AMI Tektagon OE (OpenEdition)Overview

OCP IC Meeting 9/1/2022

Connect. Collaborate. Accelerate.

OPEN Compute Project®

Root of Trust Must be Trustworthy

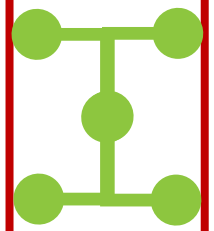
Are you aware of all the firmware running on your platform?

It's essential for every platform to be trusted at boot time

Platform trust requires validated firmware

Open-source Solution

Improves implementation and augments transparency, resulting in high-quality code.

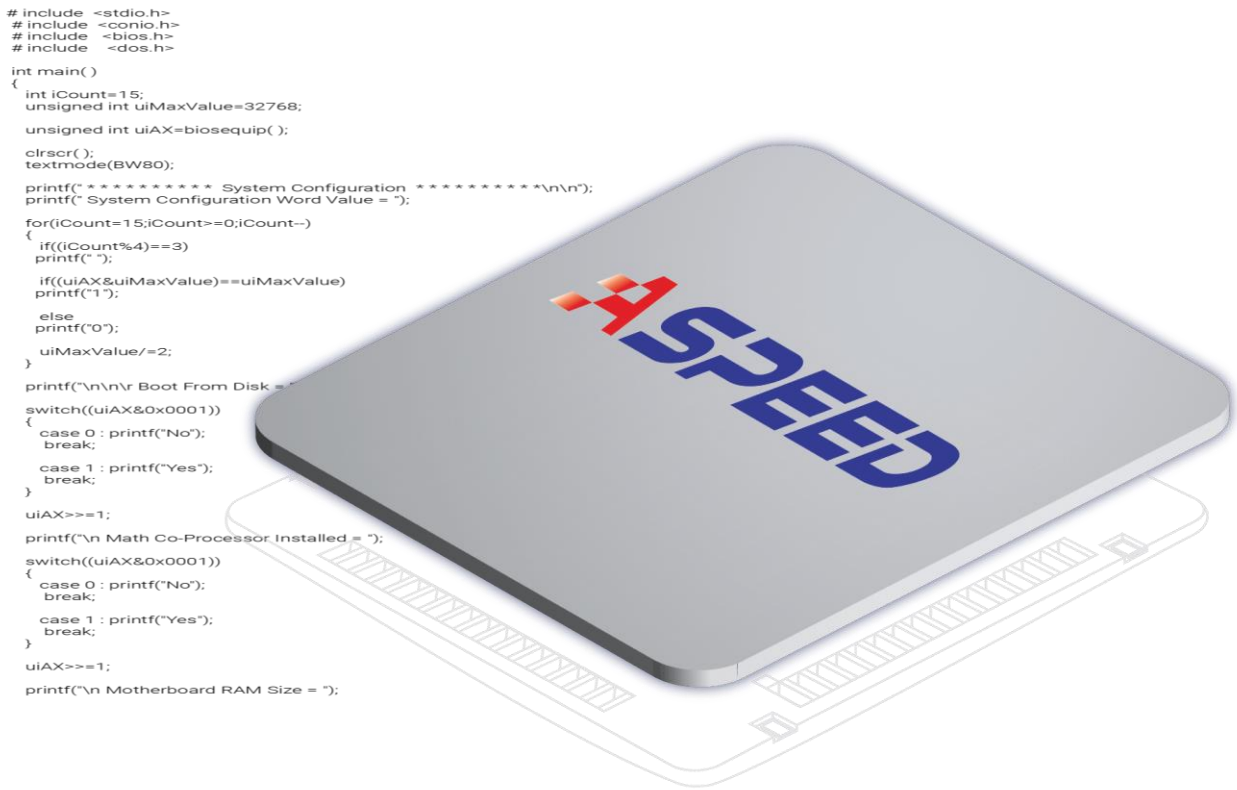


HRoT Firmware

Zero Trust firmware security that's built in, resulting in greater firmware resiliency and platform integrity.

