Secure On-board communication (secoc)

Secure on-Board Communication

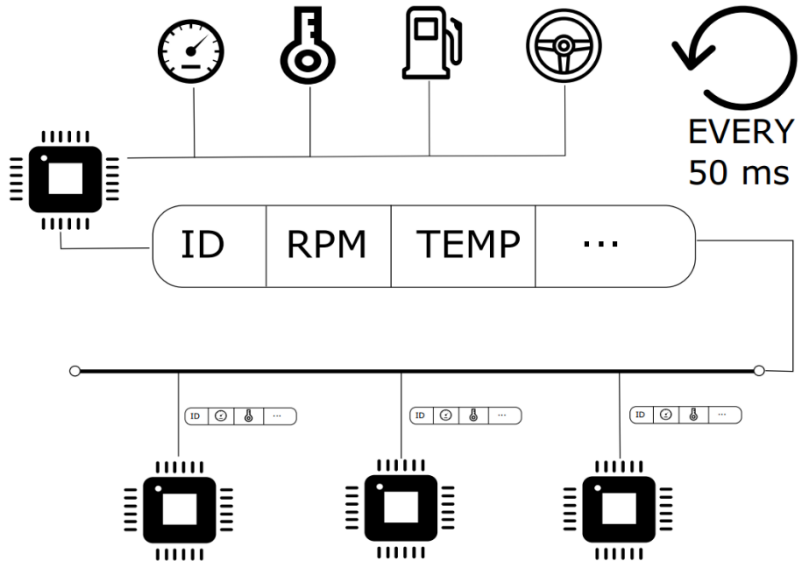
Pre-Requisties

- What is an ECU
- How does the multiple ECUs communicate
- AUTOSAR architecture
- Crypto Architecture
- Basics of crypto algorithms

Secure on-Board Communication

Why in-vehicle communication security required?

- Any node could send RPM message
  - Would be accepted as genuine
- System that prohibits this is necessary
  - But maintains advantages of implicit availability



Secure on-Board Communication

Overview

SecOC aims for resource-efficient and practicable authentication mechanisms for critical data on the level of PDUs.

– this ensures that received data comes from the right ECU and has the correct value.

Authentication: a service related to identification, applies to both entities and information.

1. Entity Authentication:
   2 parties entering into a communication should identify each other.

2. Data Origin Authentication (Data Integrity):
   Data has not been manipulated in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source.

* Data manipulation includes such things as insertion, deletion, and substitution.

