CryptoManager Infrastructure for Semiconductor Manufacturing

Industry proven, high performance, secure manufacturing provisioning infrastructure that helps semiconductor manufacturers to protect critical security information, control operating costs, and manage trust throughout the value chain.

Overview

The CryptoManager Infrastructure is a high performance, secure transaction processing and data reporting system designed to securely manage provisioning, device personalization and high value key management throughout a semiconductor's life cycle. As a critical part of the manufacturing and communications infrastructure, high availability, performance, and security are emphasized in all components of the CryptoManager Infrastructure. Security throughout the system is provided through the use of Hardware Security Modules (HSMs) in every node of the CryptoManager infrastructure. These FIPS 140-2 level 3 compliant HSMs provide tamper resistant secure storage and a secure computation environment for the necessary cryptographic computation and sensitive operations in the CryptoManager Infrastructure.

Manufacturing Control

The CryptoManager Infrastructure provides real-time manufacturing information and control for multiple manufacturing sites from one central interface for authorized personnel, providing visibility into production every step of the manufacturing process:

- Remote web UI allowing production control through a secure authenticated ticketing mechanism
- Modular, scalable solution easily grows to meet demand
- Real-time alerts, notifications and reporting to keep production running
- All manufacturing logs are encrypted to enable secure production audits

Benefits

CryptoManager Infrastructure for Secure manufacturing:

- Secures manufacturing in untrusted facilities
- Protects against IP theft and reverse engineering by controlling access to sensitive test and debug traces
- Enables devices to be configured securely anywhere in the value chain
- Provides complete and secure manufacturing activity audit

Threat Protection

Defend against a wide array of attacks to protect your revenue stream

- Protects third party keys to reduce liability and risk of the keys being compromised in manufacturing (ex. media content protection keys).
- Strong authentication and attestation capabilities – protects against counterfeit, cloning and manufacturing overruns
- Manageable root of trust to protect software assets, greatly reducing vulnerability to hijacking boot code or device firmware attacks.

Configurations

Designed for flexible deployments from the ground up

The CryptoManager Infrastructure's implementation modes are flexible, supporting single site to a globally distributed centrally managed platform with cloud data center based administration for multiple distributed manufacturing facilities to meet the highest volume manufacturing demands. Using industry standard interfaces, the CryptoManager Infrastructure provides critical information in a JSON format that is publishable through a REST API that is easily consumable by an OEM or device manufacturer's existing manufacturing flows and analytics systems.

Components

The CryptoManager Infrastructure consists of the following components:

- **CryptoManager Root Authority -** Kept in a secure facility, the Root Authority is, an air gapped - offline provisioning server that authorizes all provisioning activity, manages high value keys, and enables all CryptoManager transactions.

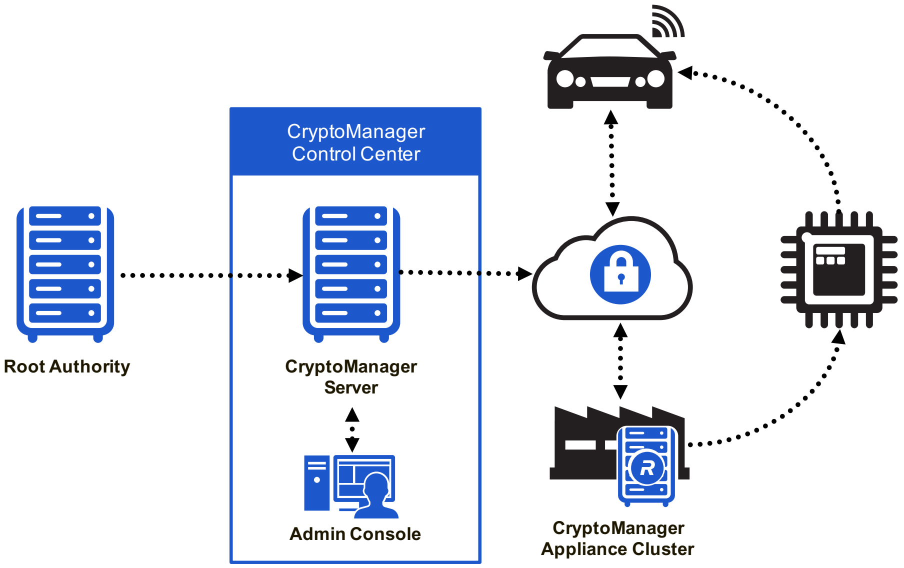
- **CryptoManager Control Center –** The Control Center monitors and manages all provisioning activity for all device manufacturing and infield management functions through a remote web based UI. The Control Center provides real-time manufacturing information from all CryptoManager Appliances within the overall Infrastructure.

- **CryptoManager Appliance –** The closest component to a target device for provisioning and management throughout the product's lifecycle. This is a fault tolerant tamperproof server cluster that interfaces with the target device either through silicon manufacturing automated test equipment (ATE) or through the cloud directly to the device.

