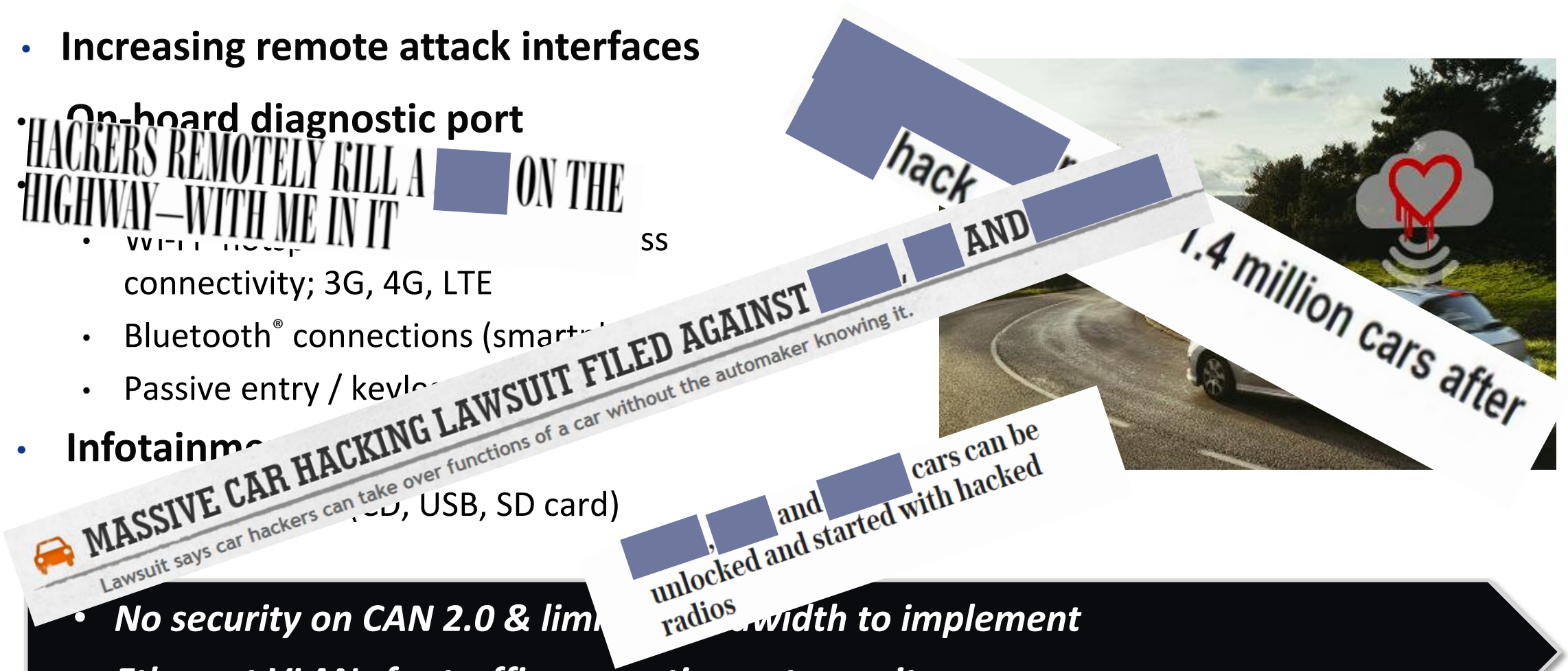
Automotive Network Security

Presenter: Peter Kwak – Principal Embedded Solutions Engineer

MICROCHIP

Attack Surface Keeps Growing

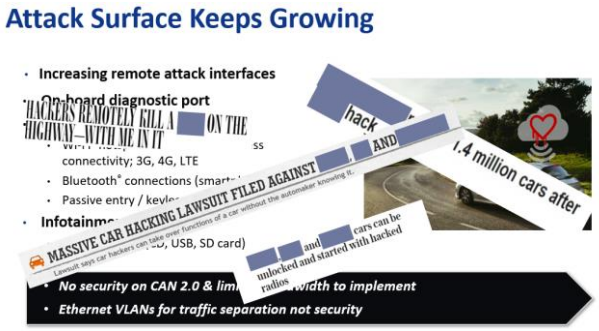
- **Increasing remote attack interfaces**
- **On-board diagnostic port**
- **Infotainm**
  - connectivity; 3G, 4G, LTE
  - Bluetooth® connections (smart
  - Passive entry / keyl
  - , USB, SD card)



- ***No security on CAN 2.0 & lim width to implement***
- ***Ethernet VLANs for traffic separation not security***

MICROCHIP

Drivers Towards Automotive Security



ISO/IEC 9797-1 / ISO 26262
ISO 27001 / IEC 62443
J3061/ J3101

Automotive Security

NHTSA

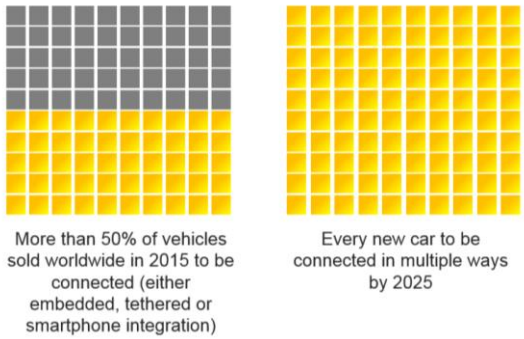
National Highway Traffic Safety Administration

CAN

CAN FD

OEM

Security Specifications



MICROCHIP

Automotive Security Priorities

Secure Key Storage

Secure Boot & Secure FW Update

Message Authentication

(Secure Communication)

