A Case Study: Securing Communication using J1939-91C Certificate-Based Authentication in Autonomous Commercial Vehicles

Joe Lotz

Sr Manager - Autonomous Vehicle Platform

KENWORTH Peterbilt DAF PACCAR ELECTRONICS

PACCAR Inc

KENWORTH Peterbilt DAF

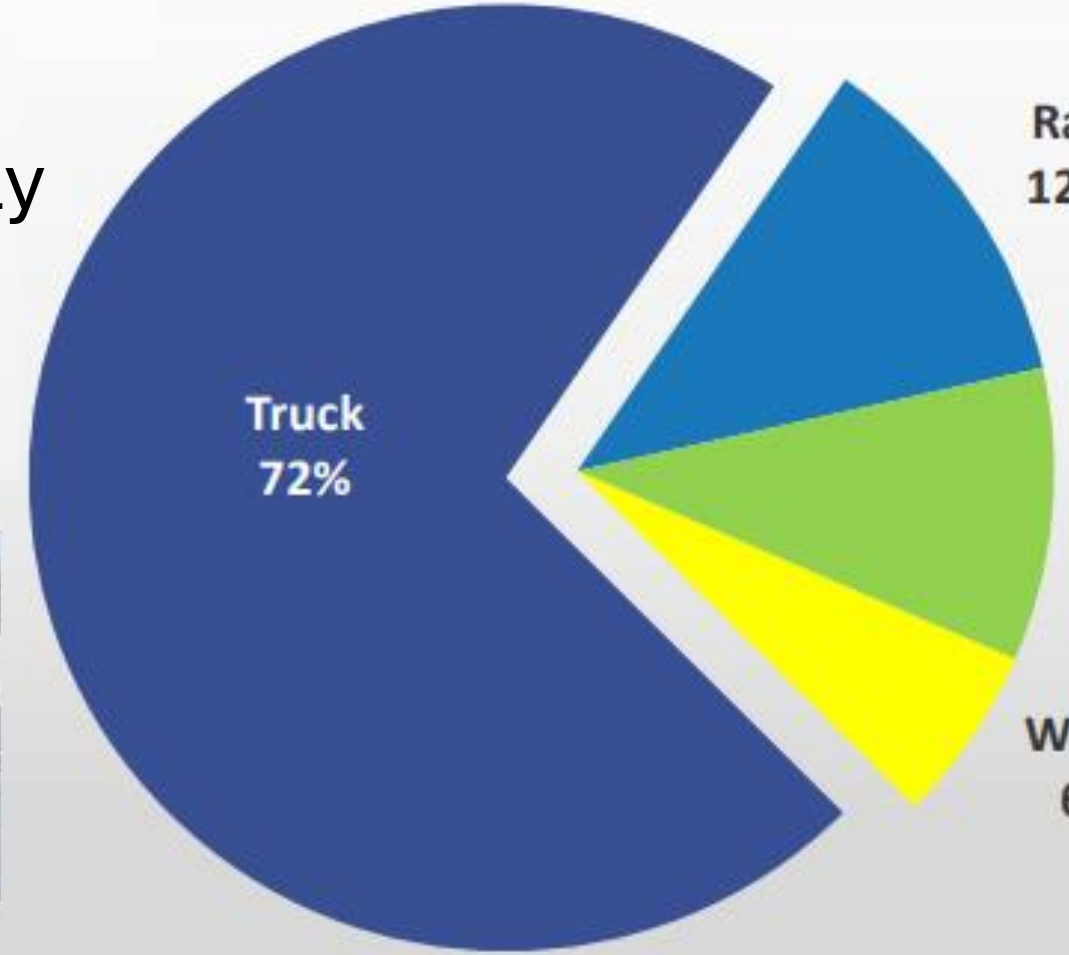
Topics

1. Commercial vehicle challenges
2. Introduce the project
3. Authentication options considered
4. Overview of J1939-91C
5. Lessons-learned