OPEN Compute Project®

Rock-solid Firmware Security



Key Features

- Utilizes ASPEED AST1060 silicon
- Open-source architecture
- Intel PFR 2.0 compatible
- Immutable Trust Code Boot ROM
- Image Verification
- Image Recovery
- Configurable Module Project
- Platform Manifest Support
- Field updatable HRoT FW
- SPI filtering during runtime
- I2C/SMBus filtering
- Secure firmware update
- Key management
- Attestation Support
- NIST(SP 800-193) compliant
- Suitable for entry server platforms

Tektagon OE Development Vehicles

Hardware - AST2600 EVB with AST1060 On-board module

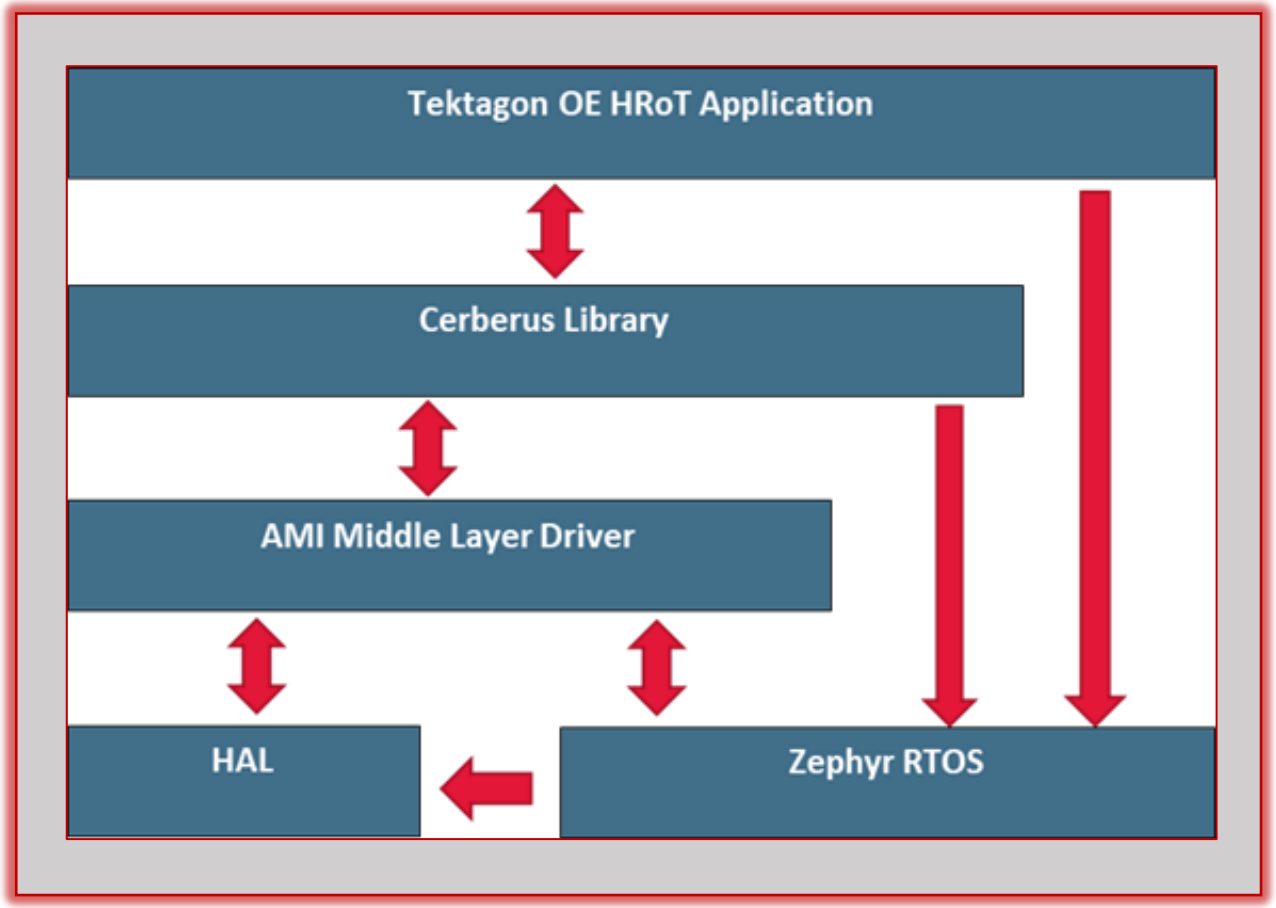
Software

- Cerberus Framework
- Zephyr RTOS
- ARM Compiler
- CMAKE
- West tool

Connect. Collaborate. Accelerate.

