Rambus

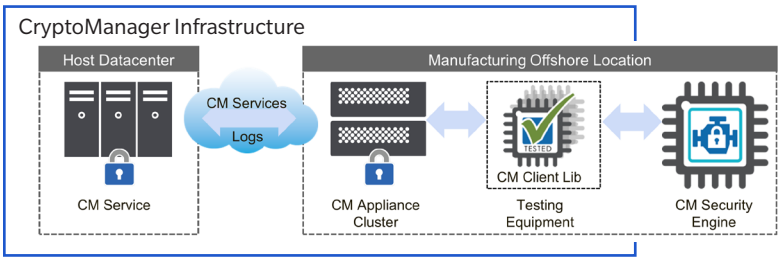
CRYPTOGRAPHY RESEARCH
CryptoManager Platform
Product Brief

CryptoManager Infrastructure

Infrastructure automates and secures the provisioning of device services across the supply chain, reducing operating costs and accelerating time-to-market.

Overview

Our CryptoManager™ Infrastructure enables the secure provisioning of device services throughout the distributed manufacturing supply chain. Device services are a broad range of secure transactions, including key delivery and programming, protection of debug modes, and chip feature management.



CryptoManager Service

The Service is a security control center with an off-line Root Authority. It manages the distribution of data assets with the appropriate authorizations to Appliances. It includes an advanced Management Console for operators to centrally manage the Infrastructure across multiple manufacturing sites.

CryptoManager Appliance

The Appliance is a tamper-resistant, rack-mounted server located at the manufacturing facility. The Appliance cluster provides local security and handles the distribution and programming of secret keys and device configuration data. It also delivers production logs and system health data to the Service.

CryptoManager Client Lib

The Client Lib is a set of software libraries integrated into the device test program in the Automated Test Equipment (ATE) or other in-factory systems. This software establishes secure communication between the Appliance and the Security Engine.

CryptoManager Security Engine

This is a silicon IP core with a hardware root-of-trust. It provides the device with a secure communications endpoint, such that it can communicate with the Infrastructure. For further details, please refer to the CryptoManager Security Engine Product Brief.

Highlights

Superior Security

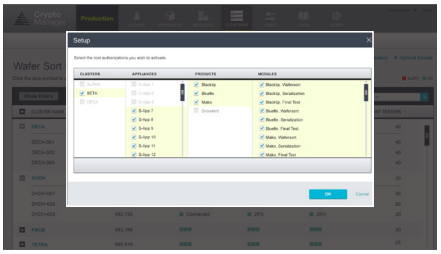
- Provide a robust, secure endpoint
- Protect valuable cryptographic keys, identity credentials, and other sensitive data
- Protect against reverse engineering and counterfeiting
- Enhance brand protection

Improved Profitability

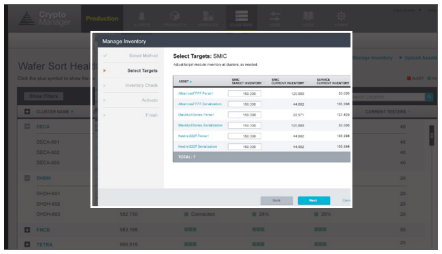
- Reduce revenue loss by preventing unauthorized access
- Enable new revenue with feature activation
- Reduce NRE, engineering risk, and operating costs
- Simplify meeting complex security requirements

Supports Secure Management Of Device Services During Manufacturing

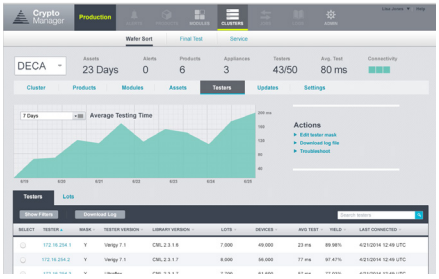
The Management Console provides operators with a dynamic overview of all their fabrications/test locations. Wizard-like tools guide users through workflows, providing extraordinary visibility and control.



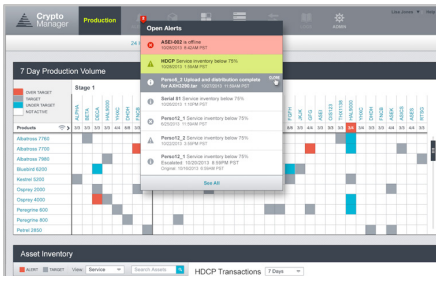
Set up factory infrastructure



Provision keys to appliance



Monitor system health



Resolve alerts proactively

System Enterprise Features

- Cluster support for high availability and scalability
- Comprehensive system monitors and alerts
- Secure browser-based management console
- Business continuity/ disaster recovery
- Meets manufacturing critical performance requirements
- Advanced key and data management
- Production service support (test/development, pre-production, and production)
- Use case extensibility via modules
- Forensic audit logging

Security Features

- End-to-end encrypted communication channel
- Root Authority for system permissions and authorizations
- Advanced encrypted key and data storage
- Two-factor user authentication
- Compatible with FIPS-140-2 Level 3
- Secure remote software/firmware updates and upgrades

rambus.com/cryptomanager

© Rambus Inc. 1050 Enterprise Way, Suite 700
Sunnyvale, CA 94089 • rambus.com