A LATTICE COMPANY

Secure, Adaptive Rack Management

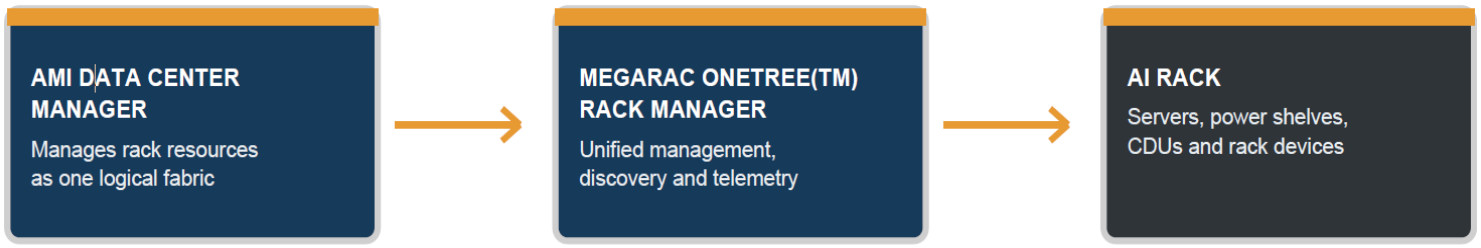
MegaRAC OneTree™ Rack Management Demonstrated on Altera OmniMC™

Problem

Data center operators need one secure and scalable way to discover, monitor, update, and manage diverse AI rack components without creating platform-specific management silos.

Solution Overview

AMI MegaRAC OneTree™ provides a unified, Redfish®-based management layer for heterogeneous AI rack infrastructure. It brings together real-time visibility, telemetry, alerts, and lifecycle management while preserving customer choice across hardware platforms and evolving rack architectures.



AMI MegaRAC AI Infrastructure Solutions

Key Benefits

- Single-pane-of-glass rack management
- Comprehensive AI rack visibility
- Scalable management for cloud, HPC, and AI environments

Key Capabilities

- Redfish management across RMC, PMC, CDU, and AI server controllers
- Automatic device discovery
- Real-time telemetry and alerts
- Metric and alert streaming to Prometheus

Open, Hardware Neutral Management

Design Principles

- Consistent management across heterogeneous rack
- components
- Customer choice across silicon and hardware platforms
- Support for OpenBMC-based environments
- Adaptable as rack architectures and requirements

Key Capabilities

- Implemented on the Altera OmniMC™ hardware platform
- Integrated processing, I/O and security capabilities
- Flexible connectivity for rack-management interfaces
- AMI MegaRAC OneTree™ Rack Management
- Redfish Interface for All Rack Devices

AMI MegaRAC™

A LATTICE COMPANY

OneTree OBMF-ICP Demo

Open Boot and Management Framework — Interface Consolidation Protocol

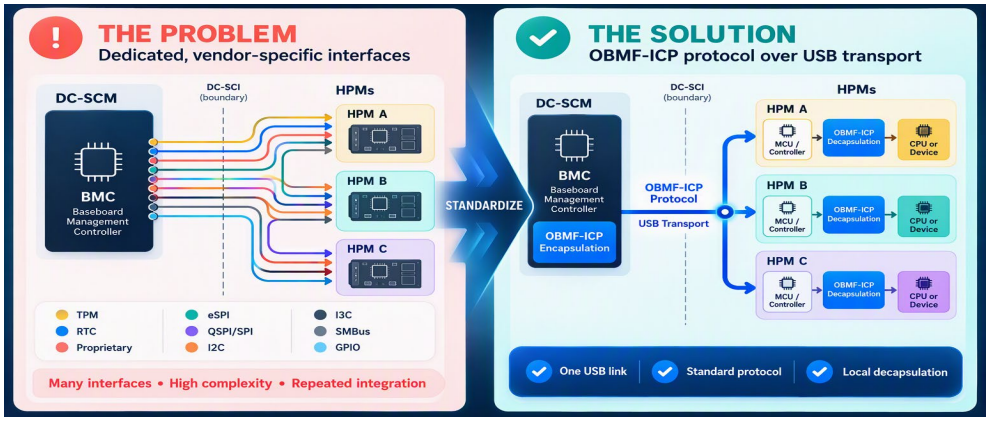
AMI MegaRAC™

Problem

Multi-protocol and multi-interface fragmentation limits firmware interoperability between CPU and device vendors. Each DC-SCM-to-HPM pairing may use a different combination of GPIO, I2C, Serial, and other out-of-band interfaces, increasing integration complexity and requiring vendor-specific implementations.

