ABSTRACT
The C2000 dual code security module (DCSM) is a security feature incorporated in C2000 devices. The C2000 DCSM Security Tool allows you to configure the DCSM module through an intuitive graphical user interface (GUI). This application report examines the features of the C2000 DCSM Security Tool.

Contents
1 Introduction ................................................................................................................... 2
2 Supplementary Online Information ........................................................................... 2
3 DCSM Security Tool Example Project ....................................................................... 2
4 DCSM Security Tool Configurable Options ............................................................... 5
5 DCSM Security Tool Generated Content ................................................................... 9
6 Adding DCSM Security Tool Support to an Existing Driverlib Project ......................... 12
7 Summary .................................................................................................................... 13
8 References ................................................................................................................ 13

List of Figures
1 Import CCS Project .................................................................................................... 3
2 DCSM Security Tool Example Project ..................................................................... 4
3 DCSM Security Tool User Interface ......................................................................... 4
4 Adding a SECURITY Module to Project .................................................................. 5
5 Use Zone Checkbox .................................................................................................... 6
6 ZONE1 Per LINKPOINTER Options ........................................................................ 7
7 ZONE1 Header Options ............................................................................................ 8
8 View Generated Files ................................................................................................ 9
9 dcm.asm Highlighting the Changes ........................................................................... 10
10 dcm.cmd Highlighting the Changes ......................................................................... 10
11 Generated Source Files in the Build Directory ..................................................... 11
12 MAP File With Security Options ............................................................................ 12
13 Enable SysConfig .................................................................................................... 12
14 SysConfig SDK Path ............................................................................................... 13

Trademarks
C2000 is a trademark of Texas Instruments.
All other trademarks are the property of their respective owners.
1 Introduction

This document guides you through the following items related to the DCSM Security Tool:

- Importing the example DCSM Security Tool (DCSM) C2000WARE project
- Exploring the DCSM Security Tool configurable options
- DCSM Security Tool generated content
- Adding DCSM Security Tool support to an existing project

2 Supplementary Online Information

For more information on the DCSM module on a specific C2000 device, see the device-specific data sheet and the corresponding Technical Reference Manual (TRM).

This application report was written using the TMS320F2837xD family of devices, but the tool also supports the TMS320F2837xS and the TMS320F07x family of devices as well. The data sheet and TRM used for this application report are listed below and in Section 8.

- TMS320F2837xD Dual-core Delfino™ Microcontrollers Data Sheet

Additional support is provided by the TI E2E™ Community.

3 DCSM Security Tool Example Project

In order to use the DCSM Security Tool, you must first import the DCSM Security Tool based example projects from the C2000WARE software development kit (SDK). The DCSM Security Tool is available in C2000WARE version 3.01.00.00 and later. For multi-core devices, DCSM Security Tool enabled example projects are available for each core.

Use the following instructions to import the DCSM Security Tool based example project.

1. Launch Code Composer Studio (CCS) version 9.2 or later and select a workspace.

---

**NOTE:** The C2000 DCSM Security Tool is a SysConfig-based tool that requires CCS version 9.2 or higher and will not work with older versions of CCS.
2. With CCS open, click **Project → Import CCS Projects...**

![Figure 1. Import CCS Project](image)

3. In the **Import CCS Projects** wizard, select **Browse...** and navigate to the folder:

   `<C2000Ware_Install_Location>\driverlib\f2837xd\examples\cpu1\dcsm`

---

**NOTE:** Dual core example is available at:

   `<C2000Ware_Install_Location>\driverlib\f2837xd\examples\dual\dcsm`
4. Select the DCSM Security Tool project and click Finish.
The project should now be imported into your workspace and look similar to Figure 2.

The DCSM Security Tool configuration is stored inside the .syscfg file.

5. Open the dcsm_security_tool.syscfg file.
The DCSM Security Tool will now open inside CCS and the DCSM Security Tool GUI is available for you to configure the DCSM module. The DCSM Security Tool looks similar to Figure 3.

Figure 2. DCSM Security Tool Example Project

The DCSM Security Tool configuration is stored inside the .syscfg file.

Figure 3. DCSM Security Tool User Interface

You can now start configuring the DCSM Security Tool. Section 4 describes all the configurable options inside the DCSM Security Tool.
4 DCSM Security Tool Configurable Options

The first step to using the DCSM Security Tool is to add an instance of the SECURITY module. This is done by clicking the ADD button at the top right corner on clicking the plus sign shown in Figure 4.

