verification of security keys between the two connected devices. A combination of data integrity checks and encryption is used to safeguard the transmitted data.

The sending device attaches a unique MACsec header to all Ethernet frames to be sent, and encrypts the data payload within the frame. The receiving device checks the header and tail for integrity. If the check fails, the traffic is dropped. On a successful check, the frame is decrypted.

2 Critical Role of MACsec in Automotive Security

2.1 Real World Applications

In the automotive sector, the increasing reliance on Ethernet for communication creates many vulnerabilities which can be exploited:

- **Electronic Control Units (ECUs)**
  Communication between various ECUs that control essential vehicle functions such as braking, steering, and engine management.
- **Advanced Driver-Assistance Systems (ADAS)**
  Real-time data exchange for features like collision avoidance, lane-keeping assistance, and adaptive cruise control.
- **Body Control**
  Monitoring and controlling various electronic accessories in a vehicle's body. Locking the doors, seat belt warning systems, or dimming the interior lighting.

2.2 Common Security Threats

In today’s interconnected world, Ethernet applications are susceptible to a multitude of external security threats:

- **Eavesdropping**
  Interception of data being transmitted over the network by an unknown party.
- **Man in the Middle Attacks**
  Insertion into the communication between two devices, potentially altering or stealing data.
- **Replay Attacks**
  The capture and retransmission of data packets to create unauthorized effects.
- **Unauthorized Access**
  Devices without proper credentials accessing the network, potentially gaining sensitive information.

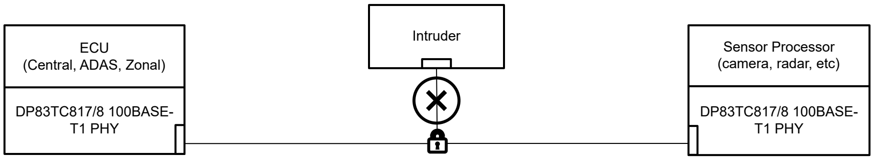

Figure 2-1. External Threat

2.3 MACsec Security Measures

- **Encryption**
  By encrypting data at the data link layer, MACsec prevents eavesdropping and makes sure that intercepted data cannot be read by unauthorized parties.
- **Integrity Checks**
  MACsec performs integrity checks on all data frames, detecting any unauthorized modifications and making sure that data has not been tampered with in transit.
- **Authentication**
  Before establishing a secure link, MACsec requires devices to authenticate themselves, preventing unauthorized devices from joining the network.
- **Replay Protection**
  By including sequence numbers and timestamps in the data frames, MACsec mitigates the risk of replay attacks.

3 How MACsec Works in a System

While MACsec provides encryption at the link layer, IEEE 802.1X offers a way to authenticate devices that want to join a network making sure only trusted devices gain access. MACsec uses a protocol called EAPOL to handle the authentication process, and within MACsec, the MKA protocol facilitates secure key exchange for encrypted communication.

For MACsec to function, the SoC must have a dedicated database to store Connectivity Association Keys (CAKs) and Connectivity Association Key Names (CKNs). In many implementations, an SoC relies on a WPA Supplicant to manage the CAK-CKN database, allowing integration with higher-level authentication protocols and network security standards.

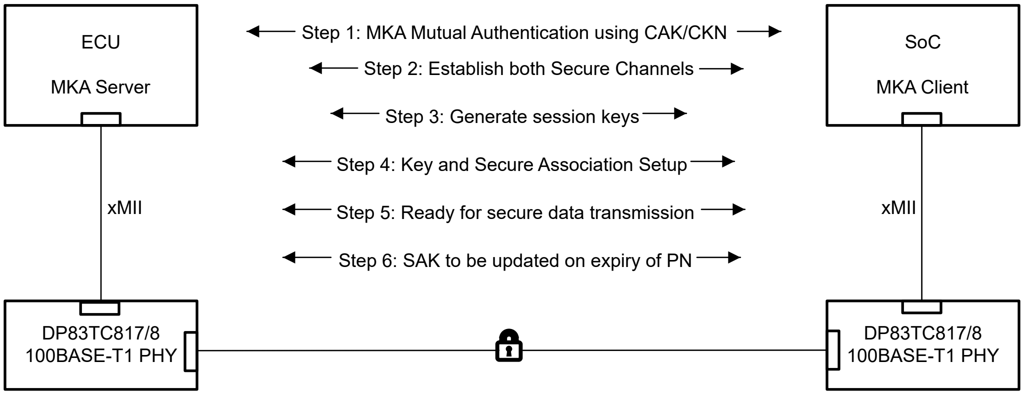
ECU
MKA Server
SoC
MKA Client
Step 1: MKA Mutual Authentication using CAK/CKN
Step 2: Establish both Secure Channels
Step 3: Generate session keys
Step 4: Key and Secure Association Setup
Step 5: Ready for secure data transmission
Step 6: SAK to be updated on expiry of PN
xMII
xMII
DP83TC817/8
100BASE-T1 PHY
DP83TC817/8
100BASE-T1 PHY

