



MICROCHIP

**CEC1736 Development Board
User's Guide
#EV19K07A**

CEC1736 Development Board User's Guide

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.

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 Information regarding device applications is provided only for your convenience and may be superseded by updates.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 <https://www.microchip.com/en-us/support/design-help/client-support-services>.

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, Klear, 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, SQL, 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: 9781668303740

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



Table of Contents

Preface	4
Introduction.....	4
Document Layout	4
Conventions Used in this Guide	5
Microchip Web Site	6
Development Systems Customer Change Notification Service	6
Customer Support	7
Document Revision History	7
Chapter 1. Introduction	
Chapter 2. Features	
2.1 CEC1736 Development Board Block Diagram	9
2.2 Hardware Features:	9
2.3 CEC1736 Development Board Layout	10
Chapter 3. Recommended Tools and Accessories	
Chapter 4. Powering the CEC1736 Development Board	
Chapter 5. Jumper Options	
Chapter 6. Running Out-of-Box (OOB) Demo Code	
Chapter 7. Getting Ready for Development	
7.1 Evaluating CEC1736 with User's System	21
Worldwide Sales and Service	22

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 “DSXXXXA”, where “XXXX” 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 document describes the Microchip CEC1736 development board usage and details the demo setup and execution.

This chapter contains general information that will be useful to know before using the [CEC1736 Development Board](#). Items discussed in this chapter include:

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

DOCUMENT LAYOUT

This document is written for anyone who wants to run the Microchip CEC1736 demo using the CEC1736 development board. The manual layout is as follows:

- **Chapter 1. “Introduction”** - Explains purpose and scope of this guide.
- **Chapter 2. “Features”** - Provides board features and layout information.
- **Chapter 3. “Recommended Tools and Accessories”** - Explains recommended tools to be used for the demo.
- **Chapter 4. “Powering the CEC1736 Development Board”** - Provides steps with illustrations for running the demo.
- **Chapter 5. “Jumper Options”** - Provides board jumper settings information.
- **Chapter 6. “Running Out-of-Box (OOB) Demo Code”** - Explains the out-of-box demo that coming with the development board.
- **Chapter 7. “Getting Ready for Development”** - Explains the steps when doing users customized development.

CONVENTIONS USED IN THIS GUIDE

This manual uses the following documentation conventions:

DOCUMENTATION CONVENTIONS

Description	Represents	Examples
Arial font:		
Italic characters	Referenced books	<i>MPLAB[®] IDE User's Guide</i>
	Emphasized text	...is the <i>only</i> 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	<u><i>File>Save</i></u>
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	<i>file.o</i> , where <i>file</i> can be any valid filename
Square brackets []	Optional arguments	mcc18 [options] <i>file</i> [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) { ... }

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.

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

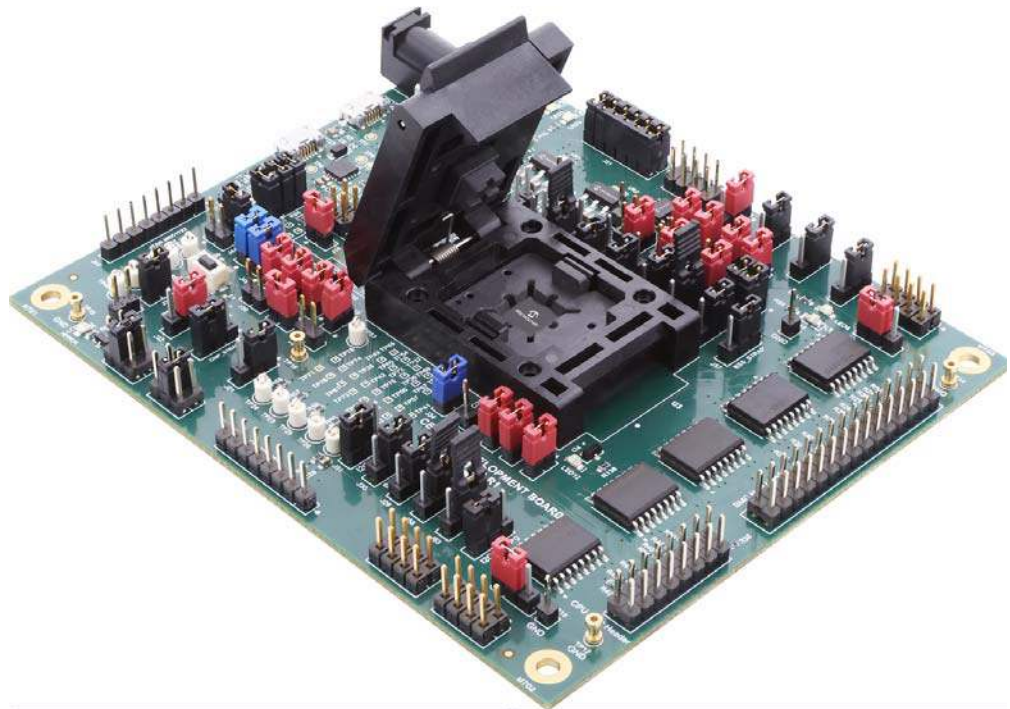
Revision	Section/Figure/Entry	Correction
DS50003324A (05-06-22)		Document release