Additional Benefits

- Secure manufacturing in high performance facilities
- Reduces operating expenses by providing a single solution for manufacturing information and production control
- Reduces cost of goods through secure feature management providing multiple SKUs from one die.
- Proven deployment - Rambus CryptoManager is proven in the most demanding of real-world semiconductor and device production environments
- Control costs - Rambus CryptoManager infrastructure secures manufacturing, controls costs, and secures devices throughout the value chain
- Increased revenue - Rambus CryptoManager platform enables chip makers to extend their value add and revenue generation opportunities throughout the full products and services lifecycle

CryptoManager Infrastructure



User Roles

Security by Design

From the lowest privilege factory operator to a system administrator or highest level security officer, all roles and functional capabilities are authenticated through the system. Roles are authenticated using hardware credentials and quorum (M of N) authentication to enable and delegate privileges. Predefined user roles are:

- **Security Officer –** Authorizes device information creation, system installation and activation, and delegation of privileges.
- **System Administrator –** Creates, manages, and monitors production runs from the Control Center. They manage flow of production information for business analytics.
- **Operator –** On-site user who connects the Appliance nodes to test equipment and monitors status through physical indicators on appliance.

How it Works

Provisioning Flow

Secure manufacturing control provided by CryptoManager Infrastructure begins with the Root Authority establishing a manufacturing root of trust, and authorizing all components and transactions in the CryptoManager system. All keys, manufacturing information and provisioning instructions are encrypted and signed by the Root Authority. These are then imported into the Control Center by an authorized Administrator for distribution to authorized provisioning appliances in a manufacturers cloud connected factory network. The Control Center distributes keys and production authorizations to the Appliances which in turn provide encrypted instructions, keys and device specific information to each device though a secure tester (ATE) interface. Once the Appliance provides this information to the target device the information is decrypted and the device information is securely provisioned. The provisioning event is logged and encrypted to be sent back to the Control Center for instant control and long term event logging and audit. Provisioning events can occur at any time in the manufacturing process from wafer sort, to packaged silicon, or at board level and even to a finished product deployed in the field.

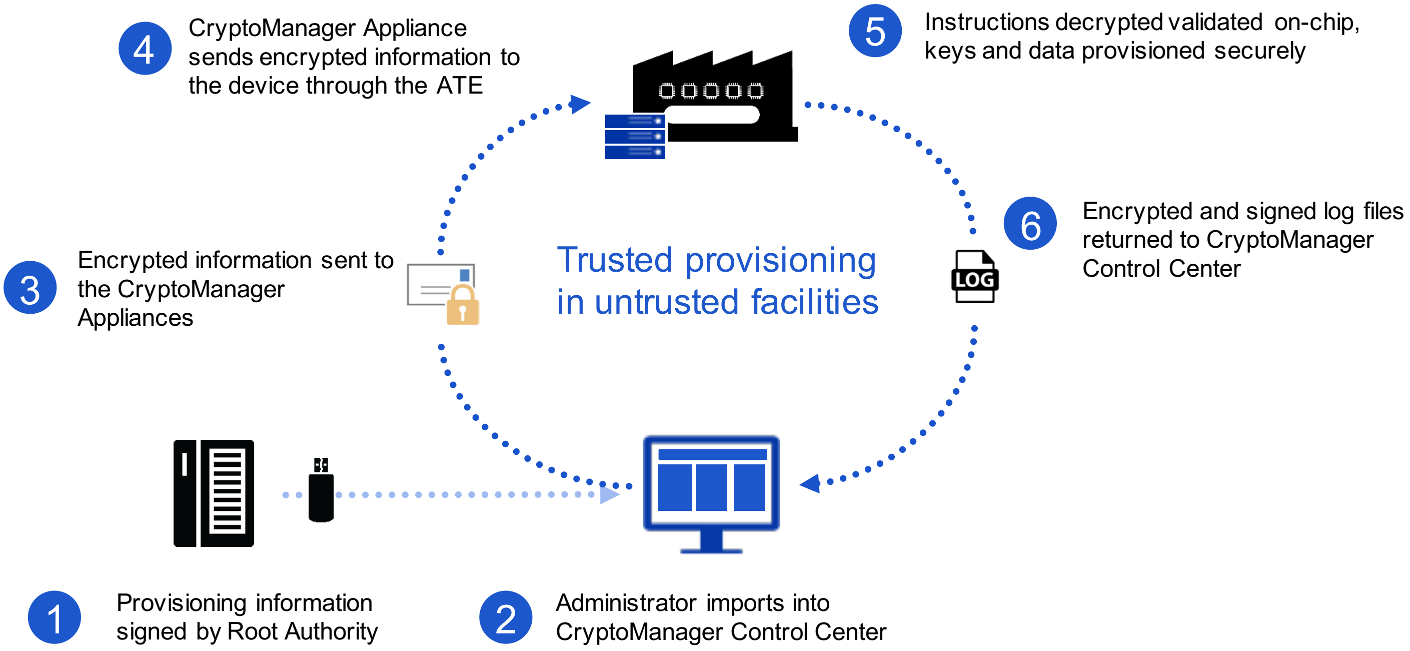
Provisioning Targets

Enhanced security through Rambus CryptoManager Root of Trust

For added control and security, utilizing a CryptoManager Root of Trust with the Infrastructure provides complete control of manufacturing for device personalization, provisioning, and feature management. This is accomplished through strong coupling of the Infrastructure with a CryptoManager Root of Trust embedded in the target silicon. Communication and management of the Secure Core is through a secure encrypted channel which enables information to be stored and operations to be executed by the Root of Trust throughout the device's lifecycle.

