Storage Analysis Report

NVIDIA Jetson AGX Orin

Firmware Version: 36.4.4-gcid-41062509
Kernel Version: 5.15.148-rt-tegra
Date: June 16, 2025

Overview

This report explains the storage configuration of the NVIDIA Jetson AGX Orin Developer Kit. It includes information about both the **Normal World** (Linux environment) and the **Secure World** (OP-TEE Trusted Execution Environment). All data has been obtained directly from system boot logs.

—

Normal World Storage

System Memory (DRAM)

Evidence:

```
[    0.000000] Memory: 63803252K/65780160K available
(18944K kernel code, 4044K rwdata, 9860K rodata,
7488K init, 551K bss, 1452620K reserved, 524288K cma-reserved)
```

Explanation:

Parameter	Value	Description
Total Physical Memory	65,780,160 KB (≈ 64 GB)	Installed DRAM capacity on the board.
Available Memory	63,803,252 KB (≈ 60.8 GB)	Memory accessible to the Linux kernel.
Reserved Memory	1,452,620 KB (≈ 1.45 GB)	Used for firmware, kernel, and internal processes.
CMA (Contiguous Memory Allocator)	524,288 KB = 512 MB	Allocated for multimedia and DMA operations.

—

eMMC Flash Storage

Evidence:

```
[    3.529389] mmcblk0: mmc0:0001 G1M15M 59.3 GiB
[    3.540398] mmcblk0boot0: mmc0:0001 G1M15M 31.5 MiB
[    3.541365] mmcblk0boot1: mmc0:0001 G1M15M 31.5 MiB
[    3.542430] mmcblk0rpmb: mmc0:0001 G1M15M 4.00 MiB, chardev
   (511:0)
```

Explanation:

Partition	Size	Purpose
mmcblk0	59.3 GiB	Main eMMC storage used by Linux (OS and data).
mmcblk0boot0	31.5 MiB	Primary boot partition (firmware/bootloader).
mmcblk0boot1	31.5 MiB	Secondary boot partition (redundant).
mmcblk0rpmb	4.00 MiB	Secure RPMB storage for Trusted Execution Environment.

—

Root Filesystem

Log Evidence:

```
[    3.478960] Root device found: mmcblk0p1
[    3.861401] EXT4-fs (mmcblk0p1): mounted filesystem with
   ordered data mode.
```

Explanation:

- The root filesystem is located on `/dev/mmcblk0p1`.
- Filesystem type: **EXT4**.
- This partition contains Ubuntu 22.04 user-space and kernel files.

—

Secure World Storage (OP-TEE)

The Secure World is managed by the **Trusted Execution Environment (TEE)** running **OP-TEE version 4.2**. This environment provides a secure runtime for cryptographic and trusted applications.

OP-TEE Initialization

Evidence:

```
I/TC: Reserved shared memory is disabled
I/TC: Dynamic shared memory is enabled
[    2.669695] optee: revision 4.2
[    2.729154] optee: dynamic shared memory is enabled
[    2.729405] optee: initialized driver
```

Explanation:

- OP-TEE version 4.2 initializes successfully.
- Reserved shared memory: Disabled.
- Dynamic shared memory: Enabled (allocated from DDR at runtime).

—

Secure Storage (RPMB)

Evidence:

```
[    3.542430] mmcblk0rpmb: mmc0:0001 G1M15M 4.00 MiB, chardev
   (511:0)
```

Explanation:

- The Replay-Protected Memory Block (RPMB) is a 4 MiB secure region in eMMC.
- It is used by OP-TEE to store encrypted and authenticated data.
- The RPMB ensures tamper-resistant storage and authenticated access.

—

Shared Memory Mechanism

Evidence:

```
I/TC: Dynamic shared memory is enabled
```

Explanation:

- Dynamic shared memory allows data exchange between Linux (Normal World) and OP-TEE (Secure World).
- This memory is allocated from normal DDR dynamically.

—

Storage Summary

Domain	Type	Size	Purpose
Normal World	System Memory (RAM)	64 GB (60.8 GB usable)	Main memory for OS and user processes.
Normal World	CMA Memory	512 MB	Reserved for GPU and multimedia.
Normal World	eMMC Main Storage	59.3 GiB	Root filesystem and user data.
Normal World	Boot Partitions	2×31.5 MiB	Firmware and bootloader partitions.
Secure World	RPMB Region	4 MiB	Secure persistent storage for TEE.
Secure World	Shared Memory	Dynamic	Runtime shared buffers between OS and TEE.

—

Extendability of Secure Storage

The 4 MiB RPMB region is fixed in hardware and cannot be physically extended. However, OP-TEE allows several methods to logically increase secure storage capacity:

Encrypted Normal-World Storage (REE FS)

- OP-TEE can store encrypted data in a normal filesystem such as `/data/tee`.
- Encryption keys are derived from RPMB secrets.
- Enables large-scale secure data storage using standard media.

External Secure Hardware

- Trusted Platform Modules (TPMs) or Secure Elements can be added.
- Provide dedicated hardware-backed secure storage beyond eMMC RPMB.

Dedicated Encrypted Partition

- A separate encrypted partition can be used by OP-TEE for extended secure storage.
- RPMB acts as the trust anchor for key verification and integrity.

—

Conclusion

The Jetson AGX Orin Developer Kit has the following storage architecture:

- **Normal World:** 64 GB RAM (60.8 GB usable), 59.3 GiB eMMC flash, and dual 31.5 MiB boot partitions.
- **Secure World:** 4 MiB RPMB secure area with dynamic shared memory support.

While the physical secure storage (RPMB) is limited to 4 MiB, it can be logically extended through encrypted filesystem approaches or external secure hardware, providing scalability and strong security for trusted embedded applications.