

AUTOMOTIVE SECURITY CHALLENGES AND THE AUTOMOTIVE SERDES ALLIANCE SOLUTION.

Dr. Lars Völker
Stefan Lachner

2020-10-14

INTRODUCTION.

- The automotive industry must cope with a changing world!
- Trend 1: Autonomous driving changes vehicles!
 - Highly critical functions are automated with increasing amounts of software.
 - For high levels the driver wants to give up control of the vehicle.
- Trend 2: Attacks against vehicles are getting more common!
 - Vehicle attacks get more interesting.
 - Attackers better understand vehicles every day.
- What happens if you combine those two?

TECHNICA ENGINEERING

AUTOMOTIVE SECURITY CHALLENGES AND THE ASA SOLUTION.

TABLE OF CONTENTS

- Introduction.
- Automotive life cycle.
- What to consider for secure SerDes?
- ASA SerDes Security!
- Summary.

THE AUTOMOTIVE LIFE CYCLE.

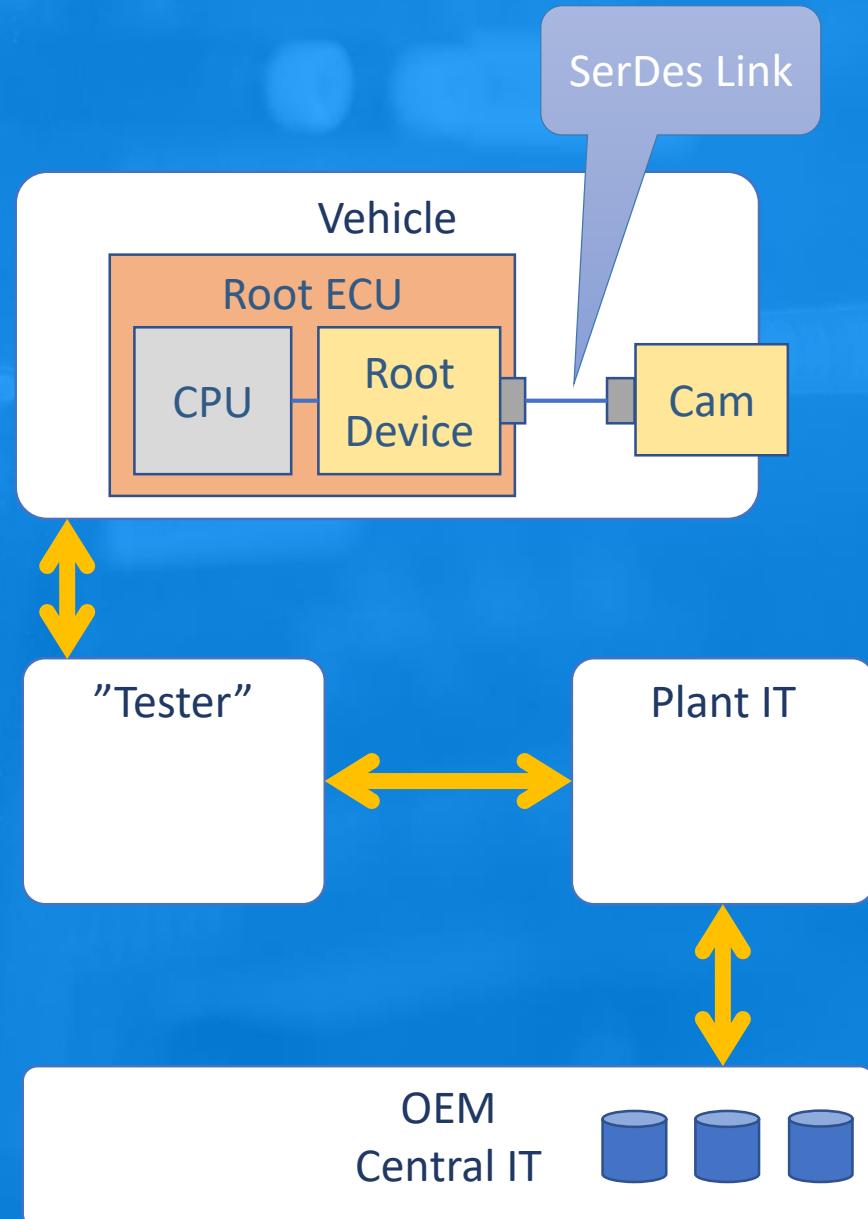
- Automotive is different and has specific requirements.
- Building vehicles:
 - Building vehicles needs to be automated and robust.
 - OEMs cannot trust every plant worldwide.
- Startup and vehicle usage:
 - Startup times and sleep cycles are very critical.
 - Scalability is very important.
 - Vehicles have a long life.
 - Service in the garage needs to be considered.
- For more details refer to [1].