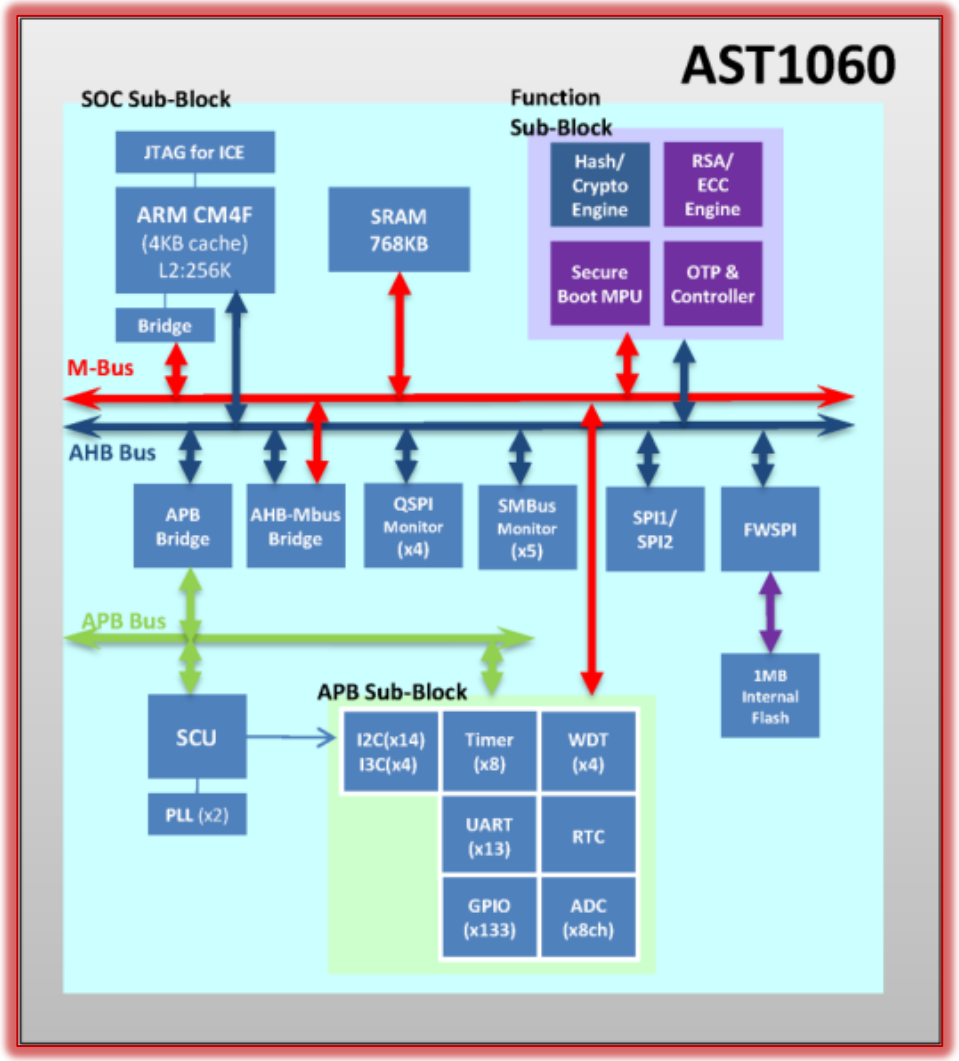
Tektagon OE High-level Design

- The Tektagon OE HRoT application is developed based on the Zephyr APPLICATION DEVELOPMENT MODEL
- CMake and West tool-based build process
- Cerberus HRoT library provides platform independent HRoT functionalities
- The AMI Middle Layer Drivers provides a bridge between the Cerberus HRoT library and HAL
- Zephyr RTOS provides the OS components to execute the HRoT Application

