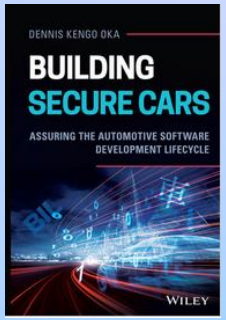
HSM Evolution Towards PQC

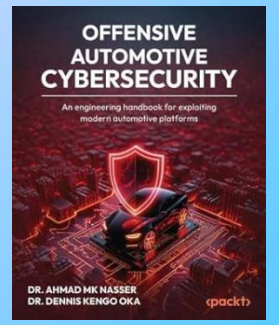
Global Technical & Cybersecurity Advisor
Dennis Kengo Oka
dennis.kengo.oka@iav.jp

GlobalPlatform Cybersecurity Vehicle Forum 2026
May 26, 2026

Dr. Dennis Kengo Oka

- Started automotive security in 2006
- Active contributor to automotive standardization and industry best practices
- 80+ publications and presentations
- Global Technical & Cybersecurity Advisor





Author of books:
"*Building Secure Cars: Assuring the Automotive Software Development Lifecycle*"
"*Building Secure Automotive IoT Applications: Developing Robust IoT Solutions for Next-Gen Automotive Software*"
"*Offensive Automotive Cybersecurity: An Engineering Handbook for Exploiting Modern Automotive Platforms*"

