

CEC1702 Quick Start Guide

© 2017 Microchip Technology Inc.

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

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates.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. 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 ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. 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, AnyRate, AVR, AVR logo, AVR Freaks, BeaconThings, BitCloud, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KEELOQ, KEELOQ logo, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, RightTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire 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, BodyCom, chipKIT, chipKIT logo, CodeGuard, CryptoAuthentication, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PureSilicon, QMatrix, RightTouch logo, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, 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.

Silicon Storage Technology is a registered trademark 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.

© 2017, Microchip Technology Incorporated, All Rights Reserved.

ISBN: 9781522420729

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
═ ISO/TS 16949 ═

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

© 2017 Microchip Technology Inc.

Table of Contents

Preface **4**
Introduction 4
Document Layout 4
Conventions Used in this Guide 5
The Microchip Web Site 6
Development Systems Customer Change Notification Service 6
Customer Support 7
Document Revision History 7

Chapter 1. Introduction
1.1 CEC1702 Quick Start Guide 8
1.1.1 Purpose 8
1.1.2 Introduction 8
1.1.3 Introduction to Hardware 10
1.1.4 Prerequisites 11

Chapter 2. CEC1702 Efuse Generator Tool Procedure
2.1 CEC1702 Efuse Programming Procedure 12

Chapter 3. CEC1702 SPI Image Generator Utility Procedure
3.1 SPI Image Generation Procedure 13
3.1.1 SPI Image Layout 13
3.1.2 Key Generation 14
3.1.3 SPI Image Generation 14
3.1.4 Programming the SPI Flash Device on a Board 16

Appendix A. CEC1702 SPI Flash Layout
A.1 SPI Image 17
A.1.1 SPI FLASH REGIONS 17

Appendix B. References
B.1 Reference List 20

Worldwide Sales and Service **21**

© 2017 Microchip Technology Inc.

Preface

NOTICE TO CUSTOMERS

All documentation becomes dated, and this manual is no exception. Microchip tools and documentation are constantly evolving to meet customer needs, so some actual dialogs and/or tool descriptions may differ from those in this document. Please refer to our web site (www.microchip.com) to obtain the latest documentation available.

Documents are identified with a "DS" number. This number is located on the bottom of each page, in front of the page number. The numbering convention for the DS number is "DSXXXXXA", where "XXXXX" is the document number and "A" is the revision level of the document.

For the most up-to-date information on development tools, see the MPLAB® IDE online help. Select the Help menu, and then Topics to open a list of available online help files.

INTRODUCTION

This chapter contains general information that will be useful to know before using the CEC1702 Quick Start Guide. Items discussed in this chapter include:

- Document Layout
- Conventions Used in this Guide
- The Microchip Web Site
- Development Systems Customer Change Notification Service
- Customer Support
- Document Revision History

DOCUMENT LAYOUT

This document describes how to use the CEC1702 Efuse Generator Tool as a development tool for CEC1702 Efuse Programming and the CEC1702 SPI Image Generator Utility for programing a binary image into a SPI flash device. The manual layout is as follows:

- **Chapter 1. "Introduction"** – This chapter provides an introduction to programming the Efuse using the CEC1702 Efuse Generator Tool and programming a SPI device using the CEC1702 SPI Image Generator Utility.
- **Chapter 2. "CEC1702 Efuse Generator Tool Procedure"** – This chapter refers to the CEC1702 Efuse Generator Tool User's Guide, reference 2 in **Appendix B. "References"**, which contains a step by step procedure.
- **Chapter 3. "CEC1702 SPI Image Generator Utility Procedure"** – This chapter describes the procedure.
- **Appendix A. "CEC1702 SPI Flash Layout"** – This appendix contains details of the SPI Flash Image.
- **Appendix B. "References"** – This appendix includes helpful references.

CONVENTIONS USED IN THIS GUIDE

This manual uses the following documentation conventions:

DOCUMENTATION CONVENTIONS

Description	Represents	Examples
Arial font:		
Italic characters	Referenced books	*MPLAB® IDE User's Guide*
	Emphasized text	...is the *only* compiler...
Initial caps	A window	the Output window
	A dialog	the Settings dialog
	A menu selection	select Enable Programmer
Quotes	A field name in a window or dialog	"Save project before build"
Underlined, italic text with right angle bracket	A menu path	*File>Save*
Bold characters	A dialog button	Click **OK**
	A tab	Click the **Power** tab
N'Rnnnn	A number in verilog format, where N is the total number of digits, R is the radix and n is a digit.	4'b0010, 2'hF1
Text in angle brackets < >	A key on the keyboard	Press <Enter>, <F1>
Courier New font:		
Plain Courier New	Sample source code	`#define START`
	Filenames	`autoexec.bat`
	File paths	`c:\mcc18\h`
	Keywords	`_asm, _endasm, static`
	Command-line options	`-Opa+, -Opa-`
	Bit values	`0, 1`
	Constants	`0xFF, 'A'`
Italic Courier New	A variable argument	*`file`*`.o`, where *`file`* can be any valid filename
Square brackets [ ]	Optional arguments	`mcc18 [options]` *`file`* `[options]`
Curly brackets and pipe character: { | }	Choice of mutually exclusive arguments; an OR selection	`errorlevel {0|1}`
Ellipses...	Replaces repeated text	`var_name [, var_name...]`
	Represents code supplied by user	`void main (void) { ... }`

THE MICROCHIP WEB SITE

Microchip provides online support via our web site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **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 consultant 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

DEVELOPMENT SYSTEMS CUSTOMER CHANGE NOTIFICATION SERVICE

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

To register, access the Microchip web site at www.microchip.com, click on Customer Change Notification and follow the registration instructions.

