AN4511

Getting Started with the PIC32CM LE00/LS00/LS60 Curiosity Pro Board

Abstract

This document aims at getting started with the Microchip® PIC32CM LE00/LS00/LS60 Arm® Cortex®-M23 based microcontrollers using their respective Curiosity Pro evaluation kits.

The PIC32CM LE00/LS00/LS60 Curiosity Pro evaluation kits are hardware platforms used to evaluate the PIC32CM5164LE00100, PIC32CM5164LS00100, and PIC32CM5164LS60100 microcontrollers.

Each kit is supported by the MPLAB® X Integrated Development Environment (MPLAB X IDE) and provides an easy access to the microcontroller's features.

© 2022 Microchip Technology Inc.
and its subsidiaries

Table of Contents

Abstract 1

1. Obtaining the PIC32CM LE00/LS00/LS60 Curiosity Pro Evaluation Kit 3

2. Tools and Software 4
   - 2.1. MPLAB X Integrated Development Environment 4
   - 2.2. MPLAB Code Configurator 5
   - 2.3. MPLAB Harmony v3 7
   - 2.4. MPLAB Discover 9

3. Getting Started with the PIC32CM LE00 Using the MPLAB X IDE and MCC 10
   - 3.1. Compiling and Programming a First Application 10
   - 3.2. Proceeding with MCC 11

4. Getting Started with the PIC32CM LS00/LS60 TrustZone Projects Using MPLAB X IDE and MCC 14
   - 4.1. PIC32CM LS00/LS60 Security Concept Overview 14
   - 4.2. Compiling and Programing a First Application 15
   - 4.3. Proceeding with MCC 18

5. Getting Started with the PIC32CM LS60 Using Trust Platform Design Suite (TPDS) v2 21
   - 5.1. Trust Platform Design Suite v2 21
   - 5.2. Running the PIC32CM LS60 Secure Boot Use Case from TPDS v2 23
   - 5.3. Adding Secure and Non-Secure Applications 28

6. Troubleshooting 31

7. References 32

8. Revision History 33

The Microchip Website 34

Product Change Notification Service 34

Customer Support 34

Microchip Devices Code Protection Feature 34

Legal Notice 34

Trademarks 35

Quality Management System 36

Worldwide Sales and Service 37

© 2022 Microchip Technology Inc.
and its subsidiaries

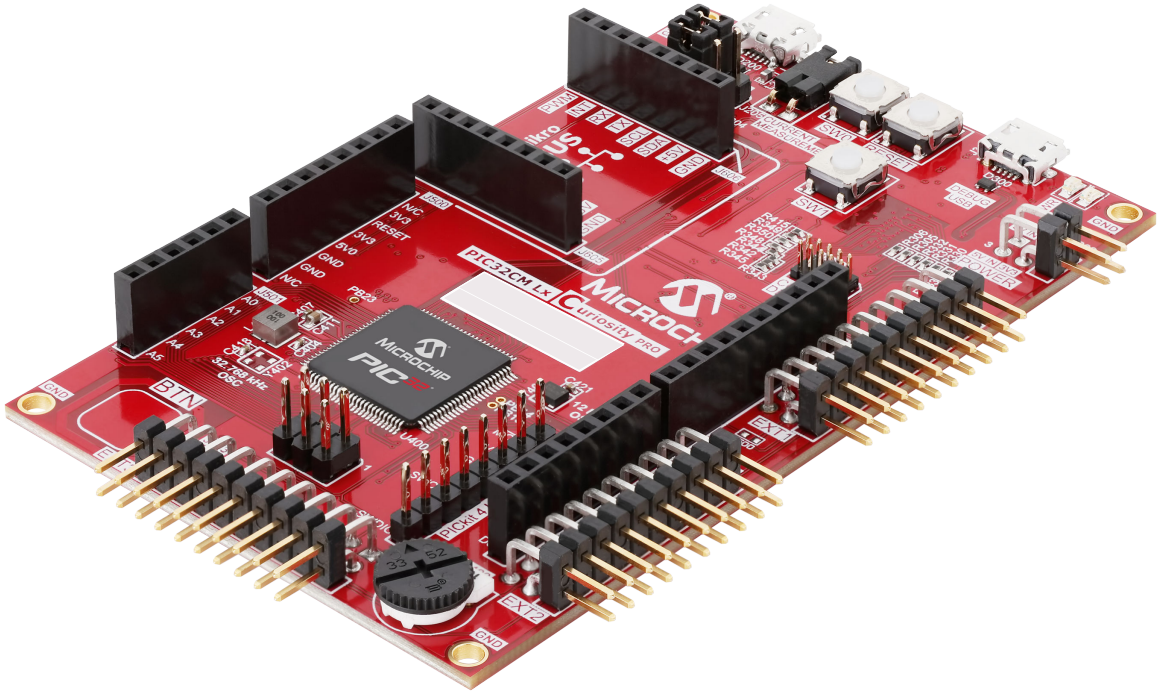
1. Obtaining the PIC32CM LE00/LS00/LS60 Curiosity Pro Evaluation Kit

The PIC32CM LE00, PIC32CM LS00, and PIC32CM LS60 Curiosity Pro evaluation kits are hardware platforms for evaluating the PIC32CM LE00/LS00/LS60 microcontrollers (MCUs). Each evaluation kit is supported by the MPLAB X IDE and MPLAB Harmony v3, featuring application examples.

The Curiosity Pro evaluation kits include an on-board embedded debugger to program or debug the target microcontroller. This enables an easy start to a project, and provides application examples that can be used in the design of a custom application.

The Curiosity Pro evaluation kits provide easy access to the features of the microcontroller, and are integrated with Arduino Uno, mikroBUS™, and extension headers to interface with Xplained Pro extension boards for a rapid prototyping and expanded functionality.

Figure 1-1. PIC32CM LE00/LS00/LS60 Curiosity Pro Board



The PIC32CM LE00/LS00/LS60 boards can be purchased at Microchip Direct.

For additional information on the PIC32CM LE00/LS00/LS60 boards and devices, refer these documents:

- PIC32CM LE00/LS00/LS60 Family Data Sheet (DS60001615)
- PIC32CM LE00/LS00/LS60 Family Silicon Errata and Data Sheet Clarifications (DS80000906)
- PIC32CM LE00/LS00/LS60 Curiosity Pro User Guide (DS70005443)
- PIC32CM LE00/LS00/LS60 Curiosity Pro Board Change Notification (DS70005491)

© 2022 Microchip Technology Inc.
and its subsidiaries

2. Tools and Software

2.1 MPLAB X Integrated Development Environment

The MPLAB X Integrated Development Environment (IDE) is an expandable, highly configurable software program that incorporates powerful tools to discover, configure, develop, debug, and qualify embedded designs for most of the Microchip's microcontrollers and digital signals controllers. MPLAB X IDE works seamlessly with the MPLAB development ecosystem of software and tools.

Figure 2-1. MPLAB X IDE Icon

Users can download MPLAB X IDE from the Microchip's website: www.microchip.com/mplab/mplab-x-ide.

Installing PIC32CM LE00 and PIC32CM LS00/LS60 Device Family Packs (DFP)

Follow these steps to install the PIC32CM LE00 and PIC32CM LS00/LS60 DFP:

1. Open MPLAB X IDE.
2. Go to *Tools* > *Packs*.
3. Install the PIC32CM LE00 and the PIC32CM LS00/LS60 DFP:
   a. To install the PIC32CM LE00 DFP, enter PIC32CM-LE in the DFP Search box to the right, and then install the latest DFP available.
   b. To install the PIC32CM LS00/LS60 DFP, enter PIC32CM-LS in the DFP Search box to the right, and then install the latest DFP available.

© 2022 Microchip Technology Inc.
and its subsidiaries

2.2 MPLAB Code Configurator

The MPLAB Code Configurator (MCC) is a free graphical programming environment that generates seamless, easy-to-understand C code to insert into projects. Using an intuitive interface, MCC enables and configures a rich set of peripherals and functions. MCC supports 8-bit, 16-bit, 32-bit PIC®, and SAM® microcontrollers. MCC is incorporated into MPLAB X IDE as a plugin.

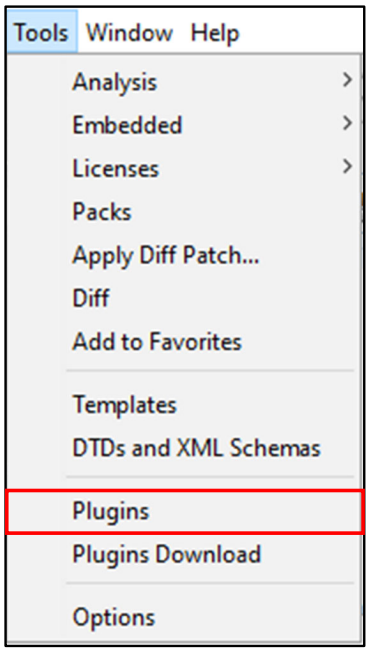
Figure 2-2. MPLAB Code Configurator Icon

Installing MCC from MPLAB X IDE

Follow these steps to install MCC from MPLAB X IDE:

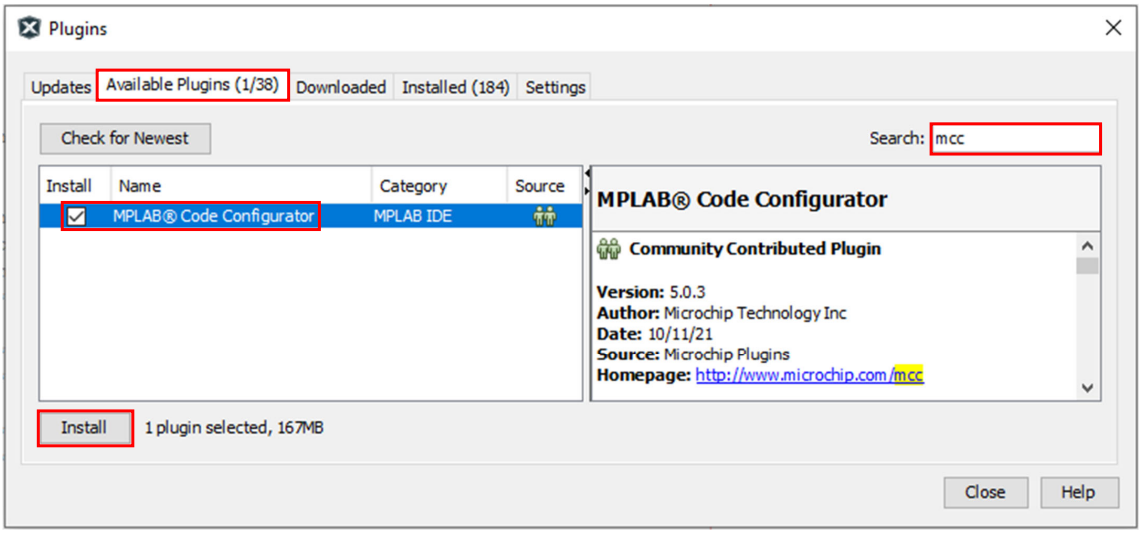
1. From the Toolbar, select *Tools* > *Plugins*.