[1] Dr. Lars Völker, BMW: "Why is network security in vehicles so hard?", Hanser Automotive Networks, 2018.

- Life Cycle:
 - Production in OEM plant.
 - Part replacement.
 - Part transfer between vehicles.
 - Development Support.
 - Lifecycle Requirements in Supply Chain.
 - Counterfeit Parts.
- Security attacks on vehicle to consider:
 - Sensor stolen and sold as spare part. (**Component theft**).
 - Man-in-the-Middle devices.
 - Manipulation of SerDes links.
 - Data leakage / data protection.

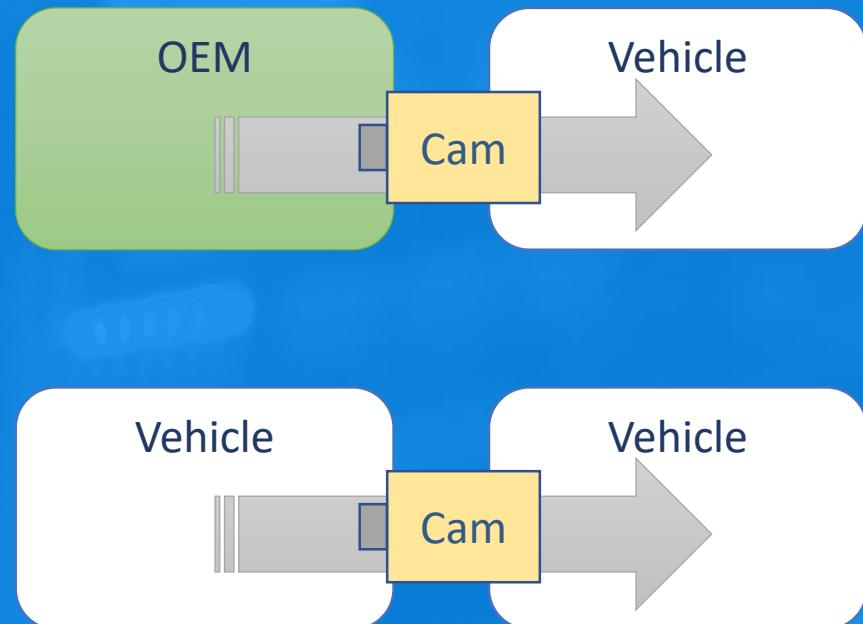


- **Production:** Vehicle assembly in OEM plant.
 - Vehicle is assembled.
 - Tester connects plant vehicle to plant IT.
 - Install Software? Coding? Generating Keys? Certs?
 - Plant IT is connected to central IT.
 - Transfer data to and from central infrastructure.
- **Requirements:**
 - Assembly needs to be fast!
 - Plant might not be online 100% of the time!
 - Plant might not be fully trusted!



VEHICLE IN SERVICE.

- Service is done by OEM owned or controlled or totally independent garage.
 - Only limited trust by OEM possible.
 - Testers in Garage might not be fully online.
- Relevant use cases:
 - **Part replacement**: exchange broken part.
 - Part broken by accident.
 - Vehicle needs to work again. Securely.
 - **Part transfer**: transfer between vehicles.
 - This needs to be possible for the owner.
 - This is very similar to “reusing stolen parts”.
 - How to separate those two?



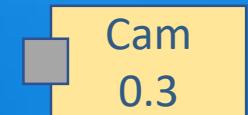
VEHICLE DEVELOPMENT.

- OEM needs to develop and validate.
 - Security needs to allow Development.



