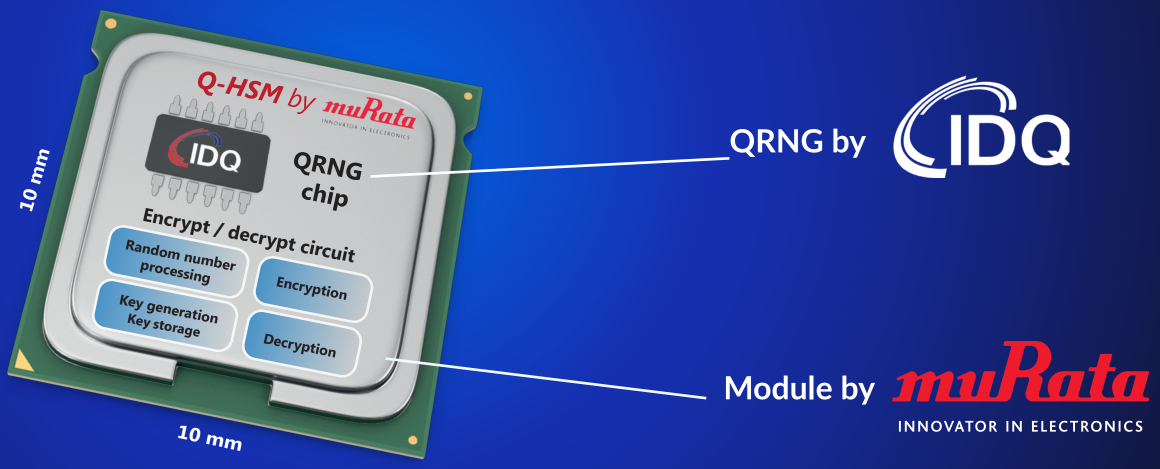
Quantum Hardware Security Module

The World's First IC Quantum based Hardware Security Module
The World's First PQC-compatible module



Quantum-Enhanced Security prevents cyber attacks

The automotive industry is in a major transition to connect, automate and electrify vehicles and to offer Mobility-as-a-Service (MaaS). This requires the use of a V2X ecosystem, where data is transmitted on-demand between data centres, the vehicle sensors and the vehicle controllers using high performance networks. Automobiles also have increased the number of in-vehicle systems that use or require over-the-air (OTA) communication to provide the best services to the consumer.

The need to exchange data between back-end systems and vehicles – as well as between vehicles directly – makes these systems vulnerable to cyber-attacks, which could lead to expensive vehicle recalls, significant safety risks and threats to human life.

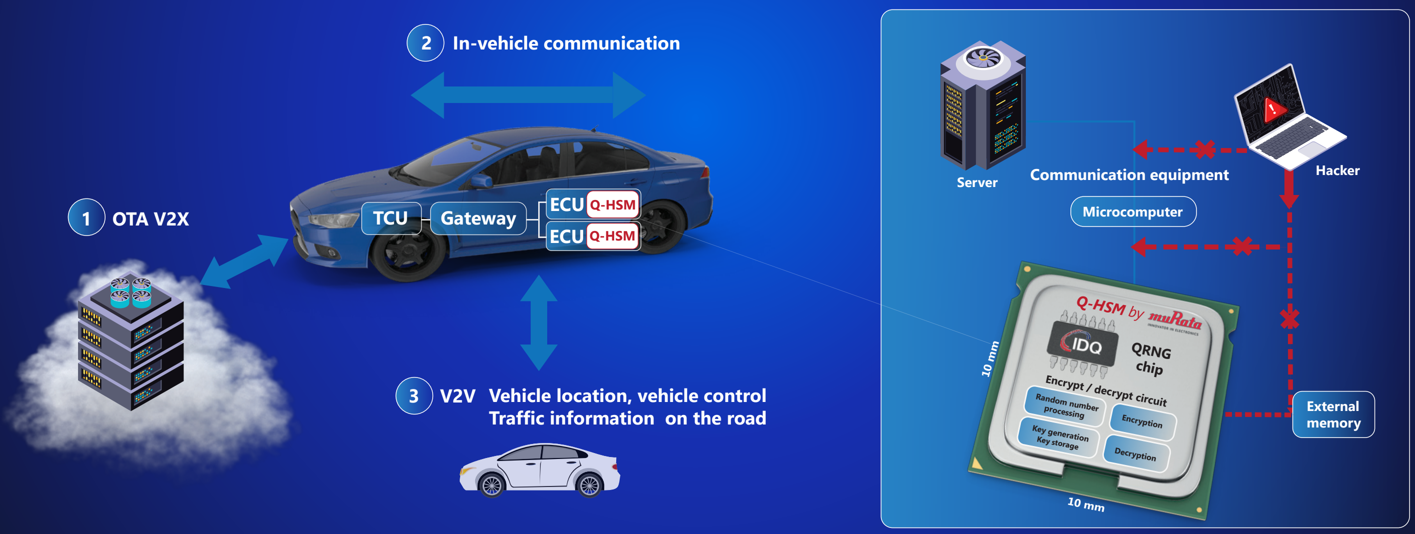
As the threat landscape evolves, the automotive sector is being targeted by not only frontal attacks on vehicle control systems (during systems updates and maintenance, for example), but also back-end breaches of the cloud or hybrid networks that form the data communication layer.

This leads to the need for both automotive Original Equipment Manufacturers (OEMs) and MaaS providers to invest in cloud security, network security and in-vehicle security.

IDQ's and Murata's joint cybersecurity integrated circuit (IC) solution is specifically designed to secure data in motion across V2X ecosystems & in-vehicle against existing and emerging threats, including those posed by quantum computing.

Quantum Hardware Security Module

Quantum-enhanced security can be embedded reliably in the security system of any car to ensure trusted and secured in-vehicle and V2X communications



*Q-HSM = Quantum Hardware Security Module

As it takes 5-7 years to design a new vehicle and vehicles stay in service typically for more than 10 years, **the time for manufacturers to act is now**

This integrated circuit Quantum hardware security module (Q-HSM) is based on IDQ's quantum RNG, and Murata's HSM technology.
Strong key generation is essential to ensure a third party cannot guess or deduce the security key for the HSM encryption.

IDQ's QRNG chip is **the world's smallest true Quantum Random Number Generator which instantly strengthen the encryption keys.**
It is ideal for integration into automotive HSMs, where its compact size, low cost, low power consumption and resistance to external environmental perturbations are critical.

Hardware Security Module

- High speed encryption
- Keystore possible
- PQC compatible

Quantum Random Number Generator

- Intrinsically and provably random
- Robust and controlled entropy
- Instant full entropy from the first bit

From a V2X ecosystem security perspective, vehicle systems, vehicle-to-vehicle networks, vehicle-to-infrastructure networks and back-end systems must be future-proofed by introducing quantum-safe cryptographic solutions as a priority.

Contact: Thomas.Stengel@idquantique.com

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.
- Q-HSM Brochure - Specifications as of March 2022.