AXIADO

Trusted Control/Compute Unit (TCU) AX3080

Redefining Zero-Trust Architecture for Accelerated Computing Infrastructure with AI

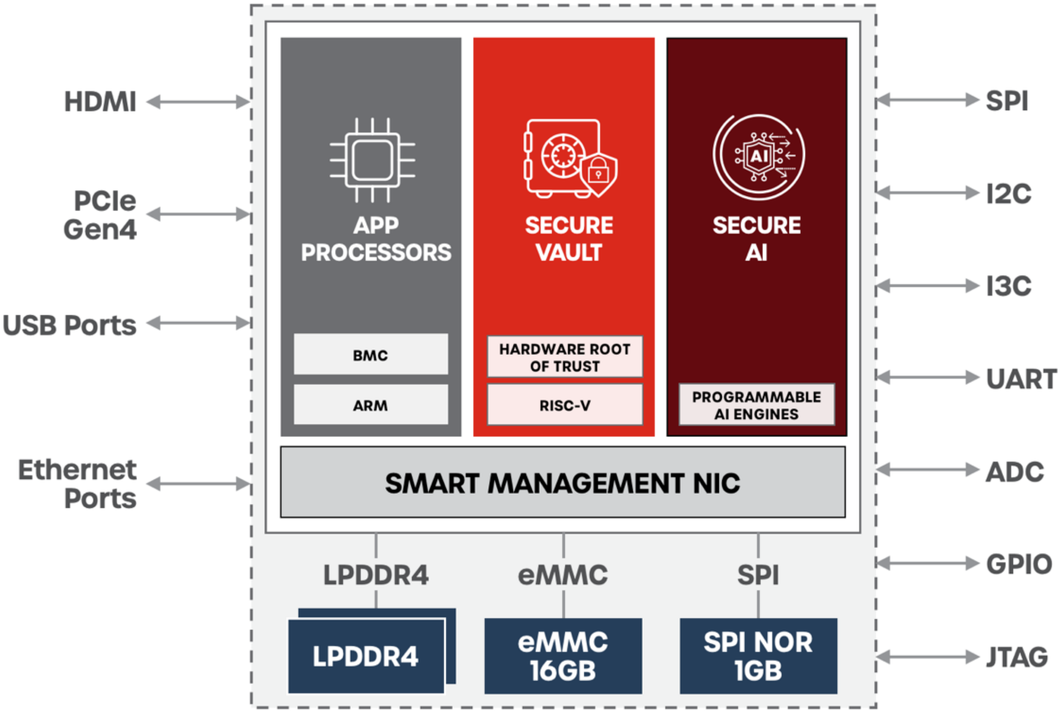
The Axiado AX3080 is a second-generation trusted control/compute unit (TCU) that offers integration of Hardware Root of Trust, Baseboard Management Controller (BMC), Trusted Platform Module (TPM), LPDDR4, eMMC and SPI NOR.

AX308x contains the following main components:

- 4x ARM A53 cores running at 1.2HGz
- RISC-V CPU based root-of-trust with crypto agility and DPA resistance
- 4x 1 TOPS AI/ML engines
- Advanced networking complex with Firewalls (4x 1GE & 1x 10GE)
- 4GB of LPDDR4 memory running at 2133MHz with inline memory encryption
- 1Gbits of eMMC memory
- 256 GPIOs /slow speed peripherals (I2C, I3C, SPI, UART, PWM, ADC, GPIOs)
- Estimated TDP is sub-8w

With the integration of LPDDR, SPI Flash and eMMC, the AX3080 further enhances platform security by eliminating the potential attack surfaces, improves power efficiency and reduces design complexity in a smallest 25x25mm2 package.

AX3080 BLOCK DIAGRAM



KEY FEATURES	DESCRIPTION
Solution Highlights	• Industry's smallest footprint (25x25mm2), enhanced zero-trust security, lowest BOM and power optimized platform security and management System-on-a-chip (SoC). • AI/ML-enabled advanced capabilities • Dynamic Thermal Management, Log Analysis, Vulnerability Management. • Flash-less host platforms and hitless upgrade support • Netboot capability, 1GE/10GE ports and advanced firewall capabilities • Integrated high-memory capacity TPM support
Key Feature Highlights	• CPU complex incorporating four 64-bit ARM A53 cores. • Secure Vault - HSM, Hardware Root of Trust and Platform Root of Trust • Secure AI with four Neural Network Processors (NNP). • Hardware-based Firewall that accelerates network policies, traffic volume rules, and security isolation rules in hardware. • Smart Management NIC Hardware Crypto Accelerators that provides classification, security protocol processing, and cryptographic algorithm acceleration.
Secure Vault	• Hardware Secure Module with dedicated secure processor • Application isolation using hardware secure enclaves • DPA-resistant crypto and authentication accelerators • Secure Key, certificates, data storage and management • Hardware Root of Trust and Platform Root of Trust • FIPS 140-3 level 2 certification
Secure AI	• Multi-Core AI Inference Processors • Up to 4 tera operations/sec neural network processor (NNP) • Real-time and Proactive threat detection and protection • Real-time vulnerability management • Side-channel attack protection and Network anomaly detection
Server/Device Management	• OpenBMC – IPMI, Redfish, iKVM, SSH support • Device provisioning with hardware-enforced device policy, apps management and authenticated remote provision/wipe • Device recovery/updates with authenticated firmware/OS update and restore
Firewall	• Supports 32 wild card rules and 4K static rule checking • Denial of Service (DoS) protection • Insider attack protection
Application Processors	• ARM CPU complex + accelerated RISC-V • GPU: full-HD graphics plane rendering for display output
Memory	• Integrated 4GB LPDDR4 • Integrated 1GB SPI NOR Flash • Integrated 16GB eMMC
Interfaces and Peripherals	• PCIe Gen4 SerDes with security • 10 GbE and multiple 1 GbE interfaces • USB 3.0 interfaces, USB 2.0 interfaces • HDMI 1.4 (4-lane) • SPI, eSPI, QSPI, • GPIO, SGPIO, I3C/I2C/SMBus, UART, PWM, TACH, ADC • Watchdog timers
Package	• 25mm x 25mm BGA
Key Benefits	• Enhanced Zero-Trust security • Reduced design complexity • Improved thermal and power efficiency • Board Area and BOM savings

AX3080 PRODUCT BRIEF