PQC: Post-Quantum Cryptography

Agenda

01

The Quantum Threat in Automotive

Vehicle lifecycles, Q-Day, and the harvest-now-decrypt-later window

02

The HSM Today

What's inside, what it accelerates, and what PQC limitations exist

03

Near-Term and Long-Term Paths

Software PQC on existing HSMs, hybrid modes, and PQC-enabled silicon

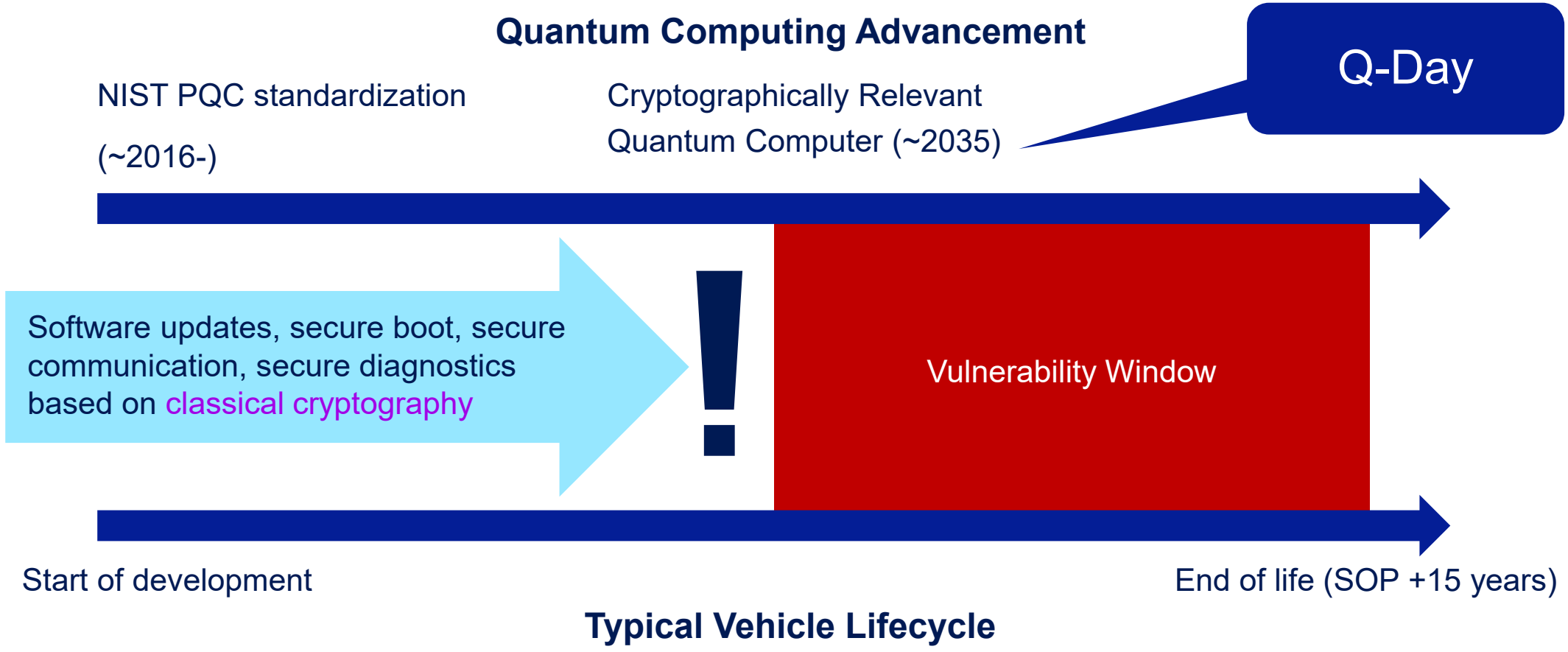
04

A Coordinated Industry Path

Roles for OEMs, semiconductor vendors, standards bodies

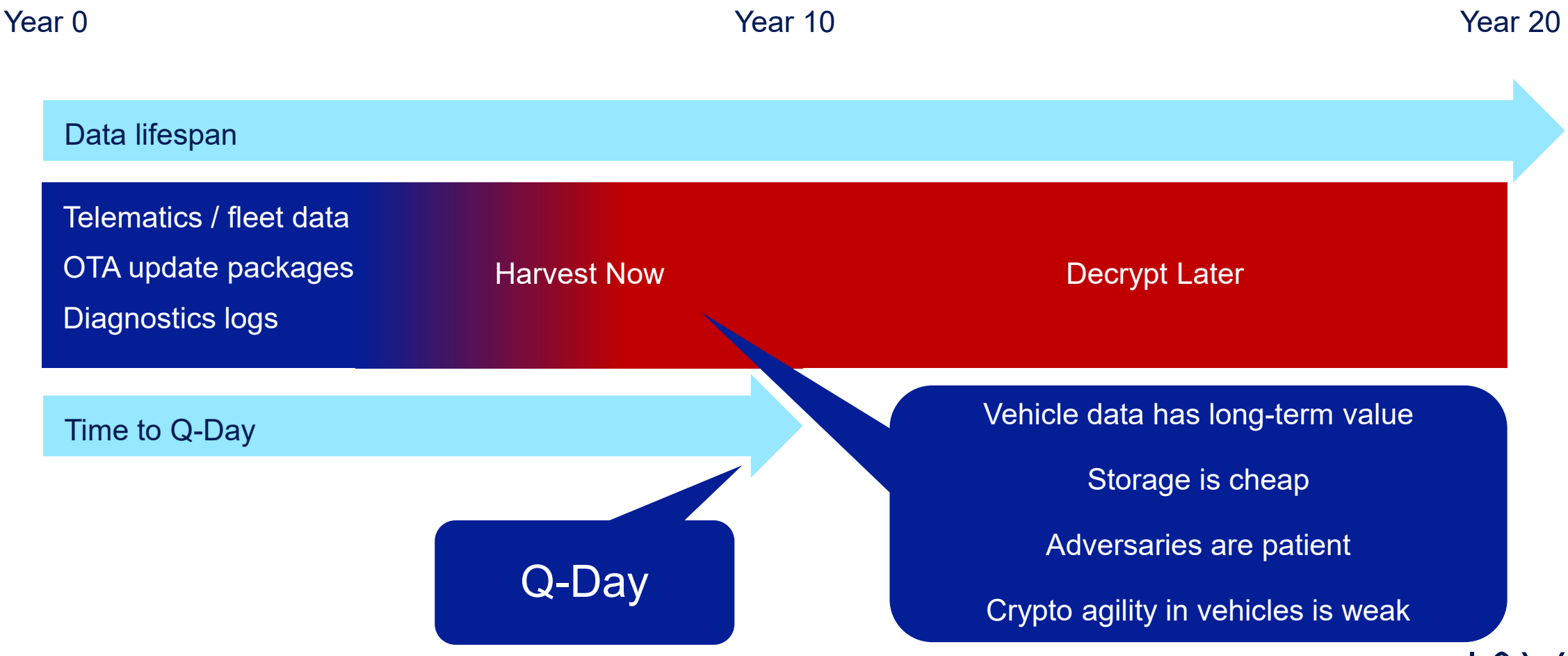
Threat → Today's HSM → Migration Path → Industry Alignment