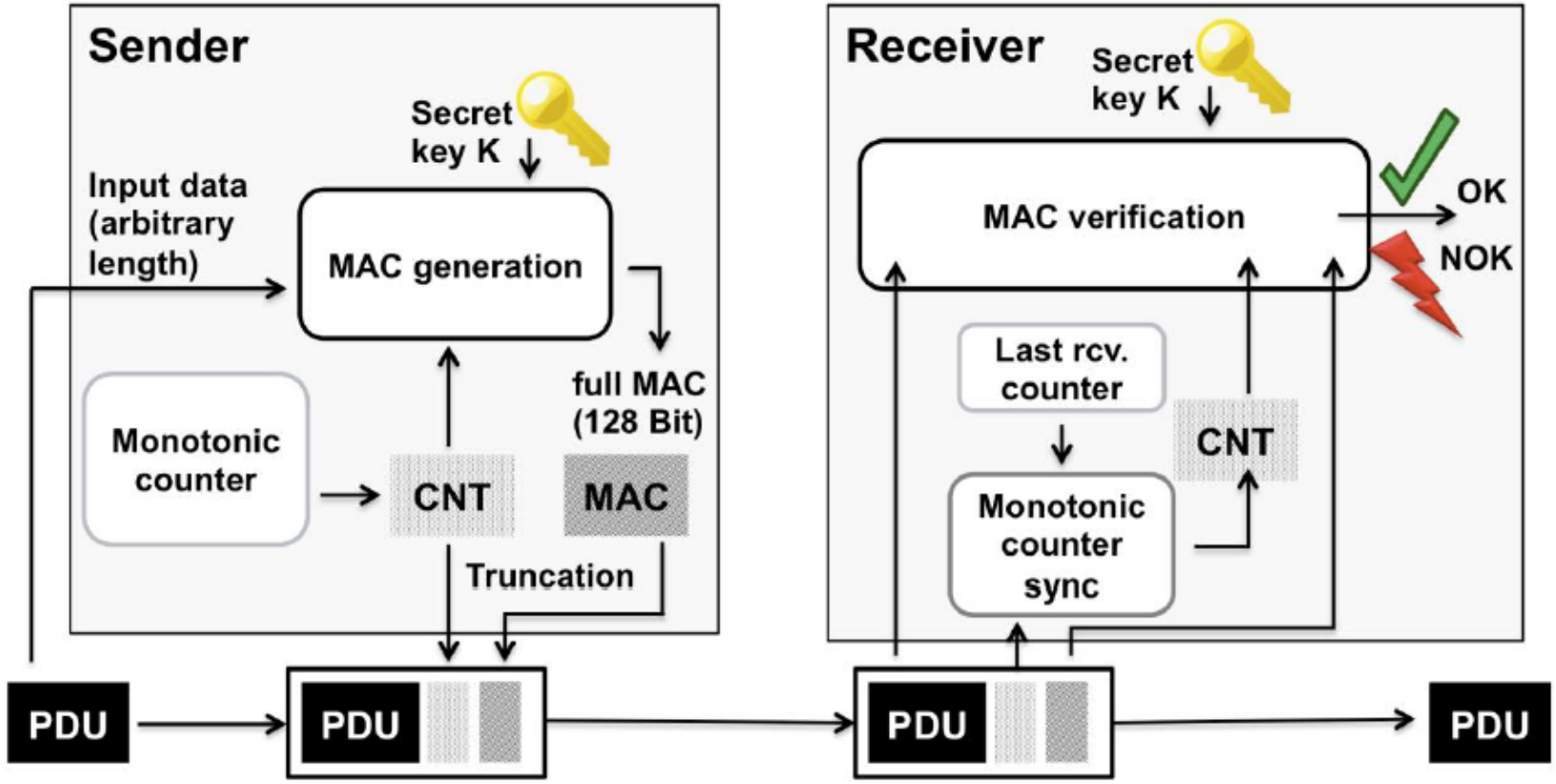
Secure on-Board Communication

Overview

For each message:
- authenticator
- freshness value

is appended

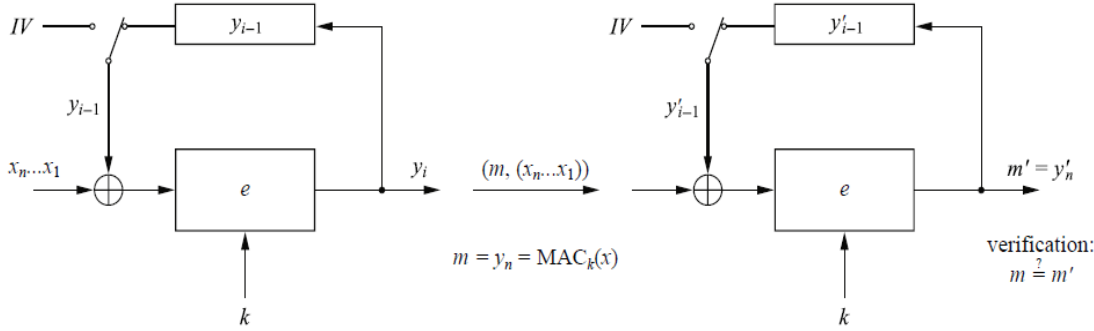
Usually, truncated CMAC and FV are appended to the message.
- 24-bit CMAC
- 8-bit FV



Secure on-Board Communication

Algorithm

Authenticator creation: AES128 CMAC



Due to using of secret key and the high security level of AES,

1. attackers are unable to manipulate the critical data during transmission -- data integrity
2. Identity of entities entering into the communication is guaranteed -- entity authentication

CMAC: CBC-MAC (Cipher Block Chaining based Message Authentication Code)

CBC is an operation mode of block cipher:

1. Encryption of all blocks are 'chained' such that y_i depends not only on x_i, but also on $x_1,\ldots,x_{i-1}$.
2. The encryption is randomized by using an initialization vector(IV).

