TMS470R1x Memory Security Module Reference Guide

Literature Number: SPNU243
October 2005

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and application s using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation.

Resale of TI products or services with statements different form or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DSP	dsp.ti.com	Broadband	www.ti.com/broadband
Interface	interface.ti.com	Digital Control	www.ti.com/digitalcontrol
Logic	logic.ti.com	Military	www.ti.com/military
Power Mgmt	power.ti.com	Optical Networking	www.ti.com/opticalnetwork
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
		Telephony	www.ti.com/telephony
		Video & Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments
Post Office Box 655303 Dallas, Texas 75265

REVISION HISTORY

Revision	Date	Changes
*	10/2005	Initial version

Contents

Figures

Tables

Memory Security Module

This document describes the TMS470R1x memory security module (MSM). The MSM is a hardware security feature for the TMS470 devices with an ARM7TDMI. The MSM and the JTAG security module (JSM) provide a hardware firewall to the TMS470R1x family of devices.

Note: See Important Notice

The MSM and JSM modules add security for the device. However, like any security measure, they are not failsafe. TI is not responsible for security compromised while using an MSM and/or a JSM. Please see the *Important Notice* at the beginning of this document for more information regarding TI's warranty.

Topic **Page**

1 Overview

The memory security module (MSM) and the JTAG security module (JSM) used together provide a hardware firewall to prevent unauthorized users from accessing private/on-chip memories via the debug/test ports or an external memory interface. Access to the TI peripheral scan chain is always blocked. Access from an external memory interface to private resources without authorization can be blocked. For more information on the JSM, consult the JSM Reference Guide (literature number SPNU245).

There are two security modes possible with the MSM/JSM:

- Security mode 1: Protects private/secret on-chip memories and still provides debug/test access to public resources like peripherals
- Security mode 2: Disables the debug/test ports with a permanent firewall activation key

1.1 Security Mode 1: On/Off Control of Debug/Test Ports and External Memory Firewall

Security mode 1 has the following features:

- It allows control over the accessibility and modifiability of on-chip memory without blocking the JTAG port completely
- Unauthorized users are prevented from reading, writing, or erasing private code and data of on-chip memories.
- It provides 128-bit password security for each securable memory area (up to two). Please see the device-specific data sheet for the location of the 128-bit MSM password.
- The MSM can protect memory regions assigned to TMS470R1x memory chip-selects, with memory bank granularity. For the specific device implementation, please see the device-specific data sheet.
- While the device is secured, secure memory **cannot**:
  - Be modified
  - Be read from any code running from unsecure memory
  - Be read by the debugger (i.e., Code Composer Studio™) at any time
- The flash is secured after a reset until the password match flow (PMF) is executed.

- ❏ Access to on-chip private memories is granted and the firewall is disengaged upon successful entry of password match flow (including 128-bit password).
- ❏ Complete access to secure memory from the CPU code and the debugger is granted if the device is unsecured.
- ❏ Default password of all 1s will unsecure the device without having to provide the MSMKEY.
- ❏ Without successful password match flow execution, read/write access to on-chip secure memories is blocked, but the following accessibility is allowed through debug tools:
  - Read/write of public (unsecure) on-chip resources
  - Read/write of off-chip memories
  - Execution of private code

1.2 Security Mode 2: Permanent Blockage of Accesses to Debug/Test Ports

Security Mode 2 provides the following features:

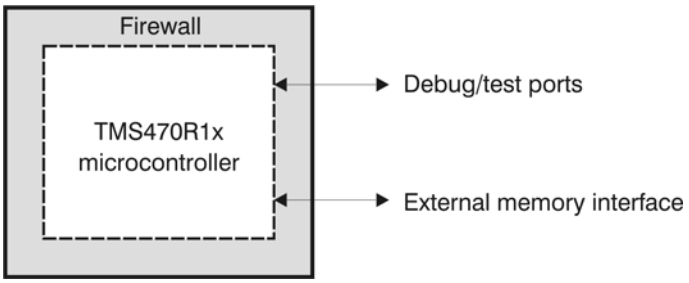
- ❏ A 64-bit firewall activation key (the JSM visible unlock code) in flash memory permanently blocks debug/test ports. Once the activation key is modified:
- ❏ Access to the ARM CPU via JTAG scan is **disabled.**
- ❏ Access to all internal memories is **disabled**.
- ❏ Debug tools cannot access the device.

Please see the device-specific data sheet for the location of the JSM visible unlock code. For more information on the JSM, consult the *JTAG Security Module (JSM) Reference Guide* (literature number SPNU245).

2 Functional Description

The TMS470R1x security features consist of a hardware firewall provided by the MSM and the JSM.

Figure 1. TMS470R1x Security Features



The security modules use a password to protect against read and write accesses to private resources through the test/debug ports or the external memory interface.

The device is secure when CPU access to the on–chip secure memory locations is restricted. A maximum of two independent zones may be defined and secured with their respective password. Security to each zone is ensured by its 128-bit password (four 32–bit words). The device is unsecured by executing the password match flow (PMF), described later in this chapter.

When secure, two levels of protection are possible, depending on where the program counter is currently pointing.

- If code is currently running from inside secure memory, then secure code can access secure data. In this case, only access through JTAG is blocked (i.e., the emulator).
- If code is running from unsecure memory, all read/write accesses to secure memories are blocked.

User code can dynamically jump into and out of secure memory, thereby allowing secure function calls from unsecure memory. For instance, interrupt service routines can be placed in secure memory, even if the main program loop is run from unsecure memory.

The standard method of running code out of the flash or ROM is to program the flash with the code (for ROM devices, the program is hardcoded at device fabrication). Since **instruction fetches** are always allowed, regardless of the

state of the MSM, the code will function correctly even without executing the PMF. Table 1 shows possible security scenarios.

