TESSOLVE

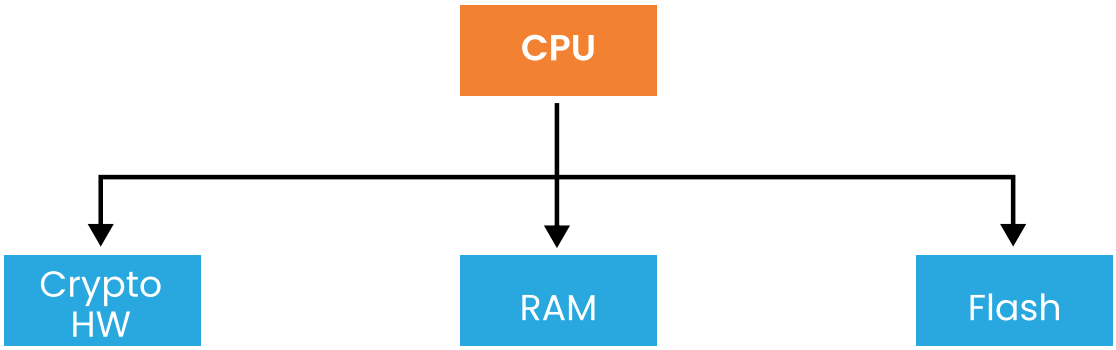


Hardware Security Module (HSM) Crypto Key & Signature Management

for AUTOMOTIVE application safe launch

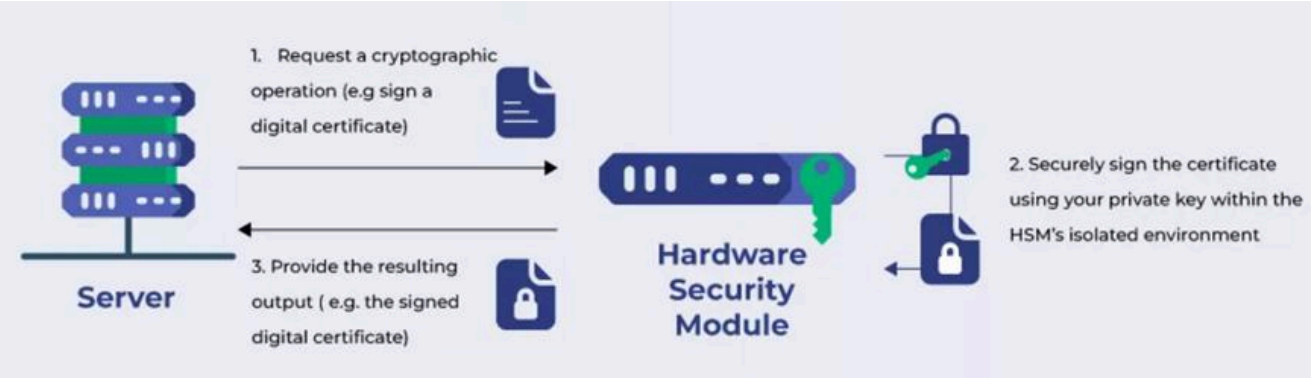
What is a Hardware Security Module (HSM)?

Hardware security modules (HSMs) are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. And its a special “trusted” network computer performing a variety of cryptographic operations: key management, key exchange, encryption etc.



HSM (Hardware Security Module)

HSMs are tested, validated and certified to the highest security standards including FIPS 140-2 and Common Criteria (which is an international standard for computer security certification, Based on ISO/IEC 15408).



Key and Signature Management with HSM

HSMs include built-in, high-quality random number generators (RNGs) that produce truly random and unpredictable cryptographic keys. This ensures the strength and integrity of the keys generated.

Cryptographic keys, especially private keys, are stored within the secure, tamper-resistant confines of the HSM. This physical isolation prevents unauthorized access and extraction, even if the surrounding system is compromised.