MAC is a function of the message and the shared secret key, sender computes the MAC value, append it to the message and receiver re-computes it and verifies with the value received.

Due to the symmetric characteristic of CMAC, truncation of the authenticator is possible and may be desired when the message payload is limited in length and does not have sufficient space to include the full authenticator.

Secure on-Board Communication

Algorithm

Threat of Replay Attack:

An attacker eavesdroping the communication channel may:

Reuse the authentication message to get authorized to participate in the communication

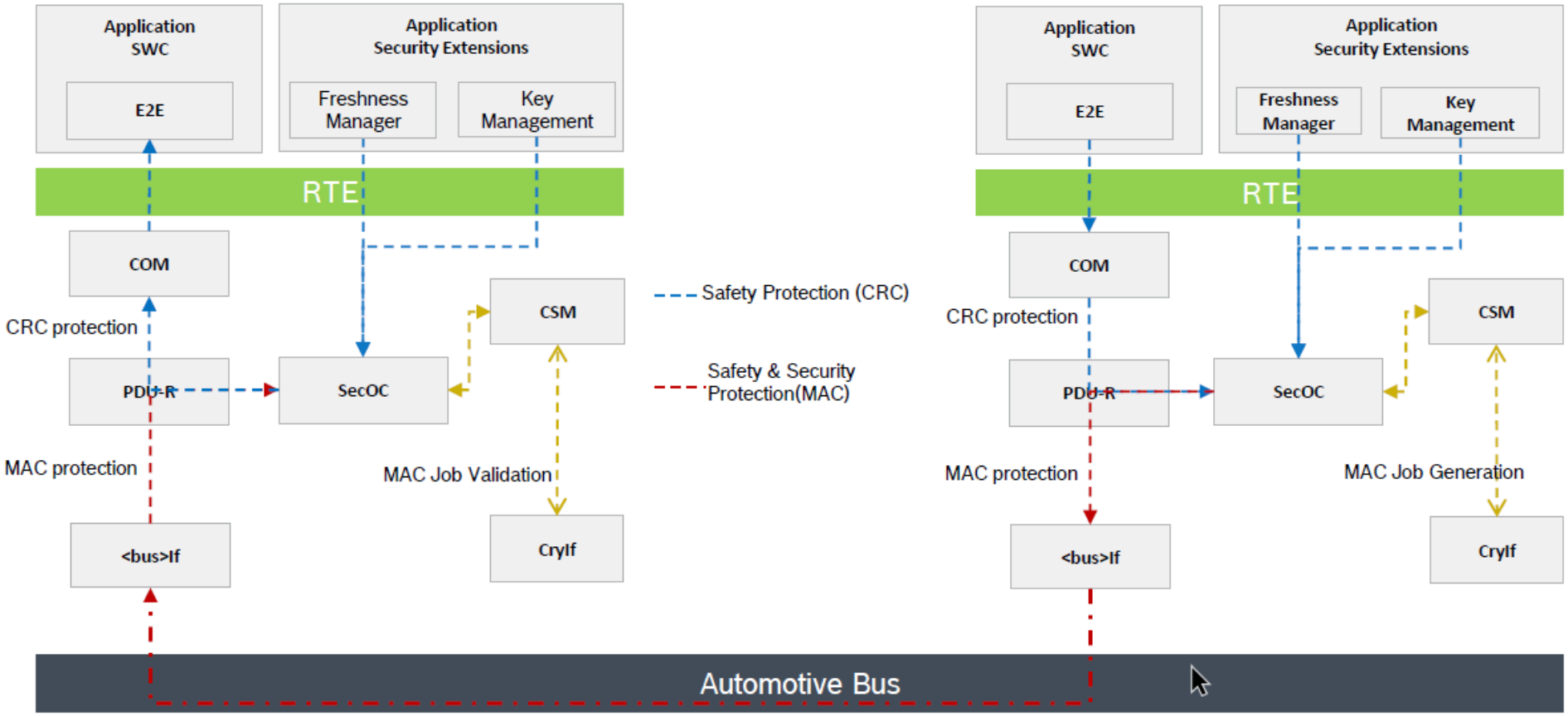
Re-send the message with valid authenticator to interfere the normal communication

