



# Platform Firmware Resiliency



## Zero Trust Security Starts with Firmware

In today's IT landscape, there are more data, more devices, more architectures, and thus more vulnerabilities. The threat landscape continues to evolve with cybercriminals getting more and more sophisticated, realizing firmware vulnerability can be the underbelly of the compute infrastructure and once they can take control of a machine, it can serve as a gateway into organizations' sensitive data. Because of this, organizations' Zero Trust strategy must start with platform firmware security. In order to secure platform firmware, root of trust must be trustworthy and requires every firmware to be validated and trusted.



## Tektagon CommunityEdition™

AMI Tektagon CommunityEdition leverages the open-source Platform Root of Trust (PRoT) solution with foundation firmware security features that detect platform firmware corruption, recover the firmware and protect firmware integrity. With support from the open-source community, Tektagon Community Edition augments transparency, resulting in high-quality code and improves implementation by providing greater customizability, and extensibility—resulting in a flexibly implementation for a wide range of platforms. Tektagon CommunityEdition is provided through the Open Compute Project (OCP) Repository.

## Features:



- Utilizes ASPEED® AST1060 silicon
- Leverages the open-source community
- Intel® PFR 2.0 compatible
- Immutable Trust Code Boot ROM
- Image Verification
- Image Recovery
- SPI filtering during runtime
- SMBus filtering
- Configurable Modular Project
- Secure firmware update
- Attestation Support
- NIST® (SP 800-193) compliant



Tektagon CommunityEdition Core Features	
<b>ASPEED Controller Flexibility</b>	Able perform secure and authenticated boot of platform and root of trust functions
<b>Cerberus PFR and Intel PFR 2.0 Detection, Protection and Recovery</b>	HRoT Image. SPI filtering during runtime. Auto-recovers on verification failure.
<b>Hardware Abstraction</b>	Host Communication through I2C
<b>HRoT Firmware</b>	PRoT firmware with boot and rollback protection. Immutable Trust Code (Boot ROM). Configuration with Firmware DevOps Project.
<b>Platform Manifest Support</b>	Cerberus PFR. Intel PFR 2.0. 3k Signed PFM Block. Support for Intel PFR 2.0 SPI filtering.
<b>Public/Private Key Management</b>	OTP key storage with revocation and authentication support. Revocation and re-provisioning injection through physical presence.
<b>Hardware Security Accelerators</b>	Supports SHA-256, SHA-384, ECDSA-256, ECDSA-384
<b>Advanced Operation and Management</b>	Key decommissioning and Recommissioning. Event logging.

Tektagon CommunityEdition Specifications	
<b>Host CPU Platform Types</b>	Intel®, AMD, Arm®
<b>HRoT Controller Support</b>	ASPEED® AST1060
<b>Motherboard Device Support</b>	BMC, BIOS Module, DC-SCM, HSM, OTP (Auth Keys)
<b>Controller OS</b>	Zephyr®, Bare Metal
<b>Boot Firmware Compatibility</b>	Aptio V, MegaRAC, Open BMC
<b>I/O Support</b>	SPI, I2C, SMBus, GPIO
<b>Tools Support</b>	Platform Manifest Creation from BIOS/BMC part, Linux® I2C
<b>Compliance</b>	NIST® SP 800-193, RSA

Intel® is a registered trademark of Intel Corporation or its subsidiaries. AMD® is a registered trademark of AMD. ASPEED® is a registered trademark of ASPEED Technology Inc. Arm® is a registered trademark of Arm Limited or its affiliates. RISC-V® is a registered trademark of RISC-V International. NIST® is a registered trademark of National Institute of Standards and Technology. Open Compute Project® is a registered trademark of the Open Compute Project® in the U.S. and other countries.

For more information please visit the request form at [ami.com/contact](https://ami.com/contact)

Copyright ©2022 AMI. All rights reserved. Product specifications are subject to change without notice. Products mentioned herein may be trademarks or registered trademarks of their respective companies. No warranties are made, either expressed or implied, with regard to the contents of this work, its merchantability or fitness for a particular use. This publication contains proprietary information and is protected by copyright. AMI reserves the right to update, change and/or modify this product at any time.