   Figure 2-3. MPLAB X IDE Plugins Tool



2. In the Plugins window, click the **Available Plugins** tab and type MCC in the search box. The MCC plugin details will be displayed (if not yet installed) as shown in the figure 2-4.
3. Select the checkbox next to the MCC plugin, and then click **Install**.

Figure 2-4. MPLAB Code Configurator Installation from MPLAB X IDE Plugins



4. In the Plugin Installer window, follow the instructions, and then select **Restart Now**, and then click **Finish** when installation is completed.
5. MPLAB X IDE will restart with the MCC plugin installed.

2.3 MPLAB Harmony v3

MPLAB Harmony v3 is a fully integrated embedded software development framework that provides flexible and interoperable software modules to simplify the development of value-added features, and reduce the customer's time to market.

Figure 2-5. MPLAB Harmony v3 Icon

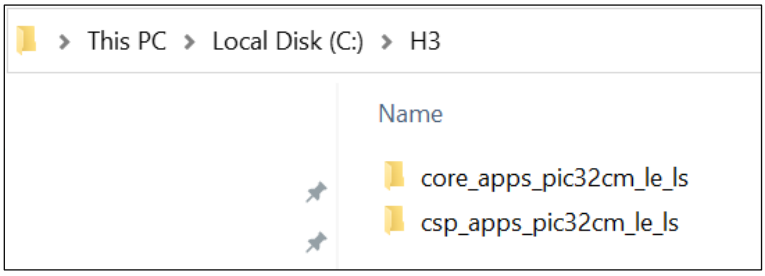
Go to the Microchip GitHub page https://github.com/Microchip-MPLAB-Harmony to download the following PIC32CM LE00/LS00/LS60 application packages:

- **csp_apps_pic32cm_le_ls:** Contains driver, FS, system service, and RTOS application examples for the PIC32CM LE00/LS00/LS60 family.
- **core_apps_pic32cm_le_ls:** Contains Peripheral Library (PLIB) application examples for the PIC32CM LE00/LS00/LS60 family.

Note: Users can download specific examples from the Microchip website: https://mplab-discover.microchip.com/.

Create a folder and name it as `C:\H3`, which is used as the MPLAB Harmony v3 framework folder. Unzip application packages files in this folder as shown in the following figure:

Figure 2-6. Application Packages Unzipped in Harmony v3 Framework

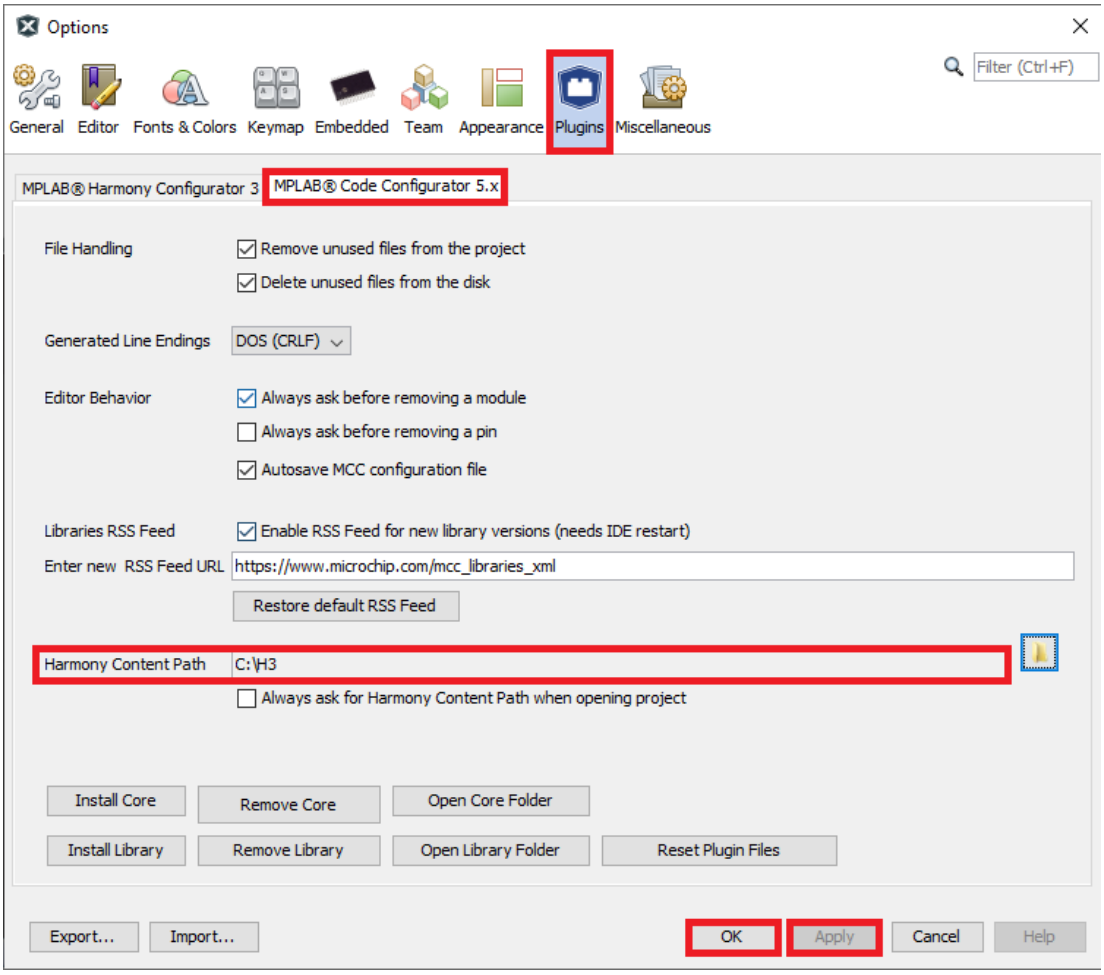


Note: The MCC's Content Manager can then be used to update the MPLAB Harmony v3 framework folder or download new packages.

Follow these steps to define the MPLAB Harmony v3 framework folder in MPLAB X IDE:

1. From the Toolbar, select *Options* > *Plugins*.
2. Choose MPLAB Code Configurator 5.x tab.
3. For the Harmony Content Path, choose the created `H3` folder as shown in the following figure.

Figure 2-7. MCC Harmony Content Path Update



Note: This step is optional for running an application only, but it must be completed to run the MCC plugin.

Users can define another path and name for the Harmony v3 Framework folder, but must ensure to define them as small as possible for tool restrictions.

Note: The `C:\H3` folder will be referenced in this document, from this point forward.

2.4 MPLAB Discover

MPLAB Discover is a catalog of fully configured and complete source codes, projects, examples and software applications for PIC® and AVR® microcontrollers to help jump-start next customer project. It features intuitive and powerful search capabilities to search for content quickly and easily.

Figure 2-8. MPLAB Discover Icon

For additional information about MPLAB Discover, go to Microchip website: mplab-discover.microchip.com/.

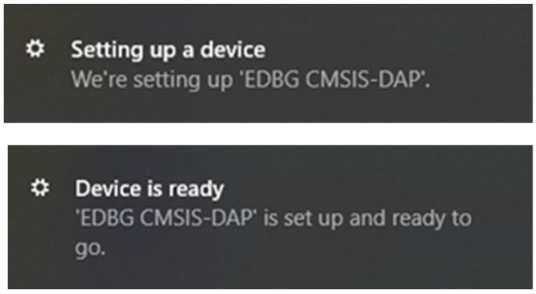
3. Getting Started with the PIC32CM LE00 Using the MPLAB X IDE and MCC

3.1 Compiling and Programming a First Application

Follow these steps to using the PIC32CM LE00 Curiosity Pro evaluation kit based on the MPLAB X IDE environment:

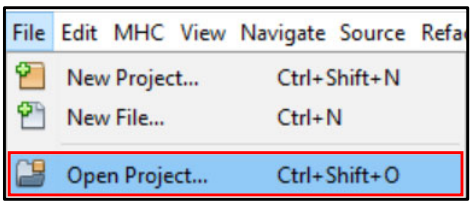
1. Launch MPLAB X IDE.
2. Connect the PIC32CM LE00 Curiosity Pro evaluation kit through the DEBUG USB connector to the PC using a micro-USB cable (Standard-A to Micro-AB). When the Curiosity Pro evaluation kit is connected to the computer for the first time, the operating system will install the software driver.
   Note: The driver file supports 32-bit and 64-bit versions of Microsoft® Windows® XP™, Windows Vista™, Windows 7, Windows 8, Windows 10, and Windows 11.

   Figure 3-1. Windows Messages



3. When the Curiosity Pro board is powered, the green power LED (PWR) will glow and the MPLAB X IDE will auto-detect the connected Curiosity Pro Kit.
   Note: The PIC32CM5164LE00100 device is programmed and debugged by the on-board embedded debugger (EDBG), hence external programmer or debugger tool is not required.
4. From the Toolbar, select *File* > *Open Project*, or click (the project icon).

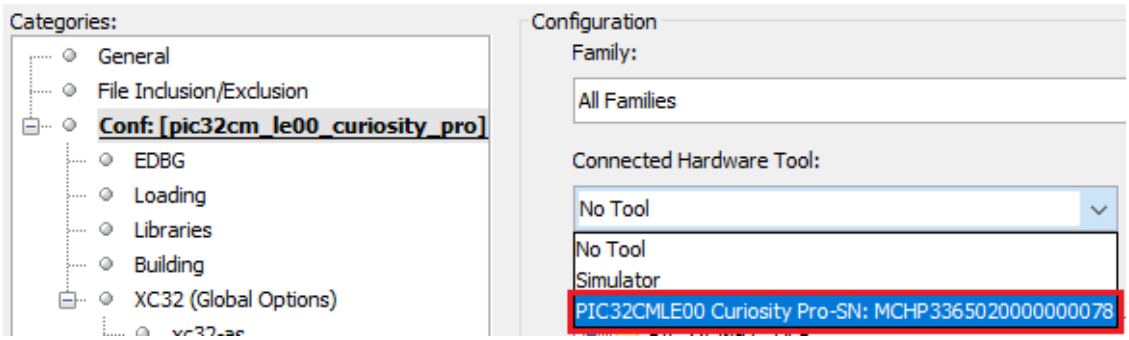
   Figure 3-2. MPLAB X IDE - Open Project



5. As an example, navigate to *C:\H3\csp_apps_pic32cm_le_ls\apps\port\port_led_on_off_polling\firmware*, and then open the `pic32cm_le00_curiosity_pro.X` project file.
   Note: The system may prompt a message to upgrade the product DFP. Upgrade if it is requested.
6. Select the *Connected Hardware Tool* by performing these actions:
   a. To set the project as the main project: Right-click on the project name, then choose **Set as Main Project**.
   b. To open the project properties: Right-click on the project name and select **Properties**.
   c. In the Project Properties, select the connected PIC32CM LE00 Curiosity Pro board from the Connected Hardware Tool drop-down list.