HSMs are crucial for digital signature management. They securely store the private keys used to create digital signatures, ensuring the authenticity and integrity of signed data or documents. They can also be used to verify digital signatures by accessing the corresponding public keys.

HSM acts as a dedicated, highly secure cryptographic processor that ensures the confidentiality, integrity, and availability of cryptographic keys and the operations performed with them, particularly in the context of digital signatures.

Key and Signature Management with HSM for Automotive

The rapid advancement of connected and autonomous vehicles necessitates robust hardware-level security to safeguard against escalating cyber threats. This white paper explores the critical role of Hardware Security Modules in automotive systems, focusing on secure cryptographic key management, digital signature enforcement, and trusted execution for advanced applications like OTA updates, V2X communications, and secure ECU firmware validation. We present an HSM architecture compliant with ISO 21434 and UNECE R155, leveraging hardware-accelerated AES-256, ECC-P256, and SHA-3 to ensure tamper-proof key storage and secure boot integrity. Key topics include secure key provisioning, anti-cloning measures, and real-time signature verification for automotive use cases such as EV battery management systems, autonomous driving modules, and vehicle-to-cloud authentication. The paper also addresses side-channel attack mitigation, HSM-assisted TLS 1.3 for V2X, and hardware-enforced secure debug access, providing a comprehensive framework for implementing zero-trust security in next-gen vehicles. By integrating HSMs with AUTOSAR Crypto Stack, we demonstrate how automakers can achieve ASIL-D compliance while balancing performance and security in resource-constrained ECUs. Finally, we outlined a test methodology for validating HSM resilience against fault injections, DPA attacks, and supply chain threats, ensuring end-to-end security from silicon to vehicle deployment.

1. Introduction 5
2. Background 5
3. Abbreviations 5
4. Current Challenges in Automotive 6
5. Objectives of Automotive HSM 6
6. Automotive HSM System Architecture 7
7. Methodology 8
8. Secure Communication 9
9. Use case 11
10. Standing strategies of Automotive HSM 12
    - Cryptographic Algorithms Development 12
    - Key Management 12
    - Test and validate the HSM's Crypto keys 13
    - Firmware OTA update 14
11. Future Scope 14
12. Conclusion 14
13. References 15

1. Introduction

The automotive industry is undergoing a transformative shift toward software-defined vehicles, connected ecosystems, and autonomous driving, amplifying the need for uncompromising hardware security. As modern vehicles evolve into rolling data centers, they face escalating threats from ECU tampering and malicious OTA updates to V2X spoofing attacks. This white paper examines the pivotal role of Hardware Security Modules (HSM) in enabling cryptographic key management, secure boot, and digital signature validation for next-generation automotive systems. By anchoring security in tamper-resistant silicon, HSMs provide a root of trust for critical functions like secure firmware updates, vehicle-to-cloud authentication, and safety-certified ADAS operations. We analyze HSM integration challenges in AUTOSAR-based ECUs, hardware-accelerated cryptography (AES-256, ECC, SHA-3), and compliance with ISO 21434/SAE J3061. The paper also explores HSM-assisted secure debugging, key lifecycle management, and resilience against side-channel attacks, offering automakers a blueprint to achieve ASIL-D security without compromising real-time performance. Through case studies on EV battery systems and autonomous driving controllers, we demonstrate how HSMs bridge the gap between functional safety ISO 26262 and cybersecurity, ensuring zero-day exploit protection across the vehicle lifecycle.

2. Background

Modern vehicles are composed of interrelated ECUs, which govern critical functionalities and interact among themselves through different protocols like CAN and Ethernet. Threat exposure thus increases with wireless connectivity. Hardware security is mandated by standards like ISO 21434 and UNECE WP.29. The Hardware Security Module prevents cryptographic operations from interference to secure vehicle software and data during its lifespan.

