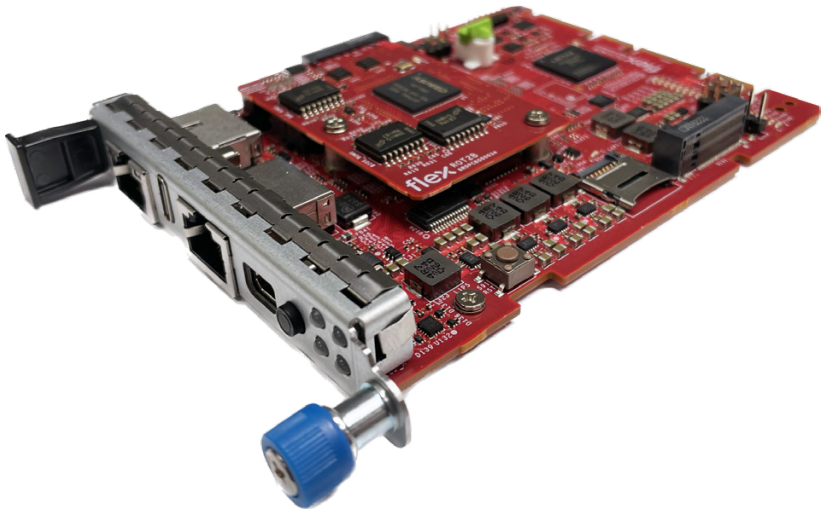
Flex Secure Control Module (DC-SCM 2.0) - SCM202A

The Flex SCM SCM202A provides common server management, security, and control functions in a common form factor module. The SCM supports Open Compute Platforms (OCP) DC-MHS Host Processor Module (HPM) implementations, as well as any server platforms with a matching Data Center-Ready Secure Control Interface (DC-SCI 2.0 pin-out).

The Flex SCM features an OCP DC-SCM 2.0 specification compliant board, a RoT module, a TPM module, and accompanying management software. The Flex SCM supports a horizontal form factor, with options to support a vertical orientation or other custom form factors.

Flex offers an OpenBMC software stack as the accompanying default management software on this module with the option to qualify additional management software stacks.



Flex Data Center Solutions

Flex data center solutions are tailored to meet your needs to deliver outstanding flexibility, performance, and value across a range of data center applications and workloads.

Industry standard components from a broad array of trusted suppliers are used to improve cost effectiveness and supply chain resiliency.

Flex will innovate based on your unique requirements to deliver a solution optimized for your application, producing a balance of performance, efficiency, and cost.

For more information, visit
flex.com/industries/data-center-power-compute

SCM202A Features

DC-SCM 2.0 board

- Compliant with DC-SCM 2.0 specification, Version 1.0 and DC-SCI 2.0 pin-out
- Aspeed AST2600 management controller, with 512MB DDR4 SDRAM
- PCB-edge gold-fingers, compatible with 'SFF-TA-1002 4C+' mating connector on HPM, with DC-SCI 2.0 keying
- 1 M.2 2260 card connector, with 'NVMe/PCIe 2.0 x2' interface to HPM
- 1 Micro-SD storage device, connected to BMC/CMC
- 1 UART interface, between 'BMC/CMC on DC-SCM' and HPM
- 1 JTAG interface between 'BMC/CMC on DC-SCM' and HPM
- 1 USB 3.1 loopback interface from host domain to HPM, through DC- SCM board
- 1 USB 2.0 loopback interface from host domain to HPM or 1 USB 2.0 interface from BMC domain to HPM
- Alternate access to BMC/CMC through HPM network interface, via NC-SI
- I/O, externally accessible on DC-SCM faceplate
  - 1 RJ45 1GbE management port connector, connected to BMC/CMC
  - 1 USB-C USB 3.1 interface connector,
  - with host CPU as master
  - 1 RJ-45 serial port connector, connected to BMC/CMC
  - 1 mini-DP video display port connector, with host CPU as master
  - 1 UID button with integrated LED, for chassis identification
  - 4 general purpose bi-color LEDs

RoT module

- Aspeed AST1060 platform Root of Trust (RoT) module (default) or customization with Lattice MachXO5D™-NX security controller device
- Commercial National Security Algorithm (CNSA) Suite 2.0 and Quantum Computing support with PQC algorithms XMSS and LMS (with Lattice MachXO5D™-NX RoT)
- Support for Intel Platform Firmware Resiliency (PFR) 4.0
- Dual 256MB QSPI NOR Flash devices for BMC/CMC firmware storage
- Dual 64MB QSPI NOR Flash devices for BIOS image storage
- I2C/I3C/GPIO connectivity to 'host Node CPUs' and BMC/CMC
- Runtime SPI and I2C/SMBus monitoring and filtering
- Hardware acceleration supporting ECDSA-384 and RSA (256 to 4096 bits)

TPM module

- Based on Infineon SLB9672 TPM controller
- Compliant with the TPM 2.0 specification

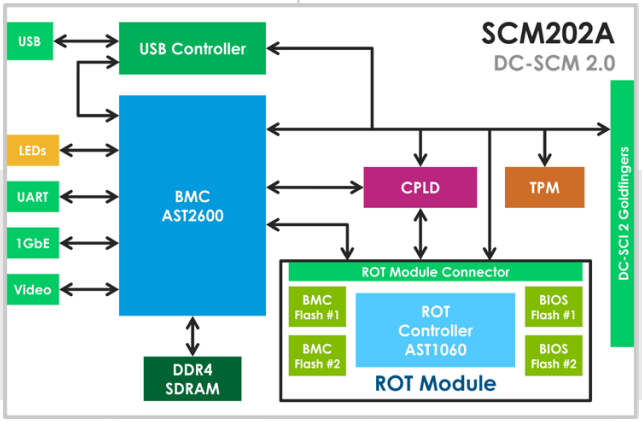
DC-SCM Adapter Board (DAB)

- Optional DC-SCM Adapter Board (DAB) with 12V power-connector for stand-alone operation and evaluation

Software

- Flex OpenBMC firmware stack (default)
- Features typical inventory, sensor monitoring, firmware updates, power management, and thermal management functions
- NC-SI, MCTP, PLDM and SPDM attestation support
- User interface access with WebGUI, Virtual KVM/Media (HTML5), IPMI, Redfish, ssh, and serial port
- Support for CA Assembly Bill A.B.1906 and Senate Bill SB-327

Flex SCM Block Diagram



We provide cloud infrastructure solutions from design, integration, and manufacturing to sustainable circular economy services, all at cloud scale. We enable our customers to accelerate innovation and time-to-market with our server reference designs, racks, power modules, power supplies, and critical power infrastructure.

Flex (Reg. No. 199002645H) is the manufacturing partner of choice that helps a diverse customer base design and build products that improve the world. Through the collective strength of a global workforce across 30 countries and responsible, sustainable operations, Flex delivers technology innovation, supply chain, and manufacturing solutions to various industries and end markets.

For more information, visit flex.com.