© 2022 Microchip Technology Inc.
and its subsidiaries

Figure 3-3. Project Properties - Connect Hardware Tool



d. Ensure to have the most recent CMSIS, DFP and XC32 version available and selected in the Project Properties window.

e. Click **Apply**, and then click **OK**.

7. Compiling and running the application:

a. To build and program the project, select *Production* > *Make and Program Device Main Project*, or click (the build icon).

b. To debug the project, select *Debug* > *Debug Main Project*, or click (the debug icon).

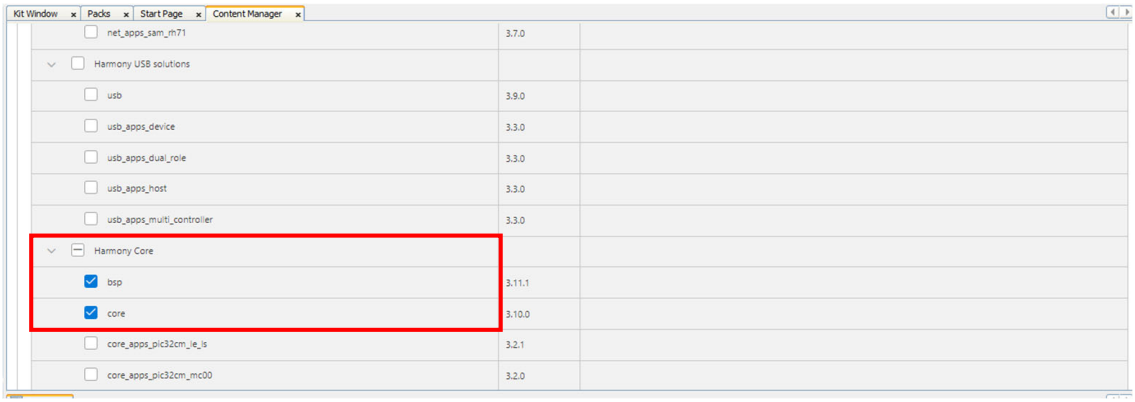
c. The application is now programmed. Press the switch button SW0 to light ON the on-board LED0.

3.2 Proceeding with MCC

Follow these steps to proceed with MCC and update the MCC core:

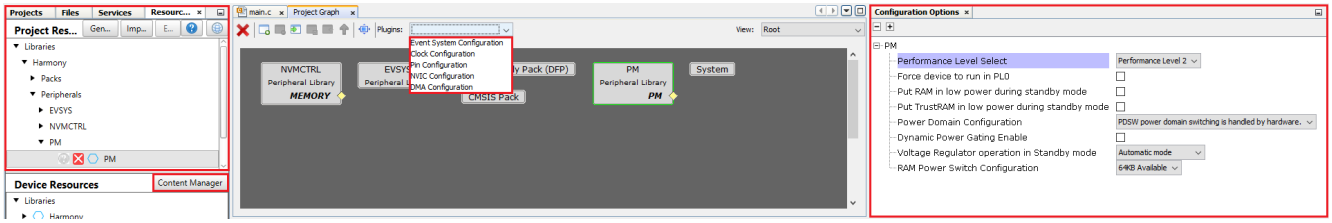
1. Go to *Tools* > *Embedded* > *MPLAB Code Configurator*, or click (the MCC icon) to open the MCC plugin. A message may prompt to update the project to latest MCC version, click **OK**.
2. Click on **Select MPLAB Harmony** in the MCC Content Manager wizard.
3. Scroll down to **MPLAB Harmony Core** and select the **bsp** and **core** optional packages as shown in the following figure:

Figure 3-4. BSP and Core Optional Packages Selection



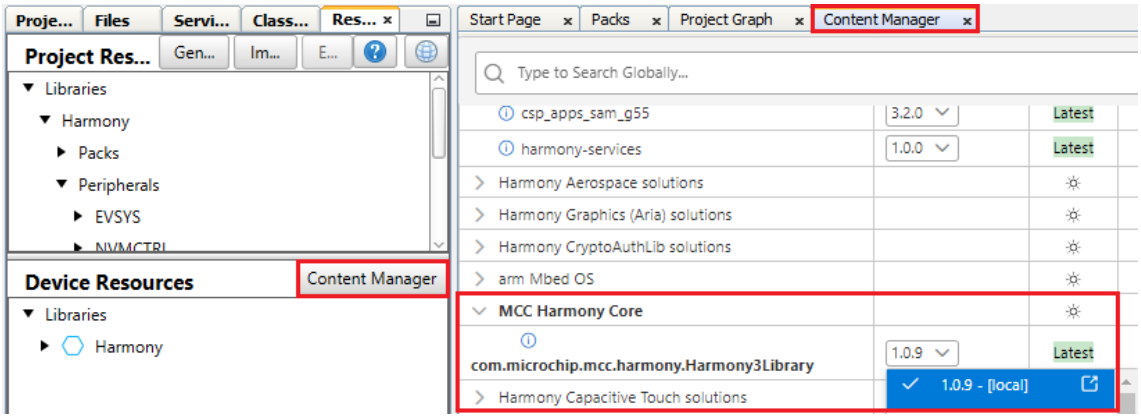
4. Scroll up and then select **Finish** to open the MCC graphical user interface (GUI). The project will take some time to open in MCC as the tool will download any missing or selected packages.
5. The following messages might be displayed:
   a. To warn that the project packages differ from the local packages. Click **Continue**.
   b. To update DFP version. Accept by entering **Yes**.
   c. To update the project's Common Microcontroller Software Interface Standard (CMSIS). Confirm by selecting **Yes.**
6. The MCC GUI will be displayed:

Figure 3-5. MCC GUI Overview for PIC32CM LE00 Curiosity Pro Board



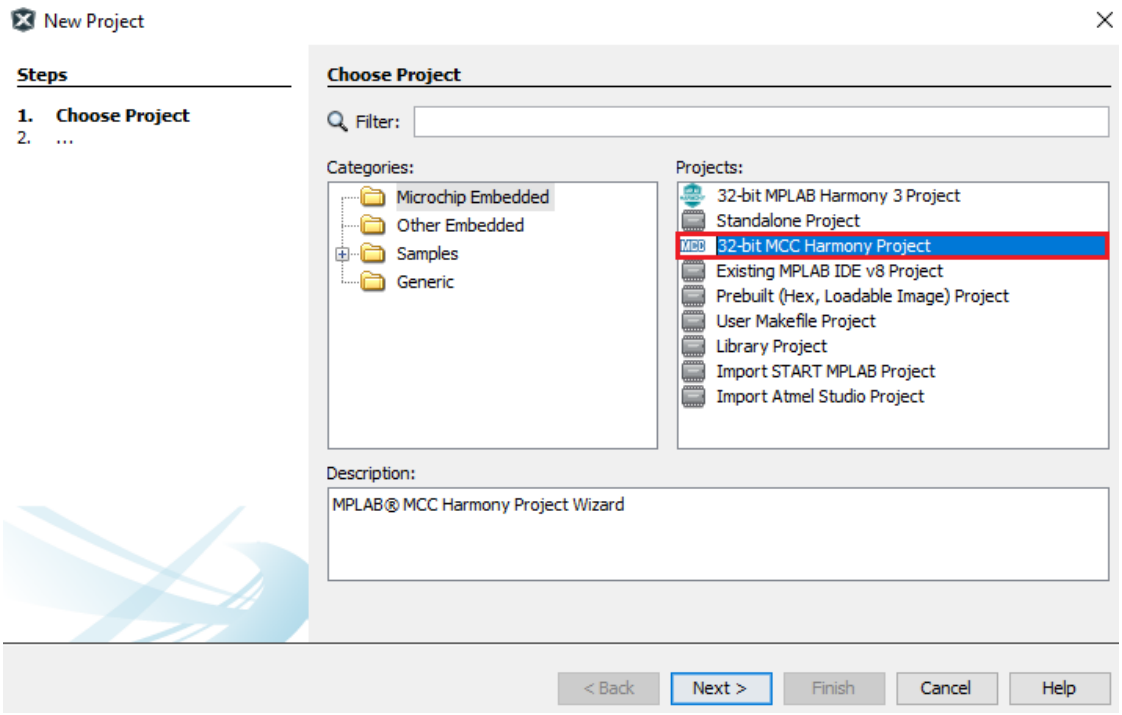
7. Click the **Content Manager** tab.
8. In the Content Manager window, scroll down to **MCC Harmony Core** and choose the latest available version (1.0.9 is shown as an example).

Figure 3-6. MCC MPLAB Harmony v3 Code Update



The MCC Core is now up to date. Users can benefit from the latest MCC features for an existing application or for creating a new project. To create a new MCC project, go to *Files > New Project > 32-bit MCC Harmony Project* as shown in the following figure:

Figure 3-7. MCC Project Creation under MPLAB X IDE



4. Getting Started with the PIC32CM LS00/LS60 TrustZone Projects Using MPLAB X IDE and MCC

4.1 PIC32CM LS00/LS60 Security Concept Overview

Using the PIC32CM LS00/LS60 requires familiarity with different security features and concepts that involve TrustZone® for ARMv8-M devices.

The TrustZone technology is a System-on-Chip (SoC) and MCU system-wide approach to security that enables Secure and Non-Secure code to run on an MCU. It enables creating multiple software security domains that restrict access to selected memory, peripherals, and I/O to trusted software without compromising the system performances. The user can consider the following deployment approaches:

- Single-developer approach (Customer A)
- Dual-developer approach (Customer A + Customer B)

The single-developer approach involves a unique developer (Customer A), which oversees the following:

- Developing, deploying, and protecting the Secure code
- Developing and deploying the Non-Secure code

In the dual-developer approach, the first developer (Customer A), oversees developing the secure application and its associated non-secure callable library. The secure application must be loaded in the PIC32CM LS00/LS60 NVM secure memory and other secure areas.

