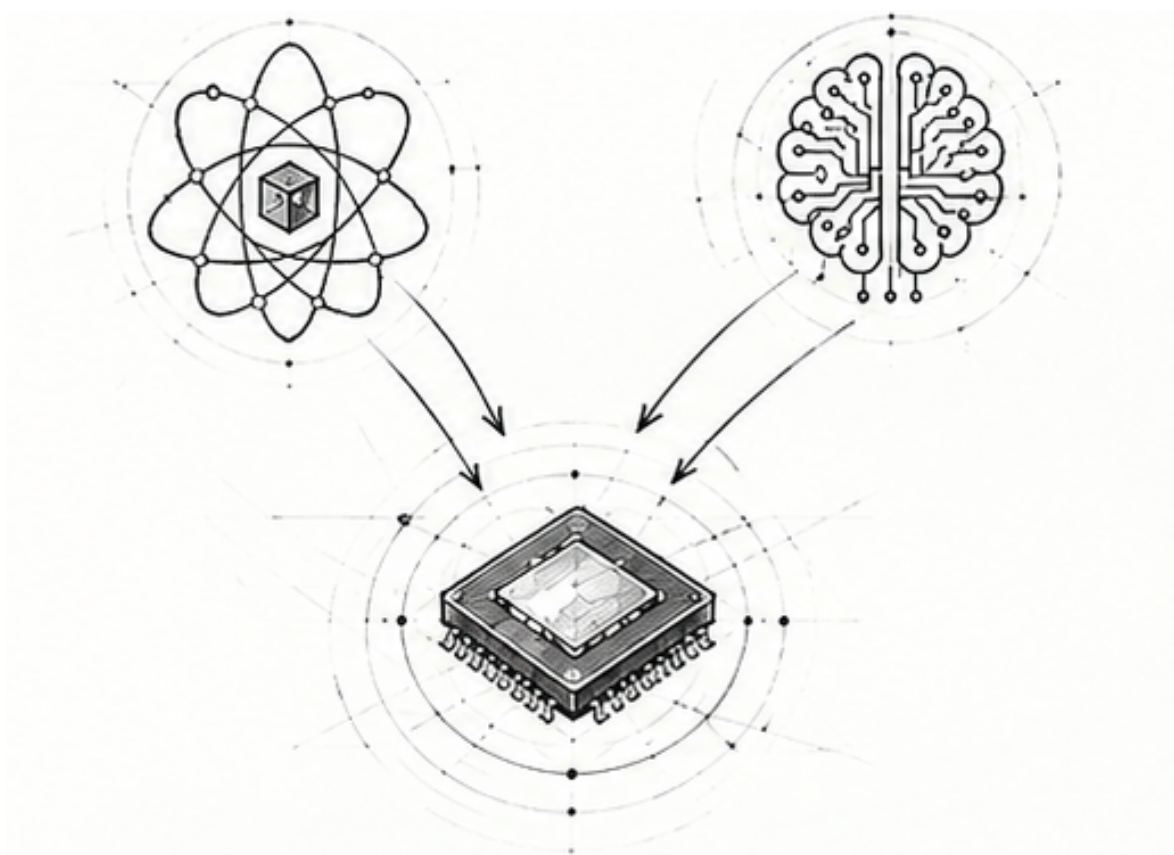


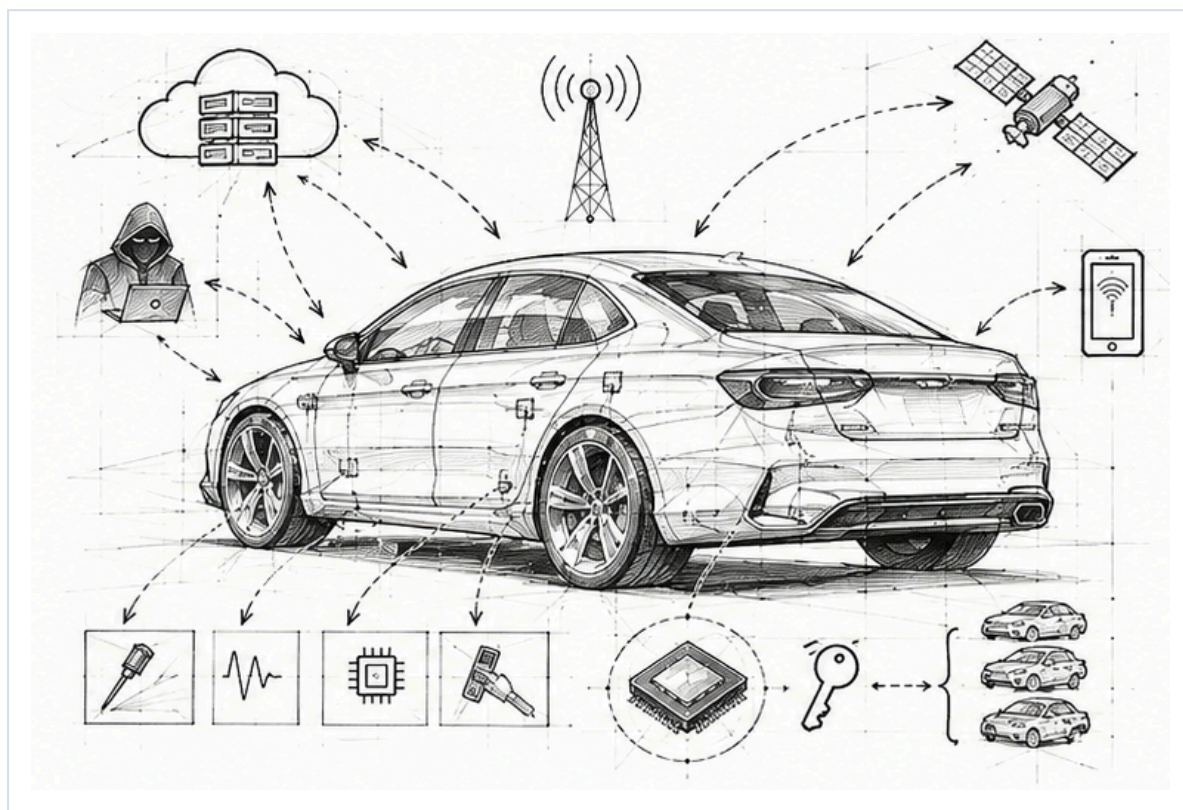
The Next Security Shift

A Trusted and Certified Hardware Foundation Is the Key to the AI and Quantum Era



Imagine an Attack on a Modern Vehicle

A modern connected car is a computer on wheels. It has powerful zonal processors, AI accelerators, wireless connections, cloud services, and over-the-air updates.



To attack it, a hacker does not need to break the cryptography itself. The real target is the chain of trust. A hacker can start with a software bug or a weak communication channel, or, because a car is physically easy to access, can attack the chip directly. A chip can leak information when it is running, through its power consumption, its electromagnetic emissions or its execution time. The hacker can then extract secret keys by reading these side-channel signals, or by injecting faults with lasers or electromagnetic pulses.