Table 1. Security Scenarios

PMF Executed With Correct Password?	Operating Mode	Program Fetch Location	Security Description
No	Secure	Outside secure memory	Only fetches are allowed to secure memory.
No	Secure	Inside secure memory	CPU has full access. **JTAG port cannot read the secured memory contents.**
Yes	Not Secure	Anywhere	CPU and JTAG port have full access to secure memory.

2.1 Implementation

The 128-bit password is stored in four 32-bit wide memory locations at a base address given by the password locations (MSMPWL3–0 for the first MSM and MSMPWL7–4 for the second MSM, as described in section 5.6 through section 5.13). These passwords are located in nonvolatile memory, either flash or ROM. The password locations MSMPWL3–0 and MSMPWL7–4 are determined during device definition. You may need to configure the TMS470 memory map to unsecure the MSM and provide access to on-chip device memories to access the password locations. In flash devices, you can change a password any time if you know the old password. In ROM devices, you cannot change a password after the device is manufactured by Texas Instruments (TI).

The user-accessible registers (four 32–bit words for **each** protected zone) that are used to secure or unsecure the device are referred to as the MSMKEY registers. These eight registers (four for each MSM) are mapped in the memory space within the TMS470 upper 512K-byte address space (see section 5.6 through section 5.13) and are only accessible in *privileged mode*.

Note:

The 64-word flash line containing the password(s) must have a majority of 0s. TI's recommendation is to program all 0s into this line except for the flash protection keys (4 words) and the MSM password (4 words if one MSM is used). If you use a second MSM, the same applies to the flash line for the second password, i.e., that flash line must have a majority of 0s.

2.2 Unsecure versus Secure

If all 128 bits of the password are 1s, the device is unsecure. Since new flash devices have the flash erased (all 1s), only a read of the MSMPWL3–0 or MSMPWL7–4 is required to bring the device into unsecure mode.

If all 128 bits of the password are 0s, the device is secure, regardless of the contents of the MSMKEY registers. **The device is permenently secured.**

CAUTION

Do not use all 0s as a password or reset the device after performing a clear routine on the flash (programming all 0s). If a device is reset when a password is all 0s, the device will be permanently locked and can no longer be debugged or reprogrammed.

If the MSM key locations have been cleared (i.e., all bits programmed to 0), it is STRONGLY recommended to immediately erase the sector in which the MSM keys reside before generating any type of device reset, to avoid permanently locking the device.

Note:

The only circumstances under which you would wish to clear the MSM keys and leave them in the 0s state would be when you are ready to ship the part in the end application, with the MSM-protected memory segments permanently locked.

3 MSM Impact on Other On–Chip Resources

The MSM has no impact on the following on–chip resources:

- ❏ Memory regions not defined as protected by the MSM during device definition. These could be RAM banks, flash banks, or boot memory, i.e., any memory region assigned to a TMS470 chip-select. These unprotected memory blocks can be freely accessed and code run from them, whether the device is in secure or unsecure mode.
- ❏ The interrupt vectors at addresses 0x00 to 0x1F are public and excluded from protection.
- ❏ On–chip peripheral registers: The peripheral registers can be initialized by code running from on–chip or off–chip memory, whether the device is in secure or unsecure mode.

It is possible to load code onto the non-protected or public on–chip program RAM via the JTAG connector without any impact from the MSM. The code can be debugged and the peripheral registers initialized, independent of whether the device is in secure or unsecure mode.

3.1 Securable or Private Resources Protected by the MSM

The MSM protects the following resources. Table 2 lists the resources protected by a system with two MSMs.

- ❏ DMA registers
- ❏ DMA command buffer RAM
- ❏ Flash wrapper registers
- ❏ Selected flash banks (chip-select dependent)
- ❏ Selected RAM banks (chip-select dependent)
- ❏ Selected ROM banks (chip-select dependent)

Table 2. Securable Resources Protected by a System with Two MSMs

MSM_1	MSM_2
Selected flash banks	Selected flash banks (other than in primary zone)
Selected RAM banks	Selected RAM banks (other than in primary zone)
Selected ROM banks	Selected ROM banks (other than in primary zone)
Flash wrapper registers (for primary zone)	Flash wrapper registers (for secondary zone)
DMA registers	
DMA command buffer RAM	

4 Incorporating Code Security in User Applications

Code security is typically not required in the development phase of a project; however, security is needed after a robust code is developed. At this stage of code development or before code is committed to ROM, a password should be chosen to secure the device. A maximum of two MSM modules may be included in a TMS470R1x device, defining a maximum of two separate and independent securable memory areas. Each one of these memory areas has its own password, located in the MSMPWL registers described in section 5.6 through section 5.13.

Note:

Code ported from a flash family of devices to a ROM device must have an MSM to preserve code security and protect the password. If no MSM is integrated, the password should be removed from the password location before programming the ROM.

Once a password (other than all 1s) is in place, the device is secured. That is, programming a password into MSMPWL3–0 or MSMPWL7–4 and either performing a device reset or setting the FORCESEC bit (MSMSCR.31) secures the device.

Once the device is secured, debug access to contents of secure memory by JTAG or code running off external memory requires the supply of a valid password. See Table 1 on page 5 for the different security scenarios.

Note:

A password is not needed to execute code out of secure memory (such as in a typical end–customer use)**;** however, access to secure memory contents for debug purposes requires a password.

The **MSM status and control register** (MSMSCR in section 5.5) contains one control bit, called FORCESEC, located in bit 31, and one status bit, called SECURE, located in bit 0. Setting the FORCESEC bit to a 1 resets the MSMKEY registers and the internal logic of the MSM so that the password match flow must be executed to unsecure the device again. **A write of 0 to the FORCESEC bit has no effect.** A read of the FORCESEC bit always returns a 0. A device reset also resecures the device. The SECURE bit is a read–only bit, which reflects the security state of the device. Writes to this bit have no effect. Reads of bits 30–1 in the MSMSCR are undetermined.