Figure 3-1. MACsec System Architecture

Table 3-1. MACsec Key Terms

MACsec Term	Definition
CKN/CAK	The CKN(connectivity association key name) and CAK(connectivity association key) are configured by the user and must match on both ends of the link to initially enable MACsec. This can have to be preset on both processors. CAK is a 32 hex or 64 hex key. CKN is string of hex digits up to 32 characters long.
SecY	An entity that represents the MACsec enabled port or interface on a network device.
Secure Channel (SC)	A logical connection between typically two nodes. The connection provides a secure communication path for MACsec. Responsible for managing the Macsec keys and secure associations for multiple Secy's.
Secure Channel Identifier (SCI)	Associated with each SC. This is a combination of the MAC address of the transmitting device and the port identifier. Associated with each SecY is used to identify participants in the MACsec session.
Secure Association (SA)	Represents the secure association between two MACsec devices, the SA defines security parameters like algorithms and keys, used for securing comms between the devices. Each secure channel contains two secure associations. Contains packet numbering as well.
Secure Association Key (SAK)	Encryption key used for securing devices within an SA. The SAK is dynamically generated and distributed between the devices. Used for encrypting and decrypting using the AES-GCM algorithm data frames, SAK is derived in the MKA process and is unique to a specific secure channel.

4 MACsec Block

An Ethernet frame is a data link layer unit of data and is the underlying Ethernet physical layer transfer mechanism. Each Ethernet frame starts with an Ethernet header, which contains destination and source MAC addresses as the first two fields. The middle section of the frame is payload data including any headers for other protocols carried in the frame. The frame ends with a frame check sequence (FCS), which is used to detect any in-transit corruption of data.

- Destination MAC Address: 6 bytes - Identifies the recipient.
- Source MAC Address: 6 bytes - Identifies the sender.
- EtherType or Length: 2 bytes - Indicates the type of payload or length of the payload.
- Payload: N bytes - The data being transmitted.
- Frame Check Sequence (FCS): 4 bytes - Error-checking code to make sure of data integrity.

MACsec adds security features to the standard Ethernet frame. Below is the structure of a MACsec frame:

- Destination MAC Address: 6 bytes
- Source MAC Address: 6 bytes
- SecTAG: 8-16 bytes - The security tag, which includes key information and security parameters.
- Payload: N bytes (encrypted data)
- Integrity Check Value (ICV): 8 or 16 bytes - Makes sure of integrity of the data.
- Frame Check Sequence (FCS): 4 bytes

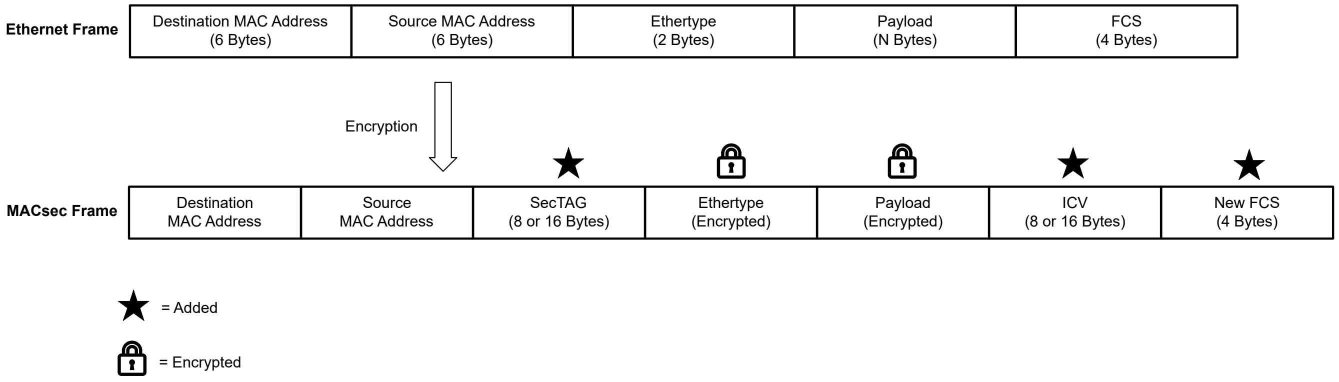

Figure 4-1. Unencrypted Ethernet Frame vs MACsec Ethernet Frame

The SecTAG is a critical part of the MACsec frame, providing essential security information. It contains the following:

- EtherType: 2 bytes - Indicates the frame is a MACsec frame. The MACsec ethertype is 0x88e5.
- TAG Control Information (TCI/AN): 1 Byte - Contains several pieces of info such as encryption/confidentiality presence and the association number.
- Packet Number (PN): 4-6 bytes - Used to prevent replay attacks by numbering the frames.
- Short Length (SL): 1 byte - Indicates the length of the payload (optional).
- SCI (Secure Channel Identifier): 8 bytes - Uniquely identifies the secure communication channel.