Automotive Security IC Attributes

- **Secure Key Storage**
  - CAN communication keys & certificates storage
  - CAN communication session key(s) storage
  - Trusted Ethernet nodes with secure boot & firmware update
  - TLS key protection
- **Ease of Integration**
  - Less code = lower cost
  - Minimal code updates on node microcontroller (MCU)
- **Node Authentication & Key Agreement**
  - ECU authentication & key agreement scheme
  - Encrypted and authenticated command sessions
- **Hardware Crypto Accelerators**
  - Symmetric and asymmetric algorithms
  - High-quality random number generators (SP 800-90)
  - HMAC & CMAC for serial communication protection
- **Automotive Grade-1**

Automotive Security Challenges

- **Scalability:** The complexity of the automotive network architecture requires a scalable and incremental approach. It is almost infeasible to upgrade all systems at the same time
- **Interoperability:** With multiple network protocols and multiple Tier-1s supplying ECUs for the same bus, standardization and/or flexibility is needed when enhancing the system for security purposes
- **Maintain existing performance:** Response times, power-up times and performance calculations, such as bus-load and throughput for the CAN network, all need to be taken into account
- **Hardware protection:** As cars are being connected, there is a need for dedicated HW-protected security. Adding keys in SW is not enough
- **Infrastructure/Ecosystem/Provisioning:** Provisioning concepts and supply chain are becoming more important for OEMs, while working with different Tier-1s, and applying a common security concept
- **Preserve legacy where needed:** When the only change in the ECU is the security enhancement, there should be no need to rearchitect SW and ECU – an incremental approach should be preferred. This helps keeping migration effort under control

How Keys are Protected Matters!

Scalability

Interoperability

Maintain Performance

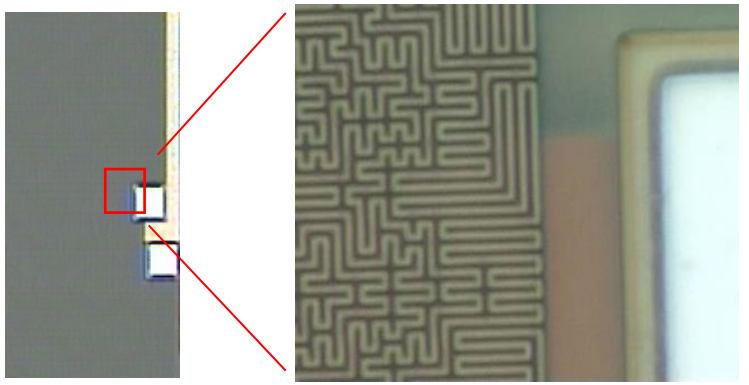
Hardware Protection

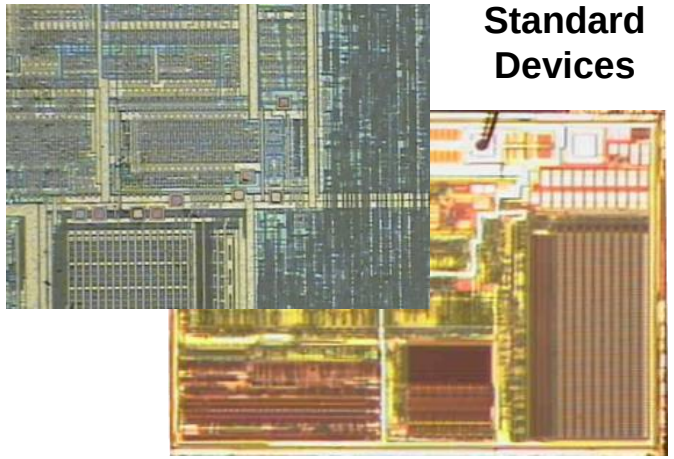
Ecosystem Provisioning

Preserve Legacy

- **Strong Multi-level HW Security**
  - Active shield over entire chip
  - All memories internally encrypted
  - Data independent crypto execution
  - Randomized math operations
  - Internal state consistency checking
  - Voltage and temperature tampers
  - Internal clock generation
  - Secure test methods, no JTAG
  - No debug probe points, no test pads
- **Designed to Defend Against**
  - Microprobe attacks
  - Timing attacks
  - Emissions analysis attacks
  - Fault, invalid command attacks
  - Power cycling, clock glitches

HW Crypto Devices





Standard Devices

Secure Boot & Secure FW Update

Scalability

Interoperability

Maintain Performance

Hardware Protection

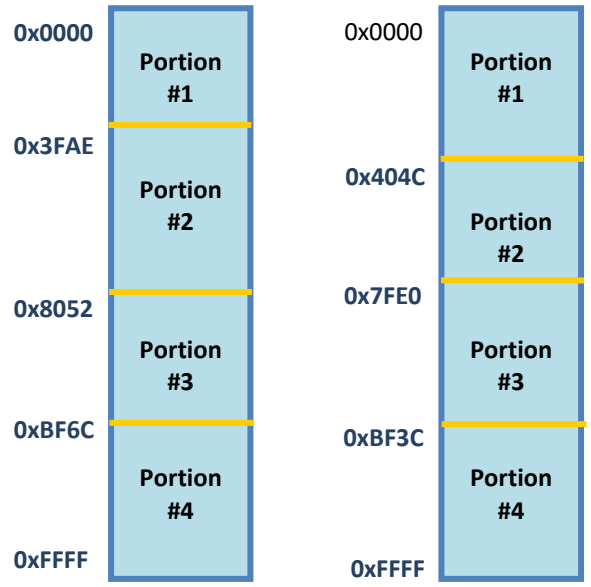
Ecosystem Provisioning

Preserve Legacy

- **Only allow ECU to be installed with (in factory) or updated with (download in field) “authentic” software**
- **Identify / only execute ECU software that has not been tampered with**
- **Requires secure storage for keys, hash values …**
- **Impact on ECU startup time**
- **Highly Configurable**
  - ECU or Security IC hashes FW
  - Full or partial
  - Unique boot code signature for every ECU
- **Works with “Any ECU/Any MCU”**