The SECURITY module contains four submodules:

- **ZONE1 Per LINKPOINTER:** This submodule contains the configurable options for zone 1 of the DCSM peripheral that can be updated only once PER LINKPOINTER update.
- **ZONE1 Header:** This submodule contains the configurable options for zone 1 of the DCSM peripheral that can only be updated **ONCE** and **ONCE ONLY**. Once these options are configured, you **CANNOT** update them even by changing the LINKPOINTER.
- **ZONE2 Per LINKPOINTER:** This submodule contains the configurable options for zone 2 of the DCSM peripheral that can be updated only once PER LINKPOINTER update.
- **ZONE2 Header:** This submodule contains the configurable options for zone 2 of the DCSM peripheral that can only be updated **ONCE** and **ONCE ONLY**. Once these options are configured, you **CANNOT** update them even by changing the LINKPOINTER.

ZONE1 Per LINKPOINTER/Header and ZONE2 PER LINKPOINTER/Header submodule configurable options are identical. ZONE1 options configure zone 1 of the DCSM peripheral, while ZONE2 options configure zone 2 of the DCSM peripheral. This document steps through all of the configurable options for ZONE1.
4.1 ZONE1/ZONE2 Per LINKPOINTER Submodule

The first option inside each ZONEx Per LINKPOINTER module is selecting whether that zone is configured or left unchanged. In order to configure the ZONEx Per LINKPOINTER, you must expand the ZONEx Per LINKPOINTER submodule and check the Configure this Section box.

Figure 5. Use Zone Checkbox

The ZONE1/ZONE2 Per LINKPOINTER submodule contain the following configurable options:

- **Current LINKPOINTER**: This is the current LINKPOINTER value that is being used by the zone. The Current LINKPOINTER value is used to calculate the next LINKPOINTER value. You must input the Current LINKPOINTER value.

- **Update the LINKPOINTER**: This option is only available if the Current LINKPOINTER value is 0x1FFFFFFF (the default value). If you have not yet programmed the device OTP, you can use the first LINKPOINTER location by unchecking this option. If the Current LINKPOINTER value is 0x1FFFFFFF and you have already used the first LINKPOINTER location, then the Update the LINKPOINTER checkbox MUST be checked. If the Current LINKPOINTER value is any value other than 0x1FFFFFFF, the Update the LINKPOINTER option is not applicable (will always pick the next LINKPOINTER location).

- **Next LINKPOINTER**: This is the value of the LINKPOINTER automatically calculated based on the Current LINKPOINTER and the Update the LINKPOINTER option. This is the value used in the generated code for the LINKPOINTER.

- **Zone Select Block (ZSB) Offset**: This is the value of the LINKPOINTER offset automatically calculated based on the Next LINKPOINTER address. This is the value used in the generated code for the LINKPOINTER offset.

- **Password 0-4**: The four 32-bit password values.

- **CLA, RAM, FLASH Owner Selection**: These configurable options allow you to select which zone owns each securable resource. Each securable resource can only be secured by either zone1 or zone2. The options for CLA, RAM and FLASH memory sections are different.
ZONE1 and ZONE2 options are identical. You can select which zone is the owner of each section of the memory by configuring the specific memory section's option in either of the ZONEx Per LINKPOINTER submodule. In the case of an error (where a memory section is assigned to be secured by both zone1 and zone2), the tool will notify you.

### 4.2 ZONE1/ZONE2 Header Submodule

The first option inside each ZONEx Header module is selecting whether that zone's header is configured or left unchanged. In order to configure the ZONE, you must expand the ZONEx Header submodule and check the **Configure this Section** box.

ZONE1/ZONE2 Header submodule can only be configured **ONCE** and **ONCE ONLY**. Once these options are configured, you **CANNOT** update them even by changing the LINKPOINTER. The ZONE1/ZONE2 Header submodule contain the following configurable options:

- **Password Lock**: Disable/enable the Password Lock permanently. For more information, see the device-specific TRM.
- **CRC Lock**: Disable/enable the CRC Lock permanently. For more information, see the device-specific TRM.
- **Configure Boot Section**: This option determines whether to program the Boot Mode and Boot Pins.
- **Boot Control PIN0/PIN1**: These options select the boot pin0/pin1 for the device.
- **Get Mode**: This is the boot mode for the device. The list of available options can be found in the device-specific TRM.
- **Boot Control Key** and **Boot Control Mode**: These values are calculated based on the **Get Mode** option.