A different developer (Customer B) will then start the Non-Secure application development on a preprogrammed PIC32CM LS00/LS60 with limited access to secure resources (through calls to Non-Secure API only).

Figure 4-1. Single-Developer Approach

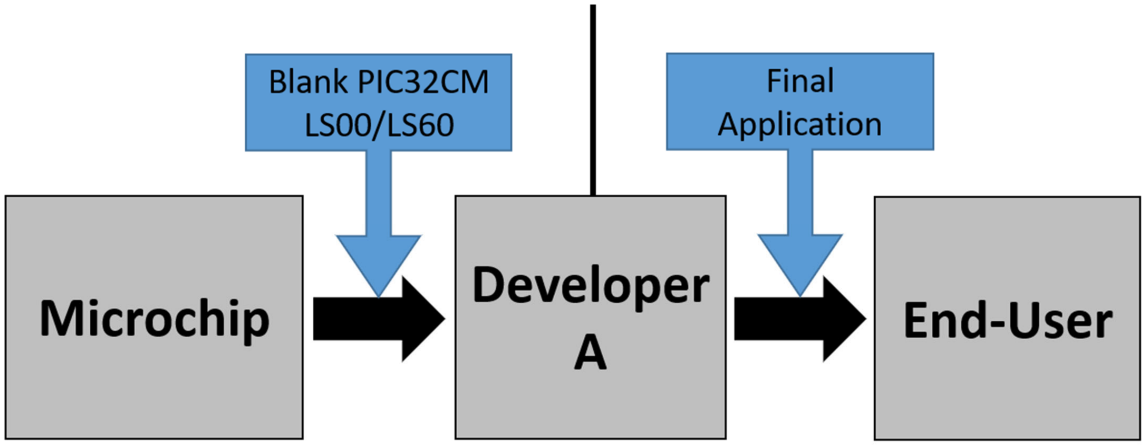
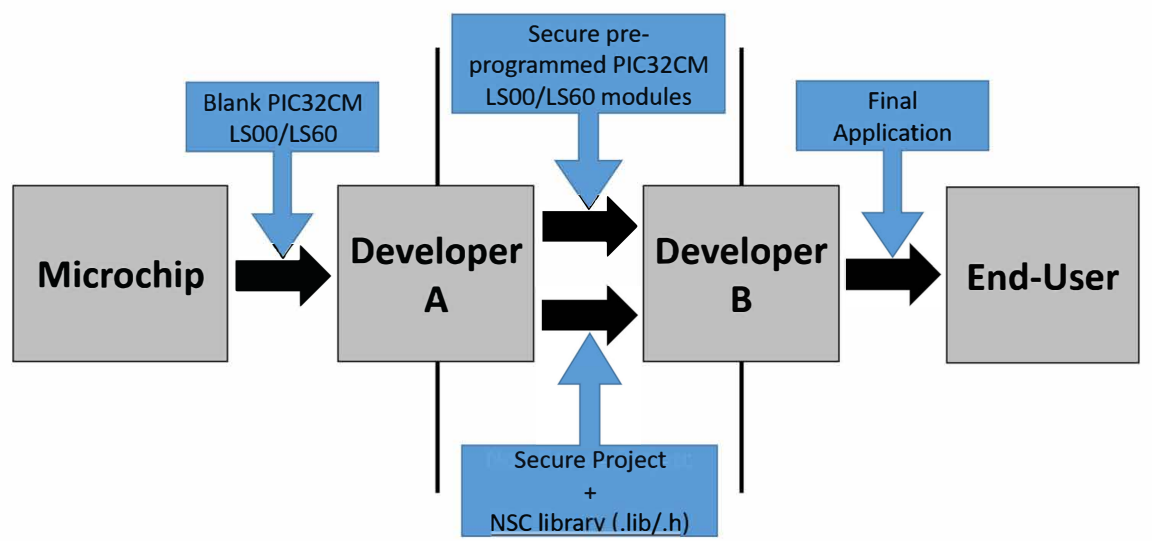


Figure 4-2. Dual-Developer Approach



This document describes how to debug an MPLAB project composed of two sub-projects (Secure and Non-Secure).

Note: Refer to the *PIC32CM LS00/LS60 Security Reference Guide (DS00003992)*, which describes the security features available in the Microchip PIC32CM LS00/LS60 microcontroller, which fulfill the security requirements of most embedded systems.

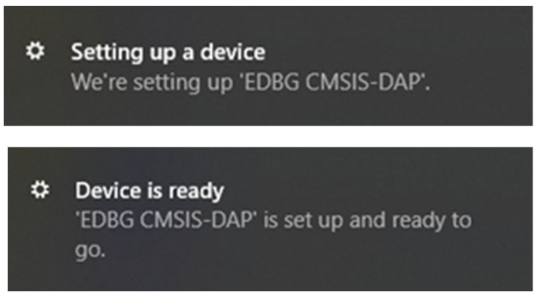
4.2 Compiling and Programing a First Application

Follow these steps to use the PIC32CM LS00/LS60 Curiosity Pro evaluation kit based on MPLAB X Environment in order to run and debug a TrustZone based project.

Note: The following steps are demonstrated based on the PIC32CM LS00 Curiosity Pro board, but are fully reproducible with a PIC32CM LS60 Curiosity Pro board.

1. Launch MPLAB X IDE.
2. Connect the evaluation kit through the DEBUG USB connector to the PC using a micro-USB cable (Standard-A to Micro-AB). When the Curiosity Pro evaluation kit is connected to the computer for the first time, the operating system will install the software drive.
   Note: The software driver file supports both 32-bit and 64-bit versions of Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, and Windows 11.

   Figure 4-3. Windows Messages

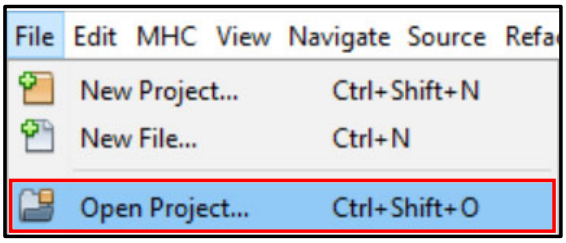


   When the Curiosity Pro board is powered, the green power LED (PWR) will glow and the MPLAB X IDE will auto-detect the connected Curiosity Pro MCU.

   Note: The PIC32CM5164LS00100 and PIC32CM5164LS60100 devices are programmed and debugged by the on-board embedded debugger (EDBG), therefore no external programmer or debugger tool is required.

3. From the Toolbar, select *File* > *Open Project*, or click (the project icon).

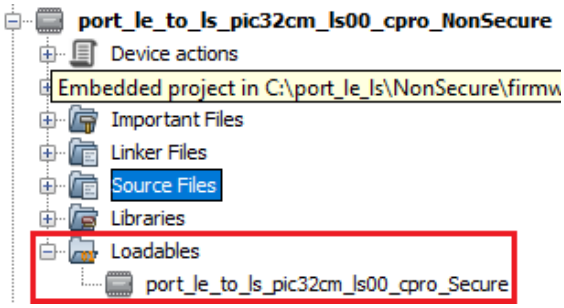
Figure 4-4. MPLAB X IDE - Open Project



4. For example, navigate to *C:\H3\csp_apps_pic32cm_le_ls\apps\trustZone\tc* and open the `secure_tc_ls00` projects group, which contains the `secure_tc_ls00_NonSecure` and `secure_tc_ls00_Secure` projects.
5. Open Secure and Non-Secure projects by double-clicking on each of the project.
   Note: A prompt message may appear to upgrade the DFP. Upgrade it if is requested.
6. Select **Connected Hardware Tool**:
   a. To set the Non-Secure project as the main project: Right-Click on the Non-Secure project name and select **Set as Main Project**

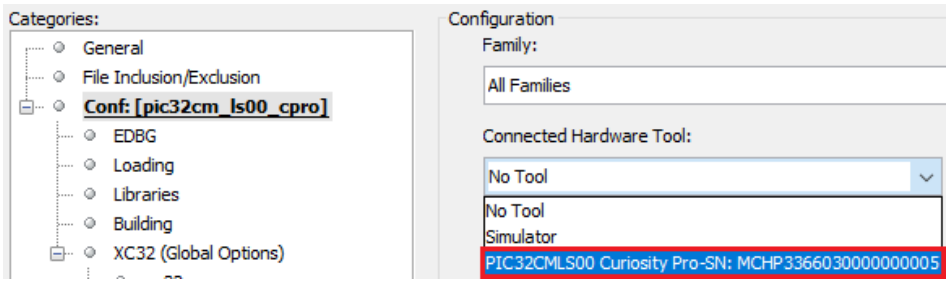
Important: When the Non-Secure project is set as the main project in a TrustZone project group, the Secure project is built before the Non-Secure project. This is possible using the project's **Loadables** feature which will load all projects defined in this section before the main project as shown in the figure below. If the Secure project is set as the main project, then only this project and its related memory regions will be built and programmed.

Figure 4-5. Secure Project Under Non-Secure Loadable Project Section



   b. To open the non-secure project properties: Right-Click on the Non-Secure project name and select **Properties**.
   c. Select the connected *PIC32CM LS00 Curiosity Pro board* from the Connected Hardware Tool drop-down menu.

Figure 4-6. Project Properties - Connected Hardware Tool



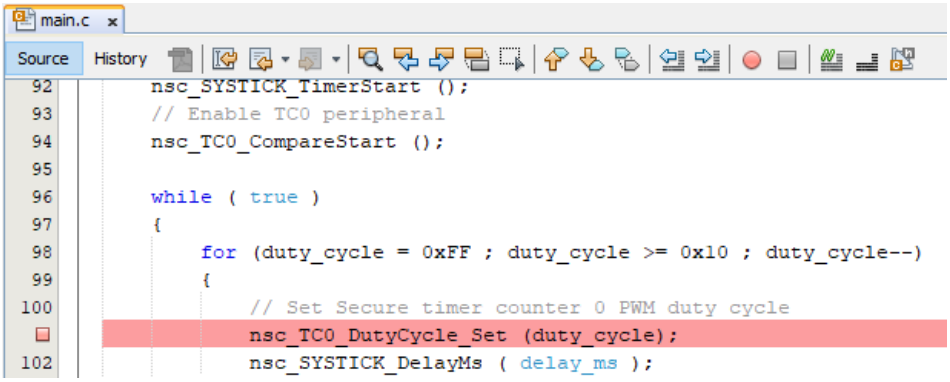
d. Ensure to have the latest CMSIS, DFP and XC32 versions available and selected in the Project Properties window.

e. Click **Apply**, and then click **OK**.