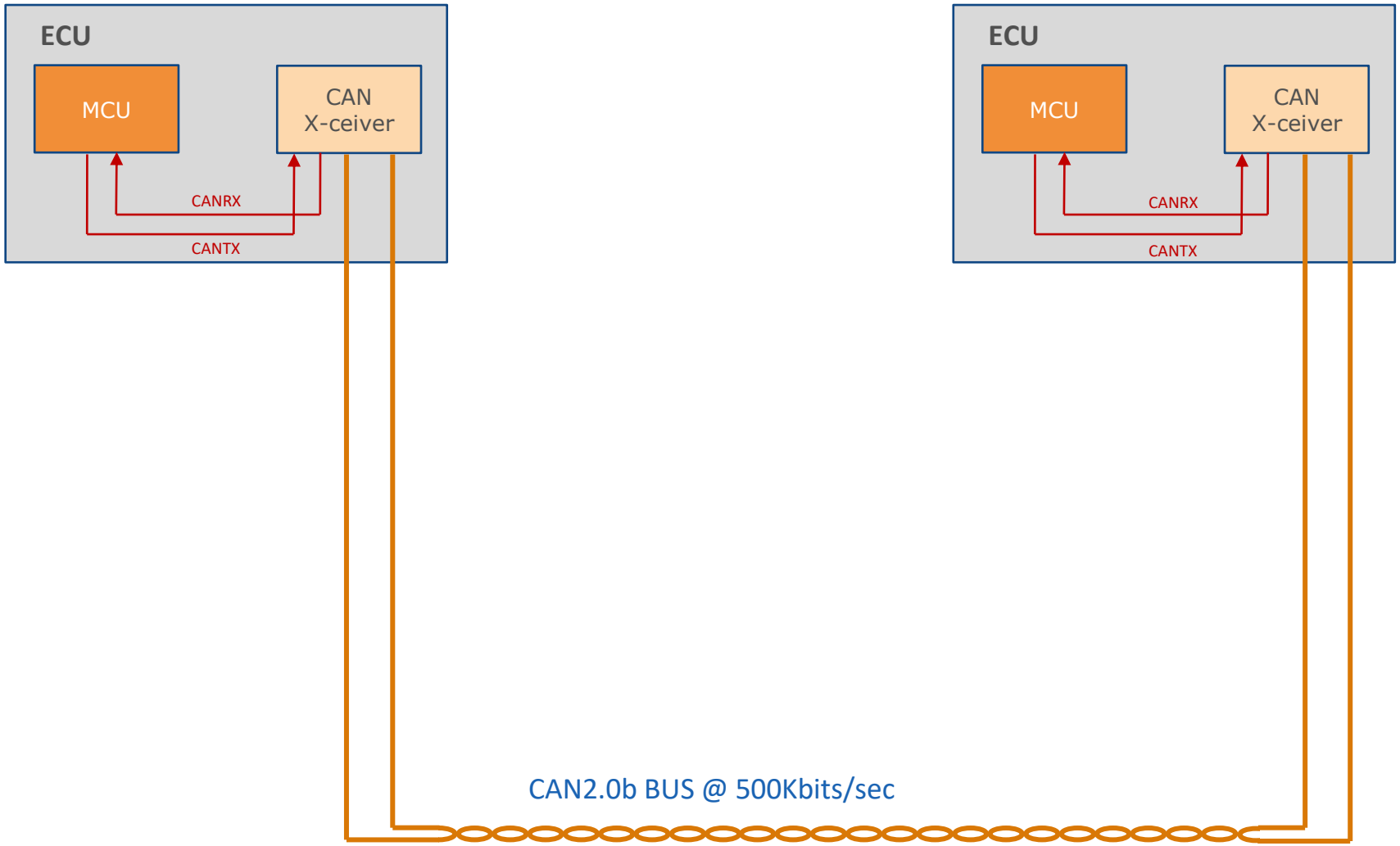
Illustration

Program memory
4 Portions
Address boundary variation



MICROCHIP

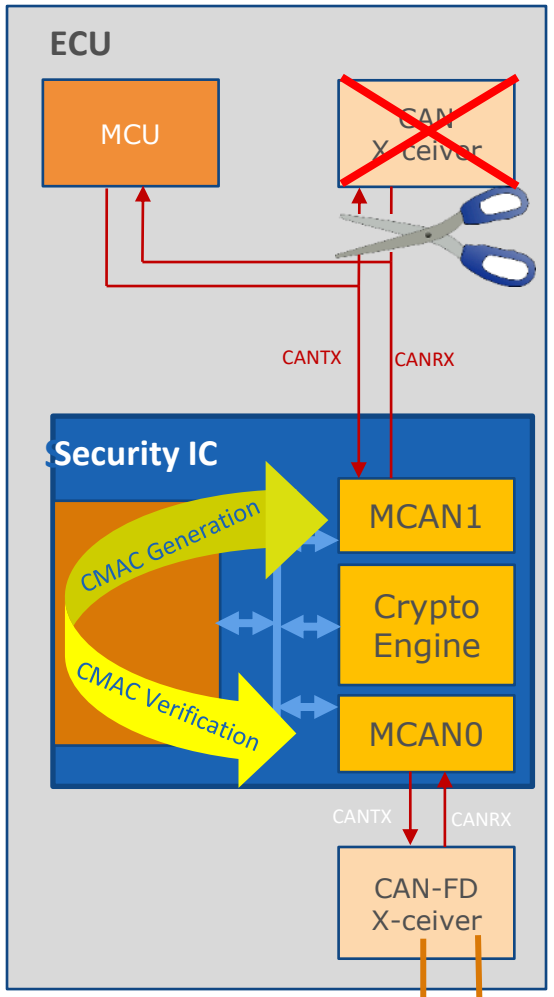
Typical ECU Today



MICROCHIP

Adding Security IC to ECU

- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy

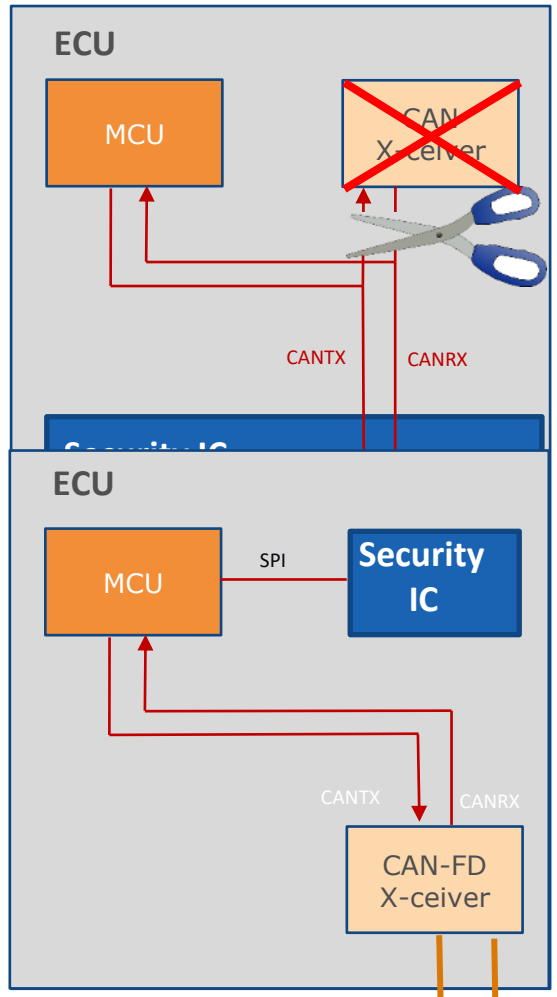


Minimize ECU HW Impact: S-IC appears as CAN transceiver to the Host MCU

Minimal ECU SW Impact: Authentication transparent to the Host MCU

Store & Forward