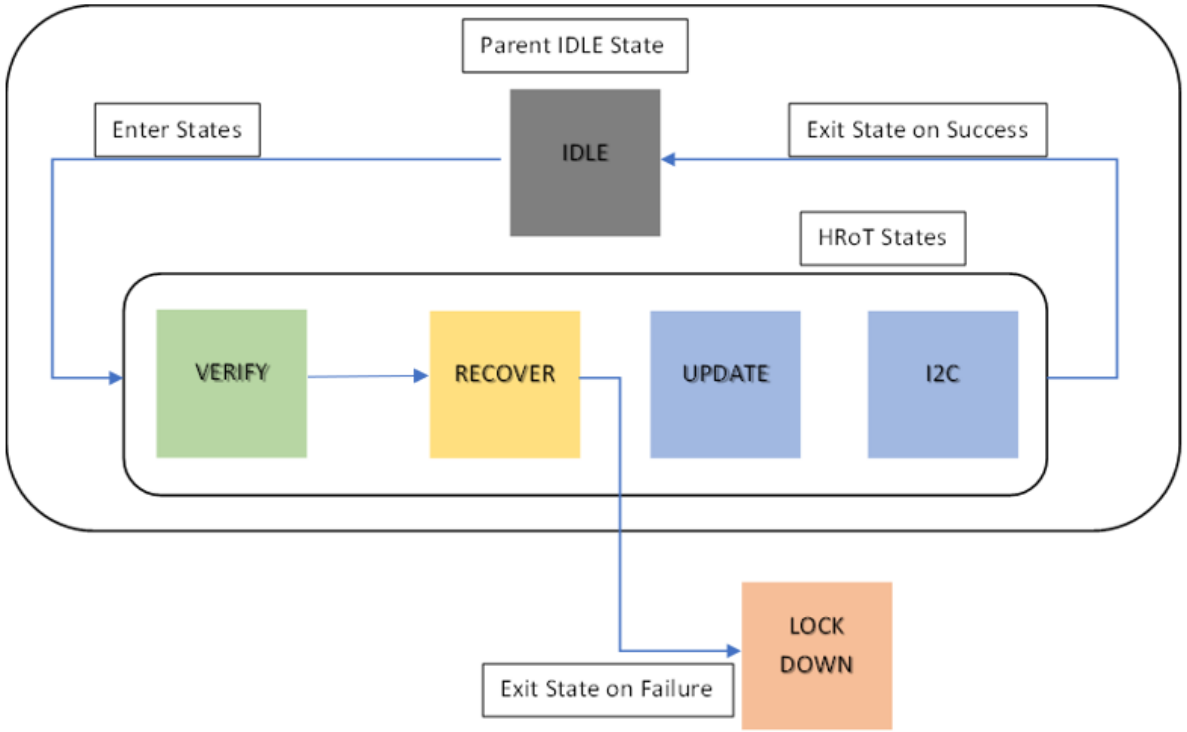


AST1060 Block Diagram Architecture

- AST1060 is a platform root of trust processor introduced by ASPEED Technology Inc.
- Able perform secure and authenticated boot of platform and root of trust functions
- In-built Cortex-M4f ARM processor
- Supports following Hardware Interfaces
  - Embedded security block
  - Hardware detection and protection engine
  - Control interface
  - QSPI memory interface
  - GPIO pins for PFR control
  - Support 768KB internal SRAM buffer
  - JTAG interface for development debugging purposes
  - 1MB Internal Serial Flash

