

FEV Signature Solutions Quantum-Resistant Vehicle

FEV.io

Make your next generation vehicles future-proof against quantum threats

FEV offers

- ▶ Future-proof vehicles secured against emerging quantum threats with Post-Quantum Cryptography (PQC) for next generation vehicles.
- ▶ Due to strict compute and memory constraints in automotive ECUs, direct execution of full PQC workloads is not feasible. Our PQC solution addresses this by limiting PQC-heavy computation to a powerful central controller, minimizing the impact on constrained ECUs.
- ▶ Hybrid Classical + PQC protection using the latest NIST-Standardized algorithms.
- ▶ For all domains – passenger cars, commercial vehicles, aerospace, marine, rail, defense

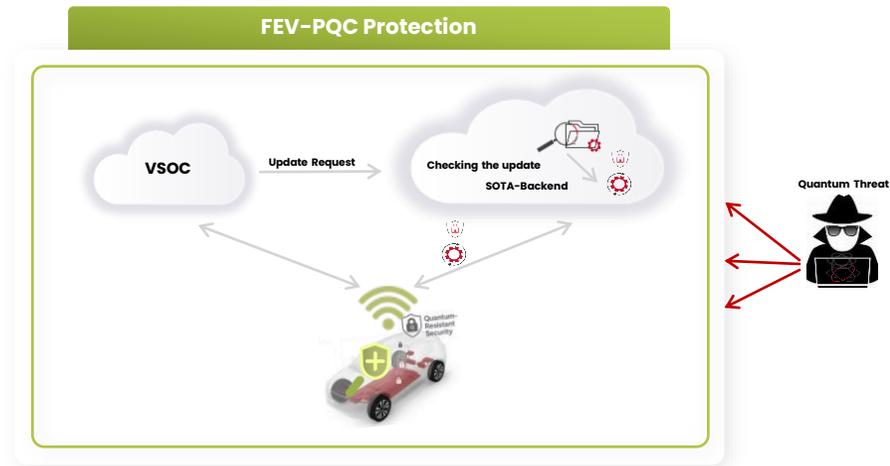
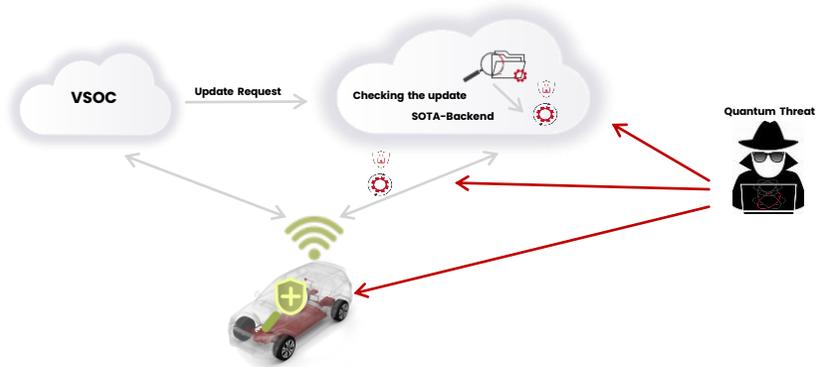
Why FEV

- ▶ **Proven expertise:** Over 40 years of automotive engineering excellence, trusted by global OEMs and Tier-X suppliers to deliver innovative, production-ready solutions with deep domain expertise
- ▶ **Complete lifecycle support:** From concept to series maturity, including design, simulation, prototyping, testing, industrialization, and implementation
- ▶ **Customer-centric solutions:** Transparent and customizable, enabling you to extend, integrate, and scale your own development



Reference project FEV.io

Horizon Europe program "SELFY – SELF assessment, protection & healing tools for a trustworthy and resilient CCAM" – grant No. 101069748



Key features of FEV's Hybrid PQC Protocol

- ▶ Hybrid PQC signatures ensure long-term update authenticity
- ▶ Quantum-safe protection for all OTA delivery channels
- ▶ Backend integrity checks built on PQC-resistant algorithms
- ▶ ECU installation verified with hybrid PQC trust anchors
- ▶ Clear quantum-threat boundary securing the entire update chain

Hybrid Post-Quantum Cryptography for Automotive Systems

OUR SOTA UPDATE SOLUTION – FULLY INTEGRABLE IN YOUR SPECIFIC ENVIRONMENT



Patent application
Method, device, system and
computer program product
for PQ-secure updating a data
processing unit
DE102023115999A1

Post-Quantum Security Integration

We deliver advanced cryptographic solutions that safeguard vehicle systems against potential quantum threats, ensuring long-term resilience and compliance.

Performance-Optimized PQC Architecture for Constrained ECUs

A hybrid cryptographic protocol that combines PQC and classical techniques while centralizing PQC verification in a powerful central controller, ensuring that all other ECUs remain low-cost, lightweight, and impacted only at the absolute minimal level by PQC processing.

Secure Software Update Services

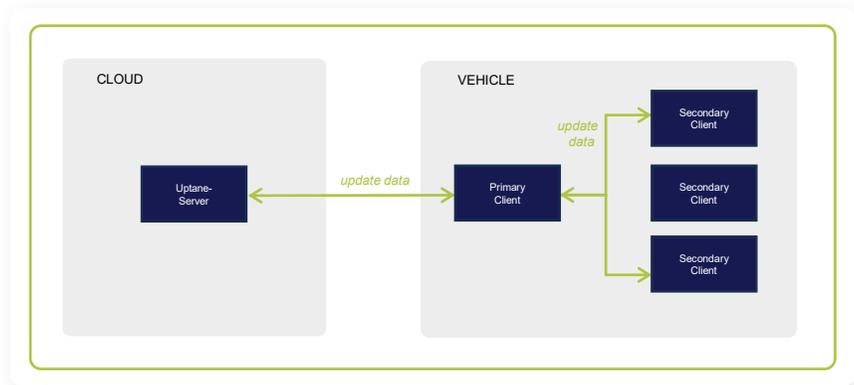
Comprehensive support for implementing secure, future-proof software update processes across all vehicle components.

Customizable Security Framework

Tailored advanced cryptographic solutions designed to meet OEM and Tier-1 needs for scalability, performance, and regulatory compliance.

Compliance and Certification Support

Guidance and implementation aligned with global standards such as ISO/SAE 21434, UNECE R155/R156, and NIST PQC recommendations.



Get in touch with us for further information



[www.fev.com/en/
signature-solutions](http://www.fev.com/en/signature-solutions)