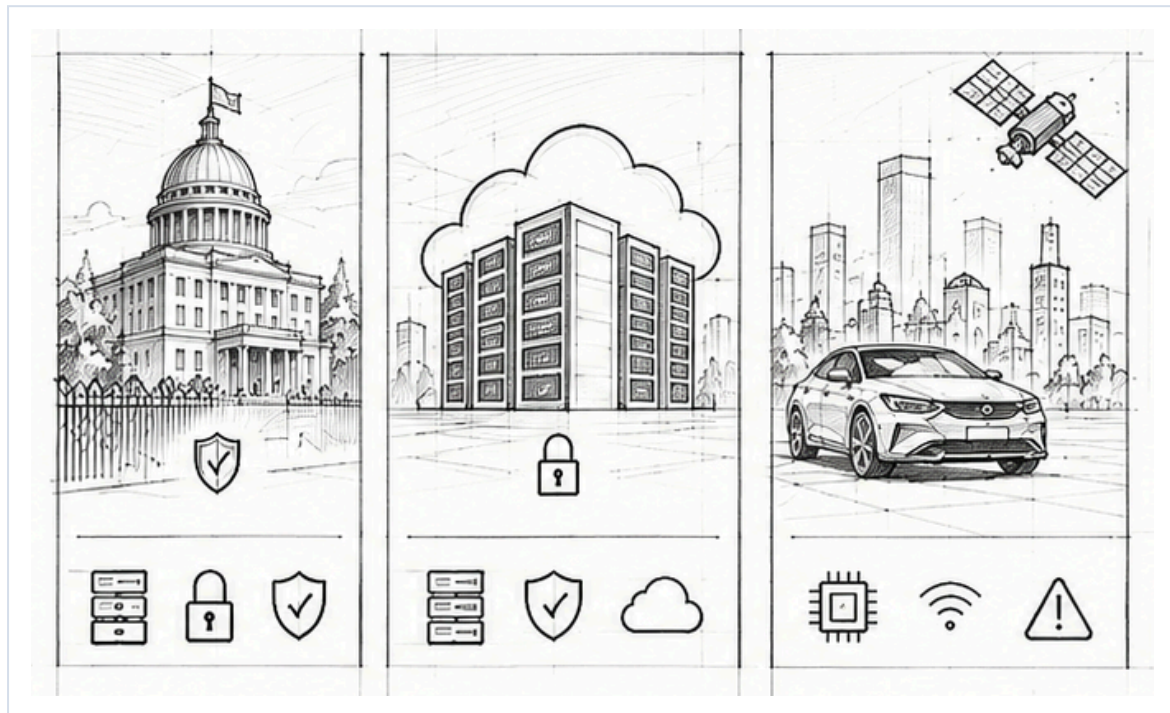
If the hacker gets a cryptographic keys, they steal the digital identity of the vehicle. They can impersonate real software, electronic control units or cloud services, push fake updates, or take control of the vehicle. And because the same platform is used in thousands of cars, one weakness can be replicated across the whole fleet. At this level, this is not just data theft. It becomes a safety and even a national-security risk: cars can be immobilized, manipulated, or even worse, turned into weapons.

This example applies to any connected device. It shows one thing clearly: cybersecurity is, at its core, a question of trust: trust in the device, trust in the software running on it, and trust in every interaction with the outside world.

Not All Cybersecurity Is the Same

Cybersecurity is usually thought of as a software problem: firewalls, operating systems, encryption.

Three main environments face very different risks.



Defense and national security

Highest level of protection, tightly controlled and proprietary systems.

Cloud computing

Protected by data centers with strong physical security, so software-based protection (virtualization, secure enclaves) works well.

Embedded systems and IoT

Payment cards, cars, medical devices, robots, industrial equipment, satellites, and billions of other products. Here, an attacker can buy the device, open it, and attack it directly. This is a fundamentally different, and much harder, problem: security must resist both cyber and physical attacks.

1 KEY MESSAGE

Security Is at a Fundamental Turning Point

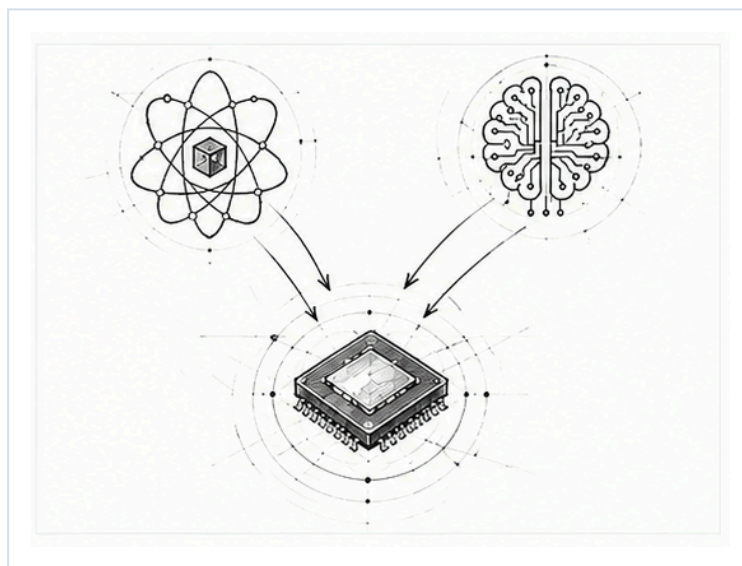
Threats are everywhere. Every connected device — a car, a robot, a meter, a medical device — is a potential target, and the consequences are no longer theoretical: a compromised car can become a weapon. This is not a future risk; it is happening now, at scale.