Chapter 1. Introduction

The CEC1736 Development Board is intended as a demonstration, development, and testing platform for Real Time Platform Root of Trust applications in Datacenter, Telecommunications, Networking, Industrial and Embedded computing markets. The board features a variety of hardware options (including a power supply, user interface, serial communications, and expansion headers) that enable rapid prototyping and development of Real Time Platform Root of Trust applications.

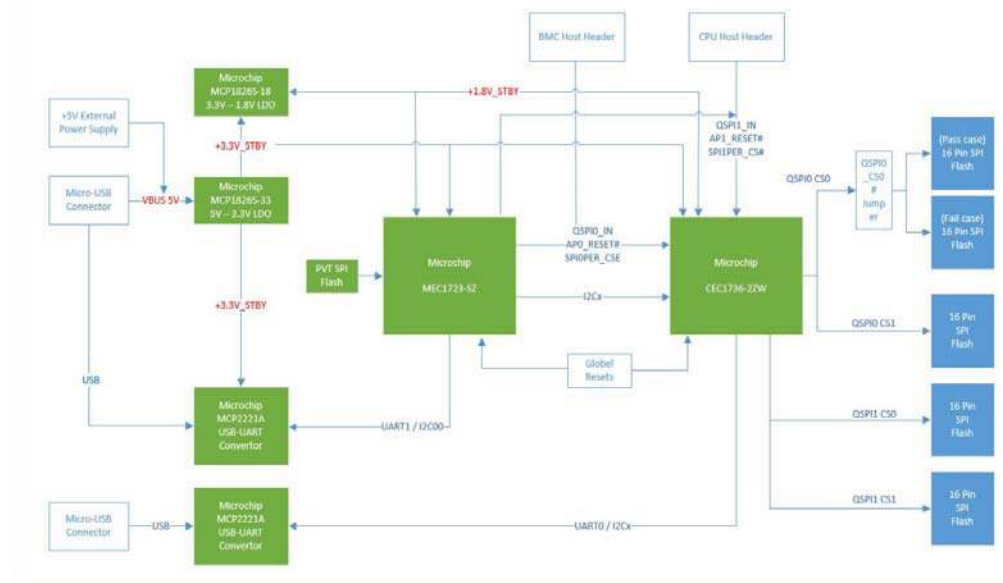
This development board is designed for great out of box experience for users with the following features:

- CEC1736 OTP - pre-programmed with pre-defined OTP features that supports demonstration example.
- CEC1736 Internal SPI Flash - pre-programmed with the latest Soteria-G3 firmware release.
- MEC1723 (emulated as Application Process) - MEC1723 Out-of-box example firmware is included and upgradeable for demonstration.
- CEC1736 socket - Users have the ability to use a production CEC1736 to develop their own OTP features for their specific designs.