3. Abbreviations

ECU	-	Electronic Control Unit
ASIL	-	Automotive Safety Integrity Level
V2X	-	Vehicle to Everything Communication
ISO	-	International Organization for Standardization
TLS	-	Transport Layer Security
PKI	-	Public Key Infrastructure
FIPS	-	Federal Information Processing Standard
AES	-	Advanced Encryption Standard

SHA	-	Secure Hash Algorithm
ECC	-	Elliptic Curve Cryptography
RSA	-	public-key cryptographic algorithm (Rivest–Shamir–Adleman)
ECDSA	-	Elliptic Curve Digital Signature Algorithm
WP.29	-	UNECE World Forum for Harmonization of Vehicle Regulations No.29
OTA	-	Over-the-Air update
DPA	-	Differential Power Analysis attack

4. Current Challenges in Automotive

The automotive system faces challenges in the secure management of cryptographic keys over distributed ECUs, the authentication of firmware in its installation and update, and the protection of V2X communications from attacks. In maintaining high security, there is a constraint of keeping up with real-time performance requirements, conforming to stringent regulatory standards, and considering the tough prospect of quantum computer-based attacks.

5. Objectives of Automotive HSM

Automotive HSMs work at the chip level as trusted components working to protect cryptographic keys, produce secure digital signatures, and provide acceleration for encryption and decryption. Being foundational security measures, they isolate sensitive cryptographic processing from vehicle main processors. Its main goals are to overcome problems in security such as secure key management, firmware integrity validation, and authenticated communications within the vehicle. Hardware Security Modules allow enforcement of automotive cybersecurity standards by embedding custom architectures and protocols within the modules. Practical implementation methodologies are evaluated about integrating the same into real-time multi-ECU systems, while the future trends focus on scaling the platforms using virtualization and post-quantum cryptography for a more secure future.