For new ECU designs: S-IC can also appear as side-by-side companion

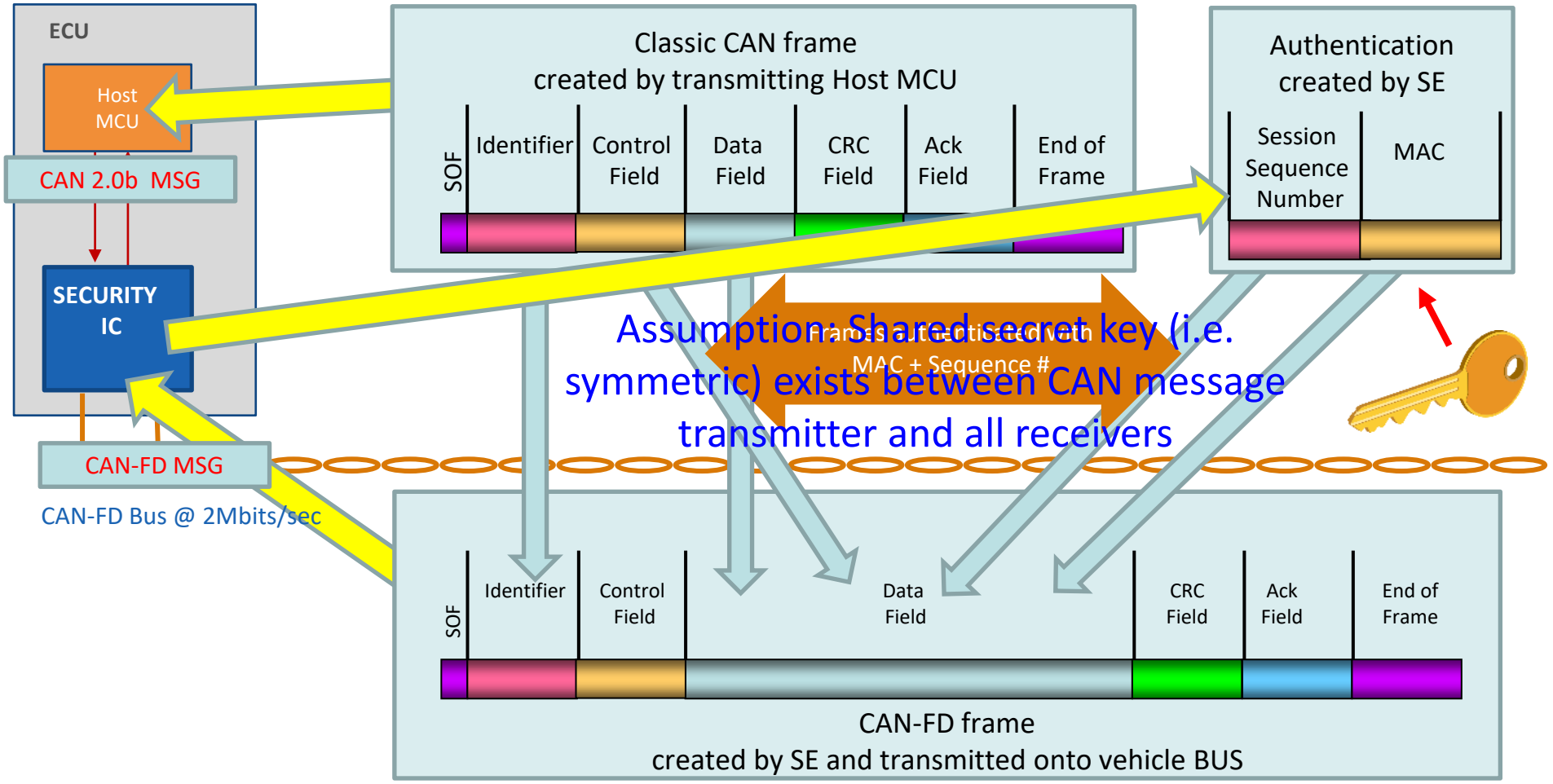


CAN-FD Bus @ 2Mbits/sec

MICROCHIP

How it Works: Transmit Side

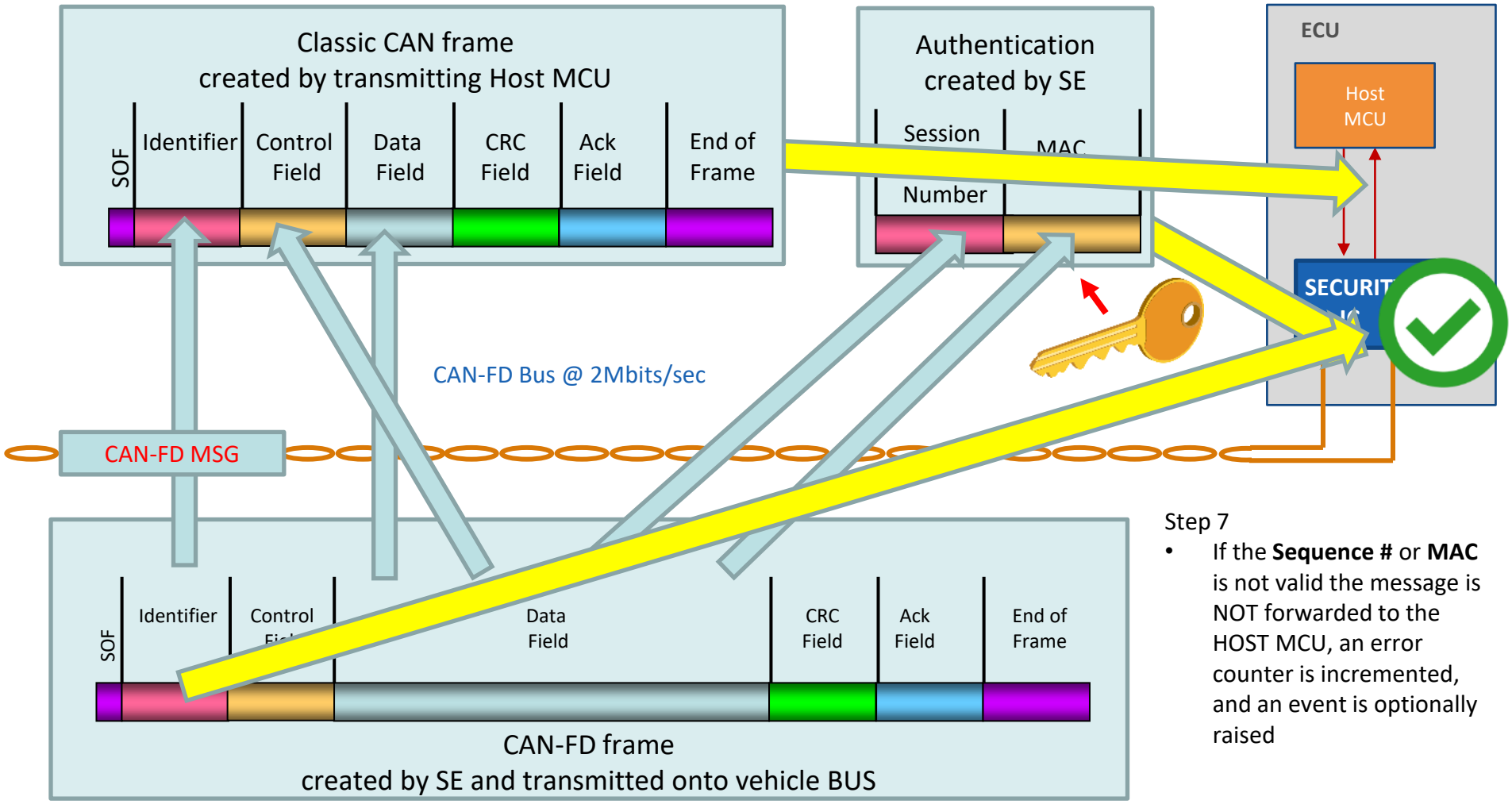
- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy



MICROCHIP

How it Works: Receive Side

- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy



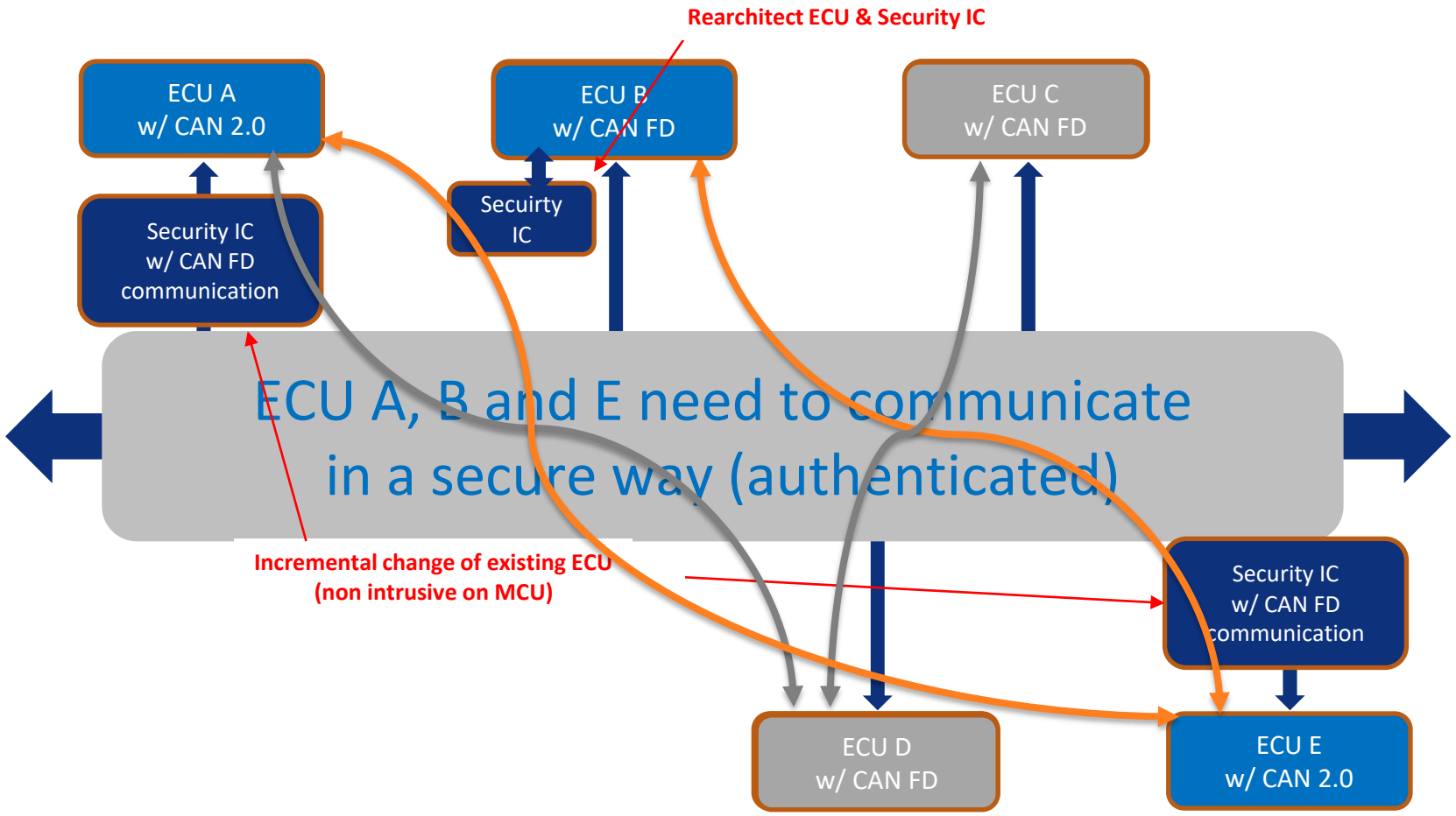
Step 7

- If the **Sequence #** or **MAC** is not valid the message is NOT forwarded to the HOST MCU, an error counter is incremented, and an event is optionally raised

MICROCHIP

Enhance Existing CAN Networks

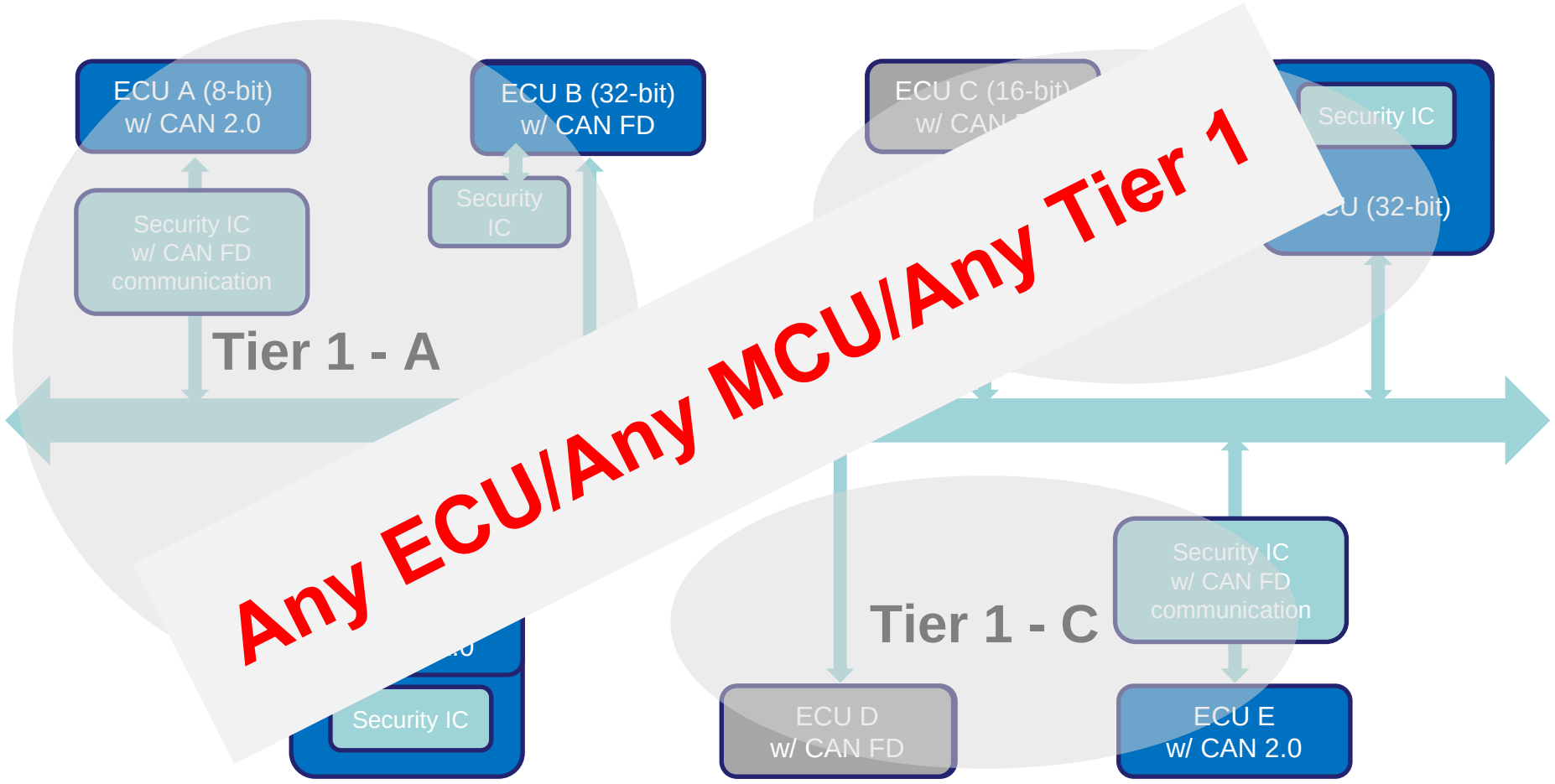
- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy



MICROCHIP

Enhance Existing CAN Networks

- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy



MICROCHIP

CAN-FD Frame Details

Scalability

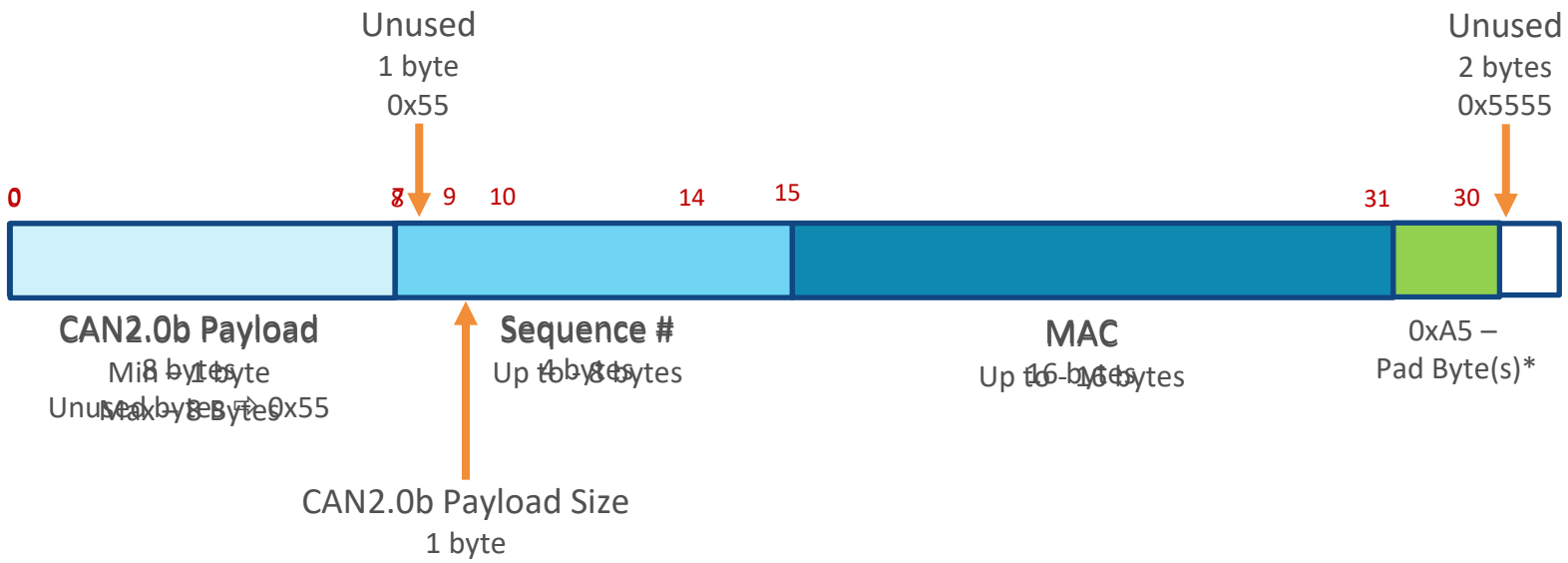
Interoperability

Maintain Performance

Hardware Protection

Ecosystem Provisioning

Preserve Legacy

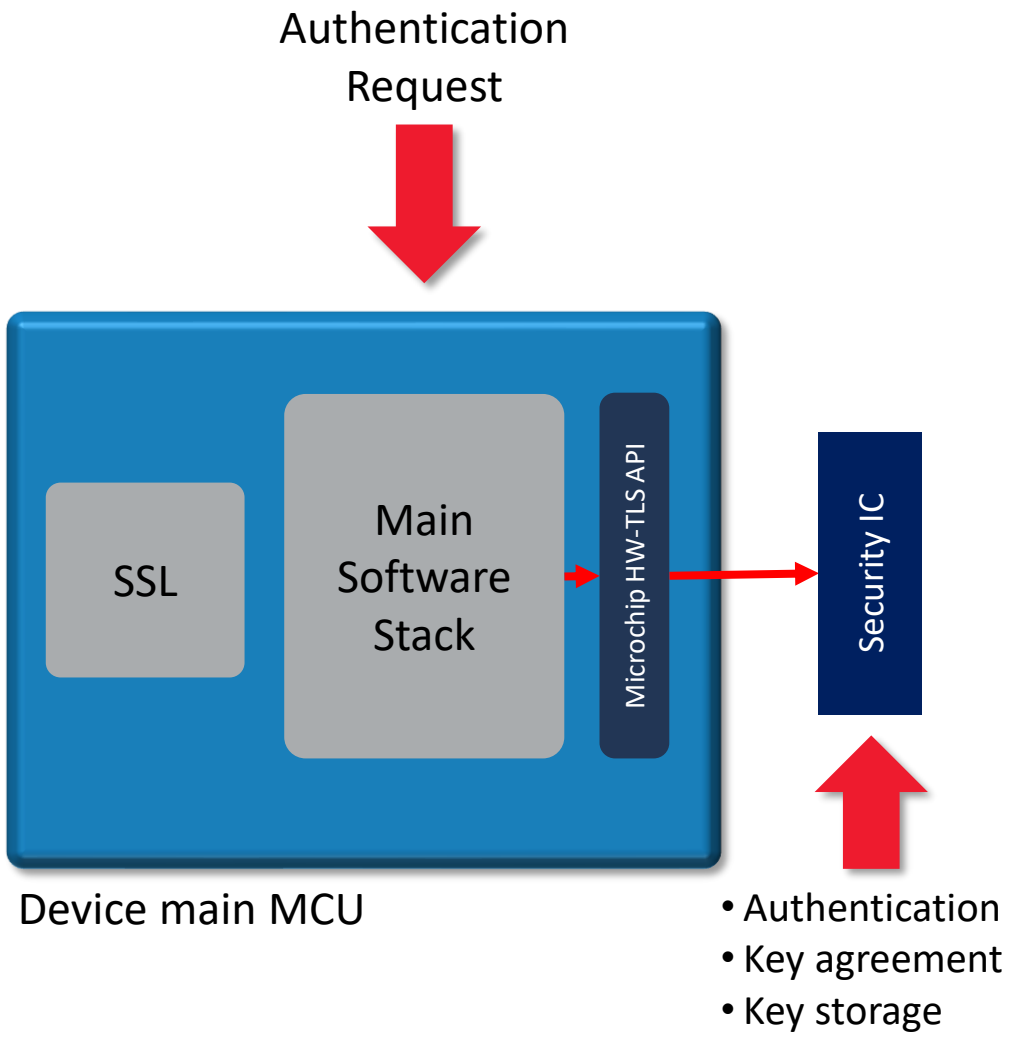


- **AUTOSAR frame format**
- **CAN-FD message size: 32 bytes**
- **Smaller size possible with reduced MAC / Sequence # (24/20 bytes)**
- **Configurable for various specifications, i.e. AUTOSAR, JASPAR, etc.**
- **Pad byte(s) – 0xA5 is added to get to valid CAN-FD frame size**

- **CAN-FD message size: 32 bytes**
- **Smaller size possible with reduced MAC / Sequence # (24/20 bytes)**

Hardware Secured TLS

- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy



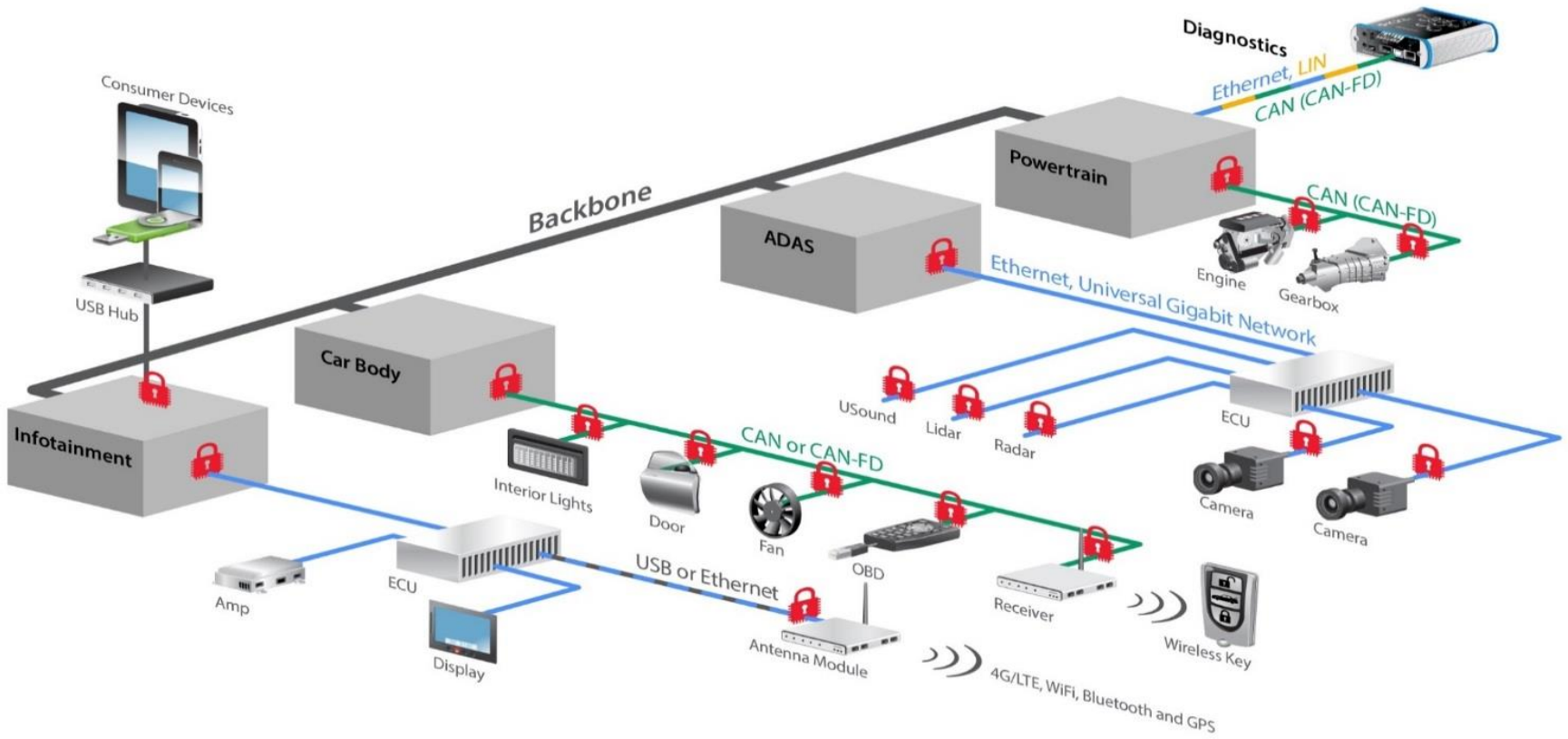
- **Hardware-TLS offloads cryptographic functions from the device MCU**
  - Access via HW-TLS API
  - Security IC handles all computation
  - Minimal code space and computational load
  - ***Keys are generated and protected in secure hardware***

• ***Keys are secure!***

MICROCHIP

Security Considerations at Every Node in the Vehicle

- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy



- ***SAE J3061*** Consider risks associated with each vehicle system

MICROCHIP

Summary

- Scalability
- Interoperability
- Maintain Performance
- Hardware Protection
- Ecosystem Provisioning
- Preserve Legacy

Three Pillars for Automotive Security

Secure Key Storage

… do you remember?

Thank You