UNIVERSITATEA LUCIAN BLAGA DIN SIBIU
HPI Hasso Plattner Institut
CLUJ IT
Sibiu IT Cluster
SID 2025
Sibiu Innovation Days
06 - 07 November, Sibiu - RO
EMERGING DISRUPTIVE TECHNOLOGIES:
Balancing Innovation, Risks, and Societal Impact

Challenges in Transitioning from Standard to Post Quantum Cryptography in Embedded Devices

Mircea Pop
Manager Security Firmware AAES NXP Semiconductors
6th Nov’25

Agenda

- Context and challenge
- About NXP and Automotive NXP
- Post Quantum Crypto – The need / Basics
- Definition of the security crypto pillars in automotive(including impact)
- Challenges for adopting PQC on legacy devices
- Strategies to address PQC on legacy devices
  - Libraries space
  - Redesign functionalities
  - Managing hybrid way of working
  - Limiting attack surface (reduce feature set availability)
- Conclusions

Context

- **Since 2020 – 0.5 Billion cars** have been **released to market**,
- Average of **80 ECUs in a car**
- More than **40 Billion of ECU's are on the streets**
- **Legacy ECUs** are **not resistant to Post Quantum processors attacks** –various security primitives are based on standard Public Key Crypto operations (RSA, ECC)
- New Silicon roadmaps that address PQ processors attacks are expected to go mass production starting 2026 (NXP included) **PQC Enabled ECUs**
- **Challenge – What are we doing to do with the Legacy ECU's ?**

Corporate Overview

A position of strength to better serve our 26,000+ customers

NXP Semiconductors N.V. (NXP) is a public Dutch company with headquarters in Eindhoven, Netherlands, and locations throughout the globe.

NXP has over 33,100 dedicated team members united by a passion to build solutions—not just products—that enhance the capabilities of people, organizations and society at large.

60+ year
history of experience and expertise

9,500
patent families

~33,100
talented team

~11,600
R&D members

Present in
30+ countries

$12.61B
annual revenue[1]

[1] Posted revenue for 2024 – Please refer to the Financial Information page of the Investor Relations section of our website at www.nxp.com/investor for additional information