Timeline

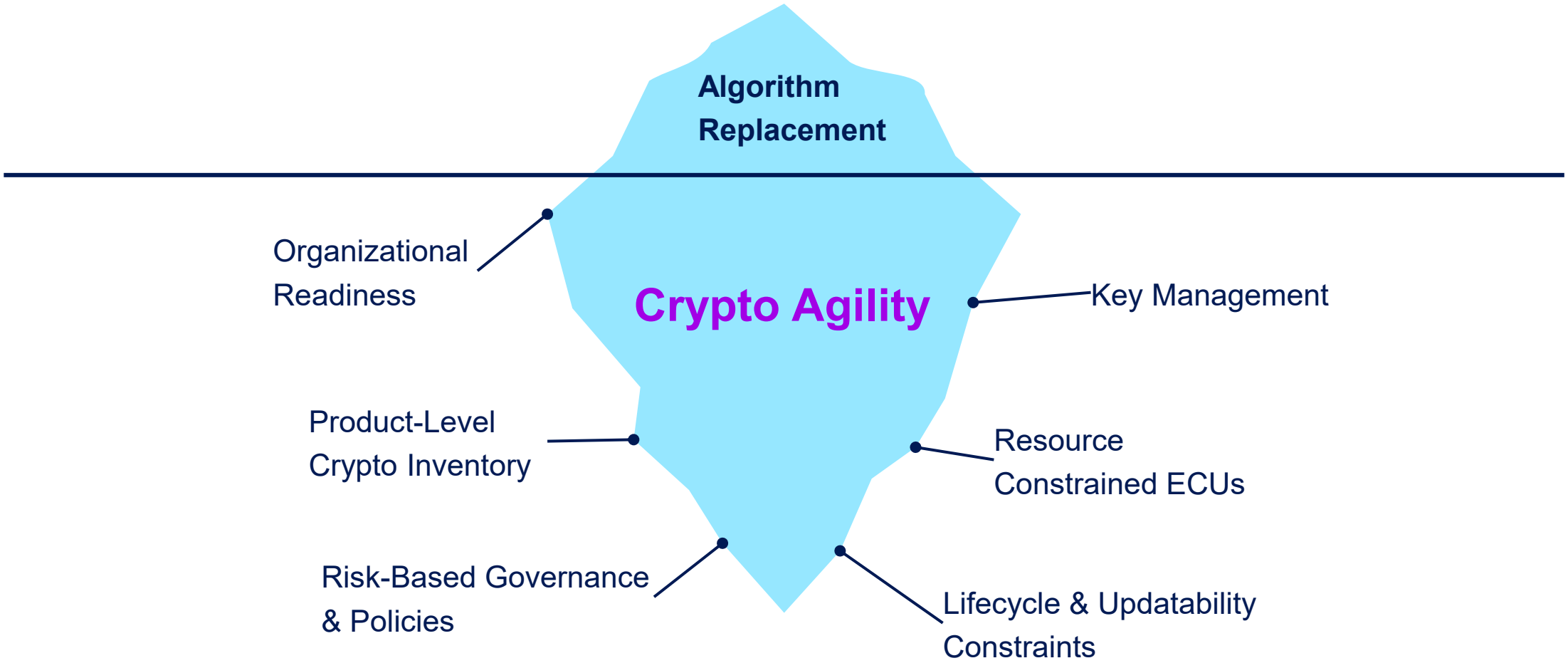


Vehicles entering production now must be secure against Q-Day threats

Invisible Timeline – Harvest Now, Decrypt Later Attack



Crypto Agility is More than Algorithm Replacement



Mapping Quantum Vulnerability Across the Vehicle Architecture

High PQC Focus
Telematics/Backend
TLS/ECDH key exchange

High PQC Focus
OTA Gateway
Software update signing

High PQC Focus
V2X
PKI infrastructure

High PQC Focus
Charging Communication
TLS/ECDH key exchange

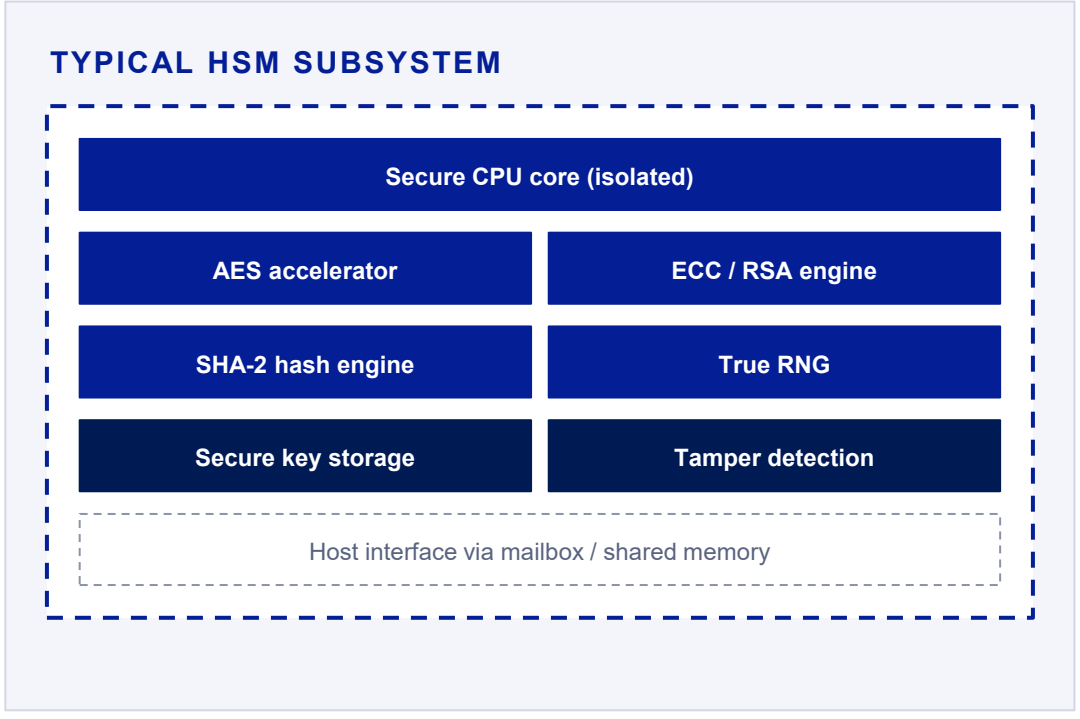
High PQC Focus
Digital Key
ECDH key exchange/PKI infrastructure

Medium PQC Focus
ECU
Secure boot

Medium PQC Focus
Diagnostics
UDS Security Access

Low PQC Focus
Internal CAN/Ethernet
Symmetric encryption/HMAC

Inside Today's Automotive HSM



Dedicated Secure Subsystem

Isolated core, isolated memory, independent of the host CPU

Fixed-function math	AES, SHA-2, ECC over NIST curves, RSA exponentiation
Bounded key storage	Typically a few KB – sized for ECC, not for PQC
Latency budget	Secure boot in ms TLS handshake in ms
Side-channel hardened	For the algorithms we have today