Countermeasures to Replay Attack:

- Freshness values:
  - Counter
  - Timestamp

Secure on-Board Communication

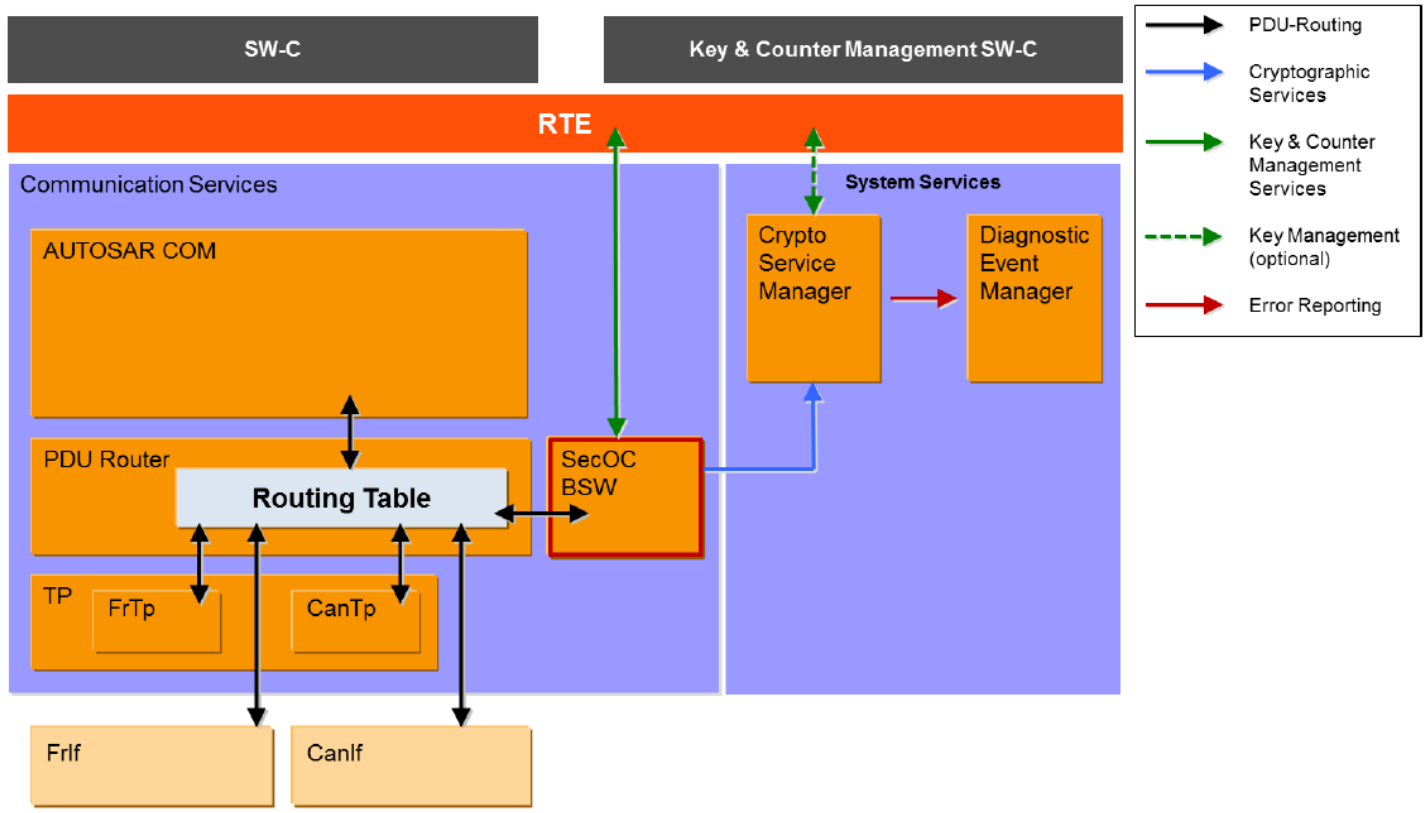
Flow of Secure PDUs



Secure on-Board Communication

Dependencies to Other Modules

- Dependency to PduR
- Dependency to CSM
- Dependency to RTE



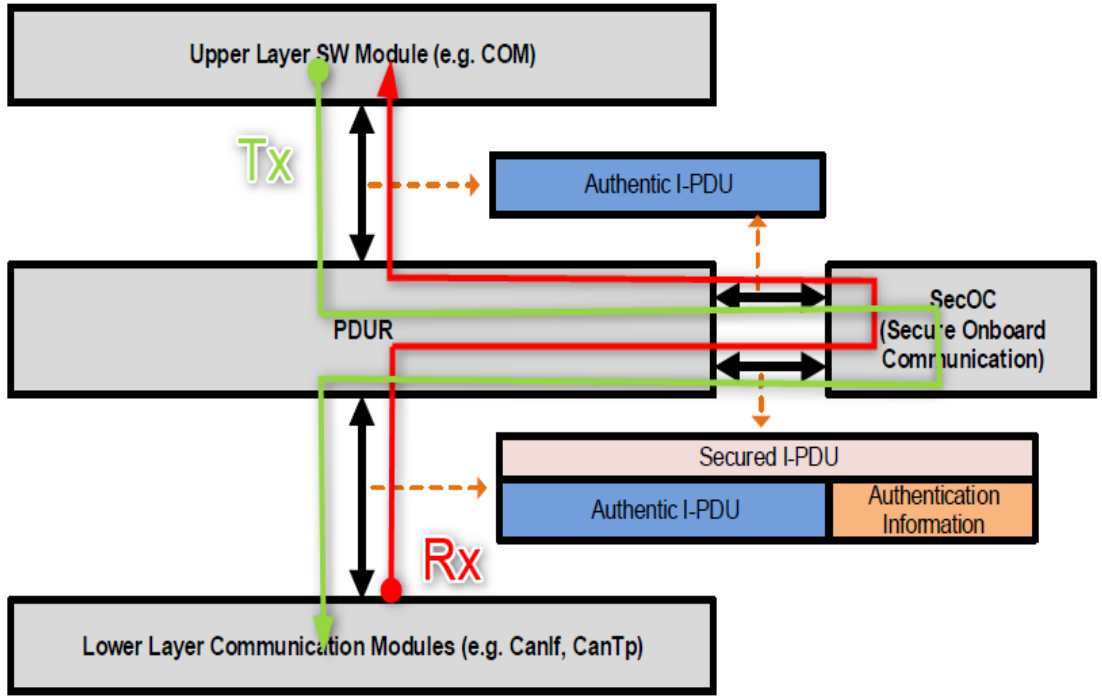
Secure on-Board Communication