Chapter 2. Features

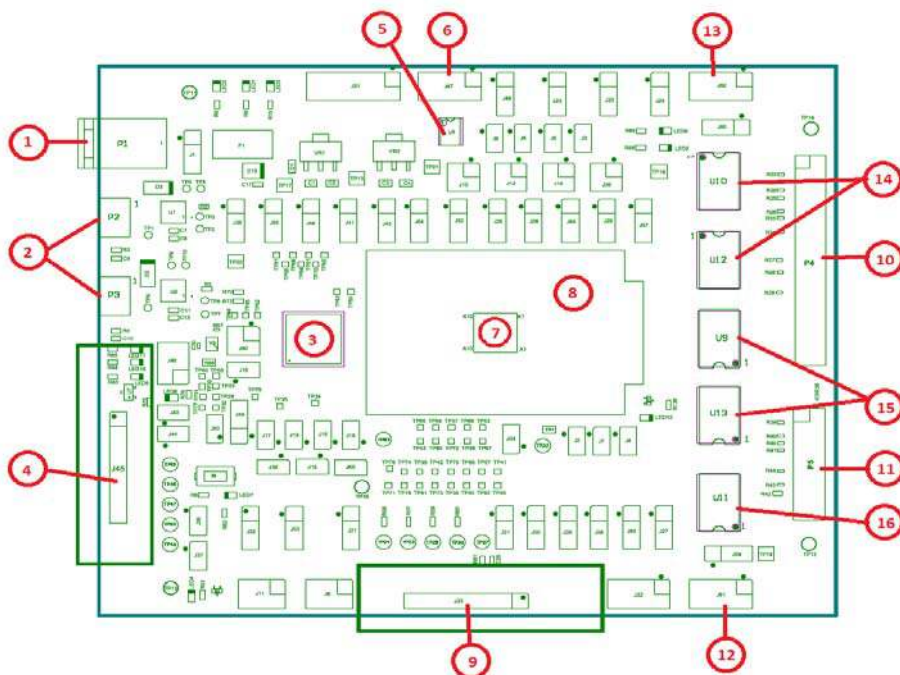
2.1 CEC1736 DEVELOPMENT BOARD BLOCK DIAGRAM



2.2 HARDWARE FEATURES:

- Socket for CEC1736 84-pin
- Four 16-pin 256Mbit SPI Flashes for normal operation
- One 16-pin 256Mbit SPI Flash for failure case demonstration
- One USB-UART/I2C port for CEC1736
- One USB-UART port for MEC1723
- BMC Host Header
- CPU Host Header
- One 1x8 PICKIT4 header for CEC1736 for debugging and programming
- One 1x8 PICKIT4 header for MEC1723 for debugging and programming
- GPIOs / I2C headers for optional customization development
- Board can be powered by Micro-USB Cable or +5V Power Adapter, which is NOT included with in the development board

2.3 CEC1736 DEVELOPMENT BOARD LAYOUT



1. Power Adapter Plug (P1) — Provides another way to power the board via external +5 V power adapter
2. USB micro-B connectors — Provides power to the board and provides an interface for serial input/output or I2C using the Microchip MCP2221A USB-to-UART/I2C serial converter to CEC1736 (P2) and MEC1723 (P3)
3. Microchip MEC1723N-B0-I/SZ (U6) - emulated as Application Processor
4. Microchip PICKIT4 1x8 header (J45) for MEC1723
5. Microchip SST26VF040A SPI Flash (U8) for MEC1723 Private Flash Boot (Optional)
6. Dediprog SF100/SF600 SPI Flash Programming Header (J47) to U8

Note: J47 Pin 7 & 8 are connected but can impact to Dediprog operation. If failure happened, please cut-off pin 7 & pin 8 connection from SFxxx to the header

7. Microchip CEC1736-S0-I/2ZW (installed in U3 socket)
8. 84-pin 2ZW package Socket (U3)
9. Microchip PICKIT4 1x8 header (J33) for CEC1736
10. BMC Host Connection Header (P4)
11. CPU Host Connection Header (P5)
12. Dediprog SF100/SF600 SPI Flash Programming Header (J61) to U9, U11 or U13
13. Dediprog SF100/SF600 SPI Flash Programming Header (J62) to U10 or U12
14. SPI Flashes (U10,U12) on CEC1736 QSPI1 channel
15. SPI Flashes (U9, U13) on CEC1736 QSPI0 channel
16. SPI Flash (U11) on CEC1736 QSPI0 CS0# channel for failure case demonstration purpose only