The Development Systems product group categories are:

- **Compilers** – The latest information on Microchip C compilers, assemblers, linkers and other language tools. These include all MPLAB C compilers; all MPLAB assemblers (including MPASM assembler); all MPLAB linkers (including MPLINK object linker); and all MPLAB librarians (including MPLIB object librarian).
- **Emulators** – The latest information on Microchip in-circuit emulators.This includes the MPLAB REAL ICE and MPLAB ICE 2000 in-circuit emulators.
- **In-Circuit Debuggers** – The latest information on the Microchip in-circuit debuggers. This includes MPLAB ICD 3 in-circuit debuggers and PICkit 3 debug express.
- **MPLAB IDE** – The latest information on Microchip MPLAB IDE, the Windows Integrated Development Environment for development systems tools. This list is focused on the MPLAB IDE, MPLAB IDE Project Manager, MPLAB Editor and MPLAB SIM simulator, as well as general editing and debugging features.
- **Programmers** – The latest information on Microchip programmers. These include production programmers such as MPLAB REAL ICE in-circuit emulator, MPLAB ICD 3 in-circuit debugger and MPLAB PM3 device programmers. Also included are nonproduction development programmers such as PICSTART Plus and PIC-kit 2 and 3.

© 2017 Microchip Technology Inc.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at:
http://www.microchip.com/support

DOCUMENT REVISION HISTORY

Revision	Section/Figure/Entry	Correction
DS50002665A (08-24-17)	Preliminary Release	

Chapter 1. Introduction

1.1 CEC1702 QUICK START GUIDE

1.1.1 Purpose

This document is intended for software engineers to program the Efuse in a blank CEC1702 device and to program a blank SPI device for use with the CEC1702.

This procedure includes generating public and private keys for authentication and/or encryption, generating custom Efuse data and creating a signed and/or encrypted SPI image for the CEC1702 to support a secure boot process for their system.

This document gives the steps involved in CEC1702 Efuse programming as well as the hardware and software requirements for the custom Efuse programming of a blank CEC1702 part from Microchip.

This document also gives the steps involved in creating a binary image to load into the SPI flash, including encrypting the image as well as generating the signature that is used by the CEC1702 to authenticate the image.

1.1.2 Introduction

The CEC1702 loads application EC firmware from an external SPI flash device into its internal SRAM, verifies its authenticity and/or decrypts it before launching the application firmware. The image is authenticated using the standard ECDSA signature protocol and may be decrypted using an AES key.

The CEC1702 utilizes private and public keys located in its Efuse and the SPI device to authenticate and decrypt the SPI image.

There are two utilities that are used to create the Efuse data and SPI image:

- CEC1702 Efuse Generator Tool
- CEC1702 SPI Image Generator Utility.

1.1.2.1 SECURITY CAPABILITIES

The CEC1702 supports the following security options for the SPI flash image:

- Authentication
  - If Authentication is enabled, the CEC1702 SPI Image Generator Utility computes a digital signature that is appended to both the Image Header and Binary Image in the SPI. The CEC1702 performs an Signature Verification of both the Image Header and Binary Image that it reads from the SPI.
  - If Authentication is disabled, a hash digest is used to verify the integrity of the image.
- Encryption
  - If Encryption is enabled, the CEC1702 SPI Image Generator Utility encrypts the firmware image in the SPI. A Key Header containing a Public key is appended to the image. The CEC1702 decrypts the firmware image that it reads from the SPI.
  - If Encryption is disabled, the image that is loaded into the SPI is not encrypted and therefore no decryption is done by the CEC1702.

© 2017 Microchip Technology Inc.

1.1.2.2 CEC1702 EFUSE GENERATOR TOOL

The CEC1702 Efuse Generator Tool is used to generate private/public key pairs and generate the Efuse programming values. The output of the tool is a binary file for programming the CEC1702 part on the Clicker board using a JTAG programming tool.