6. Automotive HSM System Architecture

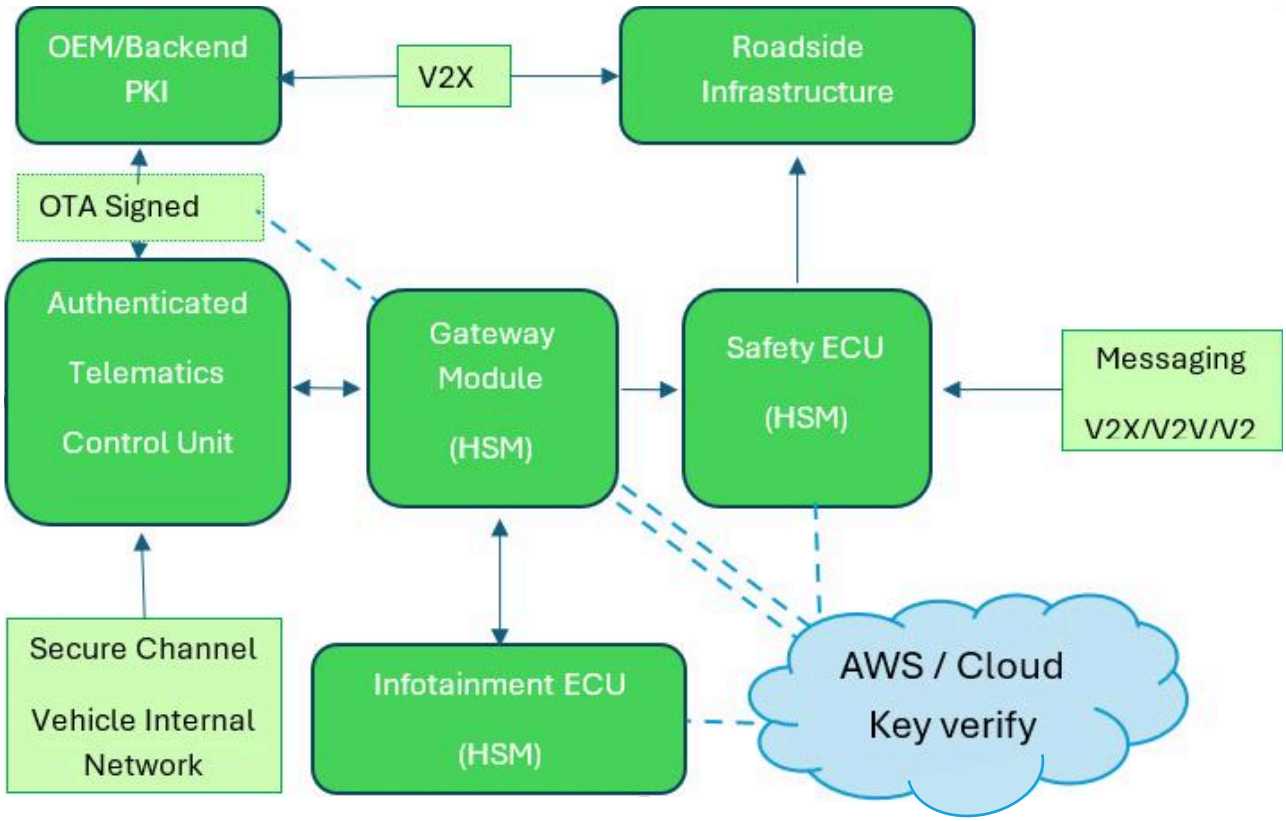


Figure 1 : Automotive HSM Enabled Security Architecture

Connected vehicles today rely on an extremely integrated cybersecurity locus for protection of internal systems and external communications. Hardware Security Modules lie at the heart of this architecture embedded in the paramount Electronic Control Units, Telematics, Gateway, Safety, Messaging, and Infotainment. The Hardware Security Module acts as the Cryptographic Backbone of a Vehicle: it stores keys with utmost security and performs all necessary critical operations such as encryption, authentication, and digital signature verification. These gatekeepers have paramount importance because they enforce that only authorized firmware and legitimate entities are recognized and unverified firmware and invalid messages cannot pass through. Supporting that is a bifurcated Public Key Infrastructure, one managed by the vehicle manufacturer or backend system for credentials for ECUs and over-the-air updates, and the other for V2X communications to facilitate secure exchanges between Vehicle and Roadside Infrastructure. OTA updates are digitally signed packages that must go through cryptographic checks against the Hardware Security Module before installation, and messages on the internal vehicle networks are encrypted using protocols like CAN or Automotive Ethernet to prevent message tampering. Security

thus offered by the V2X PKI ensures that external messages are authenticated and untampered with. As an increasing number of autonomous features and real-time data exchange puts pressure on this security model, contemporary vehicles with 70-150 ECUs-many equipped with a Hardware Security Module-need such considerations. By 2027, this protection is expected to be extended to over 100 million vehicles, with secure updates and trustworthy V2X communication being the prime motivating factors. This aligns with international standards like ISO 21434 on automotive cybersecurity, IEEE 1609.2 on V2X Security, and ISO 15118 for EV charging authentication. By this means, it constructs a sturdy defense against threats such as malicious firmware, spoofed V2X signals, unauthorized diagnostics, and internal network breaches, thus assuring that a vehicle remains safe and trusted and ready for the future.