**Figure 6. ZONE1 Per LINKPOINTER Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure this Section</td>
<td>On</td>
</tr>
<tr>
<td>Current LINKPOINTER</td>
<td>0x1FFFFFFFF</td>
</tr>
<tr>
<td>Update the LINKPOINTER</td>
<td></td>
</tr>
<tr>
<td>Next LINKPOINTER</td>
<td>0x1FFFFFFFF</td>
</tr>
<tr>
<td>Zone Select Block (ZSB) Offset</td>
<td>0x20</td>
</tr>
<tr>
<td>Password 0</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>Password 1</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>Password 2</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>Password 3</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>CLA</td>
<td>Unsecure (or secured by other zone)</td>
</tr>
<tr>
<td>RAM LS0</td>
<td>Unsecure (or secured by other zone)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Select Block (ZSB) Offset</td>
<td>0x20</td>
</tr>
<tr>
<td>Password 0</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>Password 1</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>Password 2</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>Password 3</td>
<td>0xFFFFFFFF</td>
</tr>
<tr>
<td>CLA</td>
<td>Unsecure (or secured by other zone)</td>
</tr>
<tr>
<td>RAM LS0</td>
<td>Unsecure (or secured by other zone)</td>
</tr>
</tbody>
</table>
Figure 7. ZONE1 Header Options
The DCSM Security Tool generates the following two files:

- **dcsm.asm**: The assembly file containing your LINKPOINTER value, passwords, and other options.
- **dcsm.cmd**: The linker command file containing the MEMORY addresses and SECTIONS that references the content in **dcsm.asm** file.

The tool updates the content of the two generated files and highlights the most recent changes in the configuration in real-time. In order to view the generated files, click the item shown in Figure 8 and then open **dcsm.asm** file.

![Figure 8. View Generated Files](image)
In order to see the changes in the ASM file, change the CRC Lock option in the ZONE1 Header submodule, with the `dcsm.asm` file open. Figure 9 shows the latest changes in the file highlighted.

![Figure 9. dcsm.asm Highlighting the Changes](image)

In order to see the changes in the CMD file, uncheck the Configure this Zone option in the ZONE1 Per LINKPOINTER submodule, with the `dcsm.cmd` file open. Figure 10 shows the latest changes in the file highlighted.

![Figure 10. dcsm.cmd Highlighting the Changes](image)
It is important to note that these files are auto-generated and you cannot modify them.

Save the `.syscfg` file and build the project. When the project is finished building, the generated ASM and CMD files are placed in the build directory under a folder named "syscfg". This is shown in Figure 11.

![Project Explorer](image)

**Figure 11. Generated Source Files in the Build Directory**

When the project is built, the two generated files (security.asm and security.cmd) are automatically used to generate the .OUT binary executable file.

**NOTE:** For CCS version 9.2/9.3 users, the generated CMD file must be copied out of the "syscfg" folder and placed in the top directory of the CCS project. You must then rebuild the project for the CMD file to take effect in the build process.

You can open the .MAP file in the build directory to see the DCSM Security Tool's generated content taking effect in the build process.
Adding DCSM Security Tool Support to an Existing Driverlib Project

6 Adding DCSM Security Tool Support to an Existing Driverlib Project

Use the following steps to add DCSM Security Tool support to an existing C2000WARE DriverLib Project:

1. Add the "dcsm_security_tool.syscfg" file (For F2837xD `<C2000Ware_Install_Location>/driverlib/f2837xd/examples/cpu1/dcsm/empty.syscfg`) from the DCSM examples folder to the project by copying the file into the project.

2. CCS will ask whether or not to enable SysConfig. Accept and select "Yes".

3. Open the "Project Properties" and open the Resources → Linked Resources. Add the following Variable Paths:
   a. DCSMTOOL_SYSCFG_ROOT
      `<C2000Ware_Install Location>/utilities/dcsm_tool/dcsm_syscfg`

---

Figure 12. MAP File With Security Options

![Figure 12. MAP File With Security Options](image)

Figure 13. Enable SysConfig

![Figure 13. Enable SysConfig](image)
4. Open Build → SysConfig → Basic Options.
5. Add the following to the Root system config meta data list:
   a. `$(DCSMTOOL_SYSCFG_ROOT)/.metadata/product.json`
6. In the **Name of device** (-d, --device) option, enter **F2837xD**, as shown in Figure 14.

![Figure 14. SysConfig SDK Path](image)

7 **Summary**

The C2000 DCSM Security Tool allows you to configure the DCSM module by generating the source code needed to configure the peripheral. This tool is integrated within CCS. The C2000 DCSM Security Tool helps by flagging any incorrect configuration.

8 **References**

- **TMS320F2837xD Dual-core Delfino™ Microcontrollers Data Sheet**
- **TMS320F2837xD Dual-Core Delfino™ Microcontrollers Technical Reference Manual**

Additional support is provided by the **TI E2E™ Community**.
IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2020, Texas Instruments Incorporated