

DCSM Advanced Features

Dual Code-Security-Module

PSWDLOCK / JTAGLOCK

- When PSWDLOCK is disabled, CSMPSWD locations are unsecure regardless of whether the corresponding zone is locked.
- When JTAGLOCK is enabled, all JTAG access to the device is blocked on reset.
- JTAG access can only be restored by providing the JTAG passwords in the CCS On-Chip Flash or UniFlash tool.
- JTAG passwords are split between the zone header and zone select block JTAGPSWDLx and JTAGPSWDHx.

```
Memory Browser X
Data 0x78000
Data:0x78000 <Memory Rendering 3> X
16-Bit Hex - TI Style
0x00078000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x0007800E 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x0007801C 0000 0000 0000 0000 FFF0 FFFF FFFF 4D7F FFFF FFFF FFFF FFFF 0000 0000
0x0007802A 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x00078038 0000 0000 0000 0000 0000 0000 0000 0000 0000 FFFF FFFF 5F7F FFFF FFFF
0x00078046 FFFF FFFF 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x00078054 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 FFFF FFFF
0x00078062 FFFF 1DFF FFFF FFFF FFFF FFFF 0000 0000 0000 0000 0000 0000 0000 0000
0x00078070 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x0007807E 0000 0000 FFFF FFFF FFFF AF7F FFFF FFFF FFFF FFFF 0000 0000 0000 0000
0x0007808C 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x0007809A 0000 0000 0000 0000 0000 0000 0000 FFFF FFFF FFFF 1BFF FFFF FFFF FFFF
0x000780A8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x000780B6 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 FFFF FFFF FFFF 17FF
0x000780C4 FFFF FFFF FFFF FFFF 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x000780D2 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x000780E0 FFFF FFFF FFFF BD7F FFFF FFFF FFFF 0000 0000 0000 0000 0000 0000 0000
0x000780EE 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0x000780FC 0000 0000 0000 0000 FFFF FFFF FFFF 9F7F FFFF FFFF FFFF FFFF 0000 0000
```

JTAGPSWD
JTAGPSWDHx can be programmed only once but JTAGPSWDLx are part of Zone Select Blocks hence can be changed by selecting new Zone Select Block

JTAGPSWDH0 (0x78014) (32 bits) 0x:	FFFFFFFF
JTAGPSWDH1 (0x78016) (32 bits) 0x:	FFFFFFFF
<input type="button" value="Program"/>	
JTAGPSWDL0 (32 bits) 0x:	FFFFFFFF
JTAGPSWDL1 (32 bits) 0x:	FFFFFFFF
<input type="button" value="Program"/>	

EXEONLY / Secure Copy Code

- **Secure memories can be designated as EXEONLY as an additional level of security.**
- **Memory regions designated as EXEONLY block all data read/writes, even from code secured by the same zone. Instruction fetches are still allowed in EXEONLY memory regions.**
- **To copy code from EXEONLY flash to ram, the SecureCopyCodeZx function must be used, and the ram block where code is being copied to must be designated as EXEONLY.**
- **Refer to your device specific TRM for more information on the Secure Copy Code feature.**

CRCLOCK / Secure CRC Calculation

- CRC engines cannot calculate CRCs on EXEONLY protected memory.
- CRCs can be calculated using the SecureCRCCalc function.
- When CRCLOCK is enabled, the VCU cannot calculate CRC on memory that is unsecure or EXEONLY-protected.
- SecureCRCCalc function will not work when CRCLOCK is enabled.

CMACKEY and Secure Flash Boot

- **Secure Flash Boot feature authenticates first 16KB of flash before boot.**
- **Secure Flash boot selected via the GPREG fields in the zone header.**
- **User defines a custom CMAC key in CMACKEY field in zone header.**
- **C2000 Hex Utility tool is used to generate CMAC tag from combination of CMAC key and user application code.**
- **User programs CMAC tag in hard-coded location in application code.**
- **Refer to the “Secure BOOT on C2000 Device” application note for detailed instructions.**
- **Device will calculate a CMAC tag from CMACKEY and flash contents.**
- **Calculated tag compared with user-programmed tag before boot is allowed.**

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](#)