CryptoManager Device Security

CryptoManager™ Device Security creates a trusted path from the SoC hardware root of trust, to silicon and device provisioning, to downstream cloud-based services, with a complete silicon-to-cloud security solution.

Improved Profitability

- Improved time-to-market and reduced inventory waste
- Lower inventory costs with dynamic SKU and feature management
- Reduce operating costs through unified provisioning and device key management 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

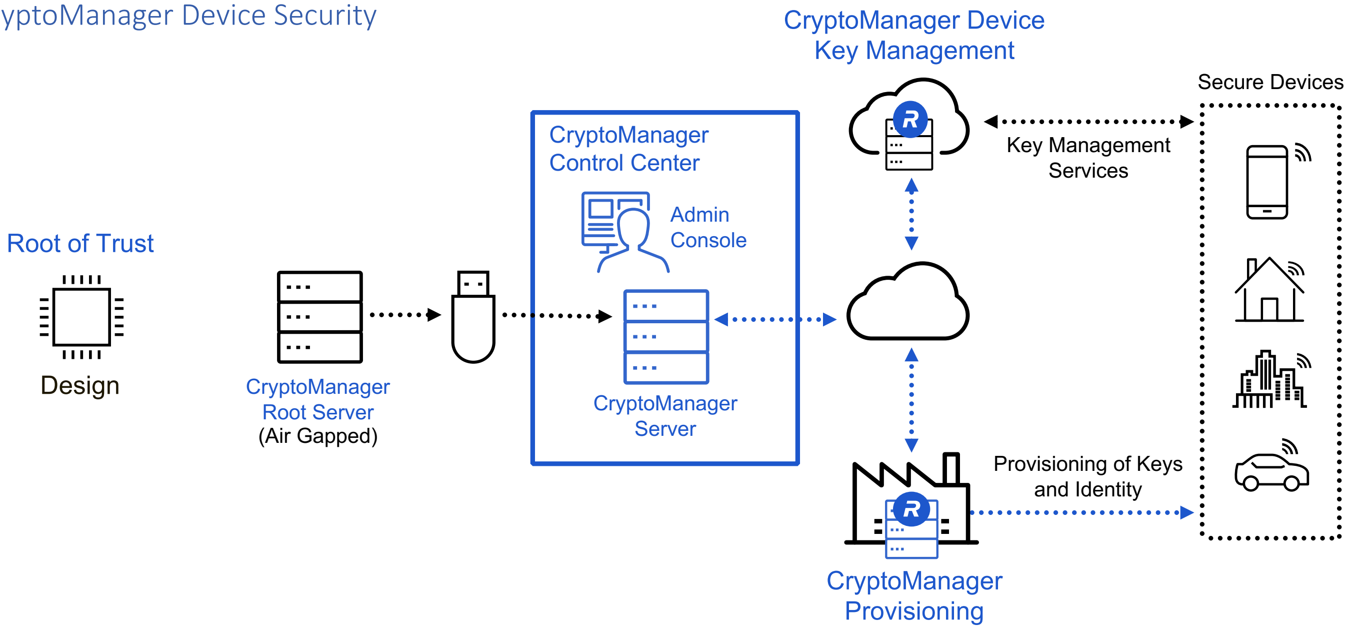
Control the Value Chain

- Actively monitor production status, availability, and inventory levels
- Validate process information through secure logs
- Leverage solutions proven in today’s high-volume manufacturing facilities worldwide

Overview

CryptoManager™ Device Security is a complete silicon-to-cloud solution, composed of security cores, provisioning infrastructure and cloud-based device key management. The CryptoManager Root of Trust provides strong SoC security anchored in hardware through a family of purpose-built secure co-processor cores. CryptoManager Provisioning performs the distribution of cryptographic keys to SoCs and devices across the manufacturing supply chain. CryptoManager Device Key Management is a cloud-based software platform enabling the deployment of key management services by chipmakers and system OEMs leveraging hardware-provisioned keys and certificates.

CryptoManager Device Security


CryptoManager Device Key Management
Secure Devices
CryptoManager Control Center
Admin Console
Key Management Services
Root of Trust
Design
CryptoManager Root Server (Air Gapped)
CryptoManager Server
Provisioning of Keys and Identity
CryptoManager Provisioning

CryptoManager Device Security includes the CryptoManager Root of Trust, a family of purpose-built secure co-processor cores that protect against a wide range of attacks with state-of-the-art anti-tamper and security techniques.

CryptoManager Provisioning provides the secure provisioning, configuration, and keying of chips and devices across the distributed supply chain. In addition to working with the CryptoManager Root of Trust, CryptoManager Provisioning is extensible to third-party security cores, providing chipmakers and device OEMs a high-performance scalable trust management solution.

CryptoManager Device Key Management builds on this secure foundation and provides a platform for downstream device configuration, feature enablement and service delivery leveraging provisioned keys and certificates.

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

rambus.com/cryptomanager