Trucking Moves the U.S. Economy

72% of freight

11B tons annually

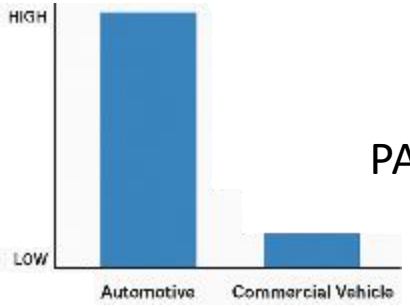


KENWORTH Peterbilt DAF

PACCAR ELECTRONICS

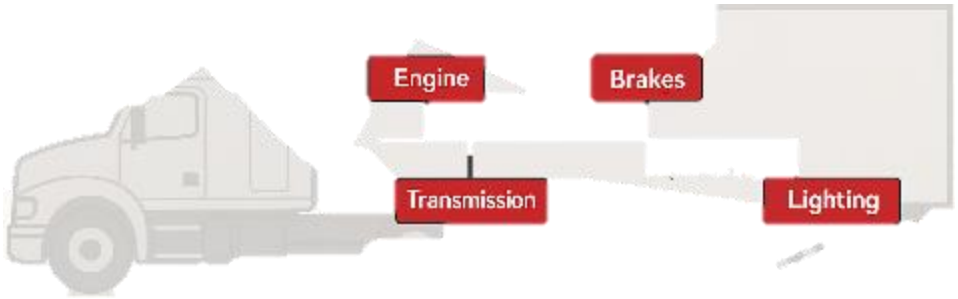
Commercial Vehicle Market

Lower Volumes



PACCAR: ~200K units annual

Legacy E/E Architecture



High Variability

Cost Sensitivities

PACCAR ELECTRONICS

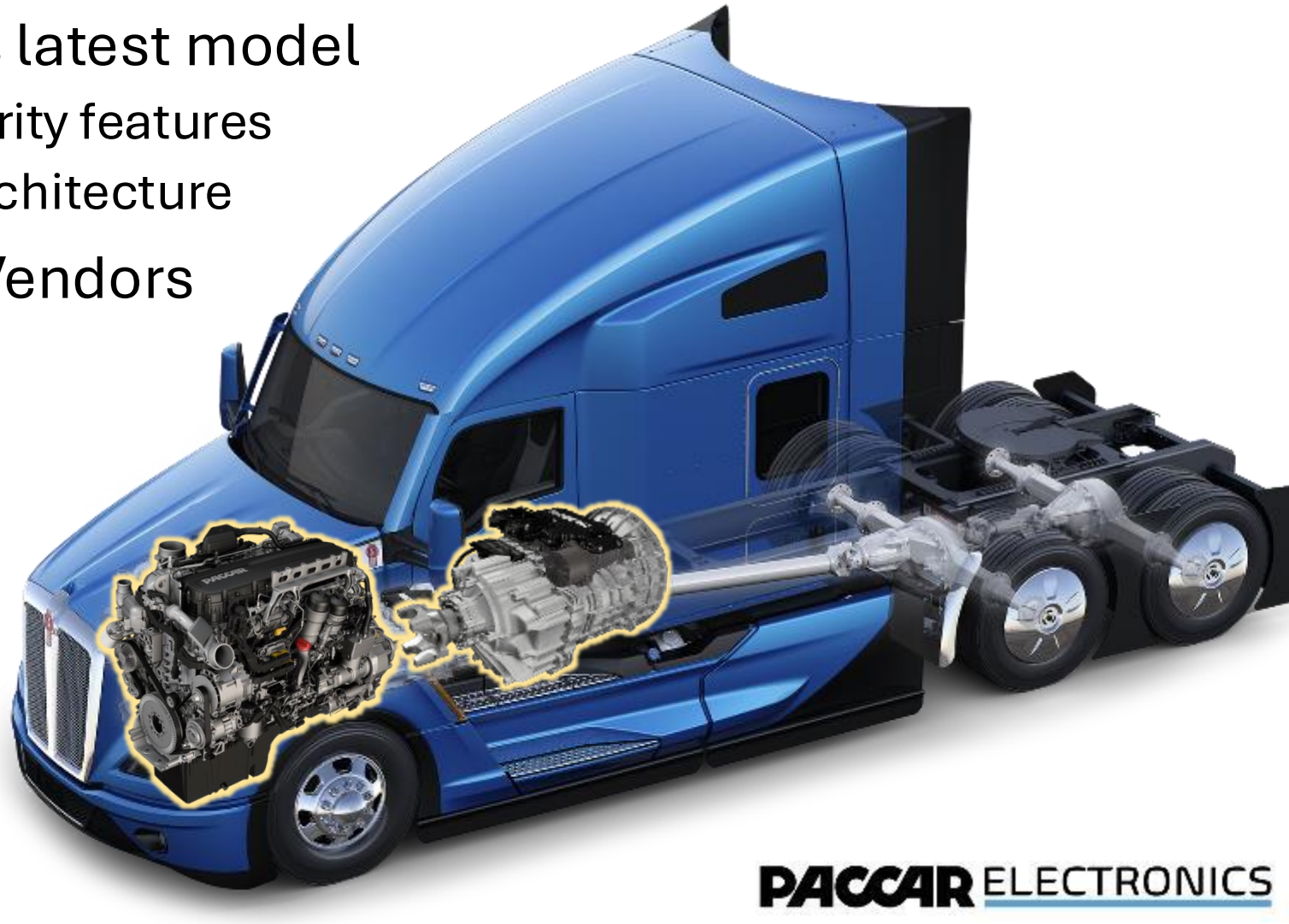
Topics

1. Commercial vehicle challenges
2. Introduce the project
3. Authentication options considered
4. Overview of J1939-91C
5. Lessons-learned