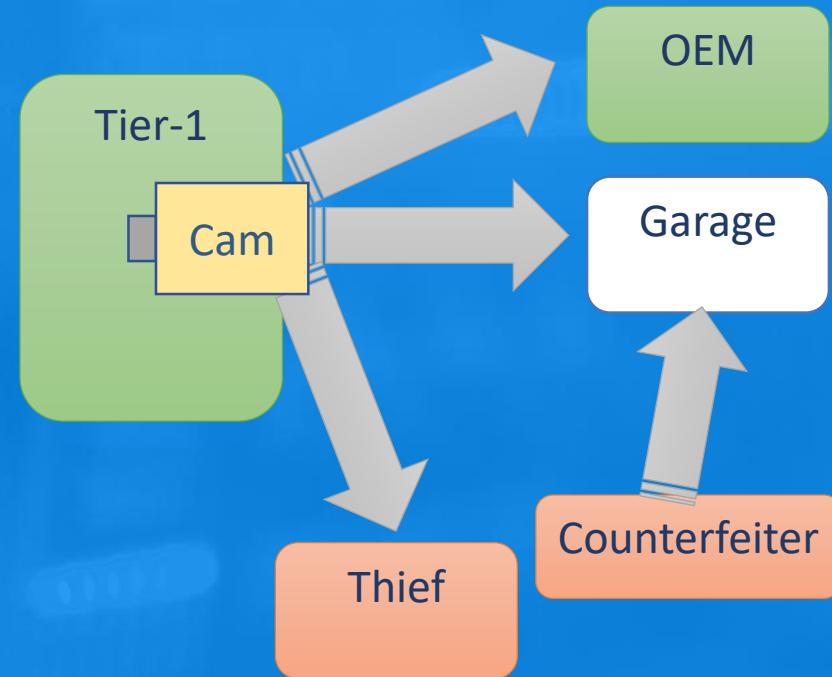
▼

- Requirements for vehicle **development**:
 - OEM needs to record and understand communication.
 - OEM needs to be able to simulate parts.
 - OEM needs to be able to transfer and modify parts.
- The same is true for Tier-1, etc.



SUPPLY CHAIN AND COUNTERFEITING.

- Parts needs to be distributed world-wide.
- Theft in supply chain is possible.
- Counterfeit parts:
 - Problems for Safety and Security!
 - Customers might be tricked into lower quality.
 - Tools might be stolen of Tier-1.
- Requirements:
 - Allow control of supply chain!
 - Stop counterfeiting.

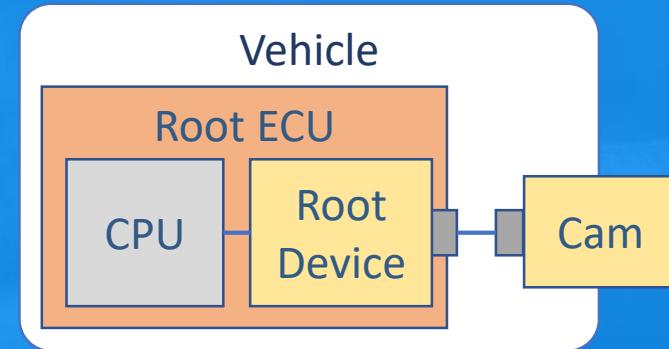


ATTACK: COMPONENT THEFT.

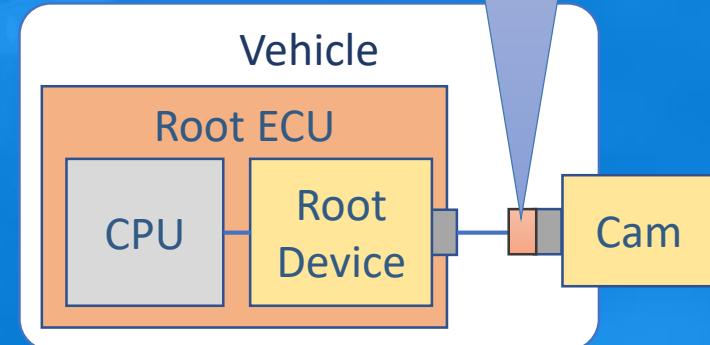
- More expensive components (RADAR, LIDAR, ...) used.
- The market for component theft is huge!
 - Replacement parts for fixing a vehicle after an accident.
 - Parts to “upgrade” vehicle features.
 - Parts to masquerade mileage manipulation.
- Component theft costs are high!
 - Vehicles are stolen or broken into.
 - Damages on vehicle are high (e.g. cut cable harness or broken window).
 - This is reflected in insurance premiums.
- **Component theft** needs to be made useless for the attacker!

ATTACK: MAN-IN-THE-MIDDLE.

- Autonomous driving requires high security but also sensors on the surface of the vehicle.
- Attack:
 - Install a device between sensor and rest of vehicle. This could be done in a very small time.
 - Attack vehicle with e.g. wrong data.
 - Attacker could be owner, too.
- Make sure that man-in-the-middle attacks are not possible.

