Rambus

SECURITY
CryptoManager Platform
Use Case

EVITA-Compliant Automotive Hardware Security Modules with CryptoManager Platform

The rapid growth in connected cars and connected services are fueling consumer and manufacturer concerns over the security of these vehicles. The automotive value chain must ensure that connected cars and the data collected from these vehicles are secure. Automotive-grade Hardware Security Modules (HSMs), a secure enclave providing a Trusted Execution Environment (TEE) within an automotive ECU, are one way to address this need.

HSMs are a hardware root of trust that provide a secure basis for communications and functions in a connected vehicle, including: V2X, Over-the-Air (OTA) updates, and secure boot. The basic function of an HSM is to protect sensitive security information, such as cryptographic keys, and to enable secure execution of cryptographic services, such as data authentication. Since the cryptographic / security information is protected by the HSM, hackers are unable to remotely access the vehicle protecting the safety critical functions within the vehicle.

The EVITA project was established to create automotive architectures to protect security-relevant components and sensitive data. The consortium established three HSM security levels (Light, Medium, and Full), with several features similar to the Secure Hardware Extension (SHE) and Trusted Platform Module (TPM) specifications.

Rambus provides embedded HSMs to silicon vendors as a part of our CryptoManager® platform that are compliant with all three levels of the EVITA standard, in addition to SHE and TPM. Our CryptoManager solutions, already deployed in automotive-grade chipsets, also provide additional features and capabilities, such as a secure key management platform, multiple trusted roots, and anti-tamper resistance. By utilizing the CryptoManager platform, automotive OEMs and Tier One suppliers can leverage a proven solution that acts as the basis for all secure vehicle communications.

Benefits

- Complete end-to-end automotive HSM solution that exceeds EVITA, SHE, and TPM specifications
- Proven hardware root of trust solutions that support multiple secure enclaves with pre-defined security policies and keys
- High volume key provisioning and management infrastructure

rambus.com/automotive