CEC1736 Development Board User's Guide

Chapter 3. Recommended Tools and Accessories

For development with the CEC1736 Development Board, we recommend the following tools:

1. Microchip MPLAB®X v6.00 or later
2. XC32 Pro Compiler v2.50 or later
3. PICKit4 In-Circuit debugger for direct plug-in
4. ICD4 In-Circuit debugger + Debugger Adapter board (mD# AC102015)
5. Tera Term v4.106 or later (or preferred equivalent) for UART debug logs
6. (Optional) Dediprog SF100 or SF600 (or preferred equivalent) for external SPI flash programming

Users may request the EV19K17A - CEC1736 Development Board technical documents via Microchip Support Case, with a Non-disclosure Agreement (NDA) in place.

- Altium Design Files
- Gerber Files
- Schematic
- Bill of Material

Please contact your Microchip Representative with any further questions.

Chapter 4. Powering the CEC1736 Development Board

The CEC1736 Development Board can be powered directly through the USB micro-B port of the USB-Serial converter (P2 and/or P3). The 5V input from the USB voltage rail is regulated to 3.3V by an MCP1826S voltage regulator.

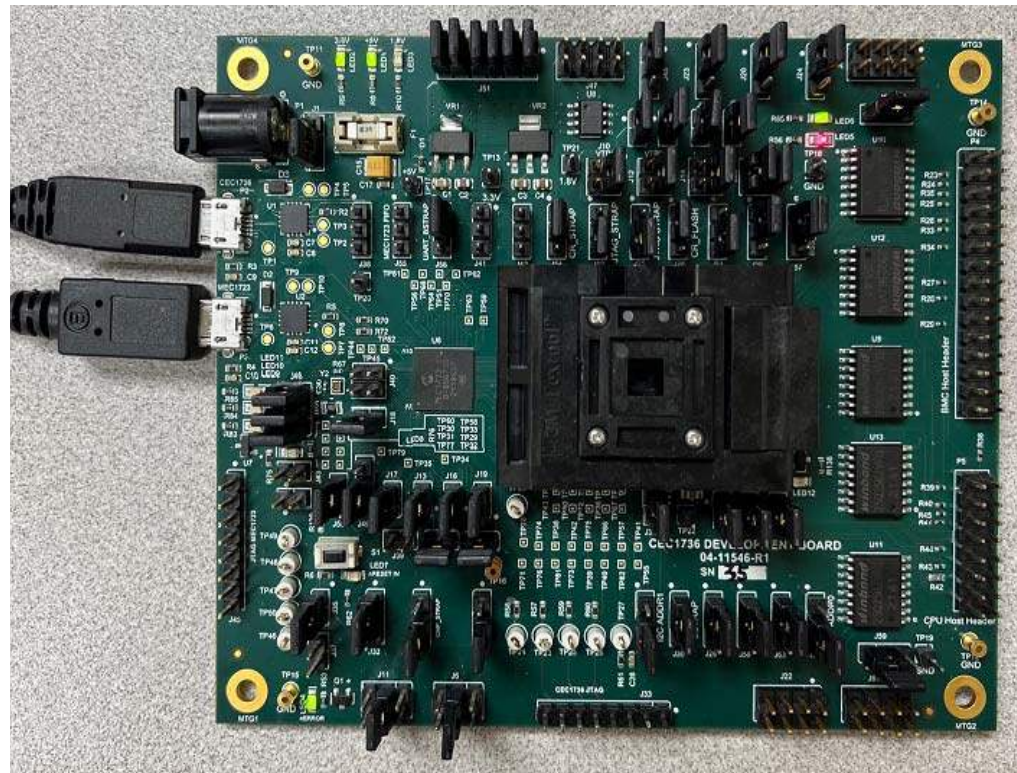
Optionally, the CEC1736 Development Board can be powered by an external power supply through the Power Plug (P1). The 5V is regulated to 3.3 V, which is the same as using USB micro-B port. This option is selected by J1 1-2, default is 2-3 power thru USB.