2 KEY MESSAGE

Post-Quantum Cryptography Is Threat, but AI May Be the Bigger Threat

Quantum computers will break today's most common encryption (RSA, elliptic curve). Moving to Post-Quantum Cryptography (PQC) is essential, and everyone is rightly working on it.

But new algorithms alone are not enough: keys and implementations still need a certified hardware foundation. Classical cyber and physical attacks will not disappear with PQC. In fact, AI may become the most important threat of all.



The cybersecurity challenge is no longer just quantum computing. AI is rapidly becoming a force multiplier for attackers, accelerating vulnerability discovery, reverse engineering, and attack automation. It analyzes code and hardware faster than any human team and makes sophisticated hardware attacks cheaper and more accessible.

Recent incidents have demonstrated how advanced AI systems can identify and exploit previously unknown weaknesses autonomously, highlighting the growing need for certified hardware roots of trust that remain resilient against both classical and AI-driven attacks.

A security solution that is not strong enough will have its weaknesses found — and AI makes this faster and easier. It is now clear that this will happen.

Trust Starts with Hardware

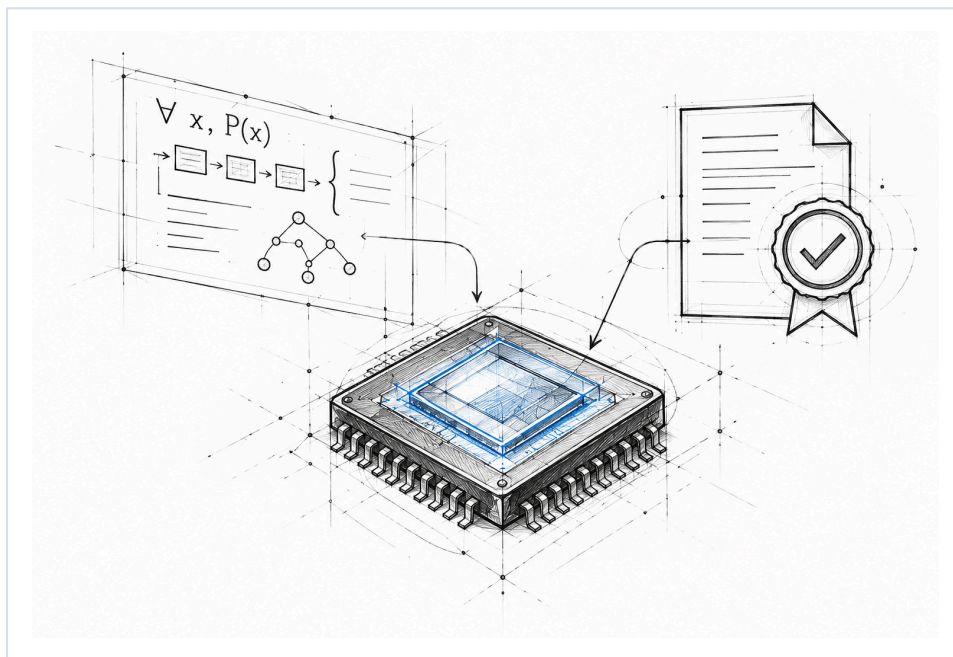
Every software security function depends on one question: where is trust established? Keys must be generated and managed properly across the whole supply chain, from chip manufacturing and key injection to device assembly, provisioning and deployment in the field. Keys must be stored somewhere that stays secure even if the software above it is compromised.

This is the role of the Hardware Root of Trust: Secure Elements, TPMs (Trusted Platform Modules), HSMs (Hardware Security Modules), and dedicated security processors — regardless of what the security silicon is called.

Certified Hardware, Proven by Formal Methods, Is a Must

Having security features is not the same as having certified security.