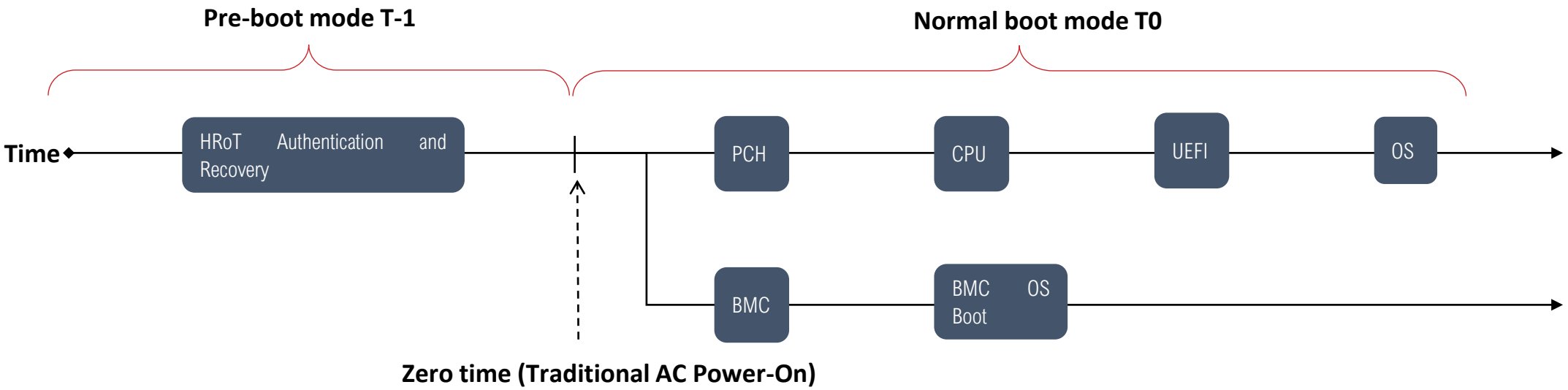


Tektagon State Machine



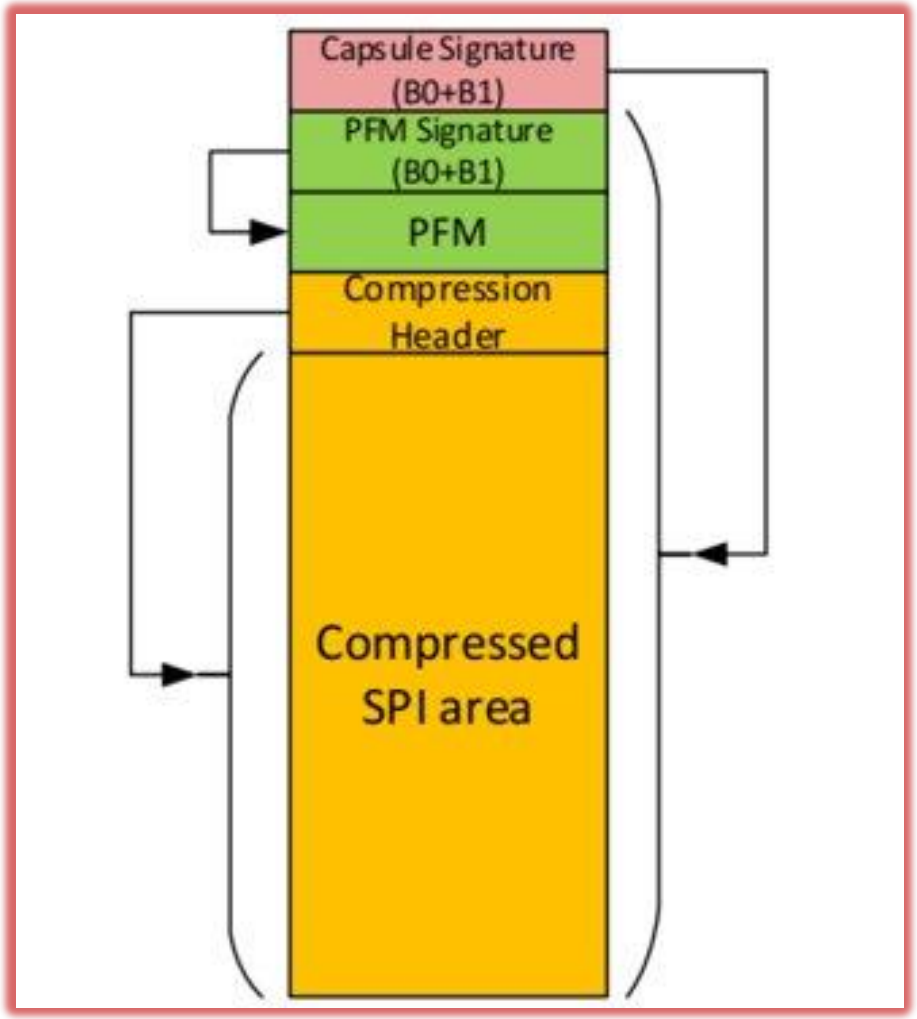
- **Tektagon OE solution uses zephyr state machine framework (SMF), an application agnostic framework, to manage the different HRoT states**
- **The Tektagon OE orchestration firmware implements the hierarchical state machine that transitions between the following HRoT states**
  - Idle
  - Firmware verification
  - Firmware recovery
  - Firmware update
  - Platform lockdown
- **State Machine allows for an entry, run, and exit action as needed for each of the states**
- **Idle State is the default state machine state**
  - All other states transition and exit back to the idle state
  - Verify state performs the verification of the flash firmware based on the manifest
  - On verification failure the orchestration firmware transitions to platform recovery state
  - The platform Update performs the update of the Active Region and Recovery region if needed to newer version
  - The Lockdown state locks the platform from booting if issues are encountered