The automotive industry is being disrupted

Time-to-market
3 - 5 yrs to
1 - 2 yrs

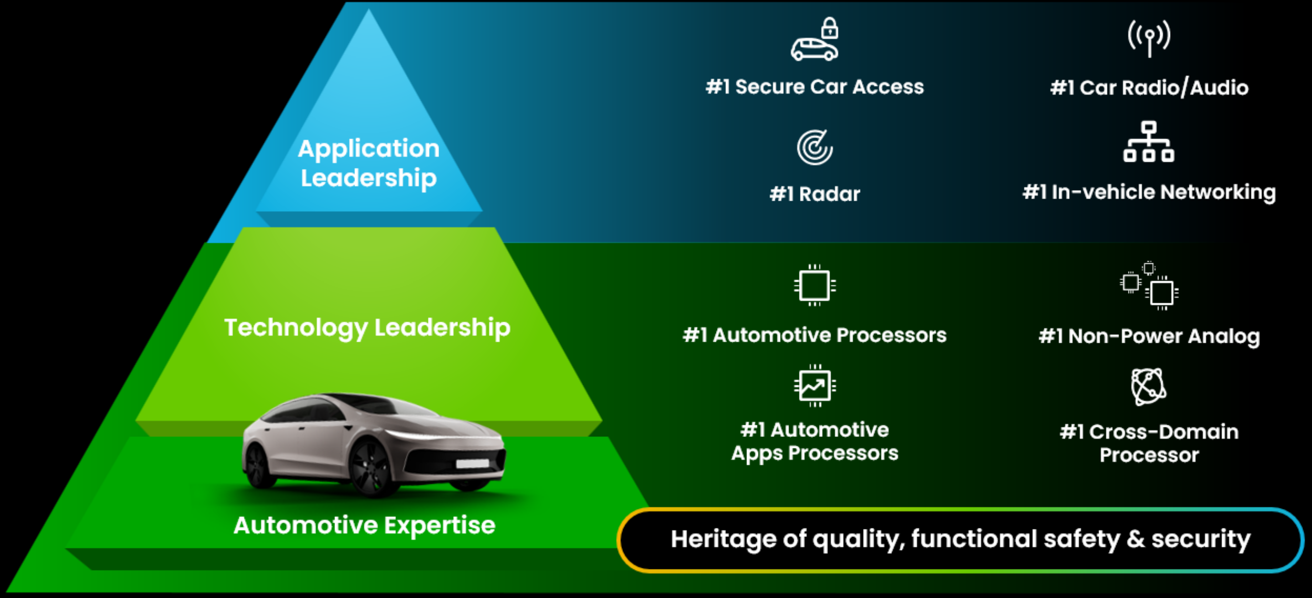
Lines of code
100M to
500M

Data in the car
50 GB
to 10 TB

ECU power
30 - 60W to
50 - 200W

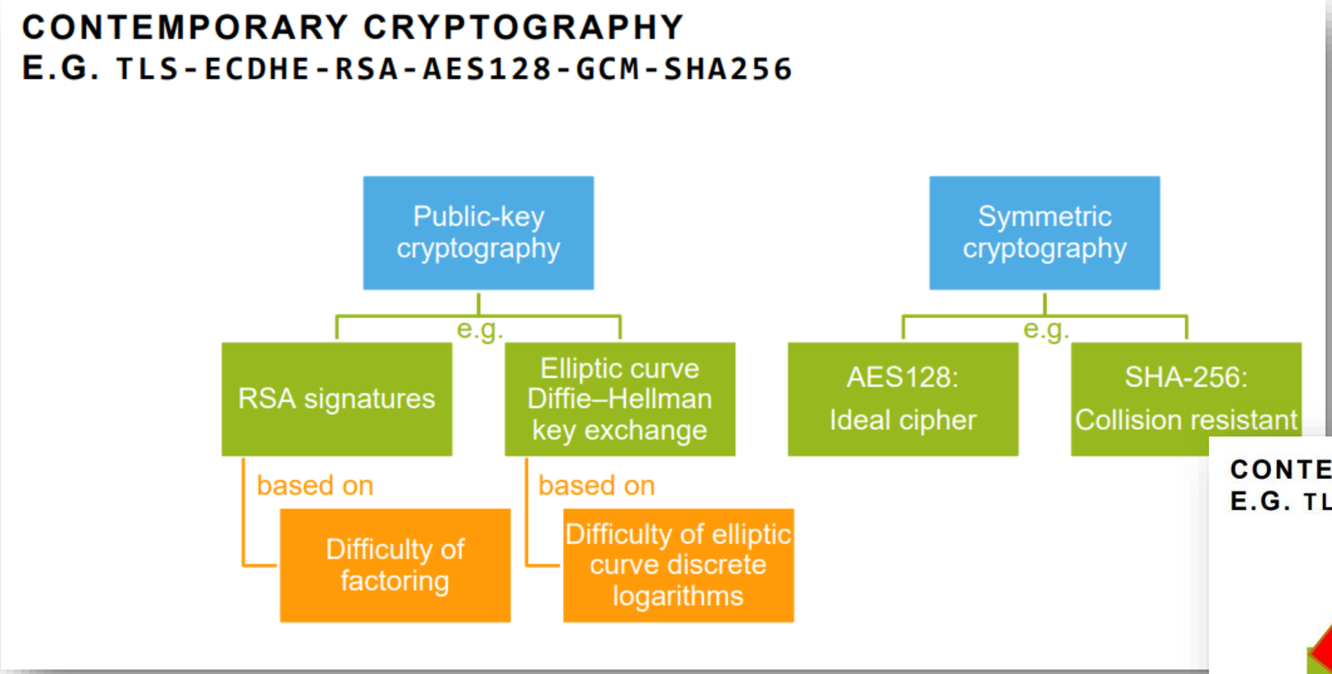
ADAS | Electric | Personalized

Shaping the future through innovation leadership



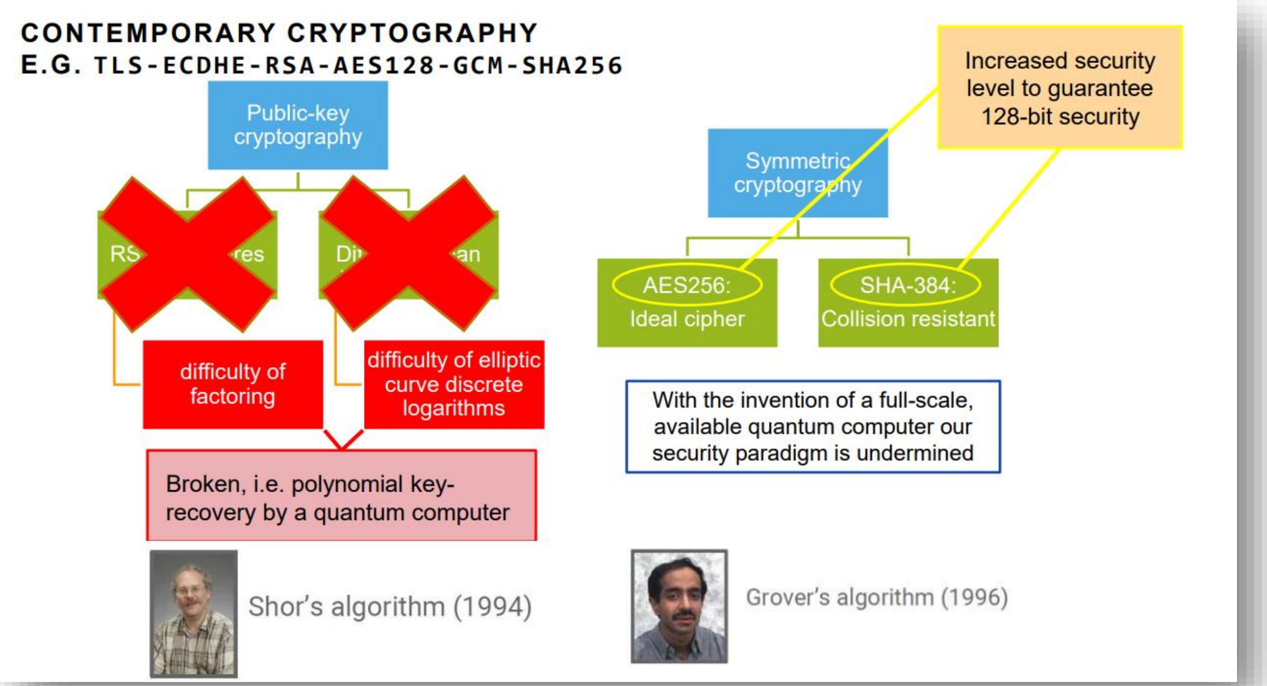
Sources: Strategy Analytics: Automotive Semiconductors Vendor Market Shares (April 2025, April 2024), Strategy Analytics: Infotainment and Telematics Semiconductors Vendor Market Shares (May 2025); Gartner: Semiconductors Market Shares (April 2025); S&P: competitive landscaping tool (April 2024)

Post Quantum computers and the impact upon standard cryptography



Introduction into Post Quantum Cryptography by Joppe Bos (NXP Semiconductors)