The base address for the first MSM is set at 0xFFFF_F700, and the base address for the second MSM is set at 0xFFFF_F600. Section 5.1 through section 5.4 illustrate the user-accessible MSMKEY registers.

4.1 Environments That Require Security Unlocking

Following are the typical situations under which unsecuring **may be** required:

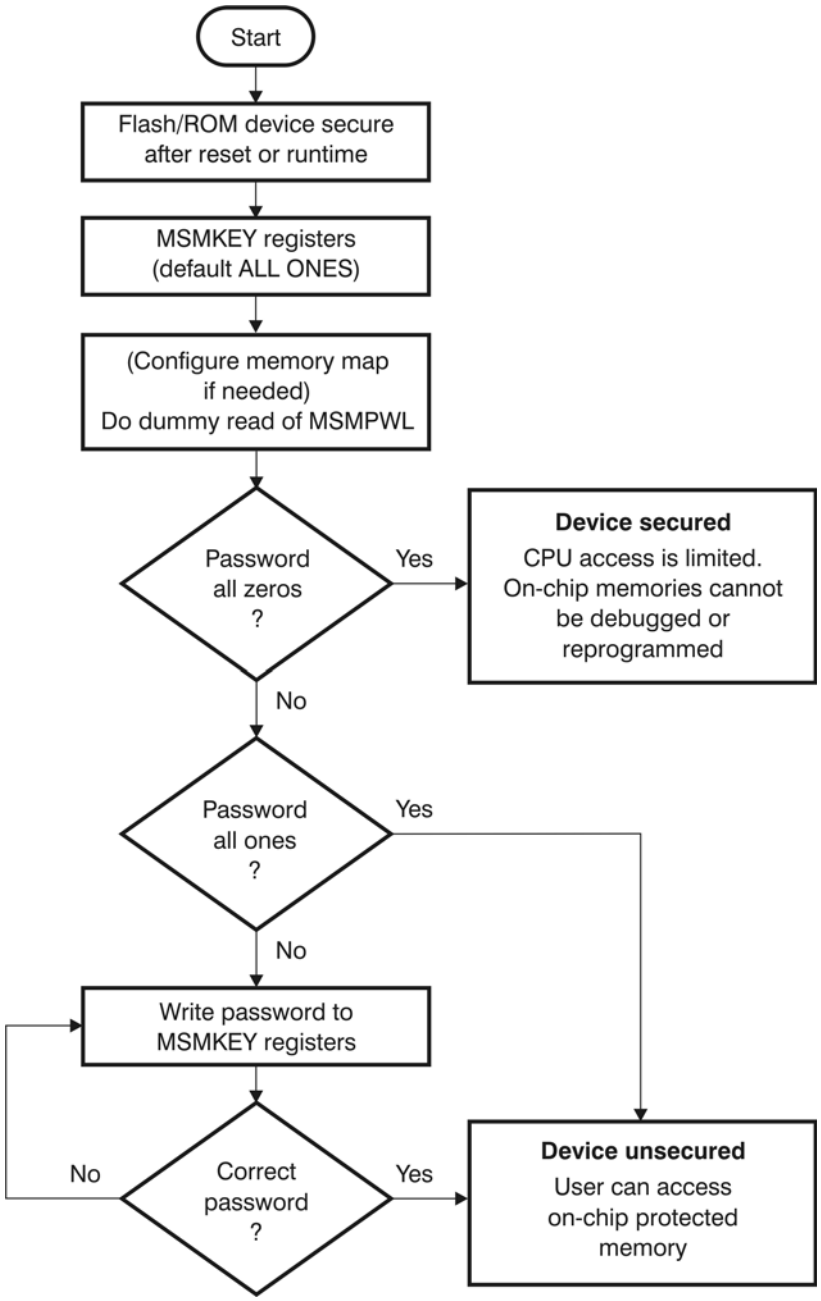
- Code development using debuggers (such as Code Composer Studio™). This is the most common environment during the design phase of a product.
- Flash programming using TI's flash utilities. Flash programming is common during code development and testing. Once the user supplies the necessary password, the flash utilities disable the security logic before attempting to program the flash. The flash utilities can disable the code security logic in new devices without any authorization, since new devices come with an erased flash. However, reprogramming devices (that already contain custom passwords) require passwords to be supplied to the flash utilities in order to enable programming.
- Custom environment defined by the application.
- In addition to the above, access to secure memory contents may be required in situations such as:
  - Using the on–chip boot loader to program the flash.
  - Executing code from external memory or on–chip unsecure memory and requiring access to secure memory for lookup table. This is not a suggested operating condition as supplying the password from external code could compromise code security.

The unsecuring sequence is identical in all of the situations above. This sequence is referred to as the *password match flow (PMF)*. Section 4.2 explains the sequence of operations that are required every time the user attempts to unsecure a device.

4.2 Password Match Flow

The password match flow (PMF) is a sequence of four reads from the password locations (MSMPWL3–0 or MSMPWL7–4) followed by four writes to the MSMKEY registers. If the device is unsecured by PMF, then the password will be visible in the password locations. Figure 2 illustrates the PMF.

Figure 2. Password Match Flow



4.3 Password Programming on Flash Devices

To write a password using TI's Flash470 program or the BP Programmer tools, follow these steps:

1) Write the old password to MSMKEY registers. This step is not needed when the password location contains all 1s.
2) Perform 4 dummy reads to the MSM password locations in flash as part of the PMF. This will clear the MSMSCR.0 bit, which specifies that the device is now unsecure.
3) Write a new password to the four MSM password locations in flash memory.
4) Read back the four MSM password locations in flash to verify if the new password write happened correctly.