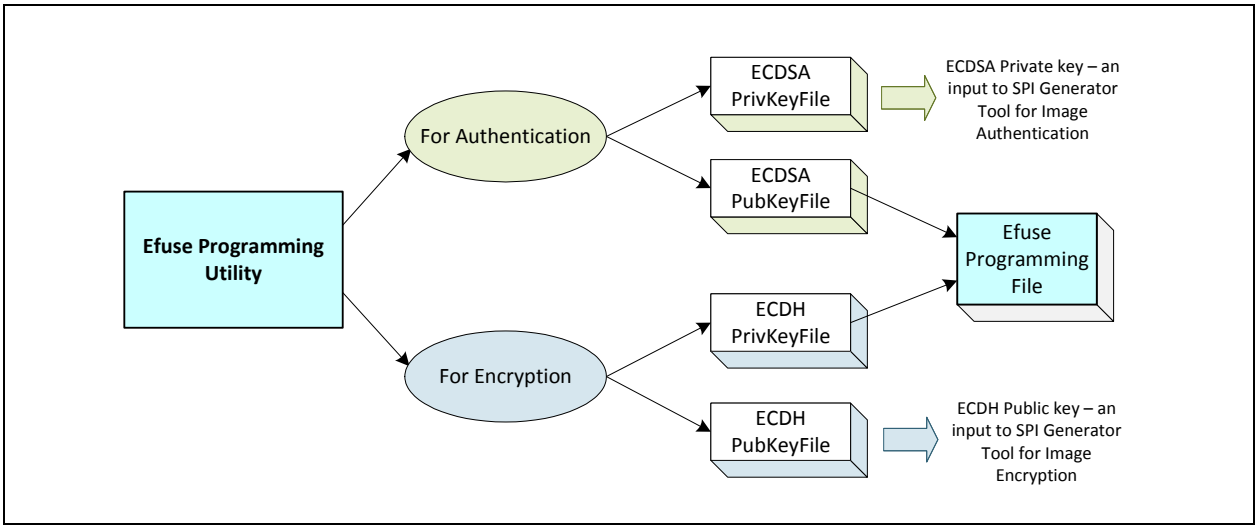
The CEC1702 Efuse Generator Tool also writes the private and public key in an output file protected with the password set by the user while entering the parameters. The keys generated by the CEC1702 Efuse Generator Tool are also used by the CEC1702 SPI Image Generator Utility.

This document refers to the CEC1702 Efuse Generator Tool User's Guide, which gives step by step information on programming the Efuse.

See **Chapter 2. "CEC1702 Efuse Generator Tool Procedure"**.

Figure 1-1 illustrates the flow of the CEC1702 Efuse Generator Tool.

FIGURE 1-1: CEC1702 EFUSE GENERATOR TOOL FLOW



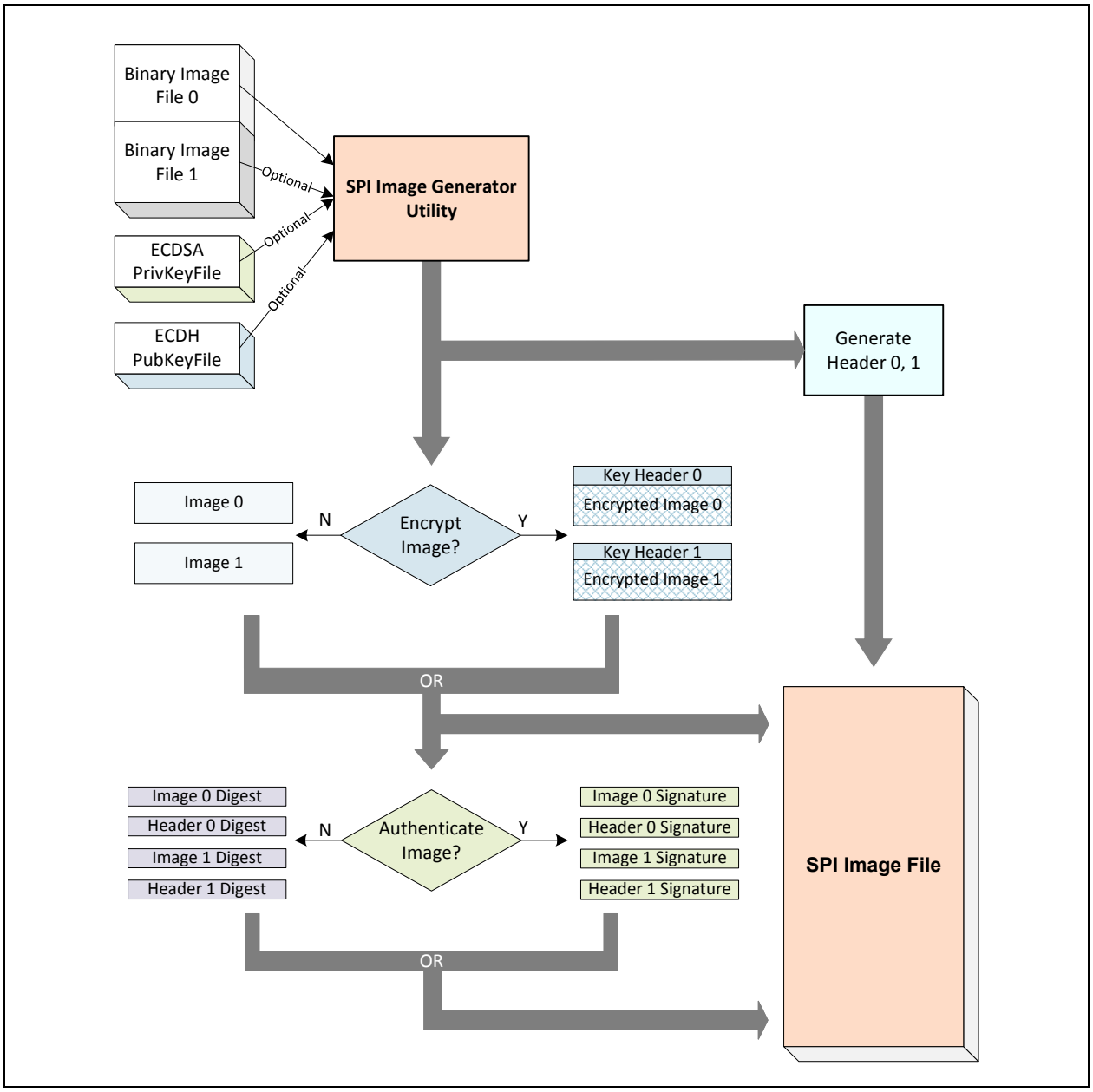
1.1.2.3 CEC1702 SPI IMAGE GENERATOR UTILITY