Autonomous Enabled Truck (AET) Platform

Platform Constraints

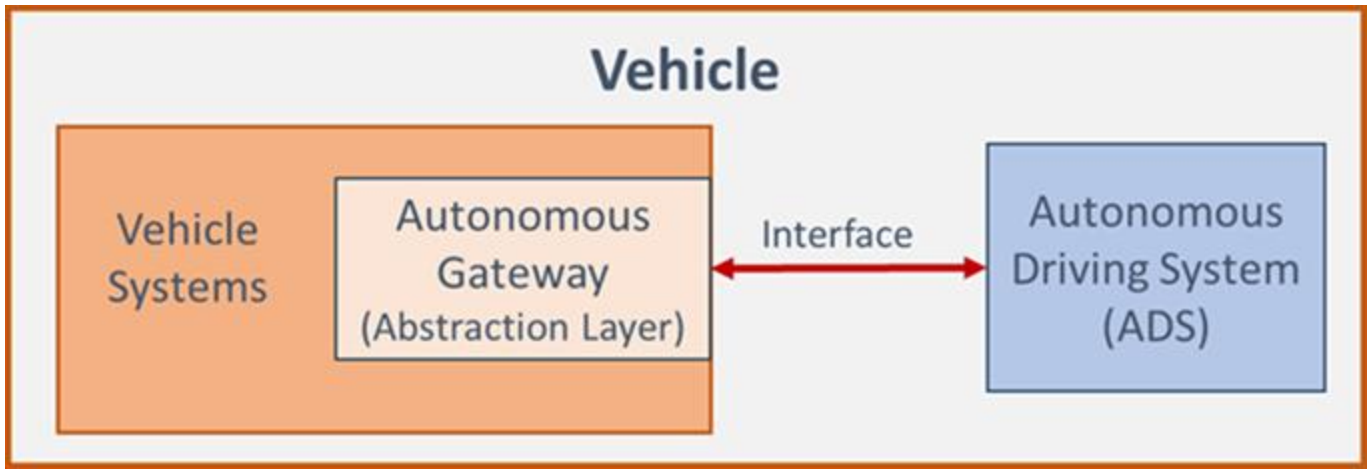
- Not “Green Field” – extends latest model
  - ↑ Able to utilize existing security features
  - ↓ Some legacy controllers/architecture
- Commercial Vehicle Tier1 Vendors
- Business Requirements
  - Protocol Constraints



KENWORTH Peterbilt DAF

PACCAR ELECTRONICS

Security Strategy (high-level)



- A federated control architecture employing a service-oriented interface between the Vehicle and ADS.
  - Isolated trust domains
  - Secure and auditable interactions
  - Unified control requests enabling system flexibility and supplier diversity

Topics

1. Commercial vehicle challenges
2. Introduce the project
3. Authentication options considered
4. Overview of J1939-91C
5. Lessons-learned

Automotive Ethernet Network

- Why not IEEE 802.3?
- For “business reasons”… program was constrained to CAN

KENWORTH Peterbilt DAF

Some CAN Authentication Options

AutoSAR SecOC	Transport-layer agnostic. Message authentication with symmetric keys.
CANcrypt	Encryption and authenticated communication based on a secure heartbeat.
CANAuth	Pre-shared symmetric keys for message authentication.
CANSec	Security layer for CAN XL. Message encryption, authentication, integrity.