Tektagon OE Runtime Flow



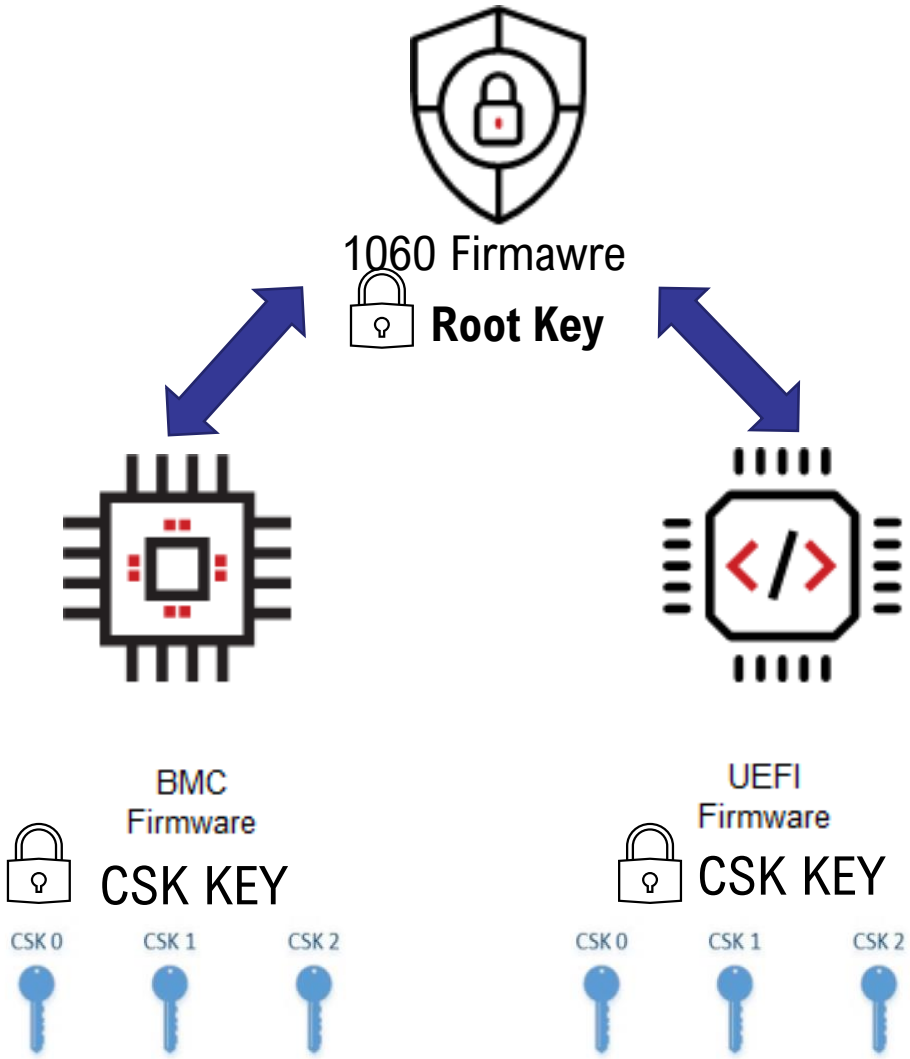
- On AST1060 power-on - the platform enters a new state pre-boot environment called T-1 during which Tektagon OE firmware performs a full platform firmware authentication and if needed the firmware recovery in isolation of any external interferences
- Upon Successful Firmware authentication - AST1060 protects the firmware regions as defined by the manifest and release the platform from reset
- Upon platform release - AST1060 continues to monitor the different platform boot phases until a successful firmware boot

Secure Firmware Updates



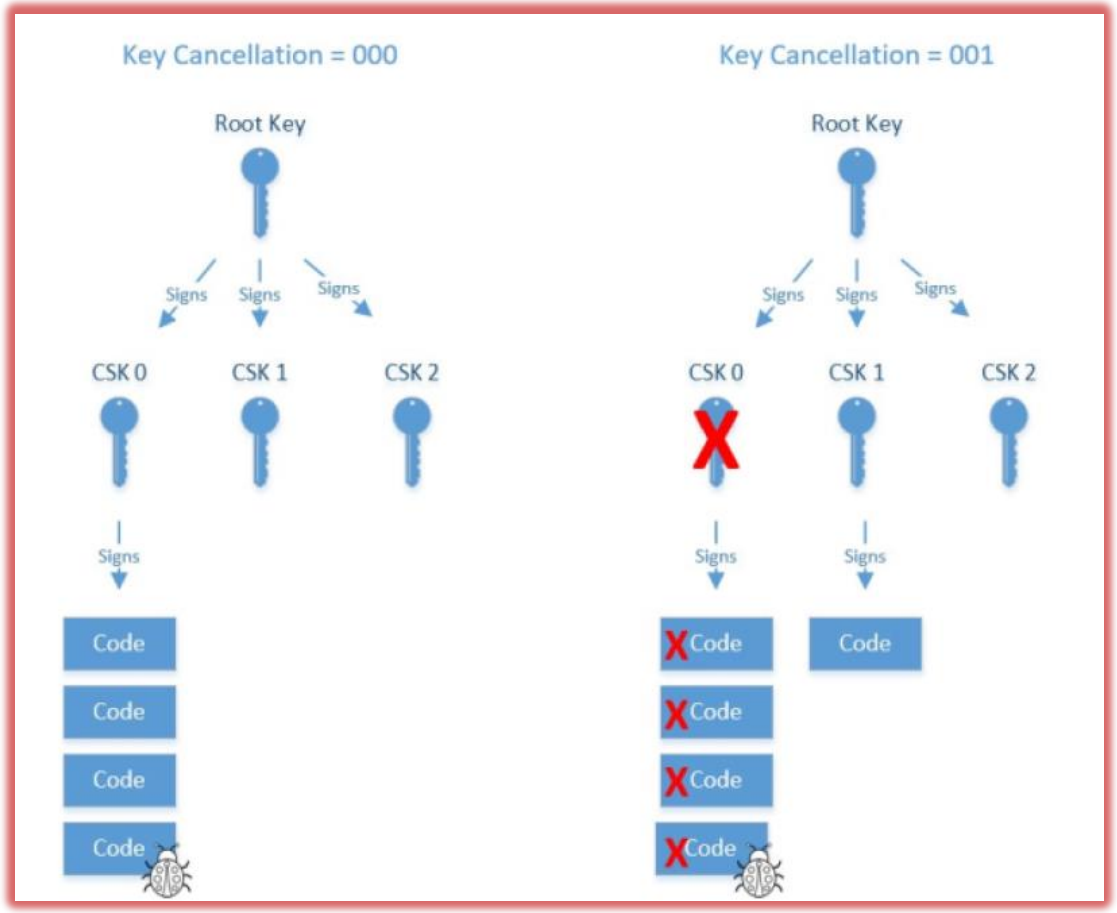
- The Intel PFR uses capsule image for firmware update and firmware recovery
- The capsule image contains the capsule signature, PFM signature, PFM, compression header and compressed SPI area
- The Capsule Signature is used for verifying the capsule image
- The PFM Signature is used for verifying the PFM.
- Capsule image use Page Block Compression to compress firmware image