A shunt diode (D1) can be used to allow measurement of the total system power consumption when using the USB micro-B port or a jumper (J1) is provided to allow measurement of the total system power consumption when using an external power supply. After the board is powered, LED1 (+5V), LED2 (+3.3V), and LED3 (+1.8V) should be turned on.

LED9, LED10, LED11 can be blinking depend on the MEC1723 Firmware Application, which indicate that the MEC1723 Firmware is loaded & executing.

LED4, LED5, LED6, LED12 can be blinking indicating that the CEC1736 Soteria Firmware is loaded and executing.

Power-Up as shown below:



Chapter 5. Jumper Options

The CEC1736 Development Board has several jumpers, summarized as follows:

JUMPER OPTIONS

Jumper	Description	Details
J1	Board Power Selection	1-2: Power by external 5V Adapter (P1) 2-3 (Default): Power by Micro-USB Port (P2, P3)
J2	VTR power to CEC1736	IN (Default): connect VTR power OUT: disconnect VTR power
J3	+3.3V power to MEC1723	IN (Default): connect +3.3V power OUT: disconnect +3.3V power
J4	VTR_PLL power to CEC1736	IN (Default): connect VTR_PLL power OUT: disconnect VTR_PLL power
J5	+1.8V power to MEC1723	IN (Default): connect +1.8V power OUT: disconnect +1.8V power
J6	CEC1736 I2C SCL selection to MCP2221A	1-2: I2C10 3-4 (Default): I2C06 5-6: I2C00
J7	VTR_ANALOG power to CEC1736	IN (Default): connect VTR_ANALOG power OUT: disconnect VTR_ANALOG power
J8	+3.3V power to CEC1736	IN (Default): connect +3.3V power OUT: disconnect +3.3V power
J9	+1.8V power to CEC1736	IN (Default): connect +1.8V power OUT: disconnect +1.8V power
J10	VTR1 power selection for CEC1736	1-2 (Default): connect +3.3V power 3-4: connect +1.8V power
J11	CEC1736 I2C SDA selection to MCP2221A	1-2: I2C10 3-4 (Default): I2C06 5-6: I2C00
J12	VTR2 power selection for CEC1736	1-2 (Default): connect +3.3V power 3-4: connect +1.8V power
J13	VTR_REG power to MEC1723	IN (Default): connect VTR_REG power OUT: disconnect VTR_REG power
J14	VTR2 power selection for MEC1723	1-2 (Default): connect +3.3V power 3-4: connect +1.8V power
J15	VTR_PLL power to MEC1723	IN (Default): connect VTR_PLL power OUT: disconnect VTR_PLL power
J16	VTR_ANALOG power to MEC1723	IN (Default): connect VTR_ANALOG power OUT: disconnect VTR_ANALOG power
J17	VTR1 power to MEC1723	IN (Default): connect VTR1 power OUT: disconnect VTR1 power
J18	VBAT power to MEC1723	IN (Default): connect VBAT power OUT: disconnect VBAT power
J19	VTR3 power to MEC1723	IN (Default): connect VTR3 power OUT: disconnect VTR3 power
J20	CEC1736 GPIO012/nEXTRST Pull selection	1-2 (Default): pull-high to VTR_REG 2-3: pull-down