Dependency to PduR

Dependency to PduR

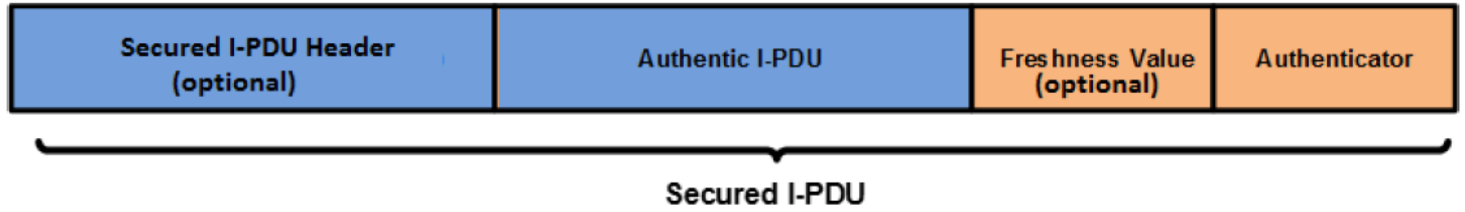
The SecOC module is arranged next to the PDU-Router in the layered architecture of AUTOSAR;

SecOC shall forward MetaData received in an authentic PDU unchanged to the corresponding secured PDU, and vice versa, depending on the API and capabilities of the PduR.