Automotive HSM workflow

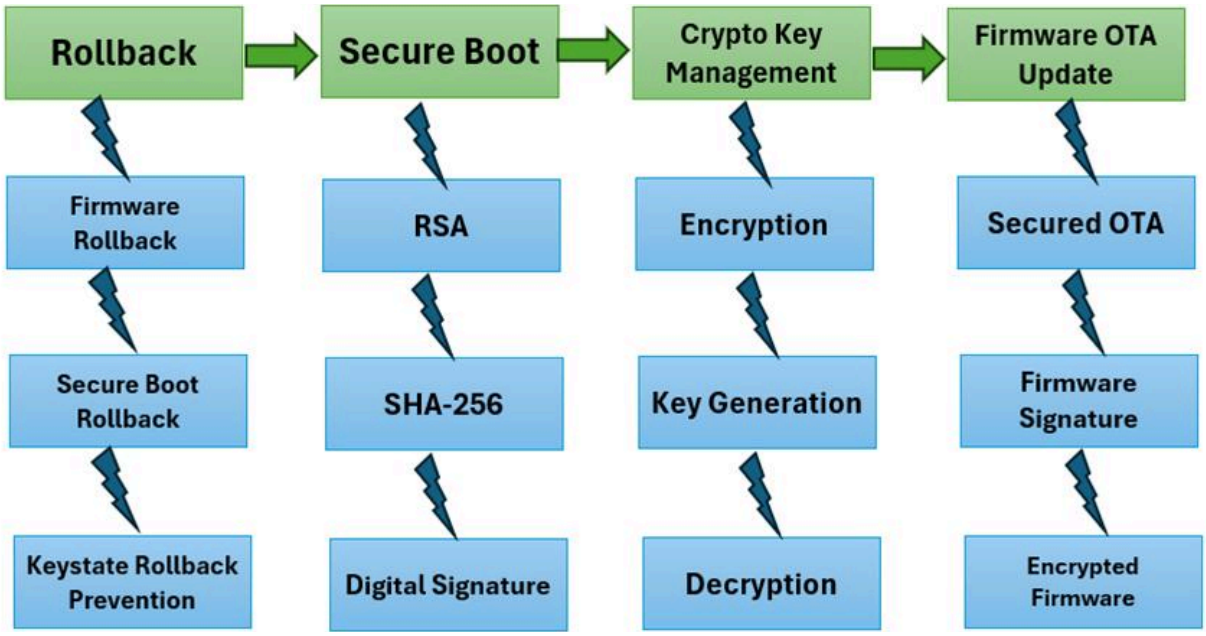


Figure 2 : Automotive HSM Workflow

7. Methodology

These Hardware Security Modules contribute to automotive security by internally generating cryptographic keys with true or pseudo random sources during ECU manufacturing. These private keys are stored securely within the Hardware Security Module and are never exposed outside; all sensitive security-related cryptographic functions such as signing and decryption must be performed inside the module. Key rotation and revocation are carried out in a secure manner by means of Over the Air update policies coordinated together with backend Public Key Infrastructure systems, thus achieving strong key governance. At vehicle boot up, the Hardware Security Modules of each ECU ensure the integrity and authenticity of the firmware by verifying stored cryptographic hashes against trusted public keys so that only authentic software runs. Over-the-Air (OTA)

updates undergo a similar rigorous process of signature verification within the Hardware Security Module before being activated, so that no unauthorized or tampered code could ever be run in it. For outgoing messages of Vehicle-to-Everything communication, those shall be cryptographically signed by the Hardware Security Module, while inbound messages are checked against certificates held by the dedicated V2X PKI, with session keys negotiated for encrypted channels kept securely within the Hardware Security Module to avoid exposure.