Note:

It is critical that, during the programming of a new password, the device is neither reset nor the FORCESEC bit set until step 4 is completed successfully. A reset or a write to the FORCESEC bit during password programming could lock the device to an unknown password.

4.4 Unsecuring Considerations for Devices With/Without Code Security

Case 1 and Case 2 provide unsecuring considerations for devices with and without code security.

4.4.1 Case 1: Device With Code Security

A device with code security should have a predetermined password stored in the MSMPWL3–0 or MSMPWL7–4 (at base address 8 words from the end of the first flash sector, with a length of four 32-bit words). The following are the steps to unsecure this device:

1) Read the four consecutive MSMPWL locations: MSMPWL3–0 for the first MSM or MSMPWL7–4 for the second MSM.
2) Write the password into the MSMKEY registers.
3) If the password in the MSMKEY registers matches the password, the device becomes unsecure. If the passwords do not match, it stays secure.

4.4.2 Case 2: Device Without Code Security

A device without code security should have 128 bits of all 1s stored in the MSMPWL. Perform the following step to use this device:

Perform dummy reads of the four consecutive MSMPWL locations: MSMPWL3–0 for the first MSM or MSMPWL7–4 for the second MSM.

Secure memory is fully accessible immediately after this operation is completed.

Note:

A dummy read of the password location registers must be performed before reading, writing, or programming secure memory, even though the device is not protected with a password.

5 Registers

The following sections describe the registers in detail.

Table 3. Control Registers Summary

Offset	Acronym	Register Description	Section
0x00(1)	MSMKEY0	Low word of the KEY register	Section 5.1
0x04(1)	MSMKEY1	Second word of the KEY register	Section 5.2
0x08(1)	MSMKEY2	Third word of the KEY register	Section 5.3
0x0C(1)	MSMKEY3	High word of the KEY register	Section 5.4
0x24(1)	MSMSCR	Status and control register	Section 5.5
0x00(2)	MSMPWL0	Low word of password register for first MSM	Section 5.6
0x04(2)	MSMPWL1	Second word of password register for first MSM	Section 5.7
0x08(2)	MSMPWL2	Third word of password register for first MSM	Section 5.8
0x0C(2)	MSMPWL3	High word of password register for first MSM	Section 5.9
0x00(3)	MSMPWL4	Low word of password register for second MSM	Section 5.10
0x04(3)	MSMPWL5	Second word of password register for second MSM	Section 5.11
0x08(3)	MSMPWL6	Third word of password register for second MSM	Section 5.12
0x0C(3)	MSMPWL7	High word of password register for second MSM	Section 5.13

1 The base address for the first MSM is 0xFFFFF700; the base address for the second MSM is 0xFFFFF600.

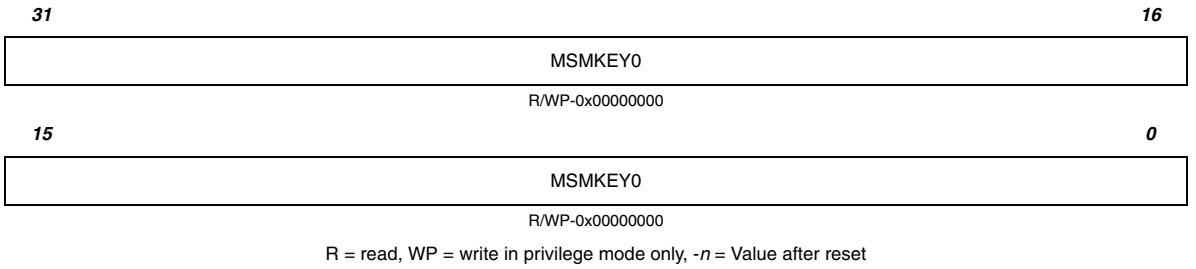
2 The base address is 8 words from the end of the first flash sector.

3 The base address is 4 words from the end of the first flash sector in the first bank of the second MSM zone.

5.1 MSM Key Register 0 (MSMKEY0)

This register provides the low word of the 128-bit MSM KEY register. Figure 3 and Table 4 describe this register.

Figure 3. MSM Key Register 0 (MSMKEY0) [Offset 0x00[(1)]]



R = read, WP = write in privilege mode only, -*n* = Value after reset

1) The base address for the first MSM is 0xFFFFF700; the base address for the second MSM is 0xFFFFF600.

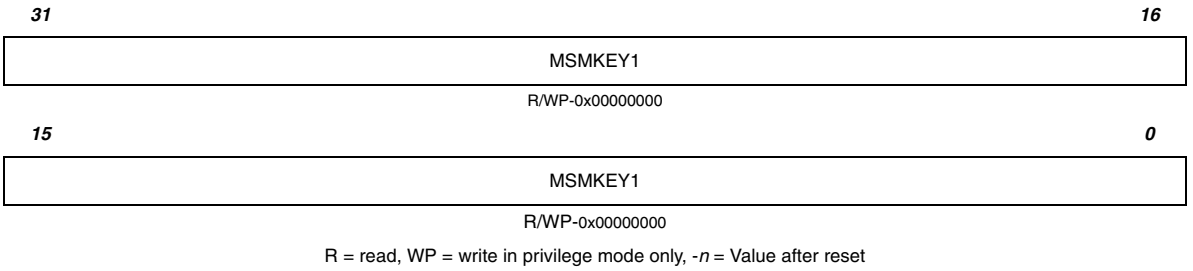
Table 4. MSM Key Register 0 (MSMKEY0) Field Descriptions

Bit	Name	Value	Description
31–0	MSMKEY0	0–FFFF FFFF	These bits provide the low word of the 128-bit MSMKEY register.

5.2 MSM Key Register 1 (MSMKEY1)

This register provides the low word of the 128-bit MSM KEY register. Figure 4 and Table 5 describe this register.