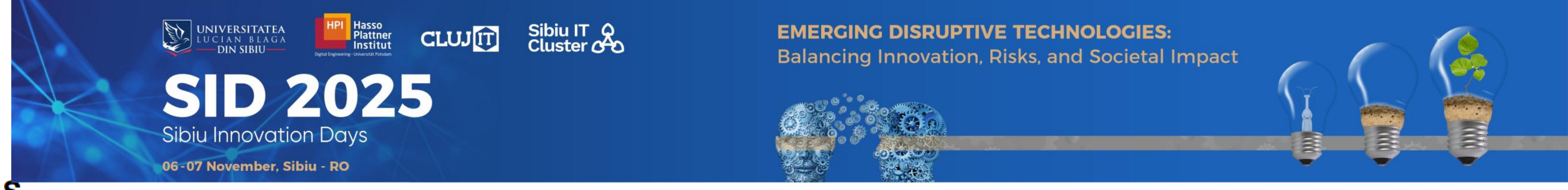
SCAN ME

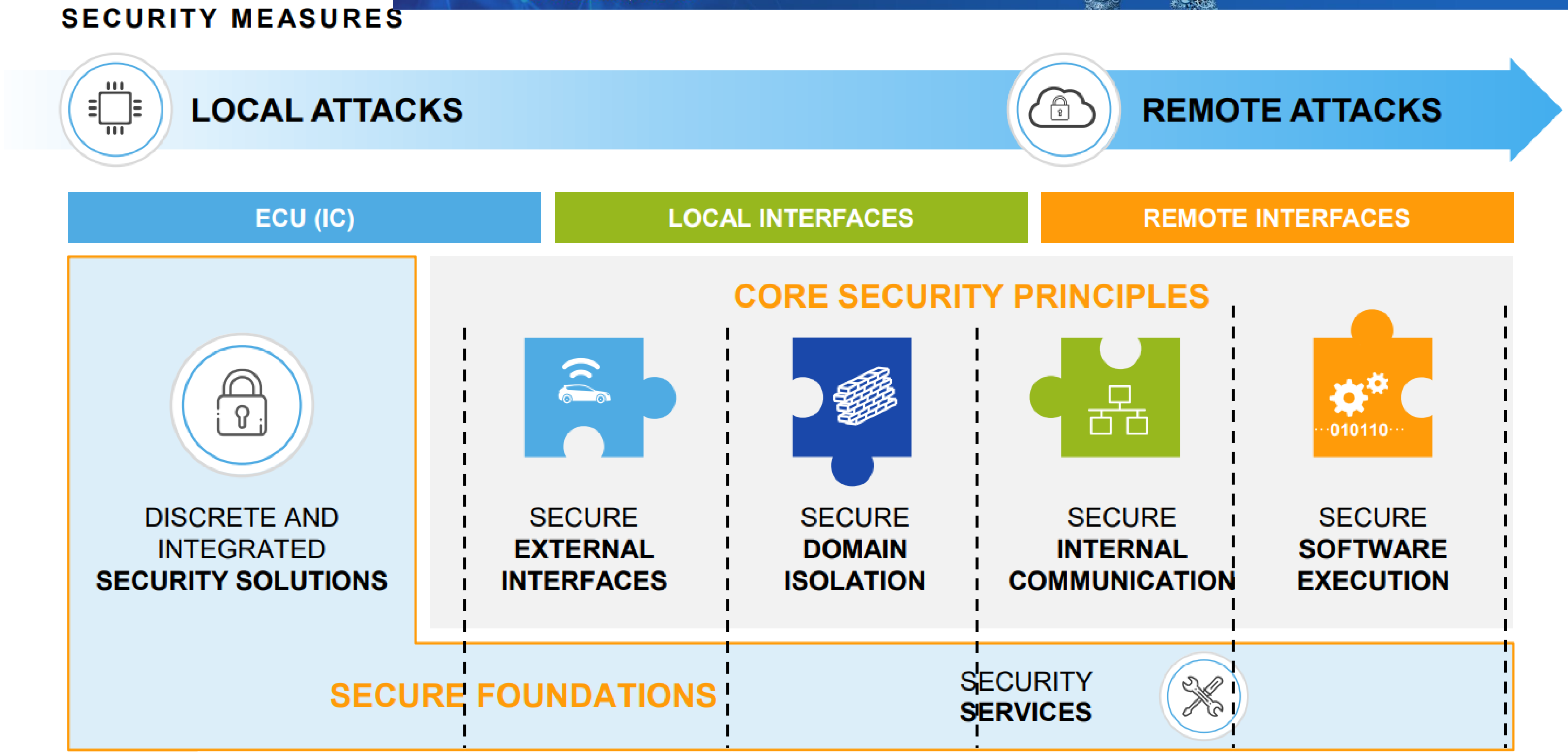


Post Quantum Crypto Algorithms statistics and sizes

Algorithm	Type	Usage	Typical Key Sizes	Typical Library Size
ML-KEM (formerly **CRYSTALS-Kyber**)	Key Encapsulation Mechanism (KEM) Lattice cryptography - Based	General encryption and key exchange (e.g., TLS)	Kyber512: Priv Key: **1632 B** Pub Key: **800 B** Kyber768: Priv Key: **2400 B** Pub Key: **1184 B** Kyber1024: Priv Key: **3168 B** Pub Key: **1568 B** Chiper size**: 768 B–1568 B**	50–70 KB (ref C), <**100 KB** (embedded)
ML-DSA (formerly **CRYSTALS-Dilithium**)	Digital Signature Algorithm Lattice cryptography - Based	Authentication and integrity **Large Keys**	ML-DSA-44: Priv Key: **2528 B** Pub Key: **1312 B** ML-DSA-65 Priv Key: **4000 B** Pub Key: **1952 B** ML-DSA-87: Priv Key: **4864 B** Pub Key: **2592 B** Signature Size: **2420 B–4595 B**	60–90 KB (ref C), ~**120 KB** (liboqs)
SLH-DSA (formerly **SPHINCS+**)	Digital Signature Algorithm Hash-based cryptography	Long-term digital signatures **Very large signatures**	SLH-DSA-SHA2-128s: Priv Key: **64 B** Pub Key: **32 B** SLH-DSA-SHA2-128f:Priv Key: **64 B** Pub Key: **32 B** SLH-DSA-SHA2-192s:Priv Key: **96 B** Pub Key: **48 B** SLH-DSA-SHA2-192f:Priv Key: **96 B** Pub Key: **48 B** SLH-DSA-SHA2-256s:Priv Key: **128 B** Pub Key: **64 B** SLH-DSA-SHA2-256f:Priv Key: **128 B** Pub Key: **64 B** Signature size: **8 KB–49 KB**	100–150 KB (ref C), ~**150 KB** (liboqs)

