

BANKSWAP

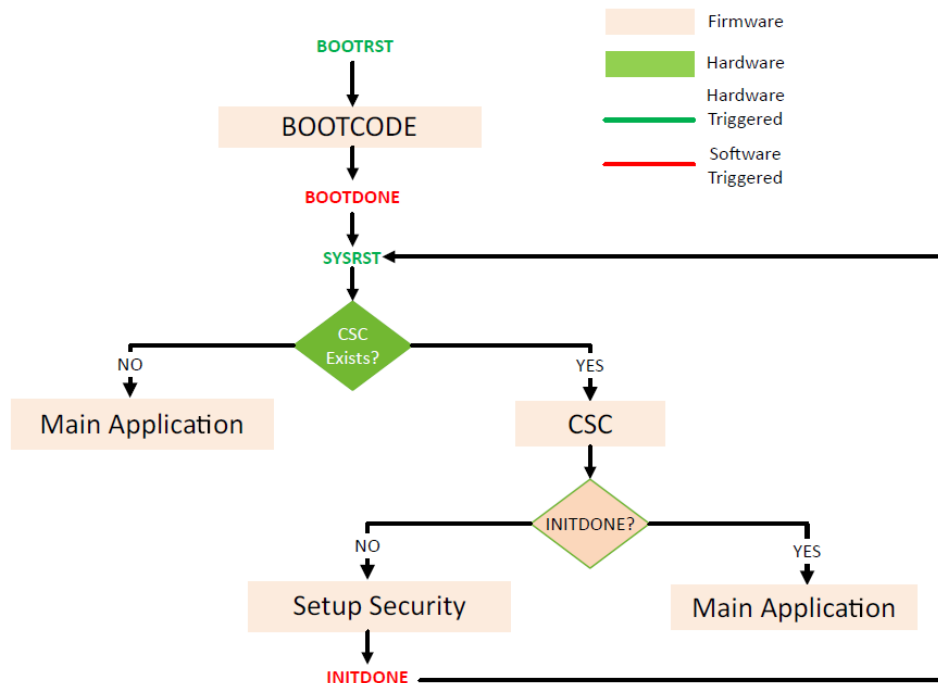


Figure 4-1. Secure Boot and Start Sequence

MSPM0 L-series TRM

4.2 Boot and Startup Sequence

```
void resetHandler(void)
{
    _asm("b __c_init00"); // this is the call to secure startup, which would issue INITDONE
}
```

The CSC will check if INITDONE has already been issued, and accordingly decide to perform application image authentication and security configuration before launching the authenticated image.

```
bool init_done = (*(volatile long *) (SYSCTL_SECCFG_SECTSTAT)) & 0x1;
If (! Init_done)
{
    setupKeystorage(); // AES symmetric keys
    entry_point = findImageEntryPoint ();
    stack_ptr = findImageStackPtr();
    setBankSwap(0 or 1); // depending on which bank the image is in

    // setup SRAM boundary
    copyFromFlashToSRAM();
    setupSRAMBoundary();
    lockSRAMBoundary();
    setupFlashFirewalls();
    INITDONE = 1; // *(volatile long *) (SYSCTL_SECCFG_INITDONE) = 1 | (0x9D << 24);
    // This triggers a HW-initiated SYSRST
}

// we will come here if INITDONE = 1 after a SYSRST
launchApp(); // using entry_point and stack pointer base from image metadata
```