The CryptoManager Infrastructure can also extend support to devices with third party secure cores, or on selected devices through a CryptoManager software agent running in privileged space. Contact Rambus RSD for more information.

CryptoManager Provisioning Process


4
CryptoManager Appliance sends encrypted information to the device through the ATE
5
Instructions decrypted validated on-chip, keys and data provisioned securely
3
Encrypted information sent to the CryptoManager Appliances
Trusted provisioning in untrusted facilities
LOG
6
Encrypted and signed log files returned to CryptoManager Control Center
1
Provisioning information signed by Root Authority
2
Administrator imports into CryptoManager Control Center

Production Control and IP Protection Use Case

Take control of your inventory and process tracking

The CryptoManager Infrastructure provides a secure way for a fabless silicon vendor to control the manufacturing of devices in untrusted environments, providing secure methods to authorize manufacturing, protect high value assets, and limit liability from leakage. The CryptoManager Infrastructure provides secure control through encrypted channels for manufacturing logs and production authorizations. The CryptoManager Infrastructure facilitates secure recording and reporting of production quantities, yields, device personalization, serialization and provisioning events, complimenting existing audit processes.

Feature Management Use Case

Secure Feature Management and SKU Management

The CryptoManager Infrastructure enables flexible feature management capabilities which can drastically increase the number of SKU's from a single die to reduce production costs and supply chain complexity. CryptoManager Infrastructure can also reduce loss due to overbuild and inventory spoilage based on uncertain manufacturing forecasts or market demands. This is accomplished by configuring a device's capabilities to be enabled or disabled by a cryptographic sequence sent to the device by the CryptoManager Infrastructure. The Infrastructure provides the ability to modify a device's feature set anytime in the product's lifecycle enabling the manufacturer/ OEM to quickly respond to the market's needs.

Lifecycle Control Use Case

Control devices through their lifecycle

OEMs deploying devices using CryptoManager Infrastructure can benefit by managing devices in-field. The simplest case being remote debug Enable/ Disable to facilitate support and limit RMAs. Device OEMs may also benefit by offering capabilities in-field through secure feature management, with the option to offer enhanced capabilities post manufacturing Over the Air (OTA) enabling additional revenue opportunities.

Hardware Specifications

Solution Specifications

All CryptoManager provisioning platform components are rugged industrial class tamper-resistant compute devices designed for deployment in high-volume manufacturing facilities and cloud services data centers with the following hardware specifications:

Physical

Components	2U standard rack mounted appliances
Dimensions	W-17.2" (437mm), H- 3.5" (89mm), Depth 5.5" (648mm)
Weight	Net Weight: 35 lbs (15.9 kg) Gross Weight: 62 lbs (28.1 kg)
Processor	Single or dual Intel® Xeon® processor 8C/16T E5-2620V4 2.1Ghz
Memory	64/128GB DDR4-2133 2R*4 ECC REG DIMM
Controller	RAID 6 controller LSI 2208 HW RAID chip w/ MFBU
Storage	900GB SAS 6Gb/s 10K RPM 128M self-encrypting drives (SED)
Power	Dual 500W high-efficiency redundant power supplies
LAN	IPMI 2.0 with virtual media over LAN and KVM-over-LAN support
Ports	Standard LP 4-port GbE Intel i350 (Shipped with single IP interface configuration)
Security	Utimaco Se1500 Series HSM

Operating Conditions (Physical)

Compliance	RoHS Compliant
Temperature	Operating: 10°C to 35°C (50°F to 95°F) Non-Operating: -40°C to 70°C (-40°F to 158°F)
Relative Humidity	Operating: 8% to 90% (non-condensing) Non-Operating: 5% to 95% (non-condensing)

Power

Power Supply	740W (1+1) Redundant high-efficiency power supply with PMBus
Input	AC Input - 100-240 V, 50-60 Hz, 9-3.5 Amp
Output	DC Output - 4 Amp @ +5V standby, 61.7 Amp @ +12V

80 Plus Platinum Level Certified

Advanced Cryptographic Solutions

Cryptographic operations performed within the CryptoManager system include: SHA-256, RSA Encryption/ Decryption and signature verification, AES Encryption/Decryption, Key Derivation, On-chip obfuscation of provisioned key material, and PGP Decryption.