Many processors now include secure enclaves and isolated execution zones. These help a lot in cloud and enterprise settings. But for devices exposed to physical attacks, this is not enough.

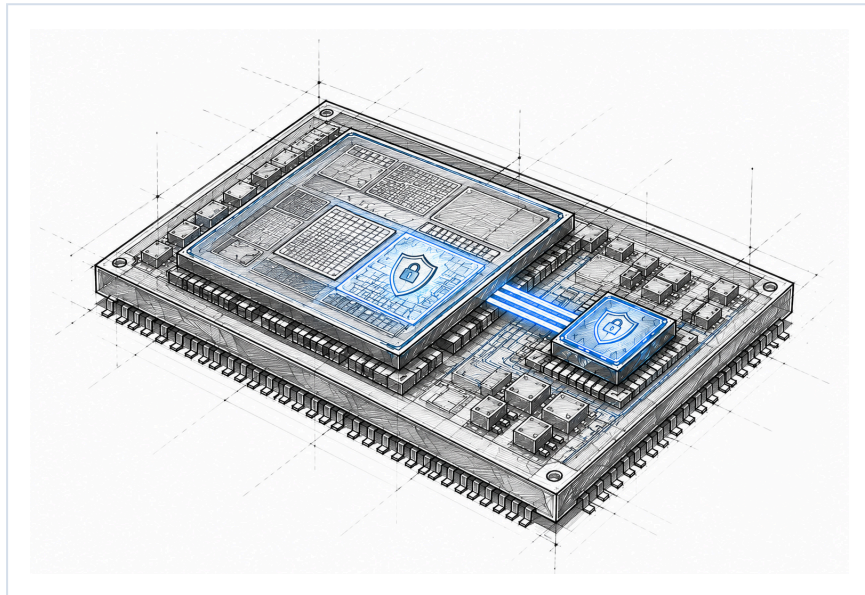


Certified components go through formal or semi-formal proof, rigorous threat analysis, and independent evaluation (such as Common Criteria), plus real testing against physical attacks.

This is no longer a debate. As AI-powered attacks grow stronger, uncertified secure enclaves and embedded elements will be broken. Independent, certified, formally proven and certified hardware protection is a requirement, not an option.

The Next Architecture — Chiplets with a Security HSM Chiplet

Another important trend in semiconductors is the shift from a single monolithic chip to chiplet (or advanced System-in-Package), architectures, where several dies are combined in one package — and this is exactly where hardware security is making a strong comeback.



Main processor & AI accelerator

The main processor and AI accelerator handle performance and run complex software, with a secure enclave close to the operating system.

Certified HSM chiplet

A separate certified HSM chiplet, connected through advanced packaging independently generate and protects keys, device identity, secure boot, and attestation.

A natural question: does the link between the two chips create a new weakness? The answer is to treat them as one trusted system, not two separate parts. During manufacturing, the secure enclave and the HSM chiplet are cryptographically bound together with unique diversified keys. They authenticate each other and build a protected channel for all further communication.

This way, each chip does what it does best: the enclave handles fast, software-close execution; the certified HSM chiplet delivers independently proven protection against both cyber and physical attacks.

Conclusion

Cybersecurity is entering a new phase. Connected devices are everywhere, quantum computers threaten today's cryptography, and AI is reducing the cost of cyberattacks while taking offensive capabilities to a new level.

The answer is not hardware instead of software. It is building systems on a trusted, certified hardware foundation — where secure enclaves and certified HSM chiplets, cryptographically bound, work together as one chain of trust.

This is the direction companies will need to follow to remain trusted in the AI and quantum era — and few are positioned to deliver it end to end.

SEALSQ

SEALSQ combines deep hardware-security expertise, strong secure software development, advanced post-quantum cryptography, and the ability to reach demanding certifications such as Common Criteria EAL5+. SEALSQ design security ICs, IP, and custom security chips built to meet the highest security and certification standards, for a quantum-safe and AI-safe future. PKI, digital identity, and certificate management extend that trust from the chip to the software, the network, and the cloud. This is how SEALSQ and WISeKey extend trust from the semiconductor to the full connected and secure system.