The CEC1702 SPI Image Generator Utility is used to create the binary image for the SPI flash. The output from the utility is a binary file that will be loaded into the SPI flash device on a Clicker board using a SPI Flash Programmer.

This document gives step by step information on generating the SPI Image using the CEC1702 SPI Image Generator Utility. This process involves generating the required keys and performing the steps necessary for encrypting the binary image and creating a digital signature for the image and its associated header.

See **Chapter 3. "CEC1702 SPI Image Generator Utility Procedure"**. Figure 1-2 illustrates the flow of the CEC1702 SPI Image Generator Utility.

FIGURE 1-2: SPI IMAGE GENERATOR UTILITY FLOW



1.1.3 Introduction to Hardware

The board used for programming the eFuse in the CEC1702 and the SPI flash device is the “CEC1702 Clicker board”.

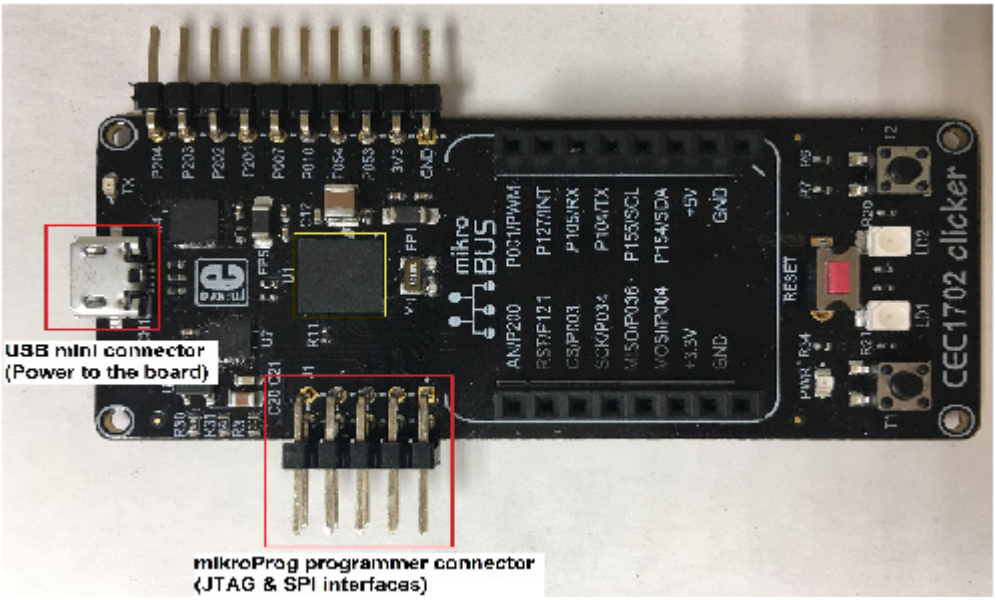
The Clicker Board consists of following interfaces

1. USB mini Connector (Power to the board)
2. MikroProg Programmer connector (JTAG and SPI)

Figure 1-3: “CEC1702 Clicker Board Interface Details” shows the Clicker Board and the location of the various interfaces listed above:

© 2017 Microchip Technology Inc.