CEC1736 Development Board User's Guide

JUMPER OPTIONS

Jumper	Description	Details
J21	CEC1736 GPIO106/AP0_nRESET Pull selection	1-2 (Default): pull-high to VTR_REG 2-3: pull-down
J22	CEC1736 GPIOs Header	For debug purpose
J23	CEC1736 GPIO1316/AP1_nRESET Pull selection	1-2 (Default): pull-high to VTR_REG 2-3: pull-down
J24	CEC1736 nRESET_IN pin	1-2 (Default): normal operation 2-3: hold CEC1736 in reset
J25	CEC1736 JTAG _STRAP pin	1-2: put in boundary scan mode 2-3 (Default): normal operation
J26	CEC1736 GPIO055 Strap Option	Don't Care
J27	CEC1736 I2C_ADDR0 Strap	1-2: pull-high to VTR_REG 2-3 (Default): pull-down
J28	CEC1736 CR_FLASH Strap	1-2 (Default): normal operation 2-3: Boot from crisis recovery flash component
J29	CEC1736 GPIO124 Strap Option	Don't Care
J30	CEC1736 BSTRAP Strap	1-2 (Default): normal operation 2-3: Boot from I2C or UART Crisis Port
J31	CEC1736 I2C_ADDR1 Strap	1-2: pull-high to VTR_REG 2-3 (Default): pull-down
J32	CEC1736 RESET_IN# Delay Circuit Power Source	1-2 (Default): connect +3.3V power 2-3: connect VTR_REG power
J33	CEC1736 PICKIT4 1x8 Header	For debug purpose
J34	CEC1736 32KHz Single-End Source	IN (Default): connect oscillator OUT: disconnect oscillator
J35	CEC1736 RESET_IN# delay circuit	IN (Default): connect delay circuit OUT: disconnect delay circuit
J36	CEC1736 GPIO157/LED1 & GPIO156/LED0 pins connection	1-2 (Default): connect GPIO157 to LED5 3-4 (Default): connect GPIO156 to LED6
J37	CEC1736 RESET_IN# pin ground	IN: hold CEC1736 in reset OUT (Default): normal operation
J38	CEC1736 UART0 debug header	For debug purpose
J39	MEC1723 Test Clocks Out header	For debug purpose
J40	MEC1723 32KHz Single-End Input selection (Optional)	1-2: connect to 32KHZ_IN pin 2-3: connect to XTAL2
J41	MEC1723 I2C02 channel header	For debug purpose
J42	MEC1723 I2C07 channel header	For debug purpose
J43	MEC1723 RESET_IN# delay circuit	IN: connect delay circuit OUT (Default): disconnect delay circuit
J44	MEC1723 RESET_IN# pin ground	IN: hold MEC1723 in reset OUT (Default): normal operation
J45	MEC1723 PICKIT4 1x8 Header	For debug purpose
J46	MEC1723 GPIO156/LED0, GPIO157/LED1, and GPIO153/LED2 pins connection	1-2 (Default): connect GPIO156 to LED9 3-4 (Default): connect GPIO157 to LED10 5-6 (Default): connect GPIO153 to LED11
J47	Dediprogram SPI Programming Header	Use for U8 PVT SPI Flash programming
J48	U8 SPI Flash power source selection	1-2 (Default): connect to board +3.3 power 2-3: connect Dediprogram +3.3 power
J49	MEC1723 XTAL2 selection	1-2 (Default): connect to 2-pin crystal 2-3: connect to single-end 32Khz source

Jumper Options

JUMPER OPTIONS

Jumper	Description	Details
J50	MEC1723 XTAL1 selection	IN (Default): connect to 2-pin crystal OUT: use single-end 32Khz source, floating
J51	U8 SPI Flash isolation jumper	1-2 (Default): connect U8 SPI_CLK 3-4 (Default): connect U8 SPI_IO0 5-6 (Default): connect U8 SPI_IO1 7-8 (Default): connect U8 SPI_CS# 9-10 (Default): connect U8 SPI_IO2 11-12 (Default): connect U8 SPI_IO3
J52	MEC1723 JTAG_STRAP pin	1-2: put in boundary scan mode 2-3 (Default): normal operation
J53	MEC1723 CMP_STRAP pin	Don't care
J54	MEC1723 CR_STRAP pin	1-2 (Default): boot from SHD_SPI flash via CEC1736 2-3: boot from PVT_SPI flash (U8)
J55	MEC1723 UART0 debug header	For debug purpose
J56	MEC1723 UART_BSTRAP pin	1-2 (Default): normal operation 2-3: Boot from UART Crisis Port
J57	MEC1723 BSS_STRAP pin	1-2 (Default): normal operation 2-3: Not boot in this application
J58	CEC1736 QSPI0 CS0 Pass/Failure Cases selection for demonstration purpose	1-2 (Default): normal pass case via U9 2-3: demo failure case via U11
J59	CEC1736 Flash Bus 1 Power select	1-2 (Default): connect to board +3.3 power 2-3: connect Dediprogram +3.3 power
J60	CEC1736 Flash Bus 2 Power select	1-2 (Default): connect to board +3.3 power 2-3: connect Dediprogram +3.3 power
J61	Dediprogram SPI Programming Header	Use for U9, U11 or U13 SPI Flash programming
J62	Dediprogram SPI Programming Header	Use for U10 or U12 SPI Flash programming
J63	U9/U11 or U13 SPI Flash Programming Selection	1-2 (Default): connect to U9/U11, select via J58 2-3: connect to U13
J64	U10 or U12 SPI Flash Programming Selection	1-2 (Default): connect to U10 2-3: connect to U12
J65	CEC1736 AP0_RESET# connect to MEC1723 RESET_IN#	IN (Default): connect OUT: disconnect