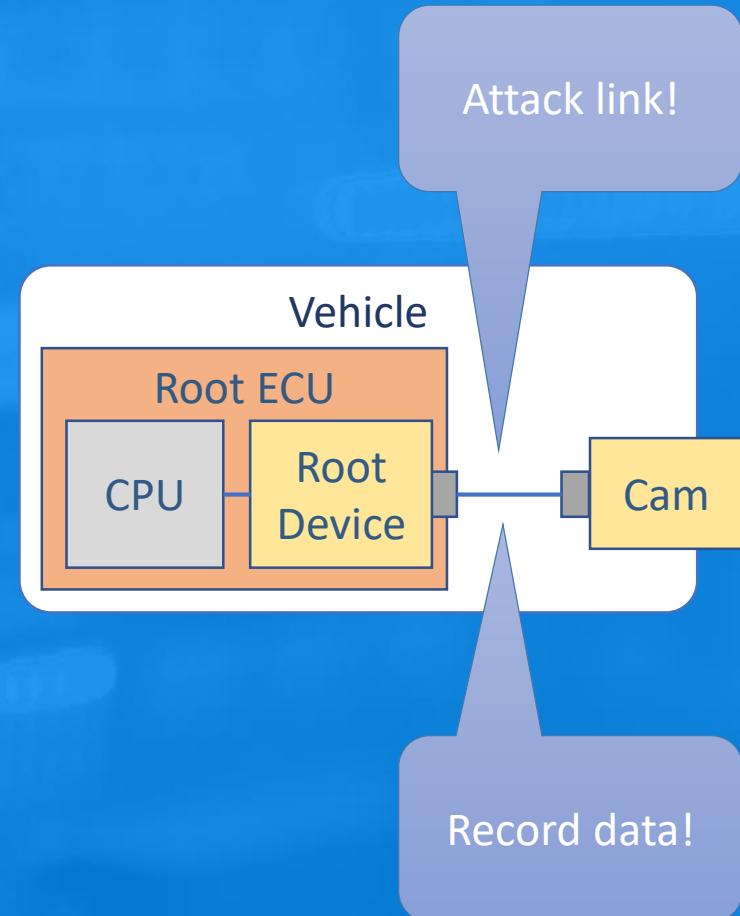


Man-in-the-middle device



ATTACK: ATTACKING SERDES LINKS.

- Attackers may attack the link, too!
- **Manipulation** of a SerDes link.
Due to regulatory and security concern manipulation of critical links (e.g. for autonomous driving) cannot be permitted.
- **Data leakage / data protection.**
Due to privacy or regulatory concerns it may become necessary to protect links against eaves dropping.

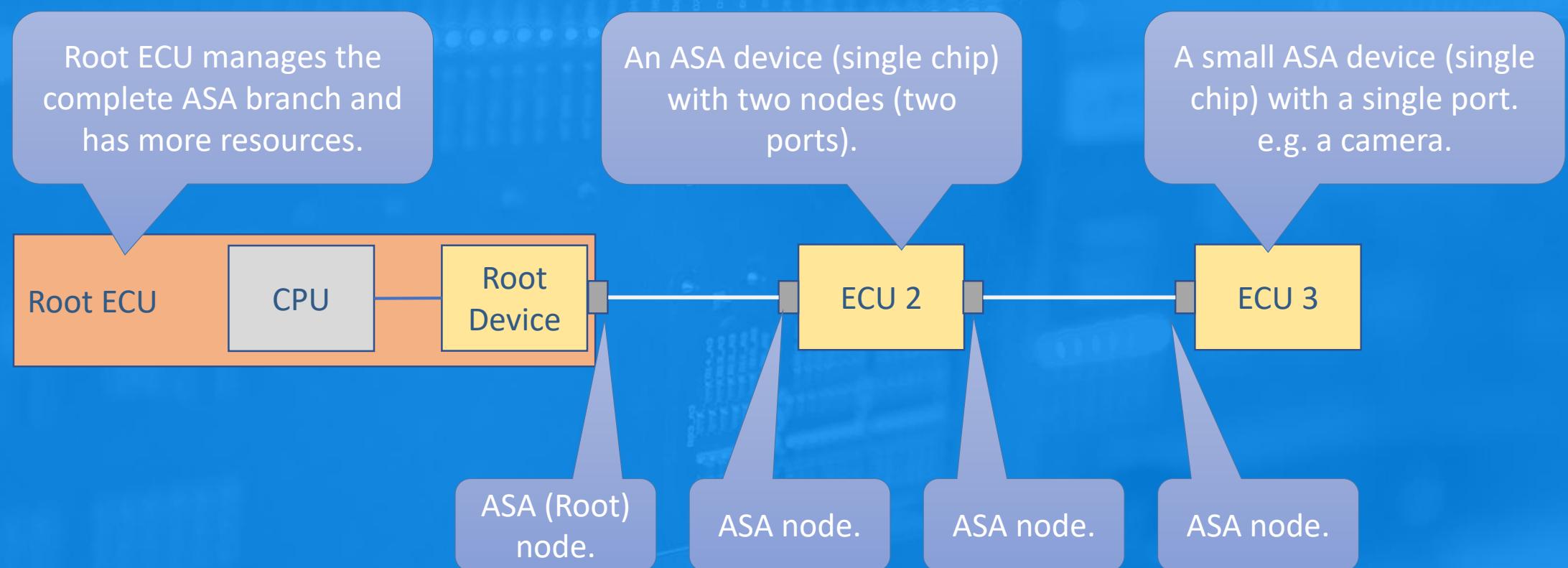


ASA SERDES SECURITY!