7. To set breakpoints to debug the complete `secure_tc` solution, follow these steps:

a. Add a breakpoint on the `nsc_TC0_DutyCycle_Set (duty_cycle)` line in the Non-Secure project `main.c` file. Click on the number to the left of the line to set the breakpoint.

Figure 4-7. Setting Breakpoint in Non-Secure `main.c` File

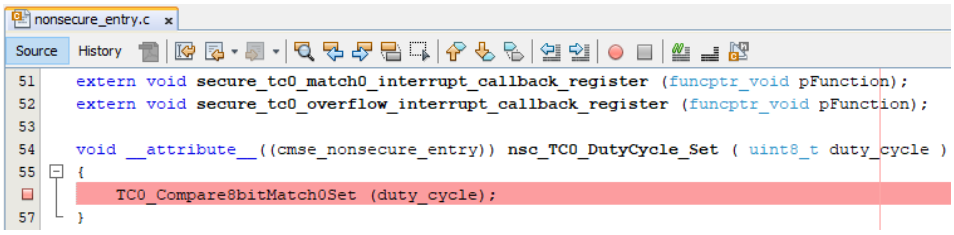


Note: In this case, the breakpoint is placed at the line `nsc_TC0_DutyCycle_Set` that calls the Non-Secure callable function named `TC0_Compare8bitMatch0Set`. This function is declared in the `pic32cm_ls00_cpro_Secure_sg_veneer.lib` file, which is generated once the Secure project is built.

The call to the Secure function `TC0_Compare8bitMatch0Set` is done in the veneer (Secure gateway).

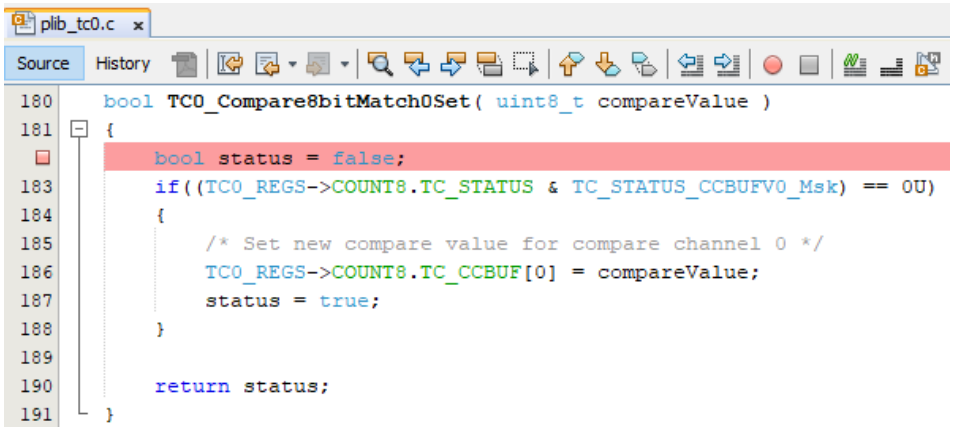
b. Add a breakpoint on the `TC0_Compare8bitMatch0Set` function call in the Secure project `nonsecure_entry.c` file, which is located at *secure_tc_ls00_NonSecure > Source Files > trustZone in MPLAB X IDE.*

Figure 4-8. Setting Breakpoint in Secure `nonsecure_entry.c` File



c. Add a breakpoint on the `bool status = false` line in the Secure project `plib_tc0.c` file located at *secure_tc_ls00_Secure > Source Files > config > pic32cm_ls00_cpro > peripheral > tc* in MPLAB X IDE project tree.

Figure 4-9. Setting Breakpoint in Secure `plib_tc0.c` File



⚠ CAUTION When debugging the secure application veneers, only hardware breakpoints must be used to stop code execution on a Secure Gateway (SG) instruction. Using software breakpoints implies the addition of a breakpoint (BKP) instruction before an SG instruction, which triggers a Secure fault during the code execution. This behavior is normal, as the first instruction to be executed when accessing the Non-Secure Callable (NSC) region must be an SG instruction.

8. To compile and run the application, follow these steps:
   a. To build and program the projects: Select *Production* > *Make and Program Device Main Project*, or click (the build icon).
   b. To debug the project, select *Debug* > *Debug Main Project*, or click (the debug icon).
   c. The application is programmed and the debugger breaks in the Non-Secure project at `nsc_TC0_DutyCycle_Set`.
9. Continue the debugging session by clicking the button.
10. As a result, the debugger will stop successively on:
    a. The `nsc_TC0_DutyCycle_Set (duty_cycle)` function call (Non-Secure project).
    b. The `TC0_Compare8bitMatch0Set` function call (Secure project).
    c. The `bool status = false` line (Secure project).

4.3 Proceeding with MCC

Follow these steps to proceed with MCC and update the MCC core.

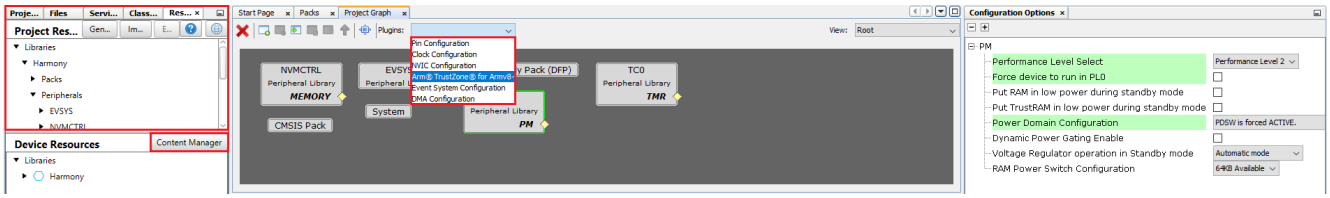
1. Go to *Tools* > *Embedded* > *MPLAB® Code Configurator*, or click (the MCC icon) to open the MCC plugin.
2. A prompt message may appear to update the project to the latest MCC version, click **OK**.
3. Click **Select MPLAB Harmony** in the MCC Content Manager wizard.

4. Scroll down to MPLAB Harmony v3 Core and select the **bsp** and **core** optional packages as shown in the following figure.

Figure 4-10. BSP and Core Optional Packages Selection

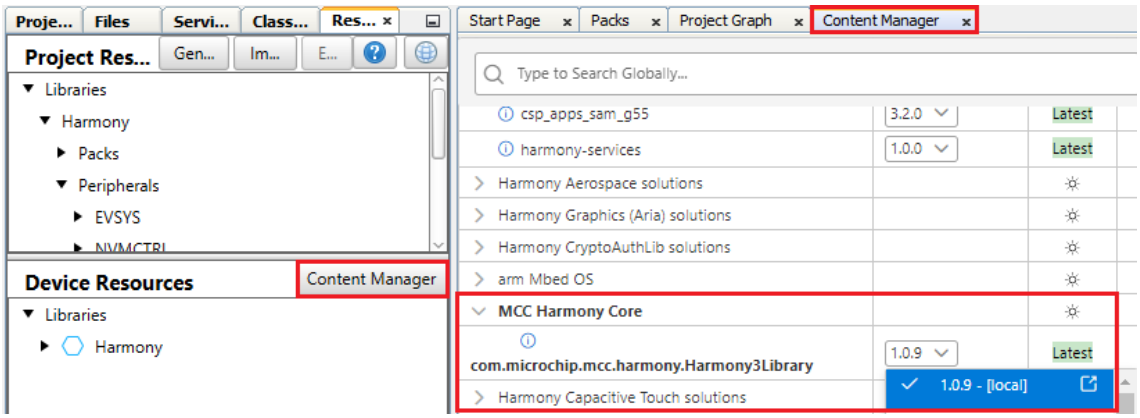
5. Scroll up and then select **Finish** to open the MCC graphical user interface (GUI). The project will take some time to open in MCC as the tool will download any missing or selected packages.
6. The following messages may appear:
   a. To warn if the project's packages differ from the local packages, click **Continue**.
   b. To update the DFP version, click **Yes**.
   c. To update the project's Common Microcontroller Software Interface Standard (CMSIS), confirm by selecting **Yes.**
7. The MCC GUI will be displayed, select **Content Manager**.

Figure 4-11. MCC GUI Overview for PIC32CM LS00/LS60 Curiosity Pro Board



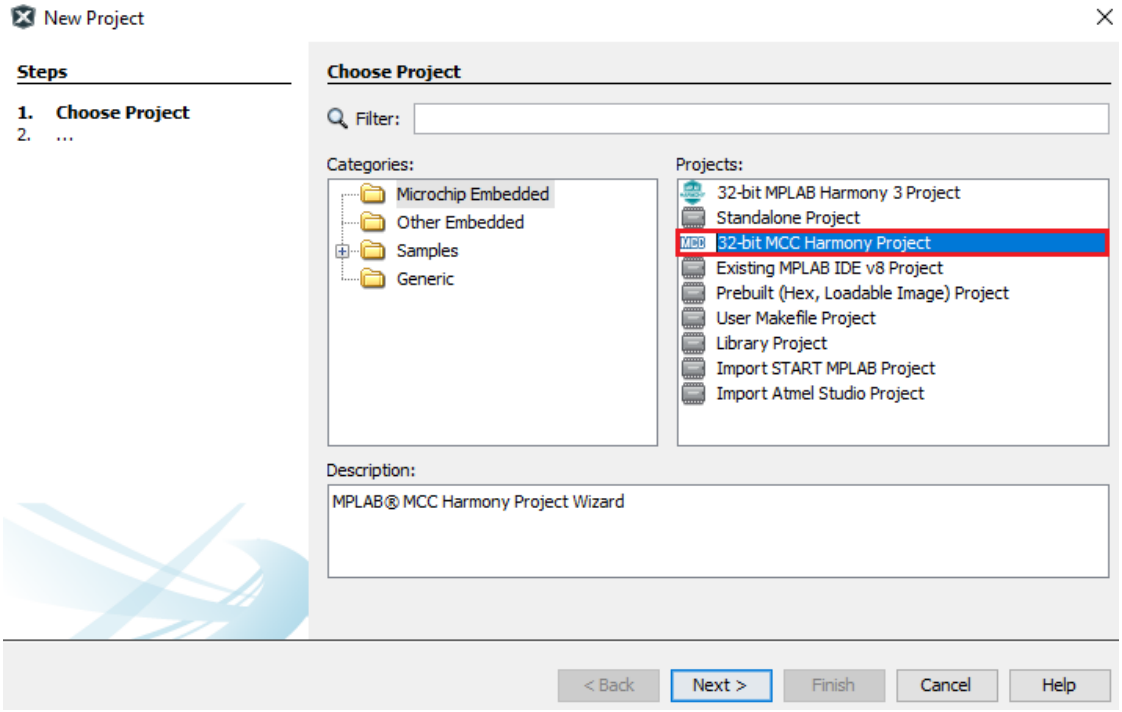
8. Scroll down to **MCC Harmony Core**, and update it to the latest version (1.0.9 is used as an example).