Security Pillars
PQC Impact





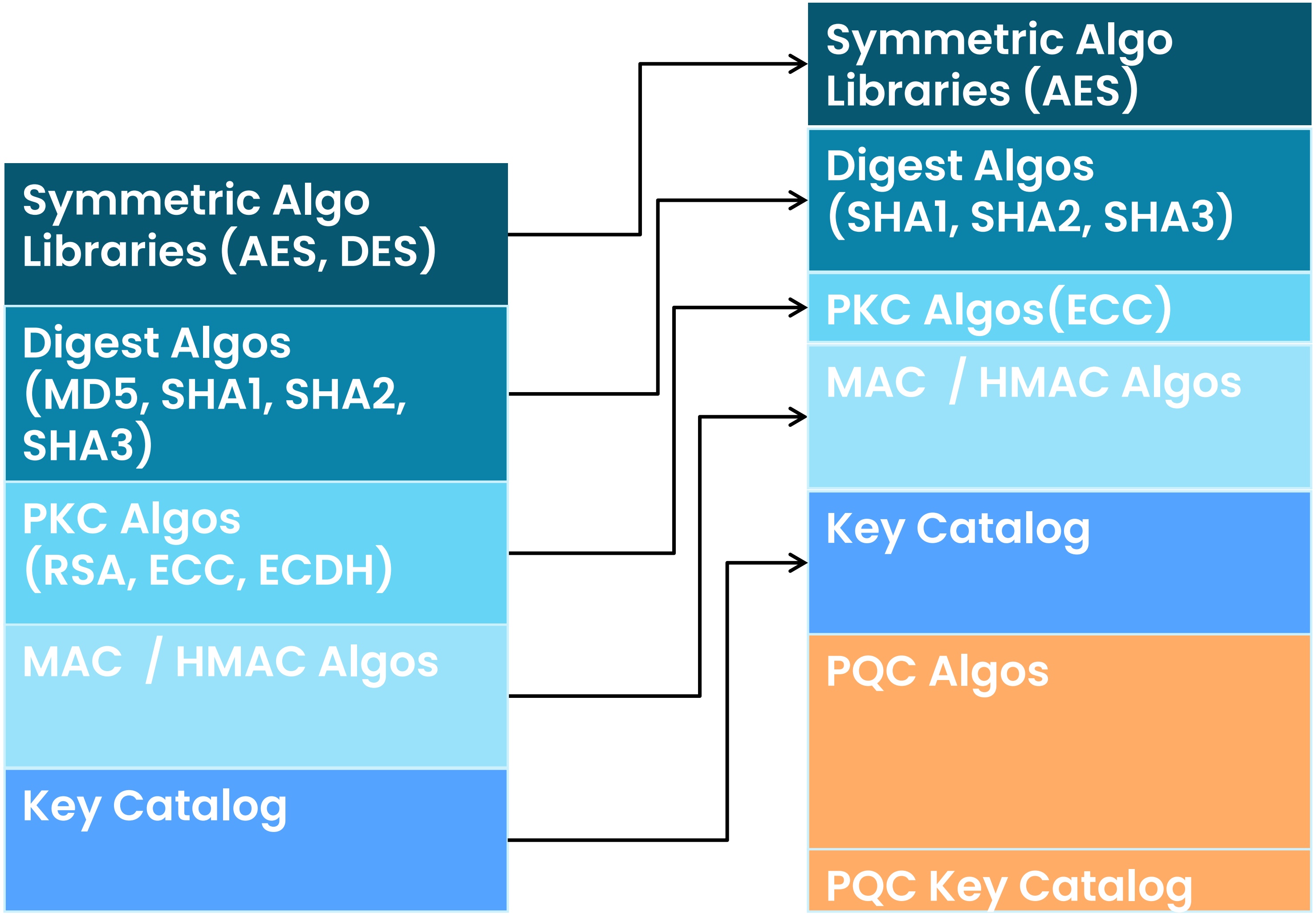
PQC Impact	High	No	Medium	Medium->High
	PKC Primitives highly used during handshake operations		PKC primitives slightly used in the Vehicle internal communication	PKC Primitives used to sign binaries during secure boot operations

Challenges for adopting PQC into embedded devices

Silicon Characteristics Challenges	Low Power Microcontrollers	Medium Performance Processors	High Performance Processors
SRAM Memory(programable memory)	**128KB-2304KB*** RAM	**8 MB**	**8MB-20MB**
Cores (NUM/Performance)	1-5 M7 @ 120-320 MHz	Arm Cortex-A53 @800 MHz 2x Arm Cortex-M7 @400 MHz	1-4 ARM Cortex A53 @ 1100-1300 MHz 3-4 ARM Cortex M7 @ 400 MHz
Internal Storage	**512KB-12MB P-Flash**	N/A (External Flash)	N/A (External flash)
Internal Secure Key Storage	**14KB**	**48KB**	**48KB**
PQC Readiness	ML-KEM(viable for Verification) MK-DSA(viable for Verification) SLH-DSA(not viable) **(only one algo can fit into device)**	ML-KEM(viable for Verification) MK-DSA(viable for Verification) SLH-DSA(viable – if signatures are kept in external flash) **(one algo can fit into device)**	ML-KEM(viable for Verification / Generation) MK-DSA(viable for Verification / Generation) SLH-DSA(viable – if signatures are kept in external flash)
	Programable memory available to adopt all PQC algorithms **L**		

