CryptoManager Embedded Security

From security cores to high performance secure device provisioning, the CryptoManager™ Embedded Security platform is a family of hardware security cores and provisioning infrastructure that creates a trusted path from the SoC manufacturing supply chain to downstream service providers with a complete silicon-to-cloud security solution.

**Improved Profitability**
- Improved time-to-market and reduced inventory waste
- Dynamic SKU and feature management lowers inventory costs
- Reduced operating costs through unified manufacturing and provisioning systems

**Superior Security**
- Provide a robust hardware root-of-trust
- Secure valuable secret keys, identity credentials, intellectual property, and other sensitive data
- Protect against cloning, counterfeiting, and reverse engineering

**Control the Value Chain**
- Actively monitor production status, availability, and inventory levels
- Validate process information through secure logs
- Proven in today’s high-volume manufacturing facilities worldwide
CryptoManager Embedded Security

Overview
The CryptoManager™ Embedded Security platform is complete silicon-to-cloud solution, composed of security cores and provisioning infrastructure, for the distribution and authentication of cryptographic keys throughout the lifecycle of a device – enabling dynamic SoC management and device personalization in the supply chain. The cores and infrastructure can be used as standalone products or integrated into a single unified system.

Complete Chip-to-Cloud Solutions

Use Cases
Our platform provides a secure foundation for chip manufacturers and OEMs alike. This foundation provides a trusted path from chip-to-cloud for a variety of use cases:

- Device personalization, authentication and attestation
- Protection of device IP against reverse engineering through test, debug, and trace-port locking
- Flexible feature management for just-in-time device configuration to respond dynamically to market demand
- Production reporting and audit through secure manufacturing transaction logs

The CryptoManager platform includes a Security Engine, which is a flexible root-of-trust implemented as hardware or software, for secure provisioning, configuration, keying and authentication throughout the lifecycle of a device. Additionally, the CryptoManager Infrastructure is extensible to third party security cores, providing chipmakers and device OEMs a high performance scalable trust management solution.

End-to-End Secure Device Services
By providing a secure foundation for downstream device configuration, chipmakers have the flexibility needed for post-manufacturing inventory management and service providers have a trusted path to consumers for feature enablement and service delivery in applications including secure mobile banking, identity and entertainment, as well as IoT device security.

rambus.com/cryptomanager