8. Secure Communication

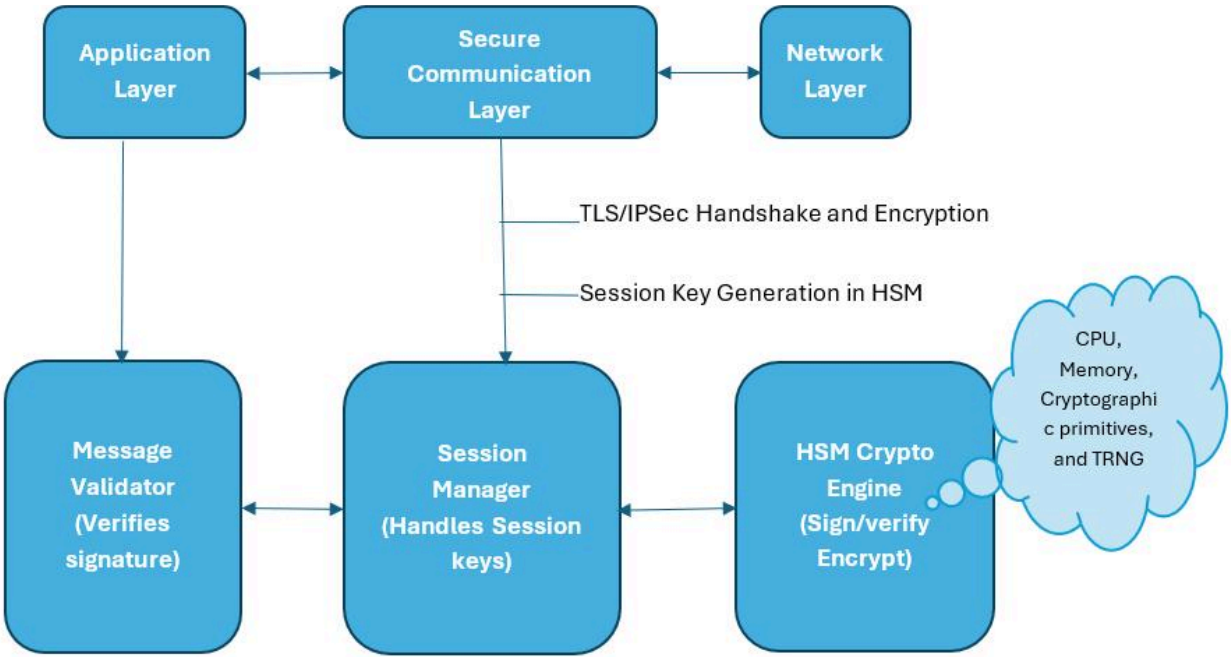


Figure 3 : Secure Communication Stack with HSM

Secure Communication Integration

Modern automotive cybersecurity is designed as a multilayered architecture for guaranteeing secure, authenticated and resilient communication among vehicle systems. At the very top resides the Application Layer, the data transport is managed, and validation of received messages is accomplished by verifying digital signatures. Below this layer, the Secure Communication Layer handles session creation and the establishment of handshake protocols based on TLS and IPSec standards, while also ensuring the secure management of session keys. Key management is often augmented with Hardware Security Modules so that it can ensure keys are only stored in and used within secure hardware boundaries. At the Network Layer is the actual data transfer, protected with cryptographic measures to protect the data from interception or tampering. Major elements provided for within such a framework are the Message Validator, that validates messages for integrity and origin before allowing further processing; the Session Manager, which implements

negotiation and establishes the secure session from cryptographic keys; and the Hardware Security Module Crypto Engine, which performs the sensitive operations such as signing, verifying, and encrypting of data in the tamper-resistant environment. Security operations such as handshake protocols, key generation, key derivation, and key confirmation are executed end to end, whereas cryptographic separation ensures that all critical operations are carried out within the Hardware Security Module with particular attention to those involving key management and digital signatures-characterizing instances of exposure to attacks. Hence, this architecture constitutes Vehicle to Everything security communications and protection for OTA firmware updates, where signatures are verified in hardware prior to installation. With modern vehicles that potentially include HSM inside every ECU, this layered approach is in accordance with global standards such as ISO 21434, IEEE 1609.2, and ISO 15118. In essence, this should provide the strongest protection from threats such as unauthorized updates, man-in-the-middle intrusions, spoofed messages, and cryptographic key extraction, making it more so the lifeblood in safety and reliability for connected and autonomous vehicles.

Performance Implications

- **Cryptographic Throughput:** Hardware acceleration of cryptographic algorithms (AES, RSA/ECC, ECDSA) intrinsically provide real-time signing and signature verification with a low latency requirement of safety unforeseen ECUs.

- **System Responsiveness:** From the perspective of isolating crypto workloads inside HSM and interacting through shared memory IPC using non-blocking mechanisms, the proposed architecture experiences less latency compared to its software security stack counterpart.

- **Resilience and Compliance:** Secure boot chains and immutable keys provided by the hardware security module stop an attacker from persisting across a reboot or a software update and are hence fully aligned with regulatory requirements in terms of auditability and key isolation.