Key Management



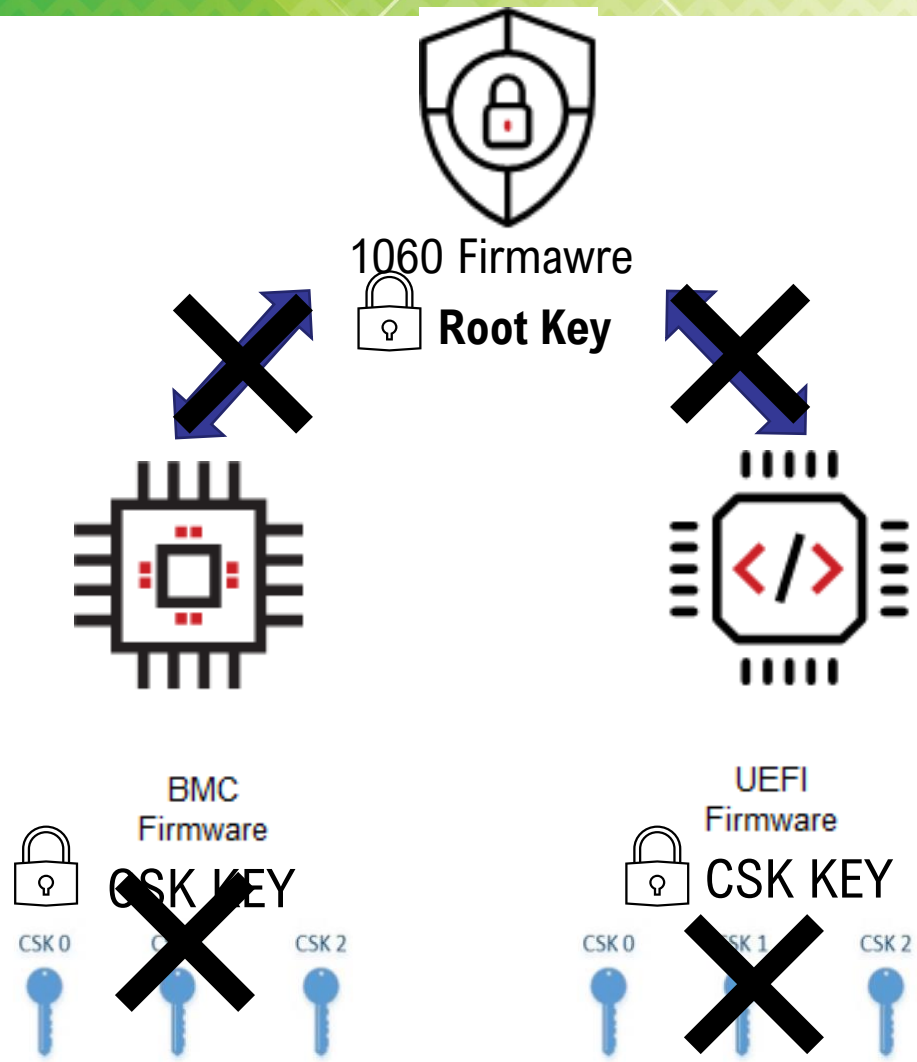
- The Intel PFR define two different key - Root Key and CSK Key
- BMC, PCH, and ROT use the same Root Key
- Root Key is used for signing CSK Key, and Root Key is unique.
- BMC and PCH use different CSK to sign BMC and PCH images, and CSK Key can use 128 keys
- Each CSK Key has Key ID