- For the newly developed open ASA SerDes standard security was considered from the beginning.
 - Security is not added on top but an integral part of the standard!
- ASA SerDes security was designed to cope with the use cases, requirements and attacks before.
- Security solution consists of two parts:
 - Key management – onboard and offboard.
 - Protection of communication traffic.

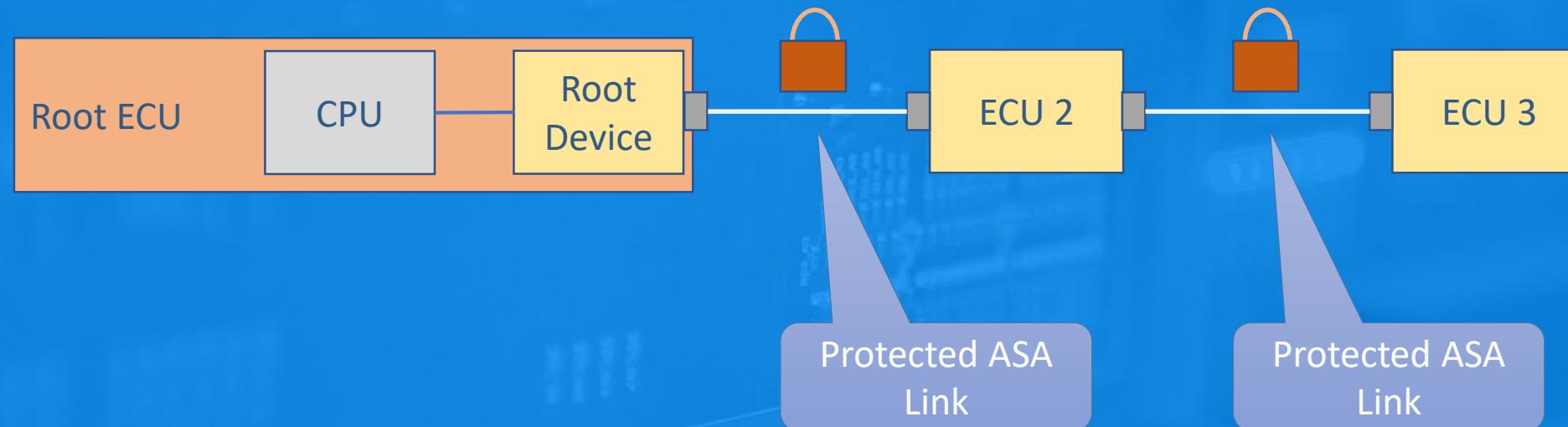
ASA BRANCH.

- ASA SerDes is based on branches and nodes.



ASA SECURITY OVERVIEW.

- ASA Security is protecting communication per link (point to point).
- ASA Security also protects against:
 - Counterfeit parts
 - Parts theft



KEY HIERARCHY.

- Key management is based on a three-level hierarchy of symmetric keys:
 - Symmetric → fast startup and low overhead.
 - Three levels → control device, control binding to vehicle, keys to protect link.
 - Each level protects the installation of the next levels keys.



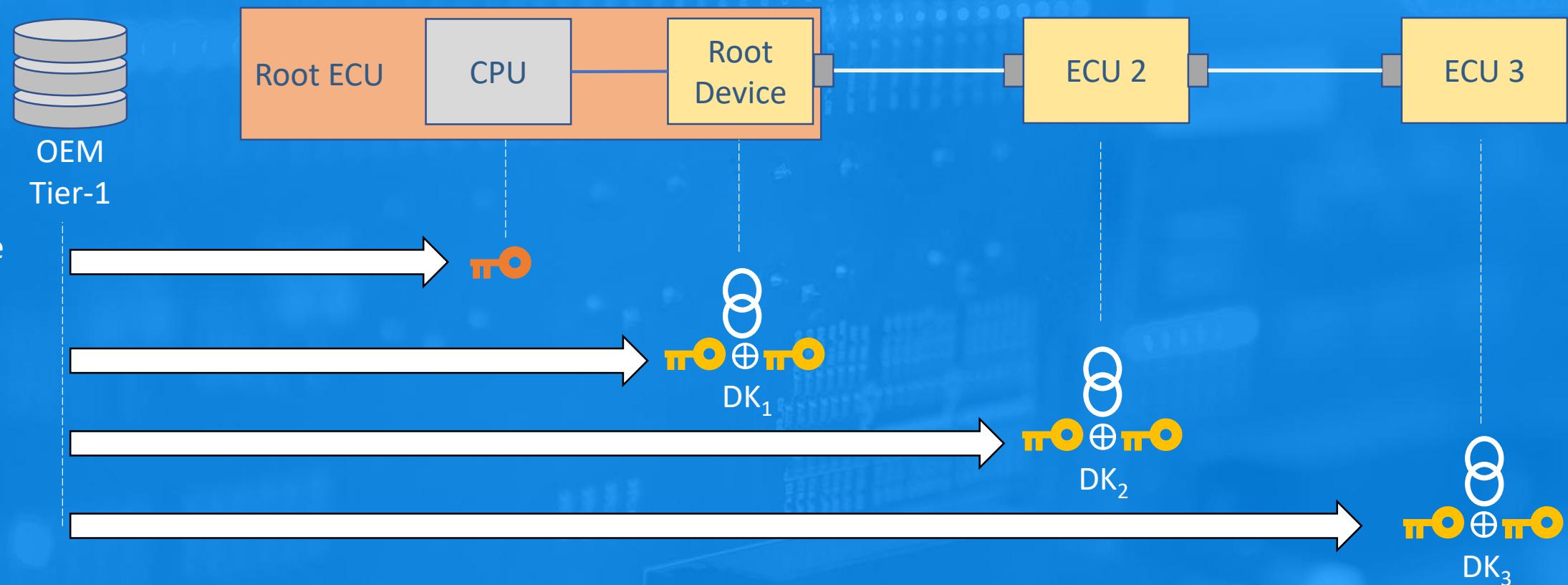
Level 1: Devices Keys to control device.