Figure 4-12. MCC MPLAB Harmony v3 Code Update



The MCC Core is now up to date. It is now possible to benefit from the most recent MCC features for an application or creating a project. To create a new MCC project, go to *Files > New Project > 32-bit MCC Harmony Project* as shown in the following figure:

Figure 4-13. MCC Project Creation under MPLAB X IDE



5. Getting Started with the PIC32CM LS60 Using Trust Platform Design Suite (TPDS) v2

5.1 Trust Platform Design Suite v2

The Trust Platform Design Suite (TPDS) v2 tool is Microchip's dedicated software platform to onboard with embedded security. In addition to offering Secure Element and security solutions, Microchip also offers a full onboarding experience to start with embedded security (including but not limited to trainings and interactive documentation) to leverage Microchip's secure and optimized provisioning flow.

Figure 5-1. Trust Platform Design Suite Tools

Users can download the TPDSv2 tool from the Microchip website, which is available under the *Embedded Software* section: https://www.microchip.com/en-us/product/SW-TPDSV2.

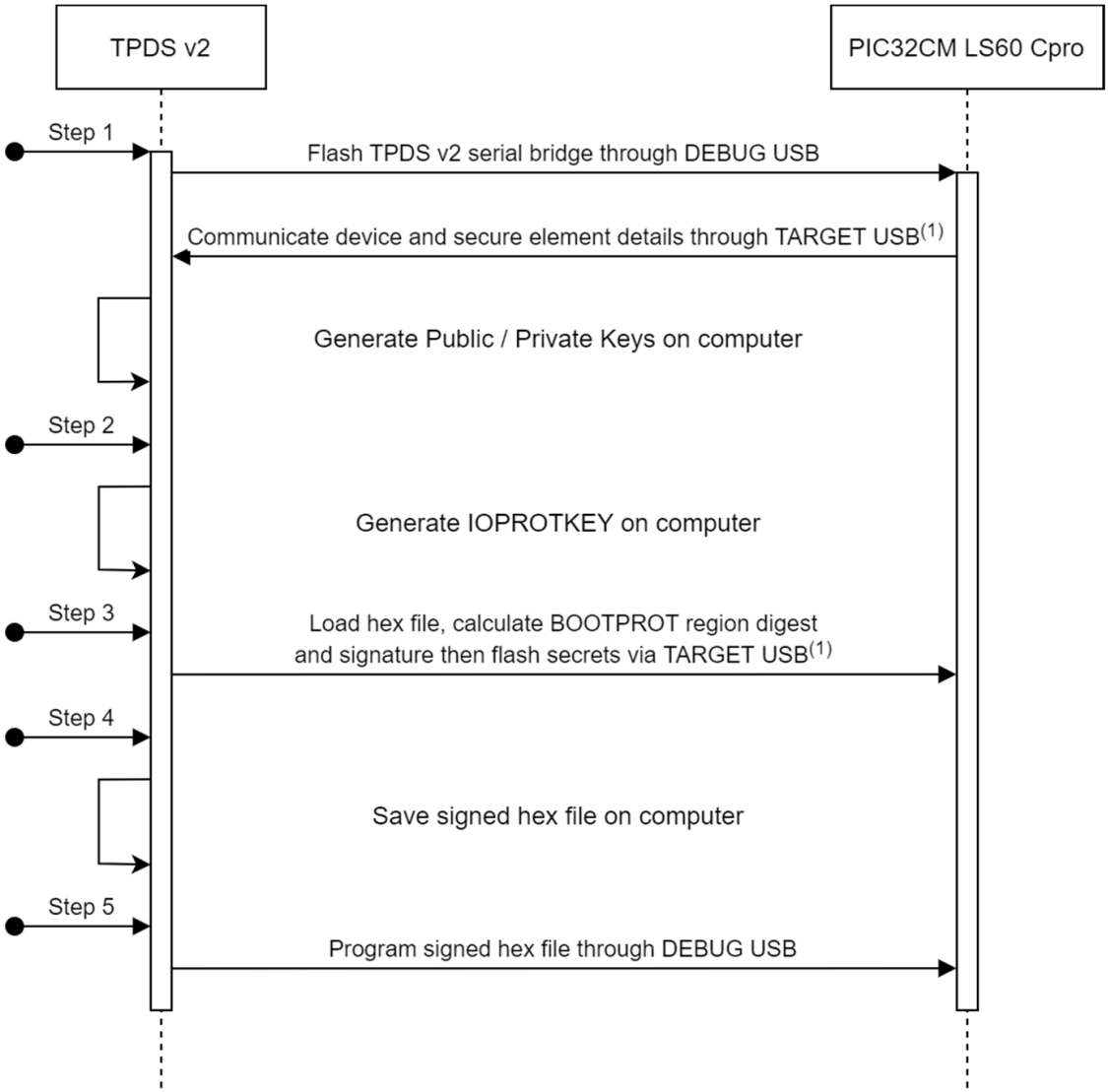
Refer to the Microchip Developer Help website to install the TPDSv2 tool: https://microchipdeveloper.com/authentication:trust-platform-v2.

5.2 Running the PIC32CM LS60 Secure Boot Use Case from TPDS v2

This section provides the detailed description of the steps to follow for running the PIC32CM LS60 Secure Boot use case in TPDS v2. The goal of this use case is to sign the boot memory region of the software to support the PIC32CM LS60 Secure Boot feature in combination with the ATECC608B embedded secure element.

The following figure illustrates the steps documented in this section:

Figure 5-2. PIC32CM LS60 Secure Boot Use Case - Sequence Diagram



Note:

1. The serial bridge programmed during step 1 is used to communicate between TPDS and the embedded ATECC608B secure element through the TARGET USB connector.

As an example, a test software (with Boot and Application memory regions defined) is provided in the TPDS v2 installation folder.

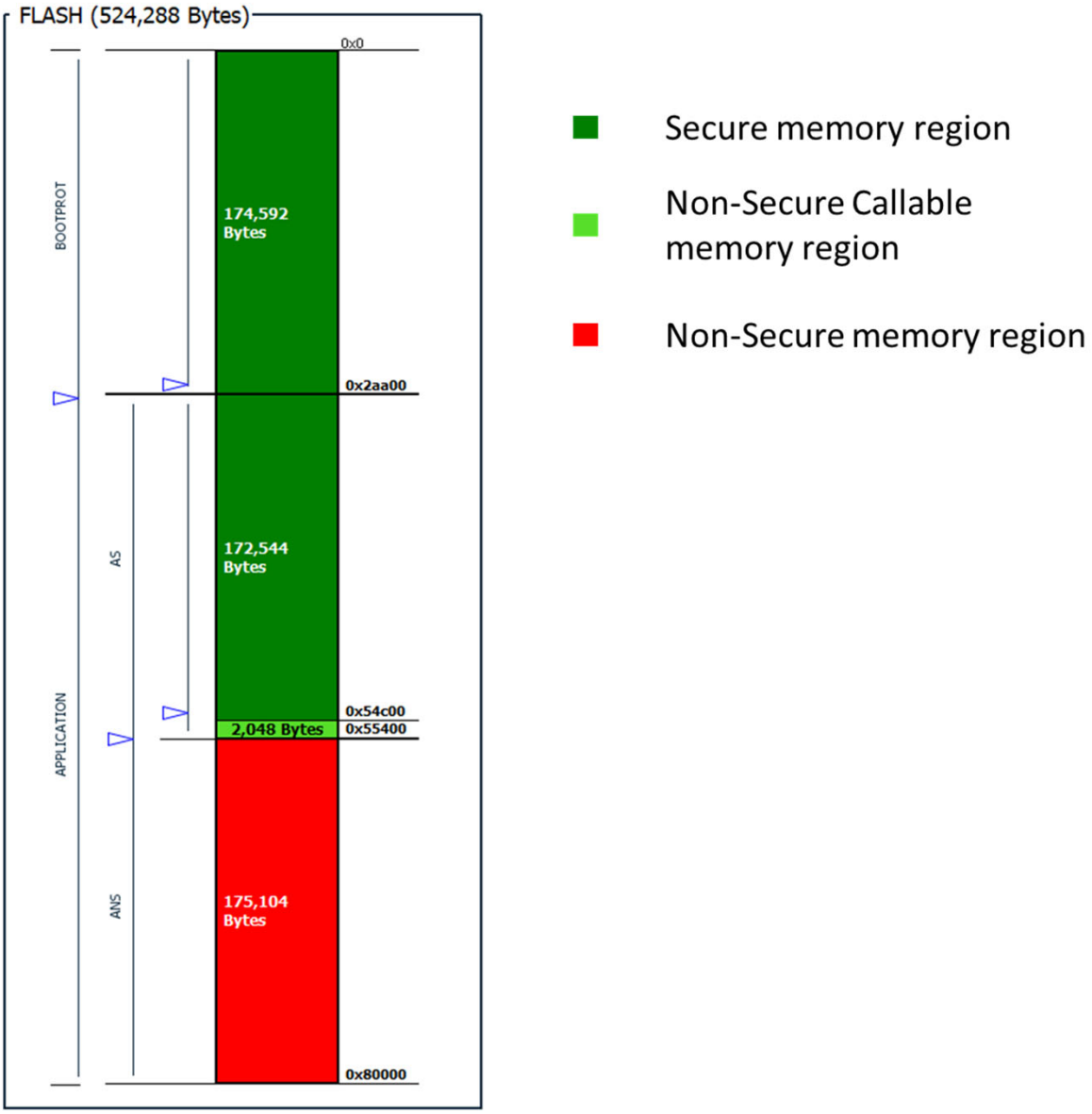
The defined boot memory region sets the device configuration and memory security attribution. This section of the software will be signed with TPDS secrets.

Refer to the **"PIC32CM LS00/LS60 Security Reference Guide"** *(DS00003992)* for additional information on Secure Boot using the ATECC608B CryptoAuthentication™ device.