Figure 4. MSM Key Register 1 (MSMKEY1) [Offset 0x04[(1)]]



R = read, WP = write in privilege mode only, -*n* = Value after reset

1) The base address for the first MSM is 0xFFFFF700; the base address for the second MSM is 0xFFFFF600.

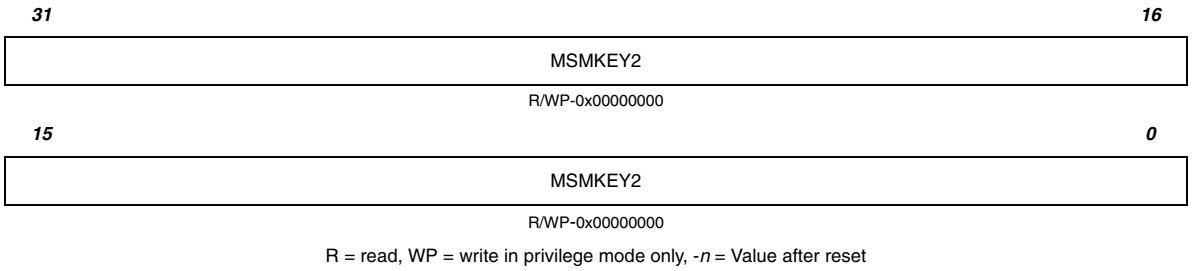
Table 5. MSM Key Register 1 (MSMKEY1) Field Descriptions

Bit	Name	Value	Description
31–0	KEY1	0–FFFF FFFF	These bits provide the second word of the 128-bit MSMKEY register.

5.3 MSM Key Register 2 (MSMKEY2)

This register provides the third word of the 128-bit MSM KEY register. Figure 5 and Table 6 describe this register.

Figure 5. MSM Key Register 2 (MSMKEY2) [Offset 0x08[(1)]]



R = read, WP = write in privilege mode only, -*n* = Value after reset

1) The base address for the first MSM is 0xFFFFF700; the base address for the second MSM is 0xFFFFF600.

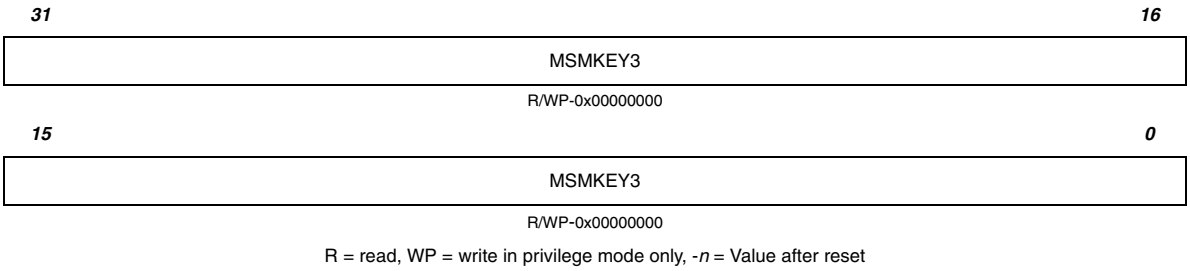
Table 6. MSM Key Register 2 (MSMKEY2) Field Descriptions

Bit	Name	Value	Description
31–0	KEY2	0–FFFF FFFF	These bits provide the third word of the 128-bit MSMKEY register.

5.4 MSM Key Register 3 (MSMKEY3)

This register provides the third word of the 128-bit MSM KEY register. Figure 6 and Table 7 describe this register.

Figure 6. MSM Key Register 3 (MSMKEY3) [Offset 0x0C[(1)]]



R = read, WP = write in privilege mode only, -*n* = Value after reset

1) The base address for the first MSM is 0xFFFFF700; the base address for the second MSM is 0xFFFFF600.

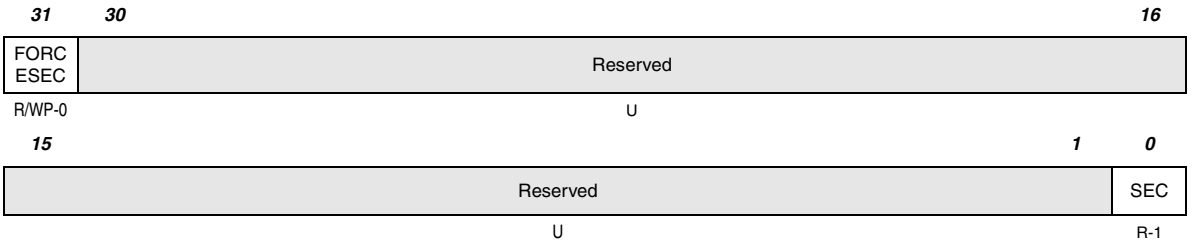
Table 7. MSM Key Register 3 (MSMKEY3) Field Descriptions

Bit	Name	Value	Description
31–0	KEY3	0–FFFF FFFF	These bits provide the high word of the 128-bit MSMKEY register.

5.5 MSM Status and Control Register (MSMSCR)

Figure 7 and Table 8 describe this register.

Figure 7. MSM Status and Control Register (MSMSCR) [Offset 0x24[(1)]]



R = read, WP = write in privilege mode only, -*n* = Value after reset, U = undefined

1) The base address for the first MSM is 0xFFFFF700; the base address for the second MSM is 0xFFFFF600.