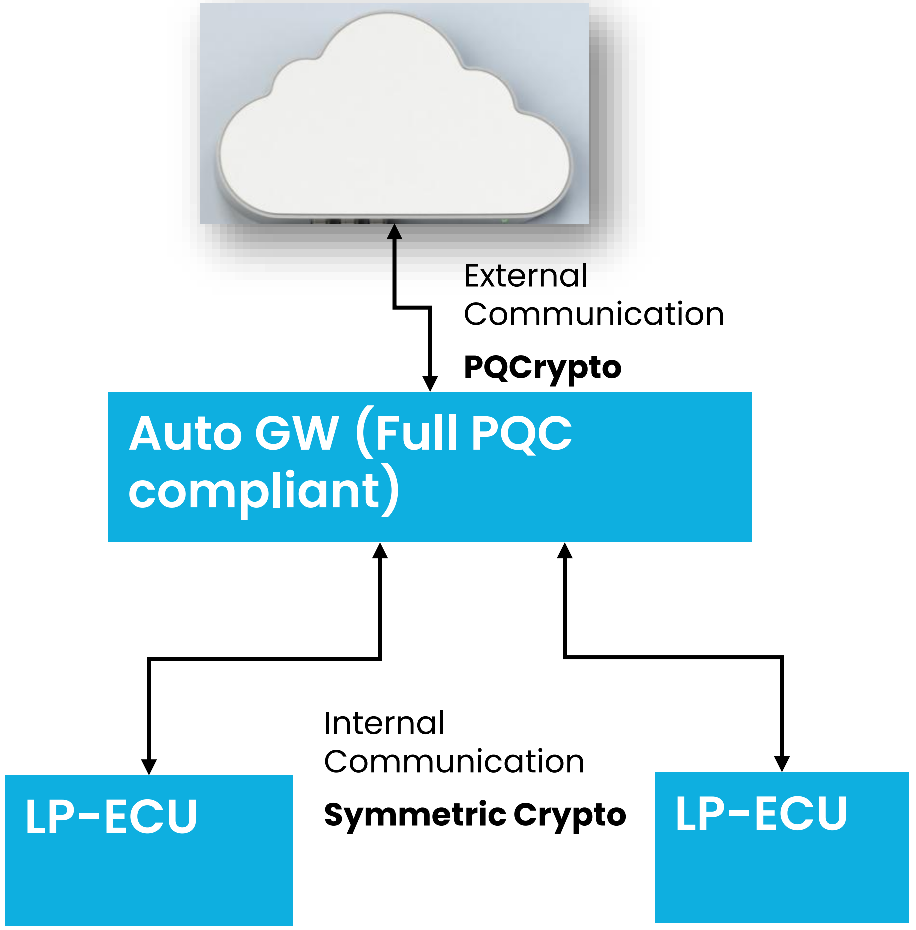
Strategies to address PQC on legacy devices

- **Libraries space memory optimization**
  - Update secure firmware layout libraries (remove algorithms / functionalities)
  - Remove crypto services related with the removed algorithms
  - Restrict usage of algorithms
- **Redesign functionalities**
  - Add support for PQC Key Catalogs – support large keys
  - Add support for large signature management (for SLH-DSA)
  - Enforce usage of symmetric crypto for secure boot scenarios



Strategies to address PQC on legacy devices

- Manage hybrid way of working ()
- Reducing the attack surface
  - **ECU Firmware updates performed using symmetric cryptography** (some OEM Key distribution systems used to create the internal communication channels) (signature verification using C-MAC)
  - **Update Secure boot** of devices instead of using PKC for signature verification – use C-MAC with device specific key
  - **Remove PKC algos +** update with PQC tailored algorithms (ML-DSA/ML-KEM) only verification on LP-ECU’s



Conclusions

- Post quantum processors generate a huge risk for the conventional cryptography
- Post quantum cryptography mitigates the risks – disadvantage – large size crypto libs, keys and signatures – requires reconsideration of the current security firmware's architectures
- Addressing potential attack surface can be a system challenge – redesigning the overall strategy of firmware update and secure boot might need to reconsider the entire security architecture of the vehicle (using central ECU’s to perform authentication of the Images planned to be deployed on LP-ECUs)

Questions