CellBE Secure Boot Process

Time

Power On Reset Sequence (POR)

Power On Event

SysCon (System Controller)

Loads configuration ring and calibrates I/O controller, will not do anything further in POR
ref. CellBE HIG - 2.2

Configuration Ring (CPU init settings)

This contains the reset vector, which is the address of lv0ldr. It also contains the initial register and cpu settings, these are passed to the CellBE
ref. CellBE HIG - 2.3.4

CellBE

Reset Vector for secure boot
NAND: 0x240_1FC00000
NOR: 0x240_1FFC0000

Location Offset
NAND: 0x0
NOR: 0xFC0000

Boot Sequence

HW Root Key

lv0ldr (Bootloader)

SPU loads and executes lv0ldr according to the reset vector provided. This differs to the process in non secure boot, where the ROM code is executed by PPU
ref. CellBE HIG - 2.2.1

The HW Root Key is stored inside the CellBE hardware. This key is unique to each CellBE and is used to decrypt and verify SPU Secure Loaders such as metldr and lv0ldr

Lv0 (SE Bootloader)

Lv0 is decrypted to the PPU RAM by lv0ldr. Lv0ldr then starts the PPU executing Lv0 from RAM at address 0x100. There is no extra loader used on the SPU in this case.

Hypervisor Init

HW Root Key

metldr (Meta Loader)

Metldr is loaded to an isolated SPU to facilitate loading of each SPU Isolated Loader.
ref. IBM Secure SDK Documentation

lv1ldr

Lv1 (Hypervisor)

From now on access to hardware resources must be done via the Hypervisor. Direct access is no longer possible.

Kernel Init

HW Root Key

metldr (Meta Loader)

lv2ldr

Lv2 (GameOS)

The Game Operating System kernel runs on top of the hypervisor. Both this kernel and the hypervisor stay present in memory while all userland operations run on top of them.

Isolated SPU Init

metldr (Meta Loader)

HW Root Key

isoldr

Isolated SPU Modules (i.e.sc_iso.self)

SPU Secure ELF Loader (SELF) are loaded by CellBE hardware to the LS address 0x400. The CellBE decrypts, authenticates and then exeutes them at 0x400.

SPU Isolated Loaders are loaded by metldr to a high LS address. Metldr then zeros itself out and jumps to their entrypoint to begin their execution.

Isolated SPU Modules are loaded by isoldr to a low LS address. Isoldr then zeros itself out and jumps to their entrypoint to begin their execution.

Userland Init

metldr (Meta Loader)

HW Root Key

appldr

Vsh (XMB)

System Files

Game

System files like vsh (XMB) or games call back to the GameOS, which then call back to the hypervisor for certain operations. The processes in userland after boot are more dynamic, but this is outside the scope of this document.

Loading a game is optional

Legend

Hardware

SPU Secure Loader

SPU Isolated Loader

PPC Secure ELF (SELF)

SPU Secure ELF (SELF)