Table 8. MSM Status and Control Register (MSMSCR) Field Descriptions

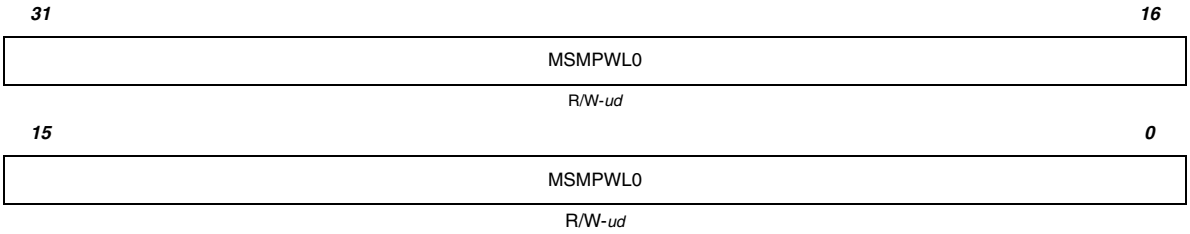
Bit	Name	Value	Description
31	FORCESEC		Force secure mode. Writing to this bit forces the device into a secure state. Reads always return a 0.
		0	Writing a 0 to this bit has no effect.
		1	Writing a 1 clears the MSMKEY registers and forces the device into a secure state.
30–1	Reserved		Reads are undefined and writes have no effect.
0	SEC		Secure. This bit reflects the state of the MSM.
		0	The MSM is not secure.
		1	The MSM is secure.

5.6 MSM 1 Password Low Register 0 (MSMPWL0)

This register provides the low word of the 128-bit MSM password register for the first MSM. Figure 8 and Table 9 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 8. MSM 1 Password Low Register 0 (MSMPWL0) [Offset 0x00[(1)]]



R = read, W = write, -*ud* = Undefined value after reset

1) The base address is 8 words from the end of the first flash sector.

Table 9. MSM 1 Password Low Register 0 (MSMPWL0) Field Descriptions

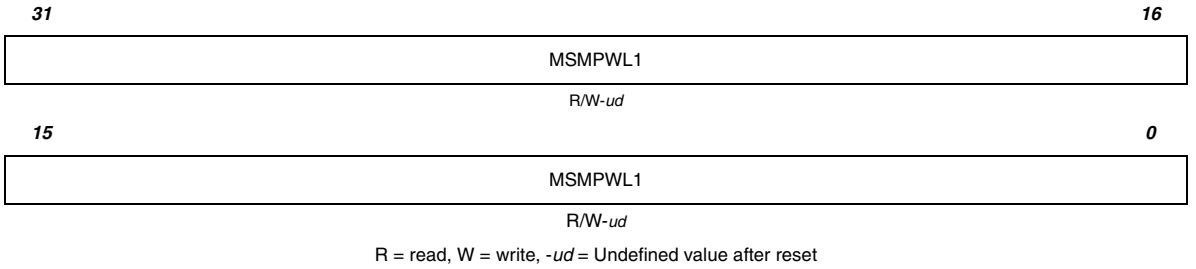
Bit	Name	Value	Description
31–0	MSMPWL0	0–FFFF FFFF	These bits provide the low word of the 128-bit password for the first MSM.

5.7 MSM 1 Password Low Register 1 (MSMPWL1)

This register provides the second word of the 128-bit MSM password register for the first MSM. Figure 9 and Table 10 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 9. MSM 1 Password Low Register 1 (MSMPWL1) [Offset 0x04(1)]



1) The base address is 8 words from the end of the first flash sector.

Table 10. MSM 1 Password Low Register 1 (MSMPWL1) Field Descriptions

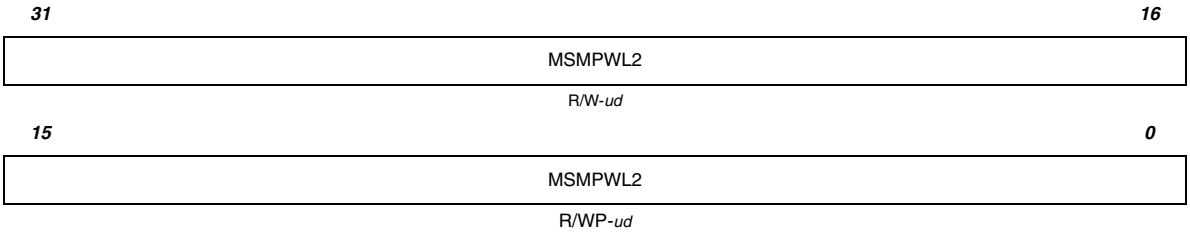
Bit	Name	Value	Description
31–0	MSMPWL1	0–FFFF FFFF	These bits provide the second word of the 128-bit password for the first MSM.

5.8 MSM 1 Password Low Register 2 (MSMPWL2)

This register provides the third word of the 128-bit MSM password register for the first MSM. Figure 10 and Table 11 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 10. MSM 1 Password Low Register 2 (MSMPWL2) [Offset 0x08[(1)]]



R = read, WP = write in privilege mode only, -*ud* = Undefined value after reset

1) The base address is 8 words from the end of the first flash sector.

Table 11. MSM 1 Password Low Register 2 (MSMPWL2) Field Descriptions

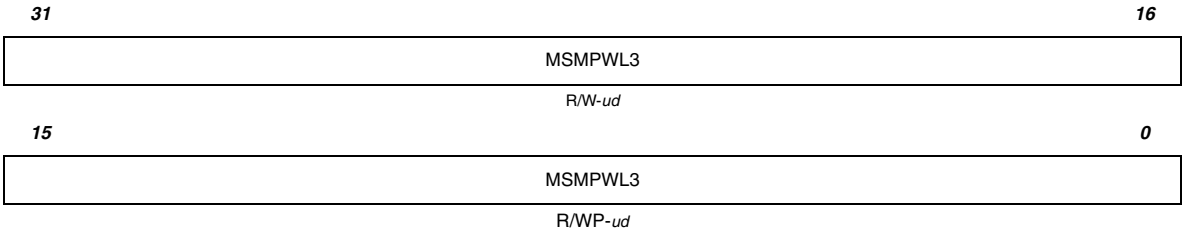
Bit	Name	Value	Description
31–0	MSMPWL2	0–FFFF FFFF	These bits provide the third word of the 128-bit password for the first MSM.