FIGURE 1-3: CEC1702 CLICKER BOARD INTERFACE DETAILS



1.1.4 Prerequisites

The following are prerequisites for programming the eFuse in the CEC1702 and programming the SPI device:

1. Clicker Board with blank CEC1702 and blank SPI Flash device should be available.
2. The hardware board must have proper input circuitry for providing 1.59V Efuse programming voltage.
3. PC should have Windows7/8/10. See Note 1.
4. The user is expected to have downloaded and installed openssl version 1.0.1e. See Note 2.
5. The user is expected to have downloaded the CEC1702 Efuse Generator Tool on a PC. If the user is using mikroProg tool for programming the Clicker Board, this utility is part of the tool package.
6. The user is expected to have any JTAG programmer tool installed on their PC for programming the Efuse hex / binary file in CEC1702 on the Clicker Board.
7. The user is expected to have downloaded the CEC1702 SPI Image Generator Utility on a PC.
8. The user is expected to have read the CEC1702 data sheet and know all the authentication and encryption modes planned to be used in their system.
9. The user is expected to know which keys need to be generated for their system and application.

Note 1:	CEC1702 Efuse Generator Tool is only supported for Windows at this time.
2:	Openssl may be downloaded from https://www.openssl.org/source/old/1.0.1/. Version number is openssl-1.0.1e.tar.gz or later.
3:	Please refer to CEC1702 Clicker board documentation for other requirements for executing step 2.

Chapter 2. CEC1702 Efuse Generator Tool Procedure

2.1 CEC1702 EFUSE PROGRAMMING PROCEDURE

The CEC1702 Efuse Generator Tool generates private/public key pairs and Efuse programming values. The output from the tool is a binary file for programming the CEC1702 part on the Clicker board using any JTAG programmer tool. The tool also writes the private and public keys into an output file protected with the password set by the user while entering the parameters.

The CEC1702 Efuse Generator Tool is described in the CEC1702 Efuse Generator Tool User's Guide (reference 2 in **Appendix B. "References"**). This document gives step by step information on programming the Efuse.

> **Note:** The keys generated by the CEC1702 Efuse Generator Tool are also used by the CEC1702 SPI Image Generator Utility. See **Chapter 3. "CEC1702 SPI Image Generator Utility Procedure"**.

Chapter 3. CEC1702 SPI Image Generator Utility Procedure

3.1 SPI IMAGE GENERATION PROCEDURE

The CEC1702 may authenticate and decrypt one of two images from a SPI flash as part of a secure boot process. The layout of these images in the SPI is described below.

