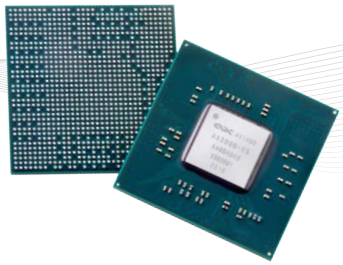
AXIADO



TCU AX3000/AX2000

Trusted Control/Compute Unit SoC Solution with Secure Vault™ Root-of-Trust, and Secure AI™

Axiado trusted control/compute unit (TCU) is a series of single-chip security processors that redefine the Zero-Trust architecture, hardware root-of-trust and attack mitigation strategies for servers, base stations and network appliances through its multiple industry-first technologies. The TCU delivers advancements in firewall protection, efficiency and performance with its quad-core application CPU subsystem, industry-best security in its Secure Vault™ secure processor subsystem, and intelligence with a multi-TOPS neural network processor (NNP) that drives Axiado's Secure AI™.

Secure Vault™ Architecture

Establishes a hardware security module for platform security through a dedicated secure processor with immutable code, signed firmware images, encrypted memory, cryptographically unique identity and secure I/O hub. Maintains integrity and recoverability even when a system is compromised.

Secure AI™ Technology

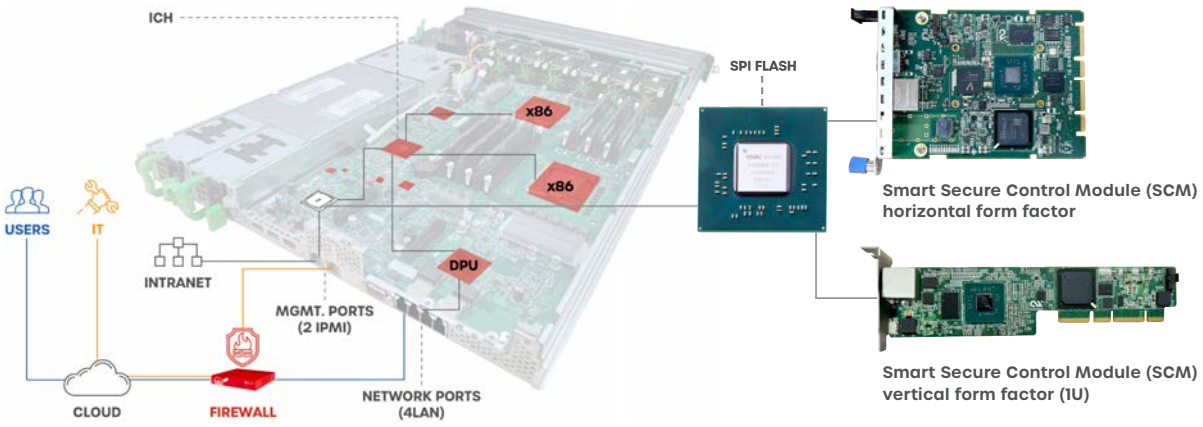
Hardware-enabled, per-platform AI/ML inference processor detects anomalies, helps enforce rules and blocks malicious attacks as they happen. Neural networks monitor and initiate responses to abnormal network and peripheral traffic, protecting against side-channel attacks.

EXAMPLE APPLICATION: SECURING CRITICAL SYSTEM ASSETS

The Axiado TCU is ideal for being the guardian of critical system assets such as firmware, keys, certificates and configuration to ensure integrity and resiliency. This is achieved by ensuring that the main processor gets its authenticated firmware image only through the secure TCU.

During normal server operation, the TCU monitors both itself and the main processor for side-channel, network and other peripheral-based attacks, using its Secure AI™ to determine anomalies to otherwise normal behaviors on these attack surfaces, logging such anomalies for forensic investigation, and enacting mitigation plans to avoid malware intrusion, proliferation and system failure.