Topics

1. Commercial vehicle challenges
2. Introduce the project
3. Authentication options considered
4. Overview of J1939-91C
5. Lessons-learned

SAE J1939 Introduction

- Suite of Open Standards
- High-layer CAN Protocol
- Used Extensively in Commercial Vehicles
- Strengths Include:
  - Deterministic
  - Fault-tolerant
  - Scalable
  - Extendable

KENWORTH Peterbilt DAF

Early SAE J1939 Weakness = Cybersecurity

First Published in 1994

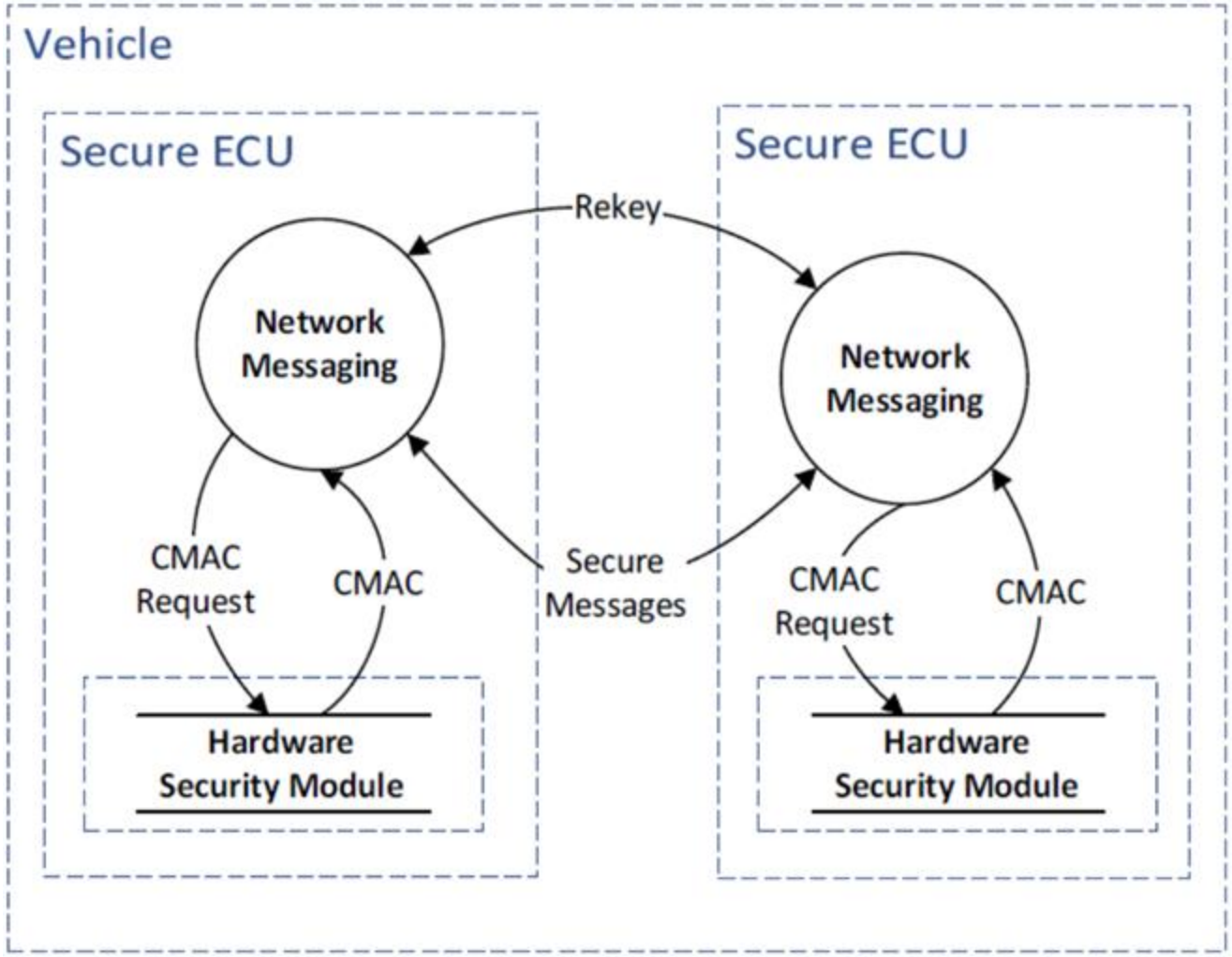
Lacks built-in security:

- ☹ Confidentiality
- ☹ Integrity
- ☹ Authentication

PACCAR ELECTRONICS

SAE J1939-91C: The Cybersecurity Extension

"J1939-91C describes Secure Onboard Communications with optional Encryption (SecOC/E) for an internal CAN FD network and the processes and infrastructure required to make [J1939] secure."
– SAE Abstract