Secure on-Board Communication

PDU structure



Secured I-PDU =

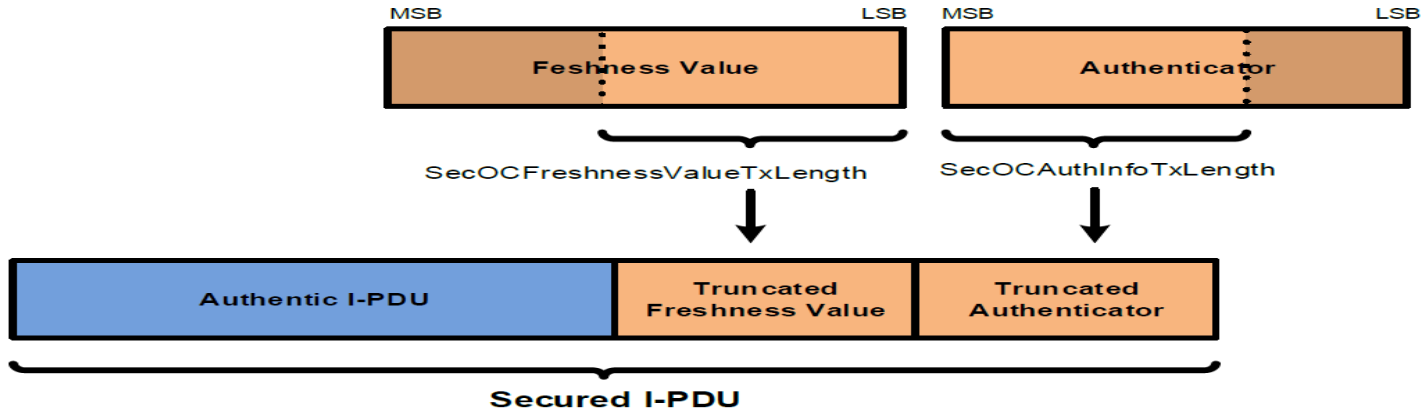
Authentic I-PDU | Trunc FV | Trunc CMAC

Data covered by Authenticator: Data ID | Authentic I-PDU | **Complete** FV

If truncation is possible,

the **Authenticator** should only be truncated down to the **most significant bits** of the resulting Authenticator generated by the authentication algorithm

the **Freshness Value** shall be truncated down to the **least significant bits** of the freshness value.



Secure on-Board Communication

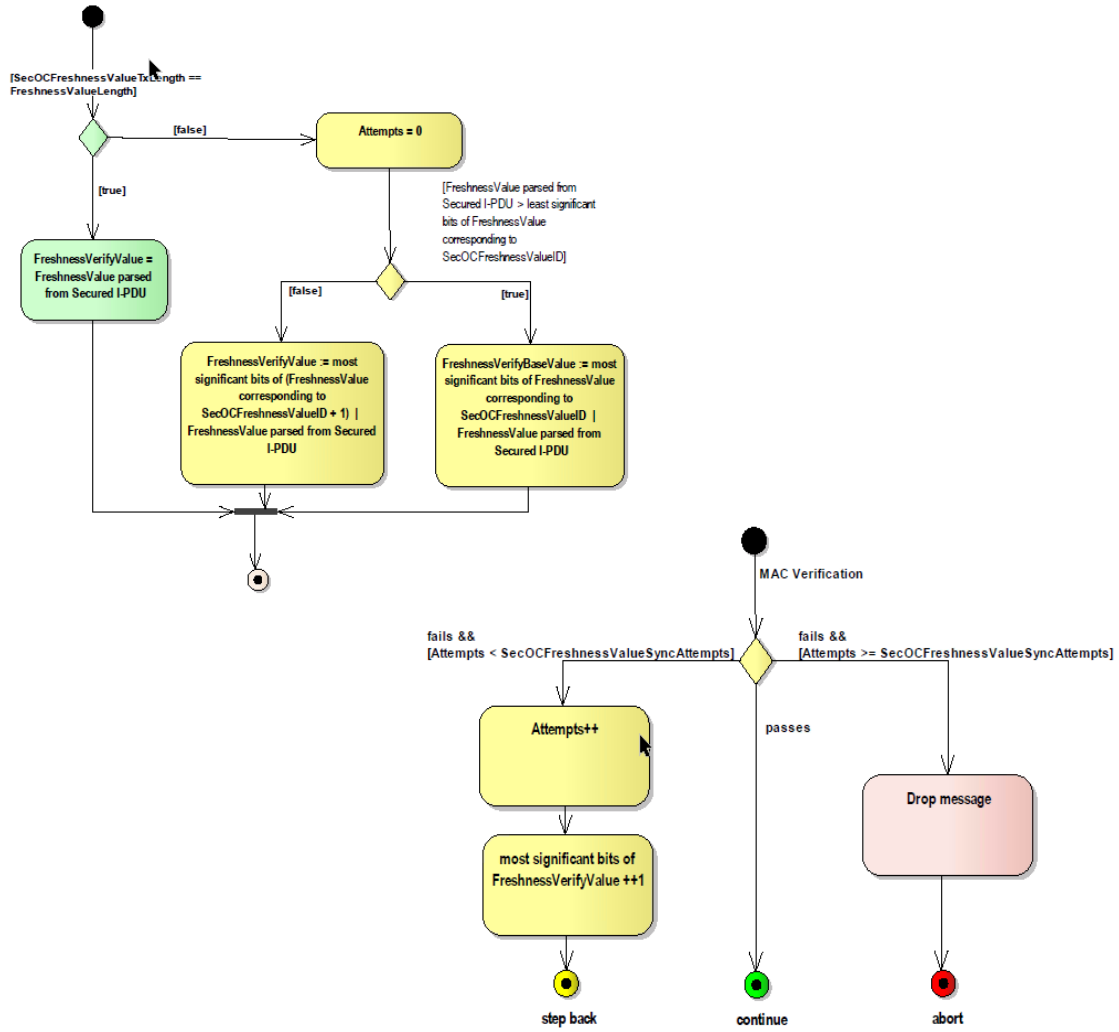
Authentication and Verification of I-PDU