AXIADO COMPREHENSIVE SOLUTION



Key Features

SECURE VAULT™

- Platform secure boot
- Remote attestation of system ownership and configuration
- Application isolation using hardware secure enclaves
- FIPS 140-3 level 2 certification
- DPA-resistant crypto and authentication accelerators
- Dedicated custom RISC-V processor (immune to speculative execution vulnerability)

SECURE AI™

- Multi-core classification, detection and recognition engine with peripheral port traffic and device authentication anomalies, and platform vital anomalies (e.g. power rails, clocks, temperature)
- Up to 4 tera operations/sec neural network processor (NNP)

SERVER/DEVICE MANAGEMENT

- OpenBMC and IPMI support
- Redfish support with read info, configure, update, iKVM and virtual media
- Device provisioning with hardware-enforced device policy, apps management and authenticated remote provision/wipe
- Device recovery/updates with authenticated firmware/OS update and restore
- Device finder/tracker with ability to locate and capture rich device metadata

FIREWALL

- Supports 32 wild card rules and 4K static rule checking
- Denial of Service protection using 1K monitoring buckets

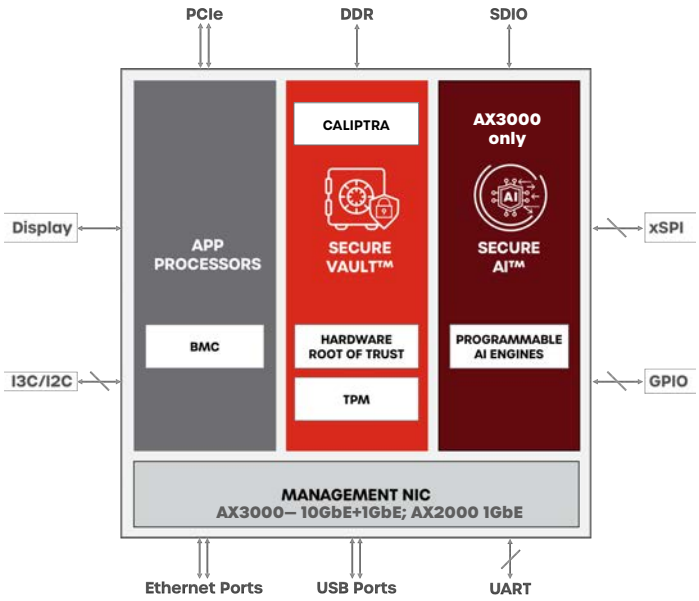
APPLICATION PROCESSORS

- ARM CPU complex + accelerated RISC-V
- GPU: full-HD graphics plane rendering for display output
- PCIe Gen4 SerDes with security
- 10 GbE and multiple 1 GbE interfaces
  - Supports wired crypto protocols: AES, 3DES, GCM, OFB, and ARC4
  - Supports wireless crypto protocols: Kasumi, SNOW3G and ZUC
  - TSN support
- USB 3.0 interfaces, USB 2.0 interfaces
- 32-bit LPDDR4-4266 with ECC; DRAM data is encrypted to prevent snooping, using multi-key region-based encryption
- HDMI 1.4/MIPI-DSI (4-lane)
- SPI, eSPI, QSPI, SDIO, eMMC with encrypted flash interfaces
- GPIO, SGPIO, I3C/I2C/SMBus, UART, PWM, TACH, ADC
- Watchdog timers

PACKAGE

- TSMC 12 nm; 23mm x 23mm BGA; low TDP, ~5W

AX3000/AX2000 TCU SoC



Key Benefits

INTEGRITY MAINTENANCE AND DATA PROTECTION

- Operational even when the system main processor is compromised or non-operational
- Survives system failure scenarios such as corrupted storage or disabled by malware, and does not boot when lost or stolen
- Encryption and multi-factor authentication to protect data at rest, in motion and in transit
- Supports run-time trust services for the system main processor

BEHAVIOR MONITORING AI/ML

- Builds profiles to find anomalies such as a compromised system, and initiates automated defenses
- Prevents malware from spreading and causing further damage

SYSTEM ADMINISTRATION

- Local and remote control of attestation and security policies
- Generates audit trail for use in forensic investigation
- Secure supply chain enablement with ownership transfers

SYSTEM RESTORATION

- Restores a system to a known state remotely

TAMPER RESISTANCE/SECURE OWNERSHIP TRANSFER

- Detects and resists tampering of hardware, software and data that may lead to reputational risk

PRODUCT AVAILABILITY: SAMPLING AS OF Q2/2023