- **IPC & Mutex/Semaphore Efficiency:** As shown in attached tables, shared memory and mutex/semaphore synchronization provide the best performance ensuring data integrity and support high-throughput low-latency real-time systems.

Feature	POSIX Threads	Processes	Pipes/ FIFOs	Message Queues	Shared Memory
Context Switch Cost	Low	High	Medium	Medium	Low
Latency	Low	Medium	Medium	Medium	Very Low
Throughput	High	Medium	Medium	High	Very High
Synchronization Ease	Moderate	Low	High	Moderate	High
Real-Time Suitability	High (with RT)	Low	Medium	Medium	High

Table 1 : IPC Method Comparison

9. Use case

Vehicle-to-Everything (V2X) Communication:

- HSMs manage cryptographic keys used to secure communication between the vehicle and other vehicles, infrastructure, and the cloud.
- HSMs verify the authenticity of messages to prevent false information from being exchanged.

Digital Key Management and Secure Boot:

- HSMs are responsible for injecting, generating, and managing keys that establish trust in the vehicle's boot process.
- This ensures the vehicle's operating system boots from a secure and authentic source.

Data Encryption and Decryption:

- HSMs encrypt and decrypt sensitive data, such as user data and operational data, to protect privacy and maintain data integrity within the vehicle.

Secure Software Updates (Over-The-Air - OTA):

- HSMs act as a secure root of trust for the OTA process, ensuring that firmware updates come from a trusted source.
- They digitally sign the firmware to prevent malicious actors from distributing fake or compromised updates.

10. Standing strategies of Automotive HSM

• Cryptographic Algorithms Development

Algorithm	Type	Purpose	Capable of HSM Dev & Test
RSA (2048–4096 bit)	Asymmetric	Digital signature generation and verification	Private key stored and operated inside HSM
ECDSA / EdDSA	Asymmetric	Lightweight signature schemes for constrained devices	Supported by modern HSMs for faster verification
SHA-256 / SHA-512	Hashing	Generates digest of firmware before signing	Used internally by HSM for signature operations
AES-128 / AES-256	Symmetric	Encrypt firmware for confidentiality	Keys stored and managed by HSM
HMAC-SHA256	Symmetric	Message authentication	Used for integrity checks in secure messaging protocols
Secure Monotonic Counter	Non-cryptographic	Prevents rollback attacks	Stored and incremented securely inside HSM

Table 2 : Cryptographic Algorithms

• Key Management

- **PKCS#11 API:** Standard interface to interact with HSM for key management and cryptographic operations by using this API.
- **OpenSSL with PKCS#11 engine:** Used to sign firmware and verify signatures using HSM-backed keys.
- **Secure Bootloader Frameworks:** Integrate HSM-based verification during boot (e.g., ARM Trusted Firmware, U-Boot with verified boot).
- **Key & Signature verification:** Custom or vendor-provided utilities to sign firmware images using HSM keys and used to inject root keys, certificates, and counters into HSM during manufacturing or onboarding.

- ## Test and validate the HSM's Crypto keys

Testing Methods	Description
Signature Verification Tests	Validate that only correctly signed firmware is accepted by the HSM
Tamper Detection Tests	Modify firmware or metadata and confirm rejection by HSM
Rollback Simulation	Attempt to install older firmware and verify enforcement of monotonic counter
Secure Boot Validation	Ensure bootloader and kernel are verified using HSM-stored keys
Key Rotation Tests	Replace signing keys and validate continuity of trust chain
Audit Log Review	Examine HSM logs for update attempts, failures, and cryptographic operations
Stress Testing	Simulate high-frequency update attempts to test HSM throughput and resilience
Side-Channel Resistance Testing	(Advanced) Evaluate HSM against timing, power, or EM-based attacks during cryptographic operations

Table 3 : Test and validation methods

- **CI/CD Integration:** Firmware signing integrated into building pipelines using HSM-backed keys.
- **Emulation and Simulation:** Use software HSMs (e.g., SoftHSM) during development before deploying physical HSMs.
- **Test Harnesses:** Scripts and frameworks to automate update delivery, signature verification, and rollback enforcement.