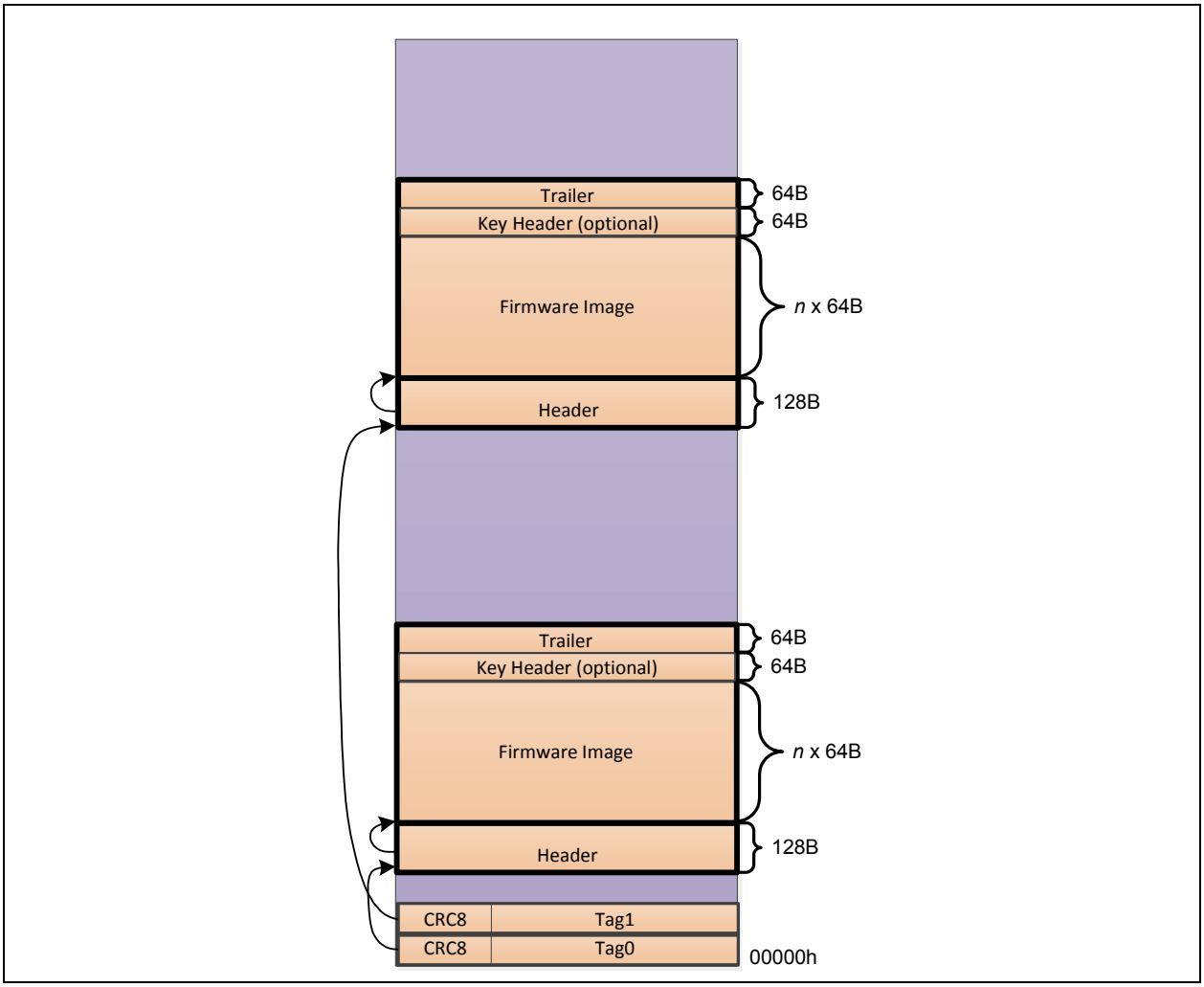
3.1.1 SPI Image Layout

The CEC1702 SPI Image Generator Utility creates a SPI image containing two firmware images. These images can be created from different files by the utility.

The boot ROM in the CEC1702 will attempt to locate a valid image in two locations in the SPI Flash. The locations are searched in the order Tag0 first, then Tag1.

The SPI image that is generated by the CEC1702 SPI Image Generator Utility is shown in **Figure 3-1: "SPI Image Layout Example"**.

FIGURE 3-1: SPI IMAGE LAYOUT EXAMPLE



Detailed information about the SPI Image is contained in **Appendix A. "CEC1702 SPI Flash Layout"**.

3.1.2 Key Generation

Prior to running the CEC1702 SPI Image Generator Utility, the CEC1702 Efuse Generator Tool must be executed to generate key files as described in the next section.

3.1.2.1 OUTPUT KEY FILES

The output directory for the output files generated from the CEC1702 Efuse Generator Tool may be defined by the user.

On program execution the tool generates two folders in the output directory "Output Dir". The ECDH private key (AES Encrypted), self signed certificate, ECDSA private key (AES Encrypted), ECDSA Self Signed Certificate and their corresponding certificate requests are stored in the "keys" directory. This is represented below:

```
<efuse_generator>
 |
 +---efuse
     +--efuse_<YYYYMMDD>_<WHHMMSS>   -> Output Dir self generated
       +---keys                      -> Contains all the keys
       |     <ECDH>.pem              -> ECDH Private key AES Encrypted
       |     <ECDH>_crt.pem          -> ECDH Self Signed Certificate
       |     <ECDH>_csr.pem          -> ECDH Certificate Request
       |     <ECDSA>.pem             -> ECDSA Private key AES Encrypted
       |     <ECDSA>_crt.pem         -> ECDSA Self Signed Certificate
       |     <ECDSA>_csr.pem         -> ECDSA Certificate Request
       |     keys_info.txt           -> Generated Key details
       |     key_file.bin            -> key_file.bin extracted key output
       |
```

3.1.2.2 KEY GENERATION STEPS

See the CEC1702 Efuse Generator Tool User's Guide for the steps required for key generation. The result of these steps are the following files used by the CEC1702 SPI Image Generator Utility.

- <"ECDSA Key filename">.pem
- <"ECDSA Key filename">_crt.pem
- <"ECDH Key filename">.pem
- <"ECDH Key filename">_crt.pem

Note that the <XXXX>_crt.pem files are used as the "Public Key Files" by the utilities.

3.1.3 SPI Image Generation

Running the executable file "mec2016_spi_gen.exe" from the command prompt will utilize a configuration file as an input and generate the output binary image file to be written to the SPI flash device.

The configuration file provides the filename and location of the key files and binary image files as well as other parameters used in the generation of the image.

By default, running "mec2016_spi_gen.exe" from the command prompt will take "spi_cfg.txt" as a default configuration file and generate the output file "spi_image.bin".

© 2017 Microchip Technology Inc.

The file can have several options as follows:

mec2016_spi_gen.exe -i <cfg_file_name> -o <output_spi_file_name> -m <merge_-file>

Where:

-i cfg_file_name

Specifies the text config file for the SPI chip & images. Defaults to spi_cfg.txt.

-o output_spi_file_name

Specifies the SPI binary output file name. Defaults to spi_image.bin.

-m merge_file

Read merge file as an existing SPI binary image and create FW images inside it. No default value.

The user is required to fill in the required information in the configuration file, including the filename and location of the key files, binary image files and other parameters. See the “release.txt” file and “spi_cfg.txt” file for more information.