The boot software will initialize the system and jump in the secure application. The application region (containing the Secure and Non-Secure regions) will light up both on-board LEDs. The green on-board LED is lit in the Secure application while the red LED is lit in the Non-Secure application.

This hex file will be used to highlight the Secure Boot use case. This example has the following memory configuration:

Figure 5-3. Test Software Flash Memory Mapping



Note:
The Secure Boot memory region length is defined by the BOOTPROT fuse, while this memory region protection and verification method is defined by the BOOTOPT fuse. For this example, BOOTPROT = 0x2AA and BOOTOPT = 0x4. Refer to the product data sheet for additional information

To run the PIC32CM LS60 Secure Boot use case in TPDS v2, follow these steps:

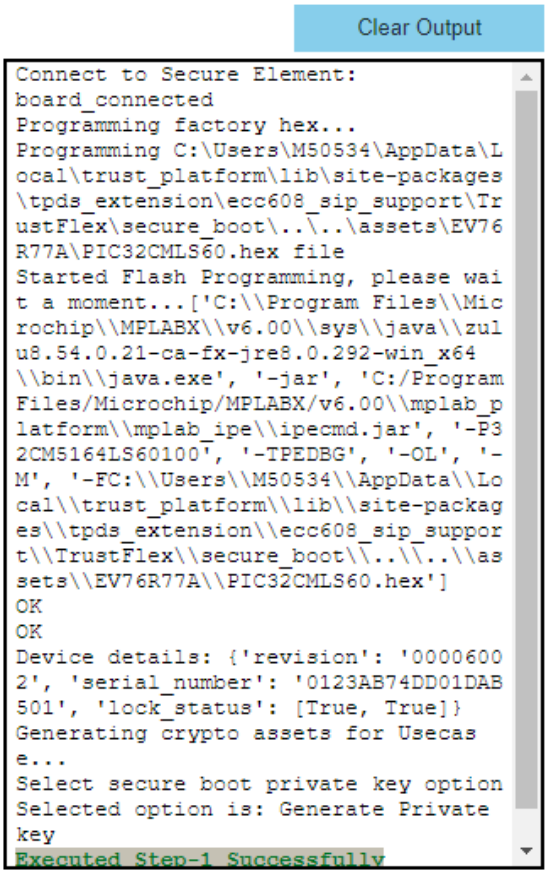
1. Open the TPDS v2 tool.
2. Select Use cases on the top menu.
3. Select the Secure Boot – PIC32CMLS60 use case: *Select Security Solution* > *Use Cases* menu.

4. Scroll down to Available solution by provisioning flow and select **Secure Boot – PIC32CMLS60 use case** under the TrustFLEX menu.
5. Connect the PIC32CM LS60 Curiosity Pro board to the computer through the Debug USB and Target USB connectors.
6. Scroll down to the use case graph and execute step 1 ‘Generate Private/Public key pair’ by clicking the icon.

   Notes:

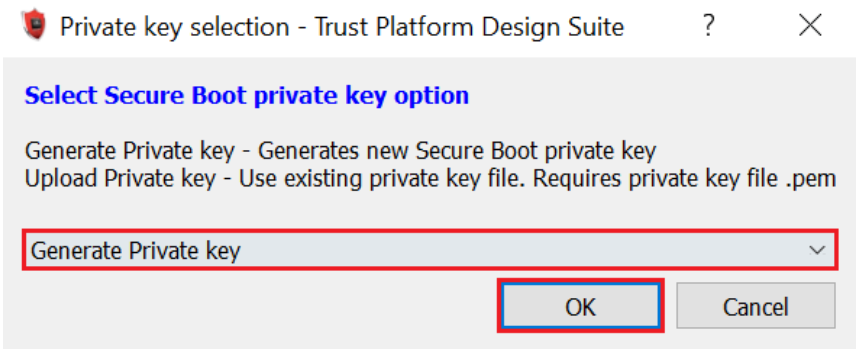
   1. If the serial bridge is not already running out of the PIC32CM LS60 Flash memory, it is programmed by the TPDS v2 tool using MPLAB X IDE, resulting in some delay before this step is completed. The progress of the programming can be tracked on the console to the right of the TPDS v2 window:

      Figure 5-4. Use Case Console Log



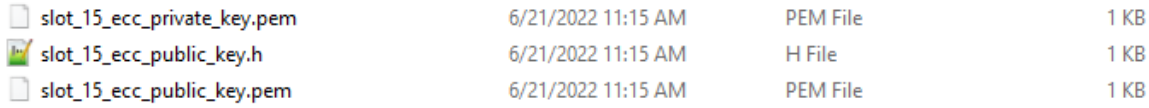
   2. When step X is completed, the “Executed Step-X Successfully” message will be displayed as shown above. Ensure that this message is displayed before executing the next step.
7. In the Private Key Selection dialog box, select ‘Generate Private key’.
8. Click **OK**:

Figure 5-5. Private Key Selection Window



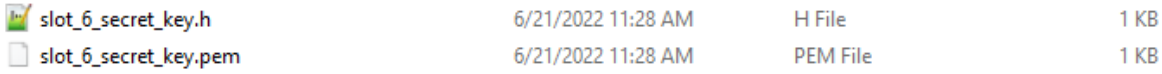
The private and public keys will be generated on the Host computer (usually at the following location: `C:\Users\XXXXX\.trustplatform\pic32cmls60_secure_boot`):

Figure 5-6. Generated Public/Private Keys



9. Execute step 2 ‘Generate IOPROTKEY Key’ by clicking the 2 icon. The IOPROTKEY key will be generated in the local folder.

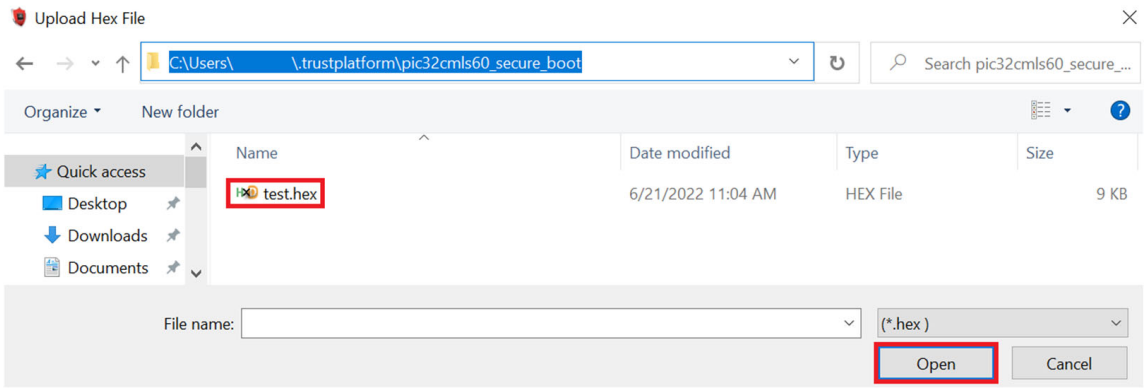
Figure 5-7. Generated IOPROTKEY Key



Note: The I/O Protection Key (IOPROTKEY) allows encrypting the communication between the PIC32CM LS60 microcontroller and the ATECC608B secure element.

10. Execute step 3 ‘Load hex file, calculate digest and signature’ by clicking the 3 icon. The local folder containing the test hex file will open in a prompt window.
11. Select the `test.hex` file, and then click **Open**:

Figure 5-8. Upload Test Software Hex File



Note: The boot memory region to sign is defined by the BOOTPROT fuse bit. This must be generated per the data sheet configuration for secure boot. Refer to the product data sheet for additional information on Secure Boot using the ATECC608B secure element.

12. Execute step 4 ‘Save new application hex’ by clicking the icon to create the signed hex file from the test hex file used at the previous step:

Figure 5-9. Generated Signed Hex File

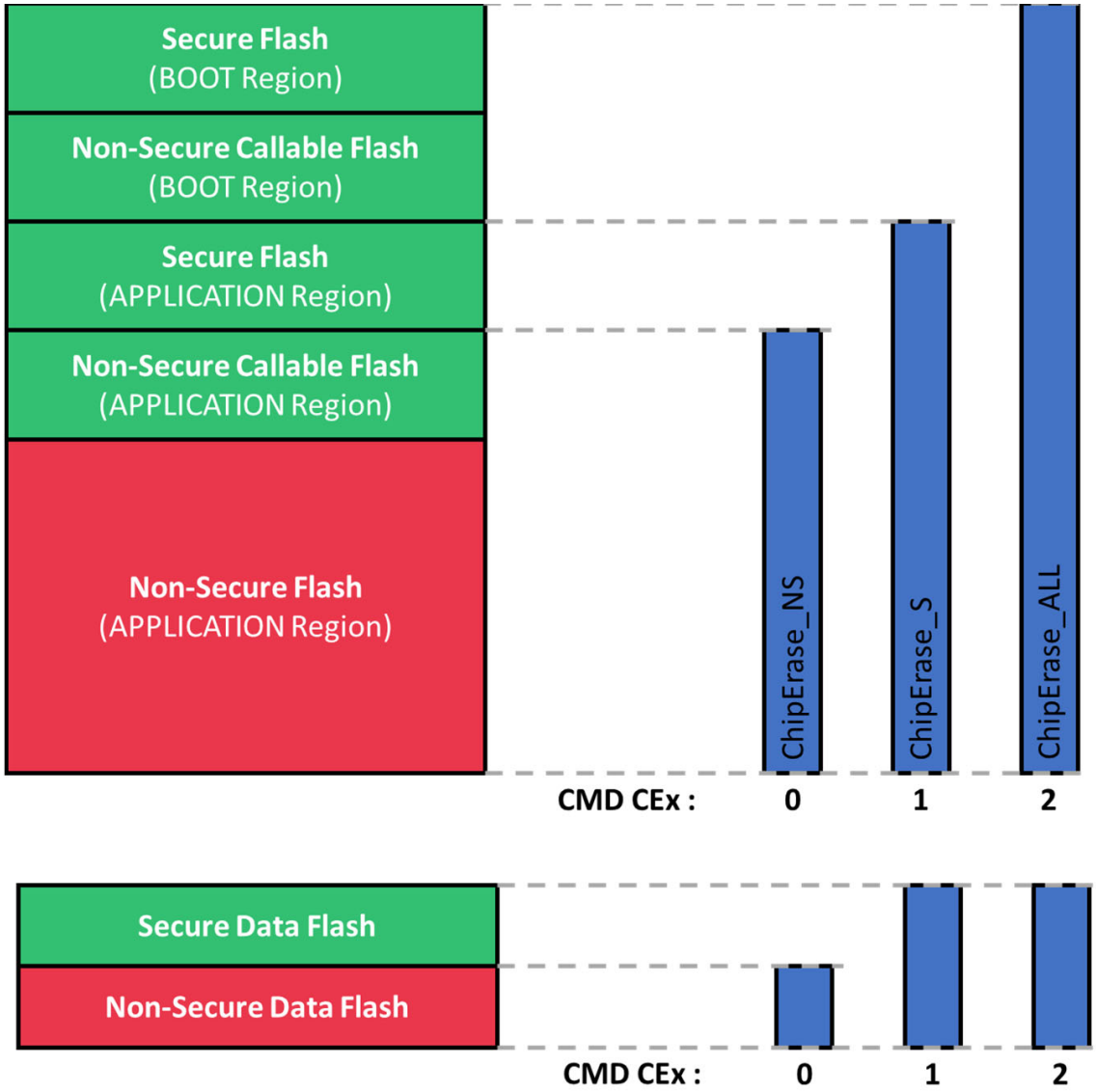
13. Launch step 5 by clicking the icon to Flash the signed hex file in the connected PIC32CM LS60 device.
Note: This step will take some time to complete. Check the completion status in the log.