5.9 MSM 1 Password Low Register 3 (MSMPWL3)

This register provides the high word of the 128-bit MSM password register for the first MSM. Figure 11 and Table 13 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 11. MSM 1 Password Low Register 3 (MSMPWL3) (Offset = 0x0C[(1)])



R = read, WP = write in privilege mode only, *-ud* = Undefined value after reset

1) The base address is 8 words from the end of the first flash sector.

Table 12. MSM 1 Password Low Register 3 (MSMPWL3) Field Descriptions

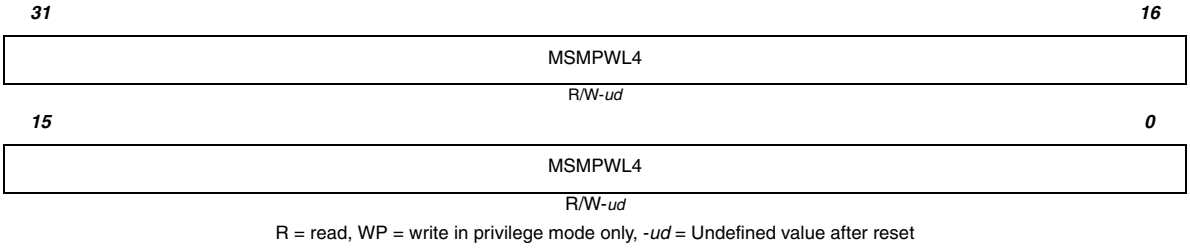
Bit	Name	Value	Description
31–0	MSMPWL3	0–FFFF FFFF	These bits provide the high word of the 128-bit password for the first MSM.

5.10 MSM 2 Password Low Register 4 (MSMPWL4)

This register provides the low word of the 128-bit MSM password register for the second MSM. Figure 12 and Table 13 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 12. MSM 2 Password Low Register 4 (MSMPWL4) [Offset 0x00(1)]



R = read, WP = write in privilege mode only, -*ud* = Undefined value after reset

1) The base address is 4 words from the end of the first flash sector in the first bank of the second MSM zone.

Table 13. MSM 2 Password Low Register 4 (MSMPWL4) Field Descriptions

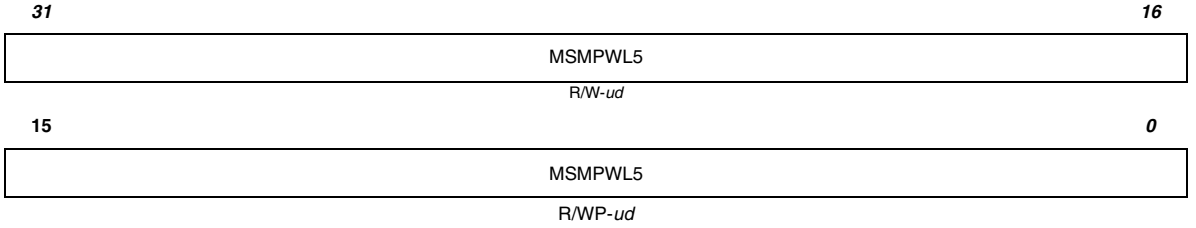
Bit	Name	Value	Description
31–0	MSMPWL4	0–FFFF FFFF	These bits provide the low word of the 128-bit password for the second MSM.

5.11 MSM 2 Password Low Register 5 (MSMPWL5)

This register provides the second word of the 128-bit MSM password register for the second MSM. Figure 14 and Table 14 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 13. MSM 2 Password Low Register 5 (MSMPWL5) [Offset 0x04(1)]



R = read, WP = write in privilege mode only, -*ud* = Undefined value after reset

1) The base address is 4 words from the end of the first flash sector in the first bank of the second MSM zone.

Table 14. MSM 2 Password Low Register 5 (MSMPWL5) Field Descriptions

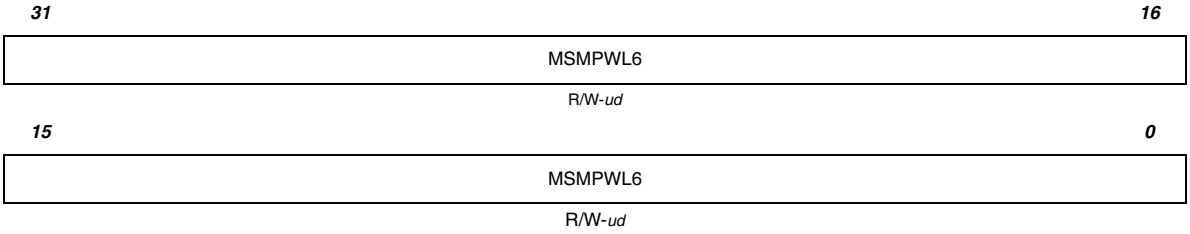
Bit	Name	Value	Description
31–0	MSMPWL5	0–FFFF FFFF	These bits provide the second word of the 128-bit password for the second MSM.

5.12 MSM 2 Password Low Register 6 (MSMPWL6)

This register provides the third word of the 128-bit MSM password register for the second MSM. Figure 3 and Table 15 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 14. MSM 2 Password Low Register 6 (MSMPWL6) [Offset 0x08[(1)]]



R = read, WP = write in privilege mode only, -*ud* = Undefined value after reset

1) The base address is 4 words from the end of the first flash sector in the first bank of the second MSM zone.

