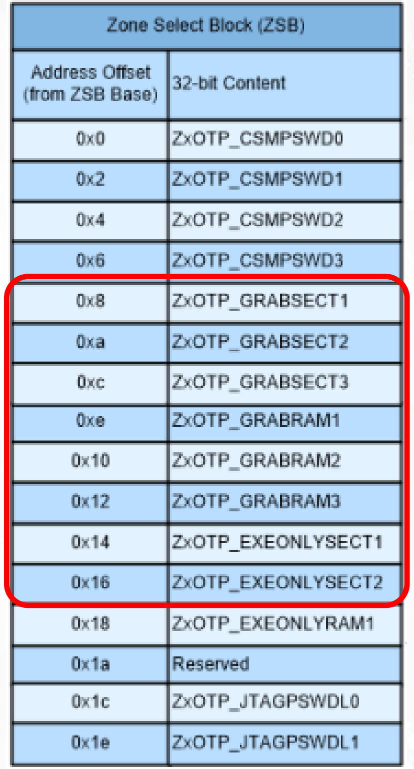
Locking and Unlocking a Device

Dual Code-Security-Module

Secure vs. Unsecure Memory

- 3 types of access: JTAG access, data reads/writes, and instruction fetches.
- Instruction fetches are never blocked.
- Unsecure memory regions allow all access.
- Secure memory allows data reads/writes only to code secured by the same zone.
- Execute-only memory allows instruction fetches only, but can be copied to other Execute-only regions.

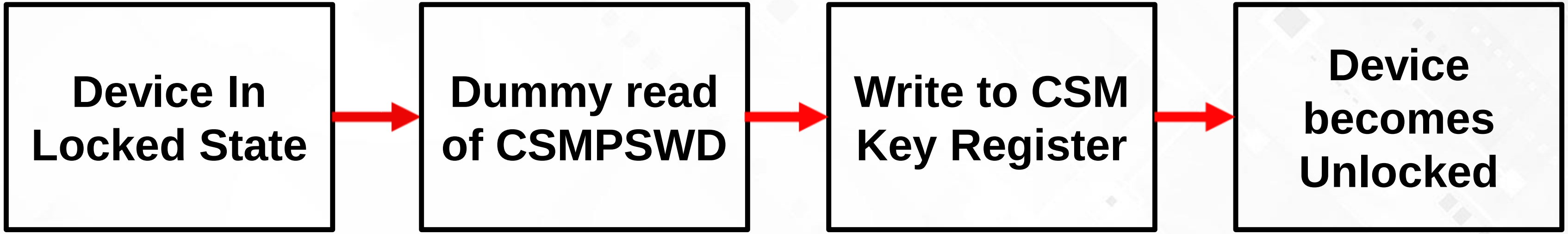


Zone Select Block (ZSB)	
Address Offset (from ZSB Base)	32-bit Content
0x0	ZxOTP_CSMPSWD0
0x2	ZxOTP_CSMPSWD1
0x4	ZxOTP_CSMPSWD2
0x6	ZxOTP_CSMPSWD3
0x8	ZxOTP_GRABSECT1
0xa	ZxOTP_GRABSECT2
0xc	ZxOTP_GRABSECT3
0xe	ZxOTP_GRABRAM1
0x10	ZxOTP_GRABRAM2
0x12	ZxOTP_GRABRAM3
0x14	ZxOTP_EXEONLYSECT1
0x16	ZxOTP_EXEONLYSECT2
0x18	ZxOTP_EXEONLYRAM1
0x1a	Reserved
0x1c	ZxOTP_JTAGPSWDL0
0x1e	ZxOTP_JTAGPSWDL1

Locked vs. Unlocked State

- “Secure” vs. “Unsecure” applies to memory regions. “Locked” vs. “Unlocked” applies to zones.
- When a zone is locked, that zone’s security settings(Secure, EXEONLY, etc.) will take effect.
- Illegal data/program reads to secure memory will return all 0s.
- Both zones are locked upon system reset.
- BOOTROM attempts to unlock zones using default CSM Passwords.
- Zones are unlocked either by BOOTROM or the user through the CSM Password Match Flow (PMF)

Password Match Flow



Device In Locked State

Dummy read of CSMPSWD

Write to CSM Key Register

Device becomes Unlocked

Additional DCSM Resources

- **DCSM Application Reports**
  - C2000 DCSM Security Tool Application Report
  - C2000 Unique Device Number Application Report
  - Enhancing Device Security by Using JTAGLOCK Feature Application Report
  - Secure BOOT On C2000 Device Application Report