Level 2: Binding Keys to connect devices and bind to vehicle.

Level 3: Link Keys to protect traffic.

KEY HIERARCHY: L1 – DEVICE KEYS.

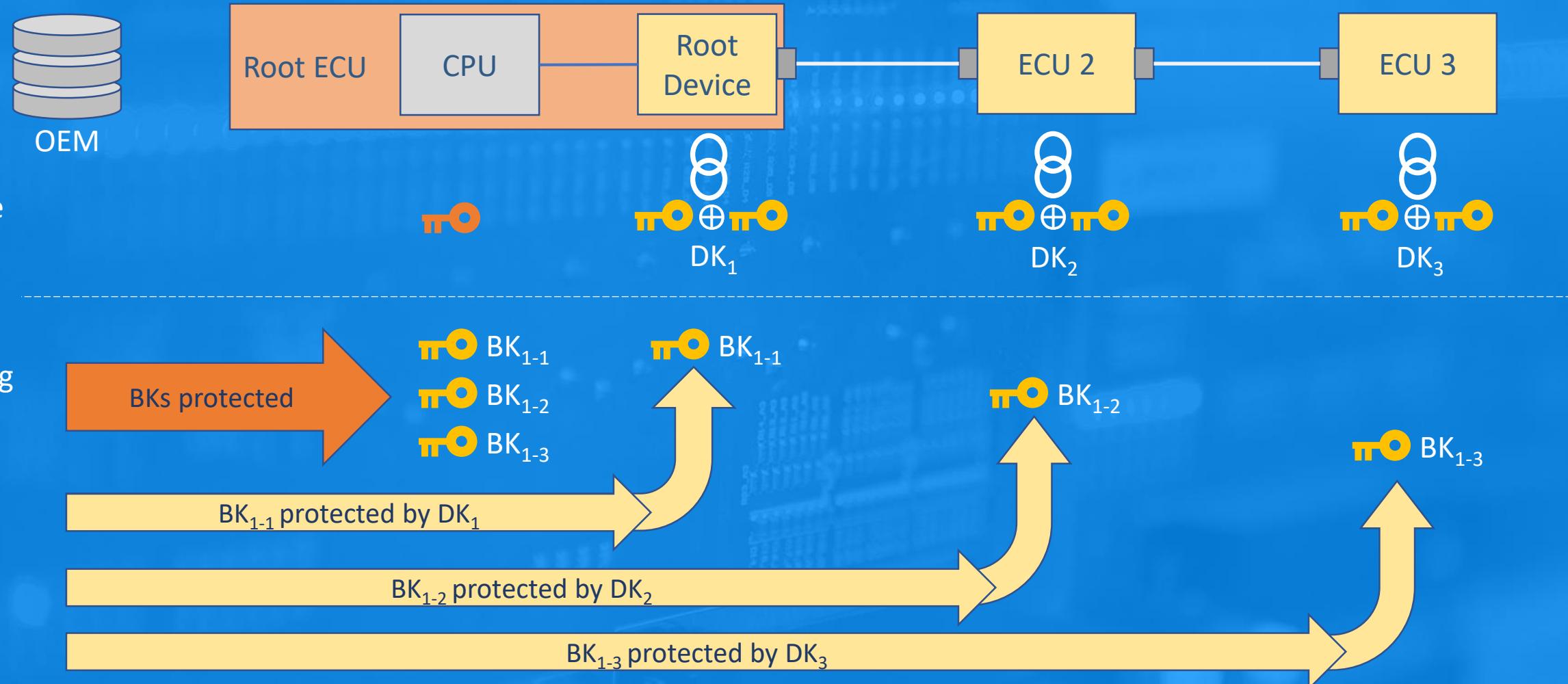
- Tier-1 controls device during logistics via first part of Device Key.
- OEM takes control via Device Key.