Table 15. MSM 2 Password Low Register 6 (MSMPWL6) Field Descriptions

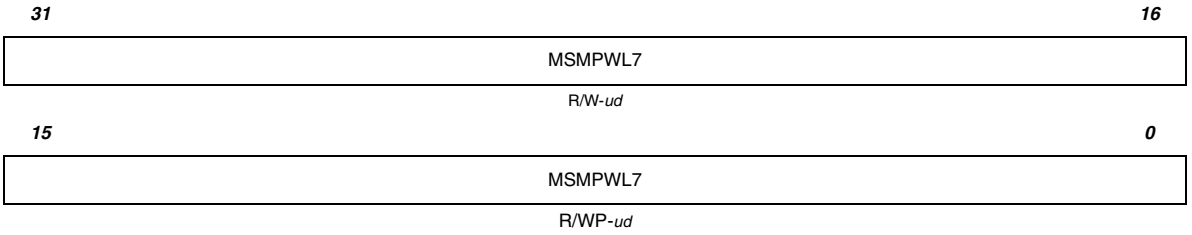
Bit	Name	Value	Description
31–0	MSMPWL6	0–FFFF FFFF	These bits provide the third word of the 128-bit password for the second MSM.

5.13 MSM 2 Password Low Register 7 (MSMPWL7)

This register provides the high word of the 128-bit MSM password register for the second MSM. Figure 3 and Table 16 describe this register.

If the password locations are in flash memory, then writes to the MSMPWL are like writes to any secure flash location. If the device is unsecured by PMF, a read of this register will show the password; otherwise, reads are undefined.

Figure 15. MSM 2 Password Low Register 7 (MSMPWL7) [Offset 0x0C(1)]



R = read, WP = write in privilege mode only, -*ud* = Undefined value after reset

1) The base address is 4 words from the end of the first flash sector in the first bank of the second MSM zone.

Table 16. MSM 2 Password Low Register 7 (MSMPWL7) Field Descriptions

Bit	Name	Value	Description
31–0	MSMPWL7	0–FFFF FFFF	These bits provide the high word of the 128-bit password for the second MSM.

6 Protecting Security Logic

The following sections provide information about actions you should do and actions you should NOT do to successfully protect your security logic.

6.1 DO . . .

- ❏ To keep the debug and code development phase simple, use the device in unsecure mode, i.e., use 128 bits of all 1s as the password, or use a password that is easy to remember. Use passwords after the development phase when the code is frozen.
- ❏ Recheck the passwords in the MSMPWL before programming the COFF file using flash utilities.
- ❏ The flow of code execution can freely toggle back and forth between secure memory and unsecure memory without compromising security. To access data variables located in secure memory when the device is secured, code execution must currently be running from secure memory.

6.2 DO NOT . . .

- ❏ If code security is desired, do not embed the password in your application anywhere other than in the MSMPWL, or security may be compromised.
- ❏ Do not use 128 bits of all 0s as the password. This will automatically secure the device **permanently,** regardless of the content of the MSMKEY registers. **The device will neither be debuggable nor reprogrammable.**
- ❏ Do not generate a reset after clearing the flash array. Clearing the flash (programming 0s) will leave 0s in the MSMPWL and a device reset will then automatically secure the device permanently regardless of the contents of the MSMKEY register. It will not be possible to debug or reprogram the device once this happens.
- ❏ Do not access the MSM registers in a device with no MSM. Such an action may assert an illegal access.

Appendix A: Summary of Registers

Section A-1 provides a summary of the MSMKEY and MSMSCR registers. Section A-2 provides a summary of the MSMPWL registers.

A-1 Summary of MSMKEY and MSMSCR Registers

Figure A-1 summarizes the bits in the MSMKEY and MSMSCR registers.

Figure A-1. Summary of MSMKEY and MSMSCR Registers

Offset Address Register	31 15	30 14	29 13	28 12	27 11	26 10	25 9	24 8	23 7	22 6	21 5	20 4	19 3	18 2	17 1	16 0
0x00[1] MSMKEY0 Section 5.1	MSMKEY0															
	MSMKEY0															
0x04[1] MSMKEY1 Section 5.2	MSMKEY1															
	MSMKEY1															
0x08[1] MSMKEY2 Section 5.3	MSMKEY2															
	MSMKEY2															
0x0C[1] MSMKEY3 Section 5.4	MSMKEY3															
	MSMKEY3															
0x24[1] MSMSCR Section 5.5	FORCE SEC	Reserved														
	Reserved															SEC

1 The base address for the first MSM is 0xFFFFFF700; the base address for the second MSM is 0xFFFFF600.

A-2 Summary of MSMPWL Registers

Figure A-2 summarizes the MSMPWL registers.

Figure A-2. Summary of MSMPWL Registers

Offset Address Register	31 15	30 14	29 13	28 12	27 11	26 10	25 9	24 8	23 7	22 6	21 5	20 4	19 3	18 2	17 1	16 0
0x00[1] MSMPWL0	MSMPWL0															
Section 5.6	MSMPWL0															
0x04[1] MSMPWL1	MSMPWL1															
Section 5.7	MSMPWL1															
0x08[1] MSMPWL2	MSMPWL2															
Section 5.8	MSMPWL2															
0x0C[1] MSMPWL3	MSMPWL3															
Section 5.9	MSMPWL3															

1 The base address is 8 words from the end of the first flash sector.

2 The base address is 4 words from the end of the first flash sector in the first bank of the second MSM zone.

Figure A-2. Summary of MSMPWL Registers (Continued)

0x00[(2)] MSMPWL4 Section 5.10	MSMPWL4
	MSMPWL4
0x04[(2)] MSMPWL5 Section 5.11	MSMPWL5
	MSMPWL5
0x08[(2)] MSMPWL6 Section 5.12	MSMPWL6
	MSMPWL6
0x0C[(2)] MSMPWL7 Section 5.13	MSMPWL7
	MSMPWL7

1 The base address is 8 words from the end of the first flash sector.

2 The base address is 4 words from the end of the first bank of the second MSM zone.