The required information includes the Size of SPI flash device and the following information for each binary image (Image 0 and Image 1):

- Location of the Header in the SPI (“ImageLocation”)
- SPI interface settings
- Filename of Application Binary File (“FwBinFile”). See Note 1.
- Offset of Binary File from end of Header - number of 64B offsets (“FwOffset”)
- Application firmware load address in SRAM (“FwLoadAddress”)
- Application firmware entry address in SRAM (“FwEntryAddress”)
- Enable/disable ECDSA Authentication of Header and Image
- Filename for the key pair used to sign and verify/authenticate the Header and Image (“ECDSAPrivKeyFile”). See Note 1.
- Password for the key pair used to sign and verify/authenticate the Header and Image (“ECDSAPrivKeyPassword”)
- Enable/disable Encryption of Image
- Filename of Public Key used to Generate the AES-256 Key/IV for encryption (“AesGenECPubKeyFile”). See Note 1. Note: this is the ECDH Public key.
- The voltage level of the three VTRx regions of the CEC1702. See the data sheet for more information.

Note 1: If the "mec2016_spi_gen.exe" executable file is not run in the same directory as the key files and binary file, then this filename must also contain the directory path of the file.

The output file from the utility is a binary file that will be used to program the SPI flash device on a Clicker board using a SPI programmer tool.

3.1.3.1 GENERATING SPI IMAGE USING MICROE TOOL

If the MikroElektronika tool will be used to generate and program the SPI device, refer to the CEC1702 Efuse Generator Tool User’s Guide, reference 2 in **Appendix B. “References”**. See **Appendix B. “Programming Steps For MikroE Tool”** in the CEC1702 Efuse Generator Tool User’s Guide. Specifically, section **B.2 “Firmware Image Encryption and Authentication”** shows the steps for enabling encryption and authentication. Note that the MicroE tool does not have all the same options that the CEC1702 SPI Image Generator Utility provides.

3.1.4 Programming the SPI Flash Device on a Board

If the MikroElektronika tool will be used to program the SPI device, refer to the CEC1702 Efuse Generator Tool User's Guide, reference 2 in **Appendix B. "References"**. See **Appendix B. "Programming Steps For MikroE Tool"** in the CEC1702 Efuse Generator Tool User's Guide. Specifically, section **B.2 "Firmware Image Encryption and Authentication"** shows the steps for programming the SPI image.

The SPI device may also be programmed as follows:

a) The Image may be loaded into the SPI device before putting it on the board
b) The Image may be programmed into the SPI device with a tool such as Ded-iProg SPI Flash Programmer.

© 2017 Microchip Technology Inc.

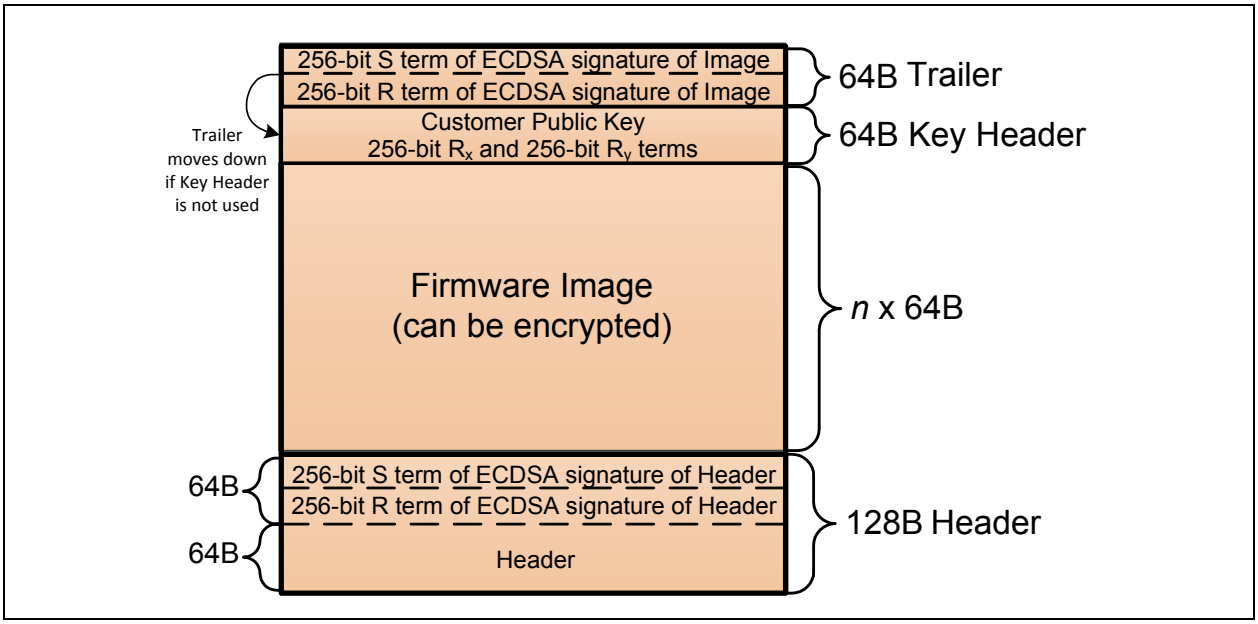
Appendix A. CEC1702 SPI Flash Layout

A.1 SPI IMAGE

The SPI image that is generated by the CEC1702 SPI Image Generator Utility is shown in **Figure 3-1: "SPI Image Layout Example"**.

The header and image region is shown in expanded form in **Figure A-1: "SPI Image Details"**.

