講演番号	158

Crypto-Agility in Automotive Real-Time Systems in Context of Post-Quantum Cryptography

Carolina Pelka [1)] Dr. Philipp Jungklass [1)] Andre Larberg [1)] Dr. Nicole Natho [1)]
Dr. Dennis Kengo Oka [2)] Tim Kaiser [1)] Dr. Claude-Pascal Stöber-Schmidt [1)]
Marco Siebert [1)] Takuya Nigoro [2)]

1) IAV GmbH Ingenieurgesellschaft Auto und Verkehr, Carnotstraße 1, 10587 Berlin, Germany
2) IAV Japan Co., Ltd., Uchikanda Chuo Bldg. 3F, 1-18-13 Uchikanda, Chiyodaku, Tokyo, 101-0047, Japan

KEY WORDS: **Open-Source, Post-Quantum Cryptography (PQC), Crypto-agility, AUTOSAR Classic Platform**

With the progress in developing powerful quantum computers, cryptographic agility has become a central concern in cybersecurity. Extending key lengths has ensured security so far, but is ineffective against quantum threats to asymmetric cryptography. This is because the mathematical challenges that underpin asymmetric cryptography can be solved far more efficiently using these advanced processors. Therefore, affected algorithms must be replaced to ensure future security. This adaptable substitution of cryptographic algorithms is referred to as crypto-agility and is especially significant for systems intended to receive software updates over several years. Software-defined vehicles (SDVs) are a key example of such systems. The goal is to define vehicle functionality through software rather than hardware, allowing for continuous expansion during operation. Resource-constrained systems, primarily used in real-time applications, present a unique challenge. These specialized control units depend on microcontrollers that offset their lower performance with hardware accelerators for specific tasks. Given the high resource demands of modern cryptographic algorithms, they are mainly implemented with hardware support. While this approach offers high-performance computation, the inability to update these hardware accelerators poses a problem for crypto-agility. Therefore, this article introduces a concept that enables the updating of existing ECUs for real-time applications based on the AUTOSAR Classic Platform. To validate the approach, all post-quantum algorithms currently standardized by the National Institute of Standards and Technology (NIST) are implemented as open-source solutions and tested on an automotive microcontroller family. The IAV Primula approach demonstrates that PQC is technically feasible when crypto-agility is considered a fundamental system requirement from the outset. This text underscores the multifaceted nature of implementing PQC in the automotive sector, addressing the challenges posed by extended vehicle lifecycles and constrained hardware resources, as well as the benefits that open-source software offers for the development and integration of cryptographic solutions.

The combination of long vehicle lifecycles, over-the-air updates, and hardware-accelerated cryptography in resource-constrained microcontrollers shows that cryptographic mechanisms cannot remain static over time. Instead, they must remain replaceable over the system lifecycle. Achieving this level of agility solely through proprietary, in-house solutions often leads to increased integration and maintenance complexity. Open-source offers a viable path forward. By exposing implementations and interfaces, it establishes a verifiable common base on which original equipment manufacturers (OEMs), suppliers, and research institutions can build. This level of transparency is particularly important for PQC, as algorithms and parameters are still evolving. In such an environment, the continued use of closed, non-auditable cryptographic implementations becomes increasingly difficult to justify for safety- and mission-critical applications. The IAV Primula implementation provides NIST-standardized PQC algorithms as an open-source solution within an AUTOSAR-compatible, crypto-agile architecture (Fig. 1). Concurrently, the open-core model enables the implementation of OEM-specific integration layers and business logic that can be maintained as proprietary. In this manner, IAV Primula integrates the openness necessary for security and credibility with the differentiation capabilities essential for competition in the automotive market. This represents more than a mere technical proof of concept; IAV Primula signifies a paradigm shift in the realm of automotive development. In this new paradigm, security-critical base technologies are progressively developed within open, collectively maintained software platforms. In a software-driven market, those who attempt to implement post-quantum security for vehicles in a purely proprietary and isolated manner often expend significant time and resources without achieving the desired outcome. This often results in a decrease of their competitiveness within the industry. Consequently, open-source software represents a practical approach for building transparent and maintainable cryptographic foundations in software-defined vehicles.

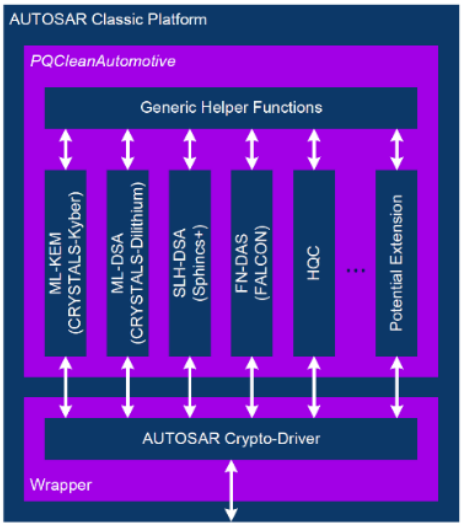

Fig. 1 Structure of a PQC Crypto-Driver for the AUTOSAR Classic Platform