- ## Firmware OTA update

- **HSM-Enforced Execution :** Encrypts firmware delivery over MQTT/HTTPS. Secure transport layer for firmware delivery, often integrated with HSM for client authentication
- **Secure Update :** Ensure bootloader and kernel are verified using HSM-stored keys by using Secure boot validation. Firmware and metadata stored in encrypted partitions, keys managed by HSM and Devices and servers authenticate using certificates stored in HSM.

11. Future Scope

- **Quantum Resistant Cryptography:** With the kickoff of quantum computing, automotive Hardware Security Module must rapidly adopt NIST standard post quantum algorithms, supporting dual cryptographic modes during migration.
- **Scalable Virtualization:** Next-generation Hardware Security Module will concentrate on virtualization-partitioning a single module's resources among many ECUs and vehicle subsystems for more scalability and cost-efficiency.
- **Automated Security Monitoring:** Integration of real-time anomaly detections and logs-on Hardware Security Module will further ensure vehicle forensics and incident response.
- **Paste Cloud Integration:** Direct, secure Hardware Security Module communication to cloud platforms shall allow fleet-wide credential management, update deployment, and over-the-air key rotation.

12. Conclusion

Hardware Security Module has become the go-to for security in software-defined vehicles. Their ability to secure cryptographic keys, authenticated boot and update processes, and secure V2X communication supports robust cyber-resilient and regulatory-aligned architectures. The Hardware Security Module undertakes real-time secure operations using hardware acceleration and lean IPC mechanisms whilst responding promptly to the system-level demands. The methodology and architecture set forth in this paper presents tried-and-tested procedures for implementing and integrating Hardware Security Module into advanced automotive platforms that would allow OEMs and suppliers to provide end-to-end security and ensure their vehicles are future-proofed.

13. References

1. **Wolf, M., Weimerskirch, A., & Wollinger, T. (2007).** "State of the Art: Embedded Security in Cars," EURASIP Journal on Embedded Systems https://www.hindawi.com/journals/jece/2007/97485/ (open access)
2. **Bock, C., Härder, M. (2021). "Automotive Security :** Issues, Challenges, and the Road Ahead," IEEE Communications Surveys & Tutorials https://ieeexplore.ieee.org/document/9413456
3. **Federal Information Processing Standards Publication:** 140 2/3 (FIPS 140 2/3) NIST official publications: https://csrc.nist.gov/publications/detail/fips/140/3/final
4. **K. Koscher et al.,** "Experimental security analysis of a modern automobile," 2010 IEEE Symposium on Security and Privacy https://ieeexplore.ieee.org/document/5505302
5. **J.Petit et al.,** "Potential cyberattacks on Automated Vehicles," IEEE Transactions on Intelligent Transportation Systems, 2015 https://ieeexplore.ieee.org/document/7103077
6. **OEM and Tier 1** Automotive Security Whitepapers (e.g., Bosch, Continental, Rambus) Bosch automotive security overview: https://www.bosch secure automotive.com
7. **ISO/SAE 21434: Road vehicles** Cybersecurity engineering Official standard overview and purchase https://www.iso.org/standard/70918.html



Author
Thetchanamoorthy Chinnakani
Sr. Project Manager,
Semicon Automotive



Co-Author
Gangaraju Renuka Ratna Hasitha
Semicon Automotive

About Tessolve

Technology drives Tessolve's role as a premier end-to-end silicon and systems partner. With over 3,000 employees across 10 countries and a robust 20+ year history, Tessolve has delivered substantial impact through its advanced labs and innovative solutions.

Connect With Us

sales@tessolve.com

www.tessolve.com

India | USA | Singapore | Malaysia | Germany | United Kingdom | Japan | Taiwan | Philippines | Canada | Netherlands