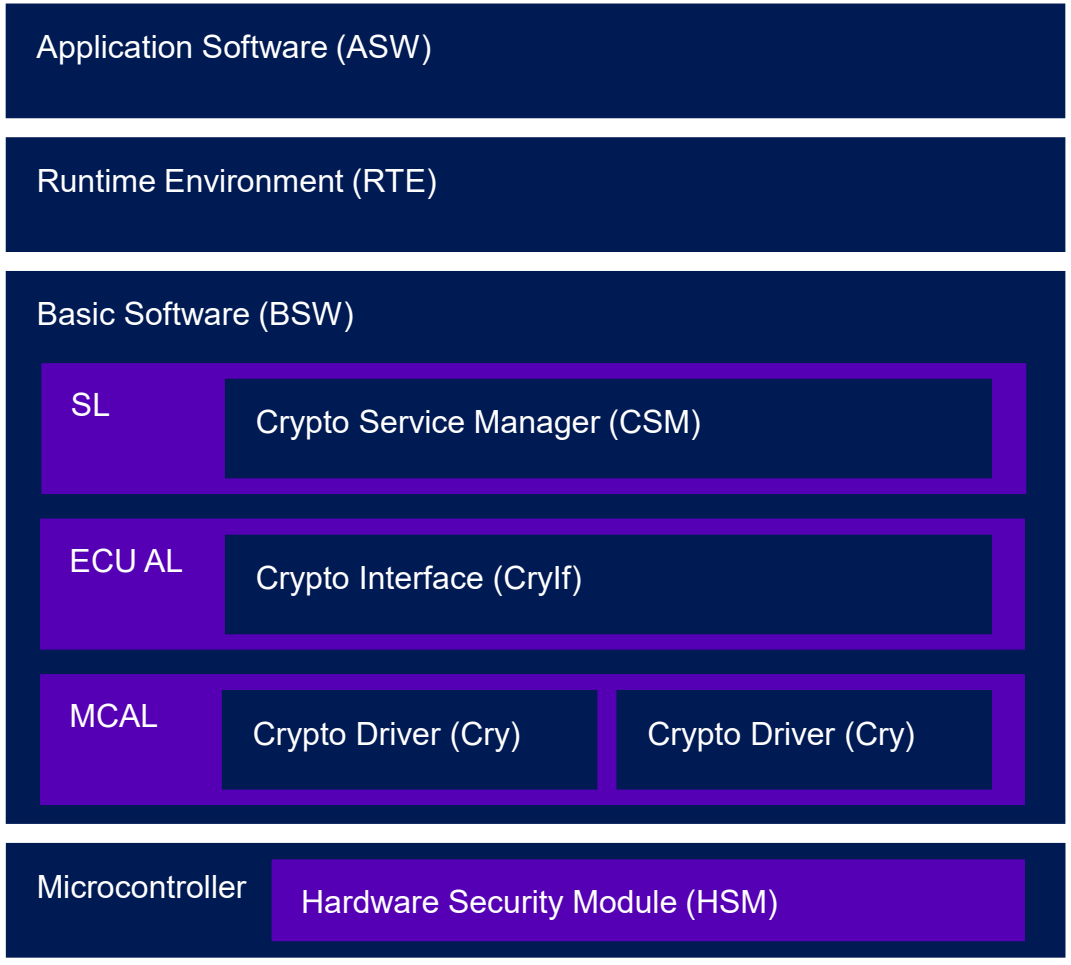
Today's HSM is purpose-built for ECC and RSA, not for PQC

In PQC Terms, Today's HSM is a Software-Only Platform

Capability	Classical (RSA/ECC)	PQC (ML-KEM, ML-DSA, FN-DSA, SLH-DSA, HQC)
Dedicated accelerator	Yes – silicon path	No – runs in software on secure core
Inner-loop primitives	Modular exponentiation, EC point math	NTT, Keccak permutation, binary polynomial multiplication
Key & signature sizes	32–512 bytes	1–50 KB - exceeds typical secure storage
Side-channel hardening	Mature, gate-level	Different leakage profile, still maturing
Standards available	Decades of deployment	FIPS 203 / 204 / 205 / 206 - 2024