*) Device Keys (orange) for the Root ECU's CPU is OEM specific and only shown as an example.

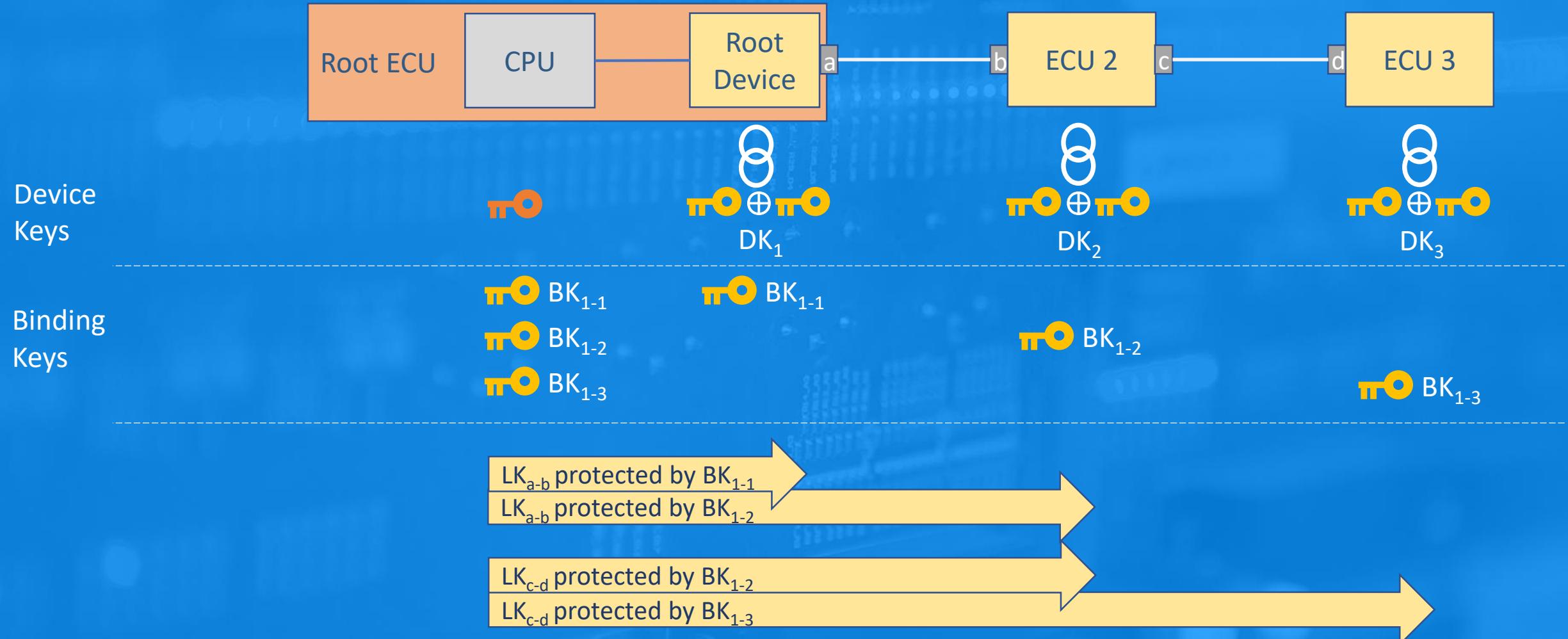
KEY HIERARCHY: L2 – BINDING KEYS.

- OEM binds devices together and to the vehicle.



KEY HIERARCHY: L3 – LINK KEYS.

- Root ECU installs link keys to protect traffic.



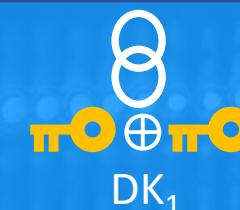
KEY HIERARCHY.



Prevents



Device Keys



By OEM/Tier-1

Prevents



Binding Keys



By OEM

Protects



Link Keys



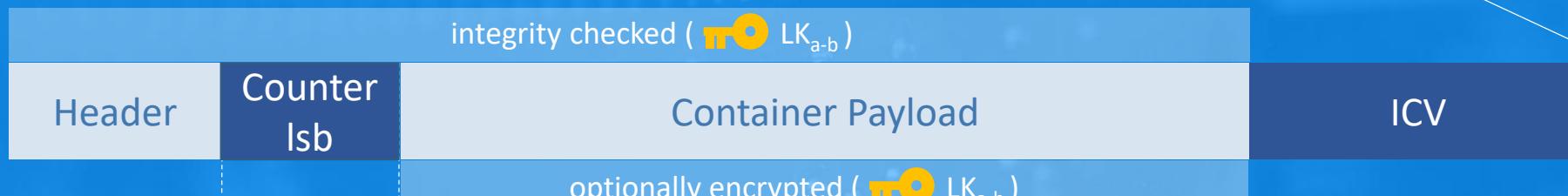
By Root ECU

- The link layer protection supports based on link keys:
 - authentication only
 - encryption + authentication

LINK LAYER PROTECTION.