Solution

OBMF-ICP consolidates these fragmented interfaces into a single vendor-agnostic management channel between the BMC and each HPM. The OneTree proof of concept implements OCP OBMF-ICP v1.0.0 (RC1) over USB using a Linux kernel host driver and a device-side reference implementation.



Features

- Implemented: GPIO, I2C, and Serial (UART).
- Linux kernel host driver paired with a device-side reference implementation.
- Validated using a real two-board USB setup.
- Ongoing: MMIO, I2C Target, I3C Controller, IPMI, SPI Controller, I/O, Memory Device, TPM, RTC, and OEM channel support, plus continued robustness and compatibility hardening

Benefits

- Simplifies BMC-to-HPM connectivity through one physical USB connection.
- Reduces protocol and interface fragmentation across CPU and device vendors.
- Improves firmware interoperability through a consistent, vendor-neutral communication model.
- Provides an extensible foundation for additional management channel types.

For more information, **visit ami.com/products/megarac/**

AMI Tektagon Platform Root of Trust

One Framework. Multiple Silicon. Firmware Security at Scale.

Unified Platform Firmware Resiliency
Silicon-agnostic Platform Root of Trust (PRoT) framework for server and client platforms.

- Supports Intel® PFR and AMI PFR resiliency models
- PQC-Ready Server Firmware Security (on supported silicon)
- Designed for NIST SP 800-193 and EU CRA alignment
- Scalable across server and client platforms

One PRoT Framework Across All Silicon

Tektagon abstracts hardware complexity:

- End-to-End Firmware Security Lifecycle
- One security model across diverse hardware ecosystems
- Write once → Deploy across multiple silicon platforms
- Rapid OEM/ODM integration

Eliminates vendor lock-in and reduces platform rework

Multi-Silicon PRoT • PQC Workflows • Client and Server Platforms

Secure Today.
Ready for Quantum Tomorrow.

Supported RoT Silicon

Server Platforms

- ASPEED
  - AST1060
- Lattice
  - Lattice MachXO3D™
  - Lattice Mach™-NX
  - Lattice MachXO5D™ (PQC-ready)
- Microchip
  - CEC1712
  - CEC1736
- Nuvoton
  - Arbel

Client Platforms

- Microchip ECs
  - MEC152x
  - MEC172x
- ITE EC
  - IT82xx2
- Nuvoton
  - OpenTitan

For more information, **visit ami.com/products/tektagon/**

A LATTICE COMPANY

Post-Quantum Cryptography (PQC) for Platform Firmware Security

Preparing Infrastructure for the Next Era of Cybersecurity

AMI Tektagon™

Why PQC Matters

Traditional cryptographic algorithms (RSA, ECC) are vulnerable to future quantum computing attacks. Servers and infrastructure deployed today must be protected not only against today's threats but also against tomorrow's quantum risk.

- Long-lifecycle platforms (5–10+ years) face future cryptographic exposure
- Firmware is a critical attack surface for persistent threats
- NIST and EU CRA frameworks increase the focus on long-term resilience

How Tektagon Enables PQC

AMI Tektagon extends Platform Firmware Resiliency with PQC-ready capabilities — including a PQC wrapper architecture for Intel® PFR — enabling secure firmware lifecycle management without hardware redesign.

- **PQC-Ready Platform Root of Trust**
  Quantum-resistant PRoT foundation
- **Cryptographic Agility**
  Transition from legacy algorithms
- **Firmware Signing and Verification**
  PQC-protected image validation
- **Recovery**
  Secure restoration of trusted firmware
- **Compliance Readiness**
  Aligned to NIST SP 800-193 and EU CRA

PQC-Enhanced Firmware Lifecycle

Pre-Boot Validation → Secure Firmware Update → Verified Recovery → Key Management

Firmware integrity is verified with PQC-based manifests; updates and recovery images are signed and validated with quantum-resistant algorithms; and keys are provisioned, rotated, canceled, and decommissioned securely.

PQC Algorithm Roadmap

Current Support
ML-DSA · LMS

→

Future Standards Evolution
XMSS · ML-KEM Attestation (SPDM)

Platform Ecosystem and Silicon Support



Current Implementation
Lattice MachXO5D™-NX 55TDQ

Planned Support (aligned with silicon availability)

- ASPEED AST1080
- Microchip TS1800
- Nuvoton Arbel 3

Key Benefits

- **Future-Proof Firmware Security**
  Protection across long platform lifecycles
- **Quantum Threat Protection**
  Defense against emerging quantum attacks
- **Compliance Readiness**
  Aligned to evolving global standards
- **Seamless PFR Integration**
  Works with existing Intel® and AMI PFR
- **Reduced Transition Risk**
  Lower cost of future hardware moves