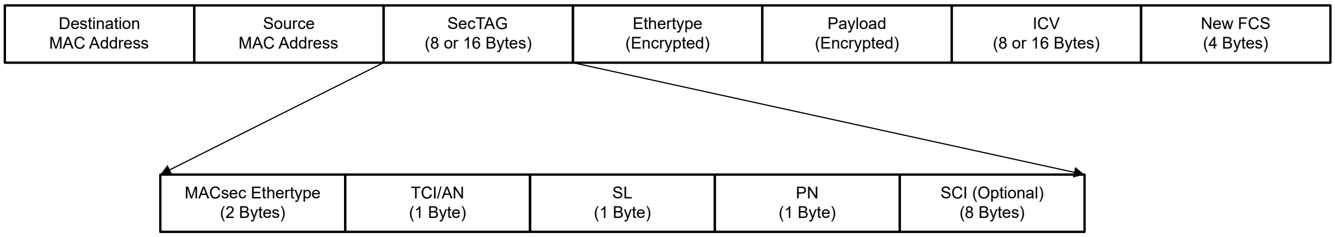

Figure 4-2. MACsec SecTAG

MACsec Features implemented in the MACsec Frame:

- EtherType: In both normal and MACsec frames, the EtherType field indicates the type of payload. For MACsec, it specifically identifies that the frame contains MACsec data.
- SecTAG:
  - SCI: The secure channel identifier makes sure that the frame belongs to a specific secure channel.
  - AN: Distinguishes different security associations within the same channel, allowing multiple secure connections simultaneously.
  - PN: Provides protection against replay attacks by making sure each frame has a unique number.
- Payload: In a MACsec frame, the payload is encrypted. Making sure confidentiality of the data being transmitted.
- ICV: Provides integrity by making sure the frame has not been altered during transit. The cryptographic checksum is calculated over the entire frame (except the FCS) using preshared keys.

5 MACsec at the PHY Level

The DP83TC817 enables robust MACsec implementation at the PHY level, delivering significant benefits across the entire system.

- Offloading encryption and decryption tasks from the SoC reduces system resource consumption, leading to lower costs and freeing up the SoC for other critical functions.
- Implementing MACsec at the PHY level optimizes overall performance, offering a more streamlined and secure data flow while minimizing latency.

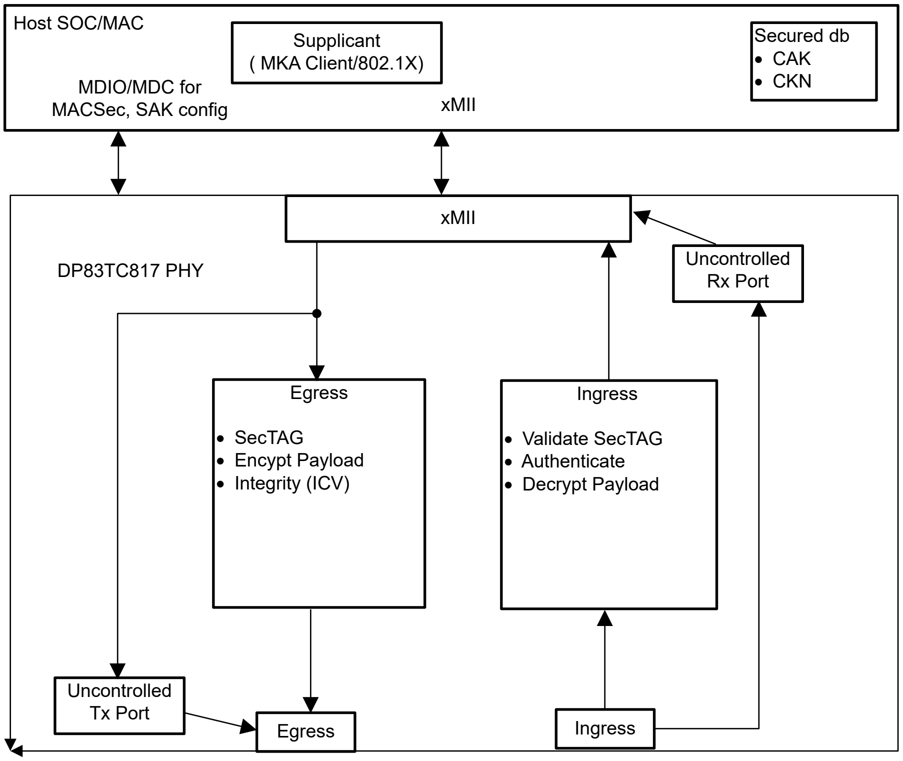

Figure 5-1. MACsec Ethernet PHY

MACsec features supported in the DP83TC817:

- Authentication, encryption at line rate
- Cipher suites: GCM-AES-XPN-128/256, GCMAES-128/256
- Secure Channel: Total 16 SAK enabling 8 Tx/Rx SC
- Auto rollover support for SAK
- Window replay protection

6 Conclusion

As the automotive industry moves towards integrating further electronic systems and sophisticated connectivity features, the need for robust security becomes more important.

MACsec offers a comprehensive design for securing automotive Ethernet networks, providing encryption and integrity checks to safeguard data. By addressing vulnerabilities such as eavesdropping, replay attacks, and unauthorized access, MACsec makes sure of secure and reliable communication within vehicles.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265