FIGURE A-1: SPI IMAGE DETAILS



A.1.1 SPI FLASH REGIONS

The SPI Flash has the following defined regions:

1. Two 8-byte Tags, each of which identify the position of one of the two load regions in the Flash. Each of the load regions consists of the following four regions.
2. A 128-byte Header
3. The EC Runtime FW body (Firmware Image), an integral multiple of 64 bytes
4. An optional 64-byte Key Header
5. A 64-byte Trailer

A.1.1.1 TAG

The Tag contains a pointer to the EC code image header. The Load Sequence first checks for TAG 0, which is located at offset 0x00 in the SPI flash.

If the data stored in TAG 0 fails the Tag validation, the FW Image Header validation, or the EC Runtime FW Binary Image validation, the Load Sequence then checks for TAG 1, which is located at offset 0x04.

A.1.1.2 FIRMWARE IMAGE HEADER

The FW Image Header is located in the SPI Flash as determined by the Tag. The Header is located at an offset in the SPI Flash that is on a 256-byte boundary. The header contains SPI interface settings and information about the image, including

- Offset of Binary File from end of Header
- Application firmware load address in SRAM
- Encryption of Image enabled/disabled

AUTHENTICATING THE HEADER

If Authentication is enabled, the Header is signed by a standard ECDSA digital signature, using SHA-256.

Using the CEC1702 Efuse Generator Tool, a customer generates a P- 256 private key, which is retained by the customer and kept a secret, and the corresponding public key, which is stored in the CEC1702 eFuse One Time Programmable (OTP) memory. The Header is signed by the CEC1702 SPI Image Generator Utility as part of the SPI image generation process.

The ECDSA verification is performed with the public key. If the ECDSA verification procedure returns an error, the load terminates.

A.1.1.3 EC RUNTIME FW BINARY IMAGE

The EC Runtime FW Binary Image contains three contiguous components as originally illustrated in **Figure 3-1: “SPI Image Layout Example”**.

1. Firmware Image

The Firmware image contains the application code that is loaded into SRAM.

The Firmware image will start on a 64-byte boundary in the SPI Flash, and consists of an integral number of 64-byte blocks. If the firmware image does not end on a 64-byte boundary, it will be padded with zero's. The number of 64-byte blocks in the Firmware Image is defined by the "FW Binary Length" field in the Header, n.

2. Key Header (Optional), Used for Encryption

The 64 bytes immediately appended to the end of the Firmware Image are used for Encryption feature.

- If Encryption is disabled in the SPI flash header, the Key Header is not used. The ROM code loads *n*X64 bytes from the Flash into SRAM.
- If Encryption is enabled in the SPI flash header, the Key Header is used to store the 64 Byte Diffie-Hellman public key used by the boot ROM Diffie-Hellman key exchange to derive the AES256-CBC decryption key. The ROM code loads *(n+1)*X64 bytes from the Flash into SRAM.

3. Trailer, Used for Authentication

The Trailer refers to the 64 bytes in the SPI Flash appended to the end of the Firmware Image.

- If Authentication is enabled, the trailer contains the ECDSA signature used to authenticate the Firmware Image.

  The signature is over the Firmware Image and, if encryption is enabled, the Key Header as well. The signature block is 64 bytes long.

  a) If Encryption is disabled, the size of the image signed is n x 64.
  b) If Encryption is enabled, the size of the image signed is (n+1) x 64.

© 2017 Microchip Technology Inc.

- If Authentication is disabled, The trailer contains a SHA-256 digest used to validate the Firmware Image has been loaded without error.
  a) If Encryption is disabled, the ROM code loads *n* x 64 bytes from the Flash into SRAM.
  b) If Encryption is enabled, the ROM code loads (*n*+1) x 64 bytes from the Flash into SRAM.

Appendix B. References

B.1 REFERENCE LIST

1. CEC1702 Data Sheet is available at www.microchip.com/cec1702.
2. CEC1702 Efuse Generator Tool User's Guide is available at the link in item 1.
3. Documentation and details of CEC1702 Clicker Board.
4. Documentation and details of CEC1702 Clicker 2 Board.
5. Openssl installable package openssl-1.0.1e.tar.gz.
6. Latest mikroC compiler is available at mikroC for ARM v5.0.0.

© 2017 Microchip Technology Inc.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://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

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon

Hong Kong
Tel: 852-2943-5100
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115
Fax: 86-571-8792-8116

China - Hong Kong SAR
Tel: 852-2943-5100
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-3326-8000
Fax: 86-21-3326-8021

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8864-2200
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

ASIA/PACIFIC

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-3019-1500

Japan - Osaka
Tel: 81-6-6152-7160
Fax: 81-6-6152-9310

Japan - Tokyo
Tel: 81-3-6880- 3770
Fax: 81-3-6880-3771

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
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

France - Saint Cloud
Tel: 33-1-30-60-70-00

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-67-3636

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: 47-7289-7561

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

© 2017 Microchip Technology Inc.