The test application is now flashed in the connected PIC32CM LS60 device. The on-board LEDs will light ON with a slight delay due to Secure Boot verification, refer to the chapter **“Electrical Characteristics”** in the product data sheet for wake-up timings.

5.3 Adding Secure and Non-Secure Applications

If the Boot software is already flashed, an application software can be added (Secure and Non-Secure). If the Boot software and the Secure applications are already flashed, a Non-Secure application can be added. However, care must be taken not to erase the existing code. The following figure illustrates the different memory regions, and the ChipErase function to apply depending on if a Secure or a Non-Secure application is programmed:

Figure 5-10. Chip Erase Commands



The following sections explain how to configure the ChipErase function applied during the Secure and Non-Secure application programming:

5.3.1 Adding a Secure Application

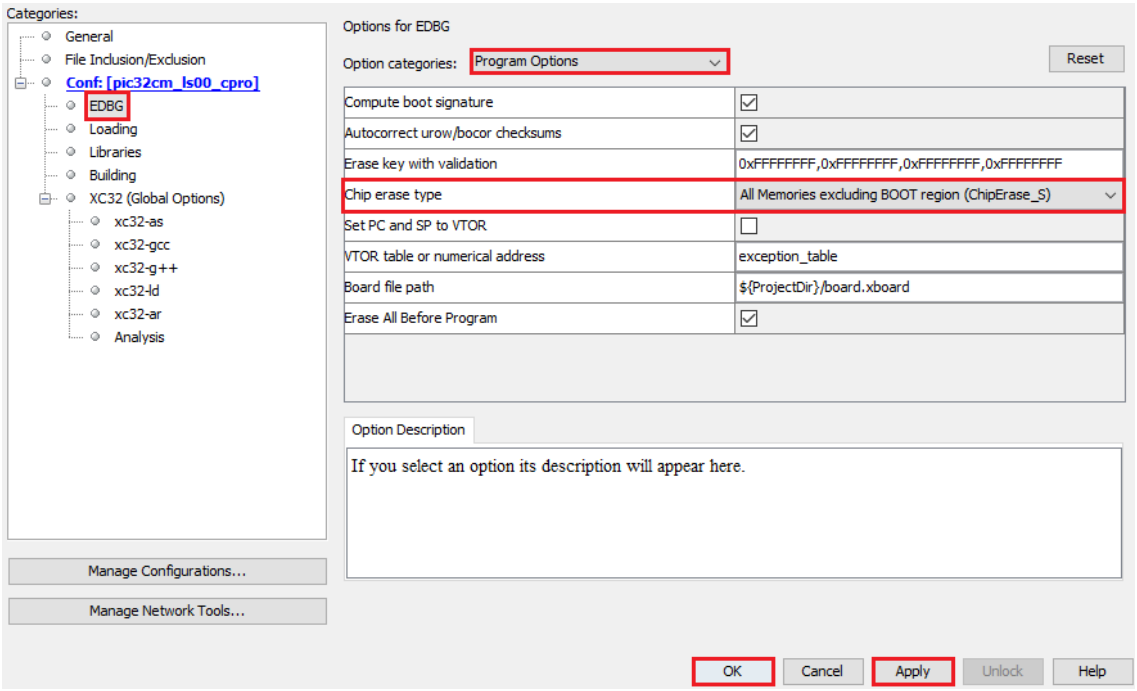
Follow these steps to add a Secure application:

1. In MPLAB X IDE, open the Secure application to program.
2. Under the project tree, select the project, and then right-click and choose Properties.
3. In the Project Properties window, select EDBG.
4. In the Options for EDBG properties page, choose and select these options:

– For Option Categories, select Program Options.
– For Chip erase type, select All memories excluding BOOT region (ChipErase_S).

5. Click **Apply**, and then click **OK**.

Figure 5-11. Secure Application - Chip Erase Type Selection



6. To build and program the project: *Production* > *Make and Program Device Main Project* or click (the toolbar icon) .

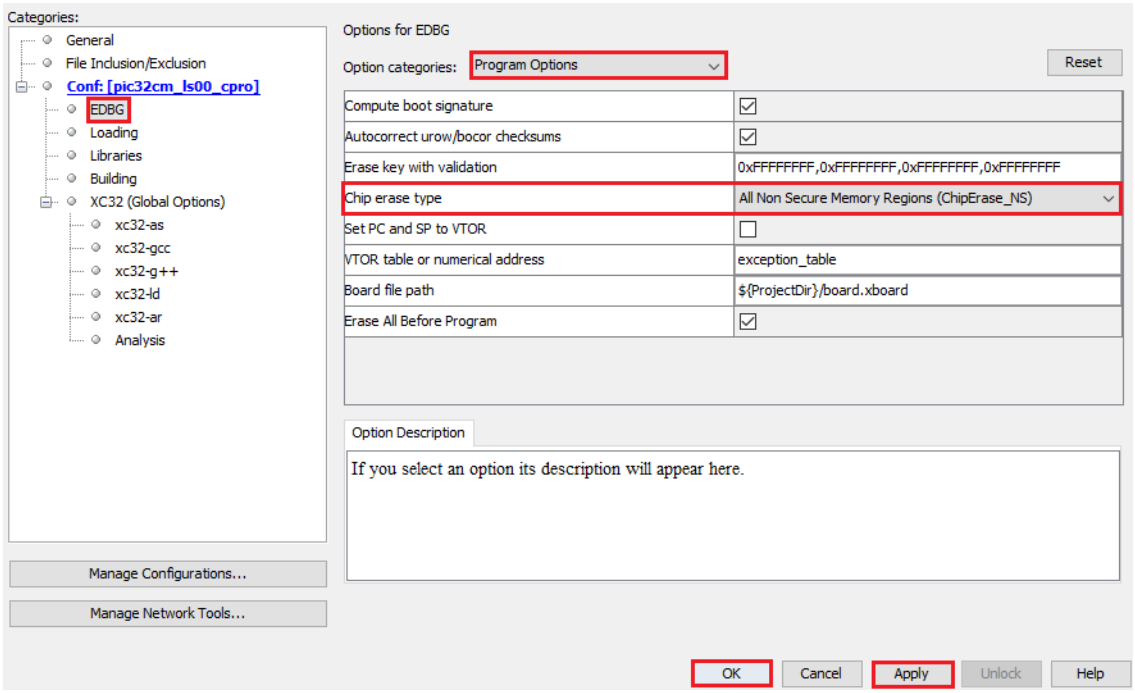
The Secure application is now flashed on the product next to the preexisting Boot Secure application.

5.3.2 Adding a Non-Secure Application

Follow these to add a Non-Secure application:

1. In MPLAB X IDE, open the Non-Secure application to program.
2. Under the project tree, select the project, and then right-click and choose Properties.
3. In the Project Properties window, select EDBG.
4. In the Options for EDBG properties page, choose and select these options:
   – For Option Categories, select Program Options.
   – For Chip erase type, select All Non-Secure Memory Regions (ChipErase_NS).
5. Click **Apply**, and then click **OK**.

Figure 5-12. Non-Secure Application - Chip Erase Type Selection



6. To build and program the project: *Production > Make and Program Device Main Project* or click (the toolbar icon) .

The Non-Secure application is now flashed on the product next to the preexisting Boot Secure and Non-Secure applications by offering a complete TrustZone experience.

6. Troubleshooting

Compilation Error Under MPLAB X IDE Due to too Long of a Project Path

If an MPLAB X IDE project path is too long, the project will not compile and an error message will be displayed. To resolve this issue, users need to move the project for compiling or programming to a smaller project path, for example, desktop or C:\.

© 2022 Microchip Technology Inc.
and its subsidiaries

7. References

For additional information regarding Microchip products and services, visit Microchip Website, or contact a local Microchip sales representative.

The following documents are provided for reference purposes.

- MPLAB X IDE:
  www.microchip.com/mplab/mplab-x-ide
- MPLAB Harmony v3:
  github.com/Microchip-MPLAB-Harmony
- MPLAB Discover:
  mplab-discover.microchip.com/
- PIC32CM LE00/LS00/LS60 Family Data Sheet (DS60001615)
- PIC32CM LE00/LS00/LS60 Family Silicon Errata and Data Sheet Clarifications (DS80000906)
- PIC32CM LE00/LS00/LS60 Curiosity Pro User Guide (DS70005443)
- PIC32CM LE00/LS00/LS60 Curiosity Pro Board Change Notification (DS70005491)

© 2022 Microchip Technology Inc.
and its subsidiaries

8. Revision History

Rev B - 08/2022
The following updates were incorporated for this revision:

- Added the following new sections:
  - Getting Started with the PIC32CM LS60 Using Trust Platform Design Suite v2 (TPDS)
  - Trust Platform Design Suite v2 (TPDS)
  - Run the PIC32CM LS60 Secure Boot Use Case from TPDS v2
  - Adding a Secure/Non-Secure Application
  - Add a Secure Application
  - Add a Non-Secure Application

Rev A - 04/2022
This is the initial release of this document.

© 2022 Microchip Technology Inc.
and its subsidiaries

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

© 2022 Microchip Technology Inc. and its subsidiaries

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, NVM Express, NVMe, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, Symmcom, and Trusted Time are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2022, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-1094-6

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

© 2022 Microchip Technology Inc.
and its subsidiaries

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820

© 2022 Microchip Technology Inc.
and its subsidiaries