Key Cancellation



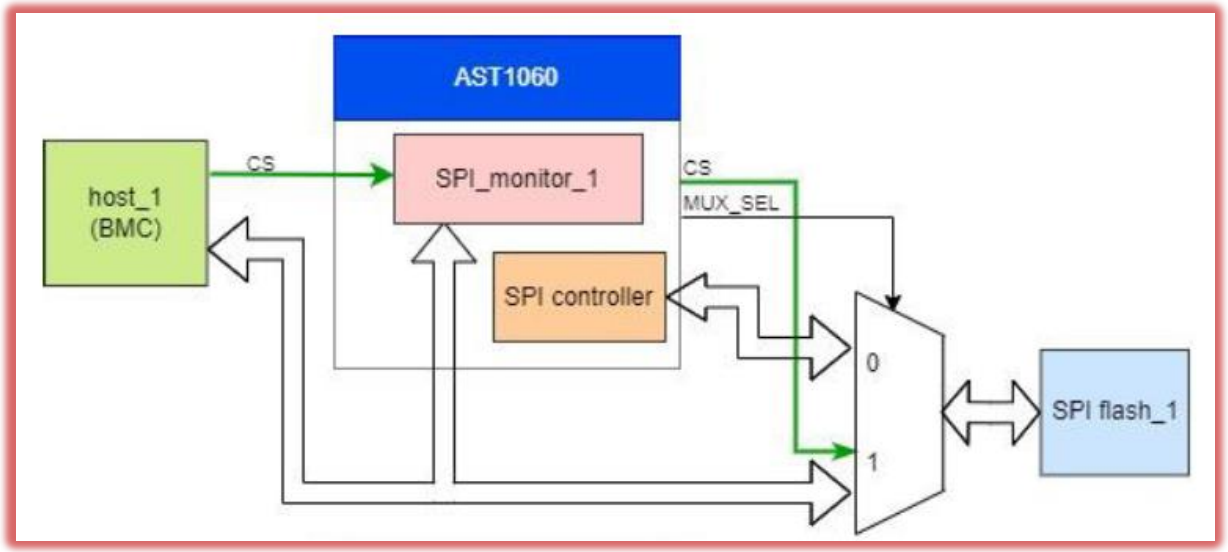
- Intel PFR design Key Cancellation to manage the CSK Key
- If one of the CSK keys is not secure, users can cancel the CSK Key's permission
- Once the CSK Key is canceled, Tektagon OE will verify and block the invalid CSK Key

Decommissioning



- Decommissioning feature is used for decommissioning Intel PFR
- After Intel PFR Provisioning, ROT, BMC and PCH will use the same root key to make sure the environment is secure
- The root key is not allowed to modify
- Users can use current root key to create decommission capsule image
- After decommissioning, ROT device will bypass to power on the BMC and PCH
- All Keys will be reset

SPI Filtering Overview



- AST1060 can control SPI flash as master mode or monitor mode
- Master Mode - AST1060 has the highest privilege to access the SPI, and the host cannot access the SPI
- Host can access SPI flash, but the whole SPI traffic , between host s and flash es is monitored by SPI monitor controllers in AST1060
- If AST1060 detects any invalid operation, the operation will be deactivated immediately

SMBus Mailbox

The SMBus Host Mailbox is designed to provide communication between the CPLD RoTand any entity on the platform which want to interact with the CPLD RoT (e.g. CPU, ACM, Host UEFI, Host OS, BMC firmware, etc.).

The SMBus Host Mailbox is emulating multiple SMBus secondary devices with various functionality in order to provide the required support for CPU root of trust performing the local authentication during CPU resets.

SMBUS WRITE BYTE MESSAGE

SMBUS READ BYTE MESSAGE

Thank You

OPEN Compute Project®

Connect. Collaborate. Accelerate.