- **Authentication of I-PDU**

  Prepare Secured I-PDU
  Construct Data for Authenticator
  Generate Authenticator
  Construct Secured I-PDU
  Increment Freshness Counter
  Broadcast Secured I-PDU

- **Verification of I-PDU**

  Parse Authentic I-PDU, Freshness Value and Authenticator
  Get Freshness Value from Freshness Manager
  Construct Data to Authentication
  Verify Authentication Information
  Send Confirmation to Freshness Manager
  Pass Authentic I-PDU to upper layer

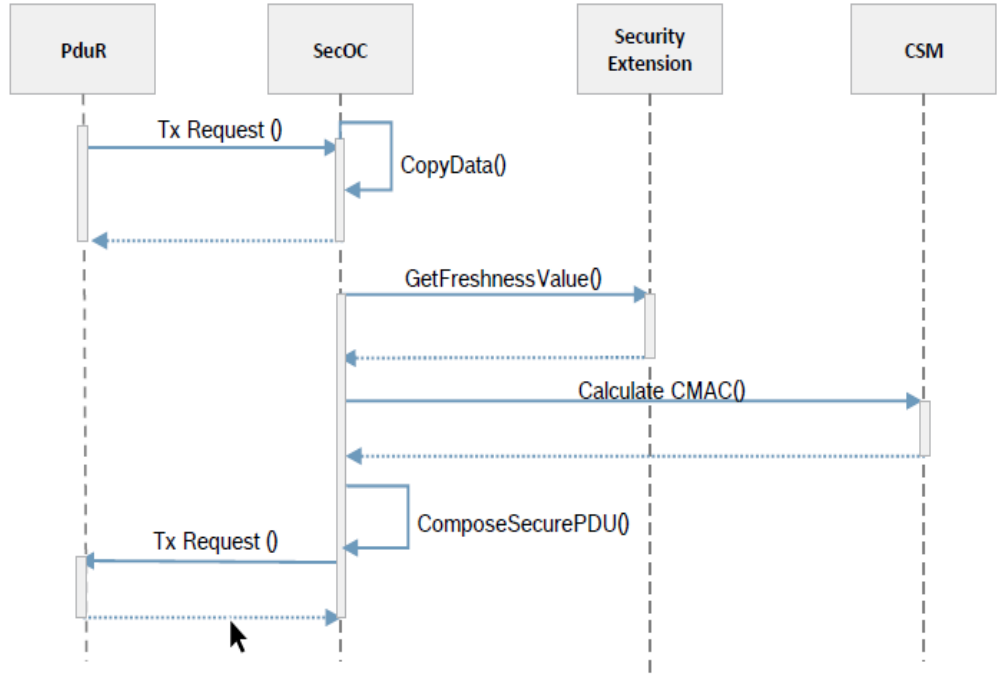


Secure on-Board Communication

Sender Side

The Secure Onboard Communication ensures the integrity and authenticity of the transmitted messages in the following way:

- Upon transmission of a PDU which is secured, the AUTOSAR module SecOC calculates a message authentication code (MAC).
- This Calculation is done over the DataID, the PDU data and a freshness value (FV)using a secret key K derived from the Dat ID.
- The SecOC append parts of this MAC(truncated MAC, TMAC) and parts of the freshness value (truncated FV, TFV) to the authentic PDU in order to form the secured PDU.

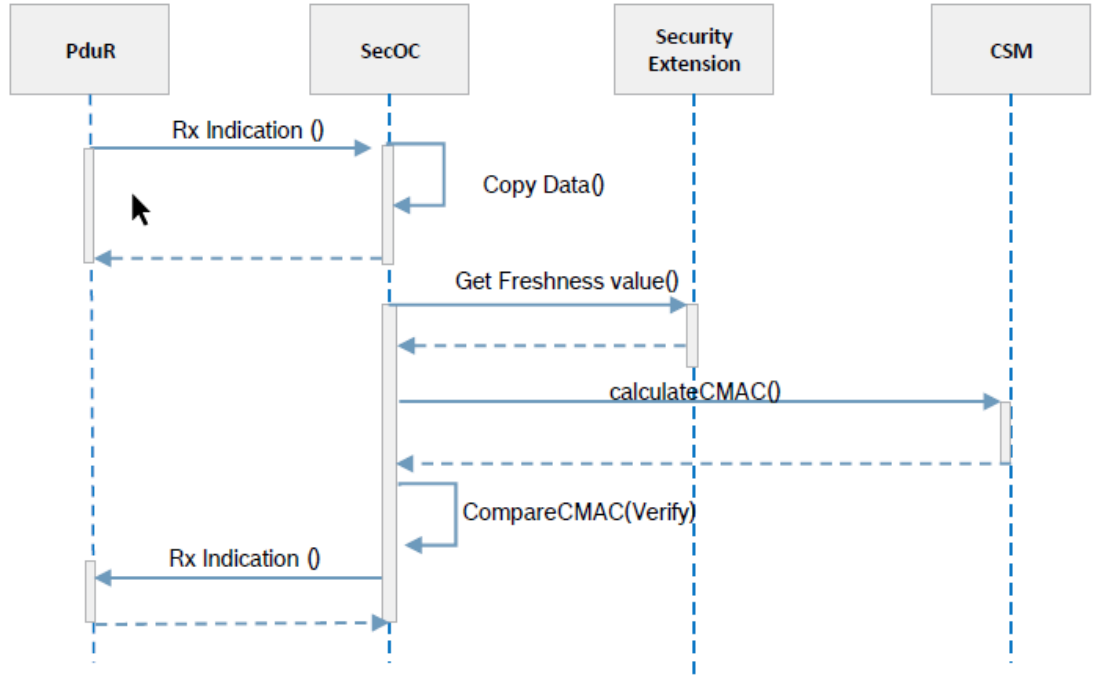


Secure on-Board Communication

Receiver Side

The Secure-On-board Communication ensures the integrity and authenticity of the received messages, in the following way:

- Upon reception of a secured PDU, the AUTOSAR module SecOC verifies the message authentication code(MAC) of the secured PDU.
- The same MAC calculation and comparing parts of the resulting value with the received truncated MAC.
- If the verification of a secured PDU succeeds, the SecOC module shall forward the verified PDU to the AUTOSAR module PduR which in turn shall forward it to the respective upper layer and signal the reception of this PDU.
- If the verification of a secured PDU fails, the SecOC module shall not forward the received PDU to the PduR but log the failed verification attempt for this PDU in the ECU's Security Event Log.



Thank you!

Bosch
Global
Software
Technologies
alt_future