The cryptographic algorithms have changed; the silicon has not, yet

Concept



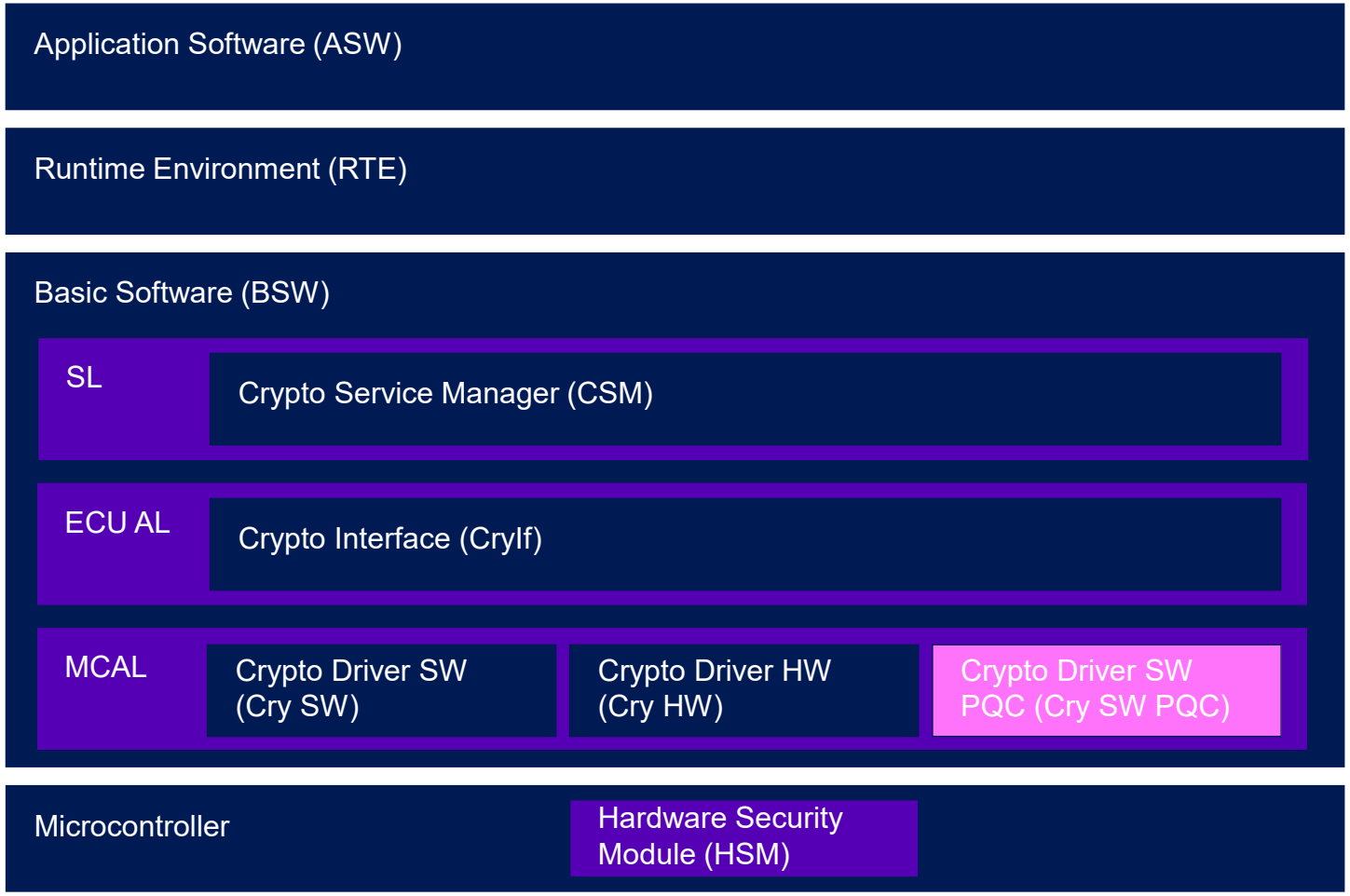
Basic Software (BSW)

- SL: provision of platform services as hardware-independent interfaces to application layer
- ECU AL: abstraction layer for the ECU (driver for additional components on the ECU)
- MCAL: abstraction layer for the microcontroller (driver modules)

Cryptographic Services (CS)

- CSM: Manager modules for administration of cryptographic requests
- CryIf: interface module to connect multiple cryptographic drivers
- Cry: cryptographic driver

