Rambus

CRYPTOGRAPHY RESEARCH
CryptoManager Platform
Solution Overview

CryptoManager Platform

From chip management to device personalization to downstream feature provisioning, the CryptoManager security platform creates a trusted path from the SoC manufacturing supply chain to downstream service providers with a complete silicon-to-cloud security solution.

Complete Lifecycle Solutions

- Robust silicon-to-cloud security
- Secure provisioning and tracking of keys from manufacturing to in-field

Improved Profitability

- Reduce NRE and operating costs
- Improve time-to-market
- Reduce inventory waste

Superior Security

- Provide a robust hardware root-of-trust
- Protect valuable secret keys, identity credentials, and other sensitive data
- Protect against reverse engineering and counterfeiting

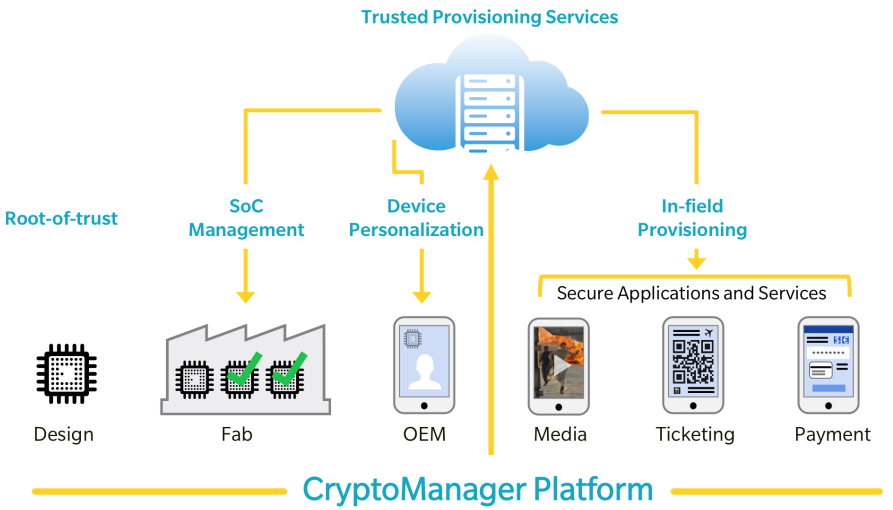
Streamline Operations

- Automate provisioning of keys
- Enable common platform across product lines
- Integrate easily into existing manufacturing flow

Overview

The CryptoManager™ security platform is complete silicon-to-cloud solution 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, and securing applications and services through in-field key provisioning.

Complete Chip-to-cloud Solutions



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. A local and cloud-based CryptoManager Infrastructure and Trusted Provisioning Services support the Security Engine, providing chipmakers, device OEMs, secure application developers and service providers a scalable and flexible trust management solution.

End-to-End Secure Devices 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.

Use Cases

Our platform provides a secure foundation for chip manufacturers, OEMs, application developers and downstream service providers alike. This foundation provides a trusted path from chip-to-cloud for a variety of use cases:

- Trusted application enablement for mobile banking, entertainment and identification
- In-field device activation and de-activation of device features and services
- Device Serialization, Device ID, and ID Management
- Secure manufacturer key personalization and processor root of trust key
- Secure transport and inventory protection through device activation and deactivation
- Protection of device IP against reverse engineering through test, debug, and trace-port locking
- Device test, debug and trace-port unlocking by authorized agents for rescreening and failure analysis
- Flexible device personalization through secure feature control management of specified features or feature sets
- Secure provisioning of sensitive cryptographic keys and digital assets both in manufacturing and in field
- Device forensics with secure IP activation and usage metering and logging

rambus.com/cryptomanager