Link Layer Frame Format



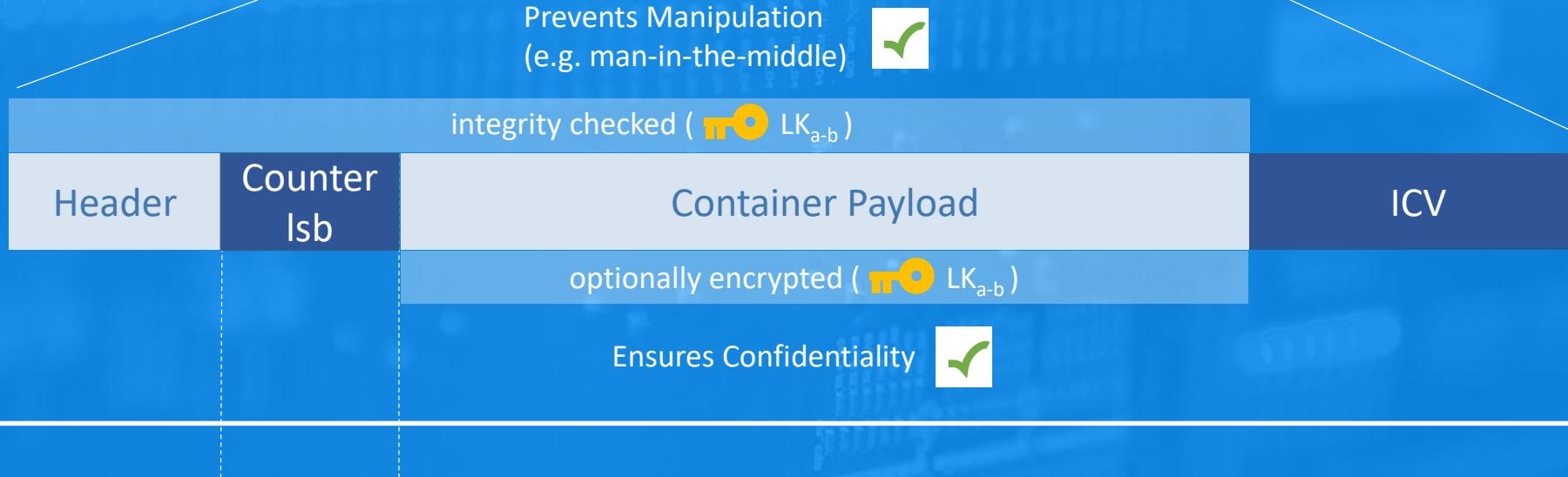
Security Counter



LINK LAYER PROTECTION.



Link Layer Frame Format



Legend	
	Standard Fields
	Security Fields

ASA SERDES SECURITY.

- The three-level key hierarchy allows the OEM to design a system for the use cases and requirements shown before, while using highly efficient symmetric keys.
 - Key level 1 allows control of devices.
 - Key level 2 allows the Root Device to secure the branch.
 - Key level 3 protects the communication between devices.
- The security can be easily implemented on small devices.
 - The Root Device takes the harder job to allow small devices.
- Protection of SerDes data is like MACsec.
 - It allows “authentication only” and “authentication + encryption”!
 - This stops the attacks shown before

SUMMARY.

- The requirements for a secure SerDes solution are challenging.
- ASA SerDes addresses the security requirements for automotive use cases with a state-of-the-art security solution.
 - A three-level symmetric key hierarchy achieves the three goals: high security, high flexibility, and high performance.
 - ASA SerDes allows for “no protection”, “authentication only”, and “authentication and encryption”.
 - For additional details (sequence diagrams, message formats, ...) please refer to the official ASA Specification.
- The authors like to especially thank Dance Wu of Marvell (chair of the ASA TC-C) as well as all participants of the ASA TC-C!

Dr. Lars Völker

Technical Fellow

Lars.Voelker@technica-engineering.de

+49 175 114 0982

Stefan Lachner

Consultant

Stefan.Lachner@technica-engineering.de

+49 151 634 338 64

Technica Engineering GmbH / Leopoldstraße 236 / 80807 Munich / Germany