Concept

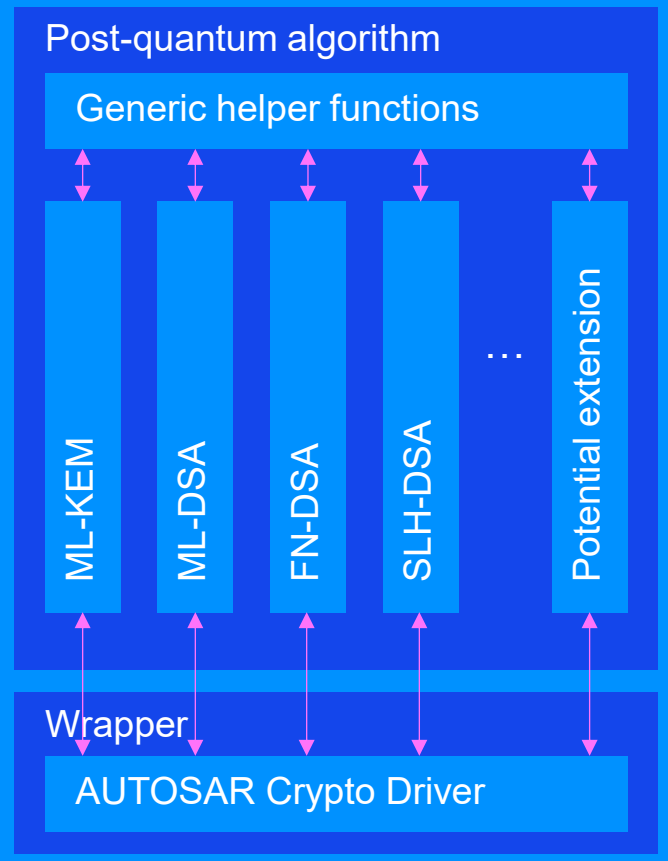


- AUTOSAR supports multiple Crypto Driver for Hardware and Software
  - Cry HW: Driver for Hardware Security Module interaction
  - Cry SW: Software library
- Connection to the Cryptography-Stack via Crypto Interface (CryIf)
  - Assignment and distribution of jobs to the various Crypto Drivers

→ **Crypto Driver of PQC**
➔ **IAV Primula**

IAV Primula

Post-Quantum Cryptography for Embedded Systems



IAV Primula is divided into two parts

1. Post-Quantum Algorithms

Platform-independent library implementing all algorithms standardized by NIST

- Implemented in C and Rust
- Available as an open-source repository on GitHub (currently the implementation in C, RUST follow in 2026)
- Extendable design to accommodate additional NIST-selected algorithms

2. Wrapper

Platform-dependent wrapper for adaption on different software architectures

- First specific implementation for AUTOSAR Classic Platform

NIST: National Institute of Standards and Technology
PQC: Post-Quantum Cryptography

Only Two Standardized Algorithms Fit Within Today's Automotive MCU Budgets

※ Benchmarked on Infineon AURIX TC399XP · single-core, scratchpad memory, performance-optimized
"Crypto-Agility in Automotive Real-Time Systems in Context of Post-Quantum-Cryptography", escar EU 2025

Algorithm	Type	Analysis	Status
ML-KEM (CRYSTALS-Kyber)	Key Encapsulation	Runtime and memory footprint are within an automotive ECU budget at all security levels	VIABLE
ML-DSA (CRYSTALS-Dilithium)	Digital Signature	Sign and verify runtime both acceptable. The default signature choice for the near term	VIABLE
FN-DSA (Falcon)	Digital Signature	Verify is fast. Sign exceed real-time budgets on resource-constrained MCUs	VERIFY ONLY
HQC (Code-based KEM)	Key Encapsulation	Runtime unacceptable. Memory footprint an order of magnitude above ML-KEM. Not viable without acceleration	NEEDS HW
SLH-DSA (SPHINCS+)	Digital Signature	Sign and verify runtime unacceptable. Not viable without acceleration	NEEDS HW

Hybrid Cryptography – Approach for Transition Period

- Defense-in-depth
  - If either algorithm is broken or downgraded by a future cryptanalytic result, the other still provides the security guarantee
- Algorithm fallback
  - Field rollback of a PQC algorithm is not a recall event. The classical leg keeps the system operational while the PQC side is patched
- Aligned with public guidance
  - IETF, BSI, and ENISA all endorse hybrid mode as the recommended transition posture through the late 2020s

From Software PQC to PQC-Enabled Silicon

NOW: 2026–2028

Software PQC on existing HSMs

- ML-KEM and ML-DSA in firmware
- Hybrid as default for external interfaces
- PQC requirements in RFQs

NEXT: 2028–2031

Transitional silicon

- Accelerators for Keccak and NTT
- Expanded secure key storage
- Side-channel hardening for lattice-based and hash-bashed operations
- First production vehicles with PQC-aware HSMs

FUTURE: 2031+

PQC-native HSMs

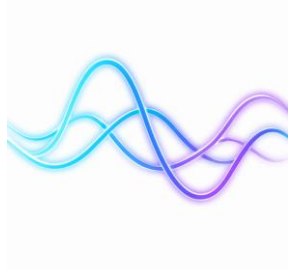
- Native PQC primitives at silicon speed
- Pure-PQC modes for new platforms
- Classical algorithms retained only for legacy interoperability

