CryptoManager Trusted Services

Flexible cloud-to-silicon secure provisioning platform to host, operate and manage on-device security services, lifecycle management and applications services for OEMs, service providers and operators.

Device Lifecycle Management
- Cloud-to-silicon security ecosystem
- Secure provisioning, authentication and device protection

Seamless Secure Connectivity
- Proven platform used to provision billions of chipsets
- Establish independent trust between devices and services

Flexible Platform Integration
- Provisioning infrastructure offered both as a cloud service and as a standalone product
- Secure services implemented via a hardware or software root of trust
CryptoManager Trusted Services

Overview
The Rambus CryptoManager™ Trusted Services platform supports a variety of root of trust configurations via a hardware core or secure software, providing a scalable and flexible security solution. Our solutions support out-of-the-box secure connectivity, key provisioning and device lifecycle management. The IoT Device Management provides a turnkey security solution that protects service high-availability for OEMs and service providers. The Trusted Provisioning Services provides local and cloud based infrastructure and provisioning services to support chipmakers, OEMs and service providers.

Complete Cloud-to-Silicon Trusted Services
By providing a secure foundation for downstream device configuration, chipmakers have the flexibility needed for post-manufacturing inventory management. Additionally, service providers have a trusted path to customers for feature enablement and service delivery in applications including mobile, automotive and IoT segments. The Trusted Services are enabled via our pre-provisioned keys, creating a seamless integration of security and value added services for OEMs and service provider.

Use Cases
Our platform provides a secure trusted foundation to chip manufacturers, OEMs and IoT Service Provider for variety of use cases:

- Secure manufacturer key personalization and processor root of trust key
- Protection of device IP against reverse engineering through test, debug, and trace-port locking
- Flexible device personalization through secure feature control management
- Replacement of device credentials in the event root keys are compromised
- Device Attestation
- Device Decommission and Reassignment

rambus.com/trustedservices