KENWORTH Peterbilt DAF

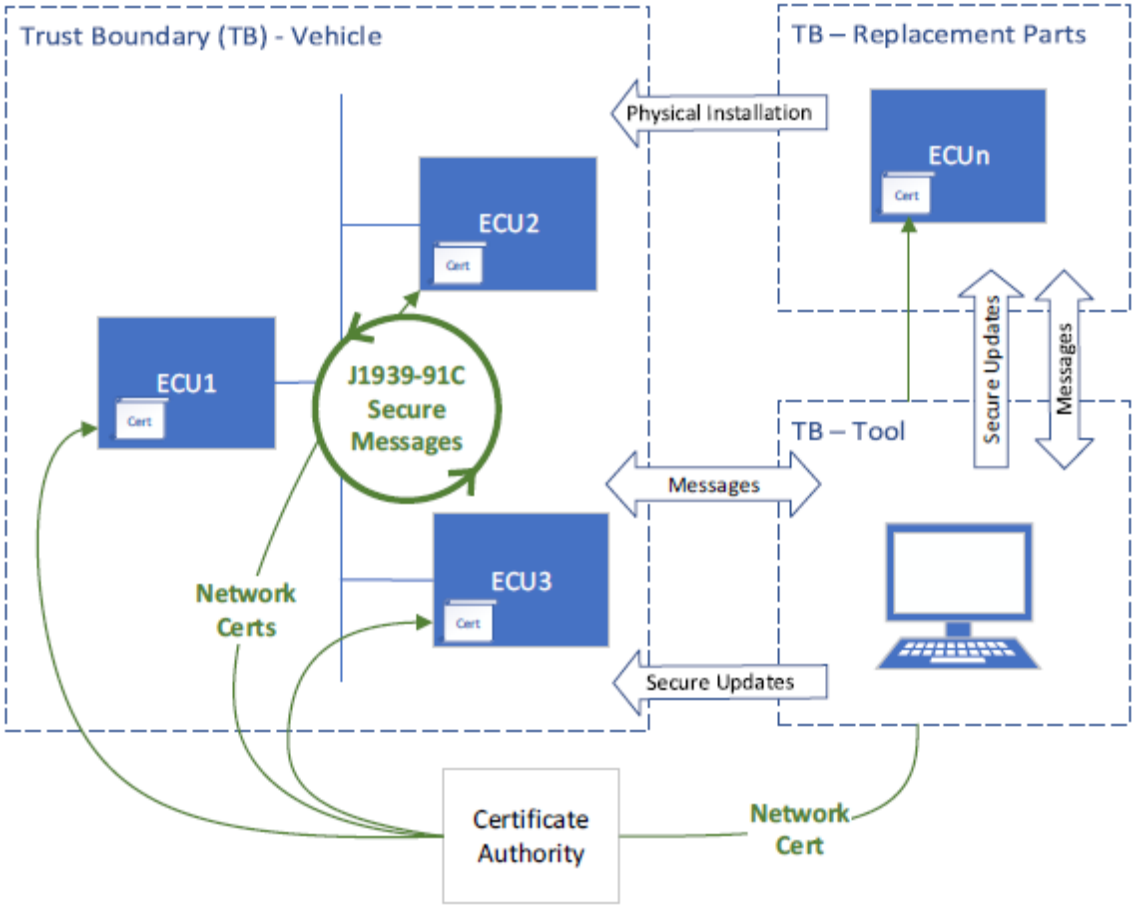
Lovingly stolen from SAE J1939-91C

J1939-91C

- Messages are authenticated via a truncated AES-128 CMAC
- Messages can be encrypted
- Messages include a Freshness Value for replay attack mitigation
- **Leverages native J1939-22 (CAN FD) data frame**

C-PG Format (Figure 19 from J1939-22)					
C-PG Header: 4 Bytes				C-PG Payload: 0-60 Bytes	
TOS	TF	CPGN	PL	PG Data	Assurance Data (CMAC&FV)
3 bits	3 bits	18 bits	8 bits	0-52 Bytes	8 Bytes

J1939-91C: ECU Authentication



- Network Formation
  - Mutual authentication of X.509 certs
  - OEM defines members
- Forward and backward secrecy
- Certificates are ECU-specific and vehicle-specific
- PACCAR mechanism for service part replacement
- PACCAR mechanism for certificate revocation and reissuance

Source: SAE J1939-91C

PACCAR ELECTRONICS

Topics

1. Commercial vehicle challenges
2. Introduce the project
3. Authentication options considered
4. Overview of J1939-91C
5. Lessons-learned

Lessons Learned

- Securely crossing different network types can be tricky
- Working with a draft standard:
  - Untested protocol implementation = unknown unknowns
  - Don’t forget about service tools, engineering tools, test tools
- Zero-trust strategy
- PKI framework requires a lot of back-office support (OEM and vendors)
- Don’t be afraid to ask for help

- Many thanks to **NCC Group**!

Thank you!

KENWORTH Peterbilt DAF

PACCAR ELECTRONICS