Software now → Transitional HSMs in late 2020s → PQC-native silicon by 2031

What Next-Generation HSM Silicon Requires

Keccak Permutation

SHA-3/SHAKE underlies ML-KEM, ML-DSA, and FN-DSA; (SLH-DSA offers both SHAKE and SHA-2 variants); Keccak acceleration benefits the majority of deployments



Number-Theoretic Transform (NTT)

The inner loop of ML-KEM, ML-DSA and FN-DSA. Dominates runtime in software and is the highest-value candidate for fixed-function silicon

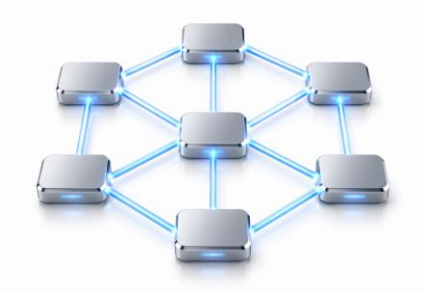
Larger Secure Key Storage

Key and signature sizes grow by one to nearly three orders of magnitude larger than ECDSA. Today's few-KB secure storage is undersized

Side-channel Hardening

Lattice and hash-based primitives have a different leakage profile than ECC. Hardening must be co-designed with the algorithm

Quantum Computing Does Not Care About Our Organization Charts



If we migrate independently

- “Twenty” incompatible PQC stacks across OEMs and tier-1s
- Charging stations and vehicles that no longer negotiate a session
- V2X communication that is incompatible among vehicles
- Digital keys that don’t roam between brands
- Diverging hybrid constructions, each provably correct but none interoperable

Result: A decade of integration pain that delays adoption

If we align

- Defined automotive PQC profiles across vehicle and infrastructure
- Common hybrid constructions for V2X, charging, and digital keys
- Shared validation suites that verify interoperability before deployment, not after
- HSM requirements converged in next-platform silicon

Result: A coordinated migration that delivers interoperability across vehicles, infrastructure, and brands from the start

Pieces Exist – Suggestions on How to Converge

Algorithms	Regulatory & Standards	In-Vehicle Stack	TEE & Secure Element	Operational Sharing
NIST	**UN R155 / ISO/SAE 21434**	**AUTOSAR**	**GlobalPlatform**	**Auto-ISAC**
FIPS 203/204/205/206: Done. HQC under draft standardization; additional algorithms expected	Cybersecurity engineering process - PQC must be integrated into existing CSMS	Crypto Service Manager, CryIf, software/hardware crypto drivers - the PQC plug-in points	Vehicle-to-infrastructure trust The convergence point for automotive PQC profiles	Threat intelligence on quantum and HNDL activity, shared in real time across members

Automotive PQC Profiles

Shared specs of algorithms, key sizes, hybrid constructions, certificate formats, and validation suites – defined per use case so vehicle and infrastructure negotiate the same way

- **V2X**: PKI, signatures, hybrid posture
- **Charging**: TLS, KEM, mutual auth
- **Diagnostics**: PKI-based Security Access
- **Secure boot**: signatures, key hierarchy
- **OTA updates**: package signing, agility
- **Digital Key**: KEM, attestation, roaming

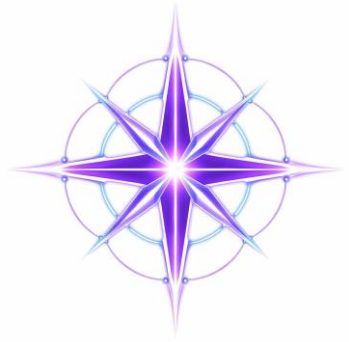
Next Steps

OEMs

- Put PQC requirements into your next platform RFQs
- Start the cryptographic inventory across the portfolio now: algorithms, protocols, libraries

Semiconductor Vendors

- Publish PQC HSM roadmaps with realistic timelines
- OEMs cannot plan against rumored silicon; published roadmaps are the primary input for next-platform RFQs



Standard Bodies

- Align on automotive PQC profiles
- Establish hybrid as the default transition mode and propose shared validation suites

All of Us

- Treat crypto agility as a platform requirement
- Crypto agility is not just algorithm replacement; it keeps every layer of the security stack adaptable as the threat landscape evolves

Contact

Dr. Dennis Kengo Oka
IAV Co., Ltd.
dennis.kengo.oka@iav.jp
www.iav.com

LinkedIn