

**Jetson AGX Orin Boot Flow**

*Structured for RAG Readability*

**1. Boot Stages Overview**

1. **BootROM (BR)**
2. **Platform Security Controller ROM (PSCROM)**
3. **Microboot1 (MB1)**
4. **Microboot2 (MB2)**
5. **Unified Extensible Firmware Interface (UEFI)**

**2. Key Components & Functions**

**2.1 BootROM (BR)**

* **Location**: Hard-coded in SoC
* **Primary Tasks**:
  + Initializes boot media (eMMC/NVMe)
  + Loads critical firmware components:
    - BR-BCT (BootROM Boot Configuration Table)
    - PSCBL1 (Platform Security Controller BootLoader)
    - MB1 & MB1-BCT
  + Performs hash verification
  + Halts after handing control to MB1

**2.2 PSCROM**

* **Role**: Security Enforcer
* **Key Features**:
  + Stores NVIDIA/OEM authentication keys
  + Audits BPMP (MB1) and PSC (PSC-BL1)
  + Provides decryption services

**2.3 MB1 (Microboot1)**

* **Execution Platform**: BPMP (R5 core)
* **Critical Operations**:
  + SoC Configuration:
    - Pinmux/GPIO setup
    - SDRAM initialization via Memory BCT
  + Power Management:
    - Enables VDD\_CPU via PMIC programming
  + Security:
    - Configures firewalls/SCRs
  + Loads Next Stage: MB2

**2.4 MB2 (Microboot2)**

* **Two Variants**:
  + **MB2 Applet (BPMP-R5)**:
    - Device detection (SKU/RAM code via fuses)
    - EEPROM board info retrieval
  + **MB2-CCPLEX (AArch64)**:
    - Flashing operations (cold-boot/RCM)
    - Host communication via Tegraflash

**2.5 UEFI**

* **Replaces**: Legacy CBoot
* **Key Features**:
  + Standardized secure boot mechanism
  + ACPI/SMBIOS compliance
  + PCIe option ROM support
  + Firmware update standardization

**3. Boot Flow Sequence**

1. **BootROM Activation**:
   * Loads BR-BCT → PSCBL1 → MB1 → MB1-BCT
   * Verifies components via hash
2. **MB1 Execution**:
   * Configures SDRAM/power/security
   * Prepares CPU complex (CCplex)
3. **MB2 Handoff**:
   * Flashing/RCM operations if needed
4. **UEFI Launch**:
   * OS-agnostic boot preparation
   * Secure boot authentication

**4. Security Architecture**

* **Chain of Trust**:

BootROM → PSCROM → MB1 → MB2 → UEFI → OS

* **Memory Carveouts**:
  + Isolated regions for firmware components
  + Enforced via hardware firewalls

**5. Configuration Files**

* **BR-BCT**:
  + Stored at boot media start (4 copies max)
  + Contains:
    - Bootloader sizes/addresses
    - Hash verification data
* **MB1-BCT**:
  + Platform-specific configurations
  + PMIC/clock/pinmux settings

**6. Developer Resources**

* **UEFI Source**: [Jetson Linux BSP Package]
* **Debug Tools**:
  + tegraflash for low-level operations
  + Serial console logs via UART

**Boot Flow Diagram Summary**:

[BootROM] → [PSCROM] → [MB1] → [MB2] → [UEFI] → [Linux]

This structure optimizes technical details for RAG systems while maintaining NVIDIA's documented workflow.

⁂