Chapter 6. Running Out-of-Box (OOB) Demo Code

This CEC1736 Development Board is designed to provide a great out-of-box experience with demonstration of key CEC1736 features.

To this end, the development board comes with a pre-programmed CEC1736 already installed with pre-defined OTP settings and Soteria-G3 firmware SPI Image.

The current demos include the following. More demos are being created and will be available via firmware upgrade.

1. Image authentication demo

- **AP image**

MEC1723 sends an I2C command to CEC1736 to authenticate the AP image, to show the current status and output to UART logs; then configure to a bad image destination and reset the CEC1736. The authentication will fail and perform golden image recovery. All the steps & status will output to UART logs.

- Soteria-G3 image

MEC1723 sends an I2C command to CEC1736 to get Soteria-G3 image authentication status and output to UART logs; then configure CEC1736 Tag0 set to a bad image location and reset the CEC1736, the authentication of bad image in Tag 0 will fail and the good image in Soteria-G3 firmware Tag 1 will be loaded. All the steps & status will output to UART logs.

2. SPI MON (Monitoring) filtering demo

- Opcode violation

Configure read, write but not allow erase permission in AP_CFG post-boot opcode settings; then MEC1723 (AP Host) performs an erase operation of any memory location on AP0 SPI Flash, CEC1736 will detect an OPCODE violation and reset MEC1723, all the steps & status will output to UART logs.

- Runtime violation

Configure to block the read operation in memory region protection of AP_CFG settings; then MEC1723 (AP Host) performs a read operation to this protected region on AP0 SPI Flash. CEC1736 will detect this read intervention runtime violation and reset MEC1723. All the steps & status will output to UART logs.

- Runtime authentication

Configure to allow read, write and erase permissions in AP_CFG pre-boot opcode settings; then MEC1723 (AP Host) reads AP0 SPI Flash a byte match image, and then a non-critical hash match image, read back image validation status as "Good to Go", then corrupt the non-critical hash match image and read the image validation status again. This time it should indicate that "FW is bad". All the steps & status will output to UART logs.

Running Out-of-Box (OOB) Demo Code

- Attestation (SPDM) demo

MEC1723 send a sequence of I2C commands to CEC1736 to fetch the entire certification chain from internal flash, then do the verification, then send “Challenge authentication” to CEC1736 to get the NONCE data and its signature back, and then verify the signature of the NONCE data. All the steps & status, data will output to UART logs.

3. Revocation demo

- Key Revocation

This demo will show how MEC1723 will fail to load an image after the key is revoked; all steps & status will output to UART logs.

- Roll back protection

This demo will show how MEC1723 will fail to load an older image after the FW revision has been updated; all steps & status will output to UART logs.

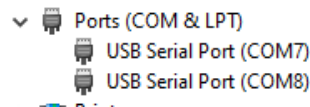
Note: Demos #1 demo is planned to be included and programed to the development board. Demos #2, #3, #4 and other future development demos will be included in a separated OOB Host sample code package releases from SDE when they're available.

Note: Please refer to OOB Demo Code release package App Note for details.

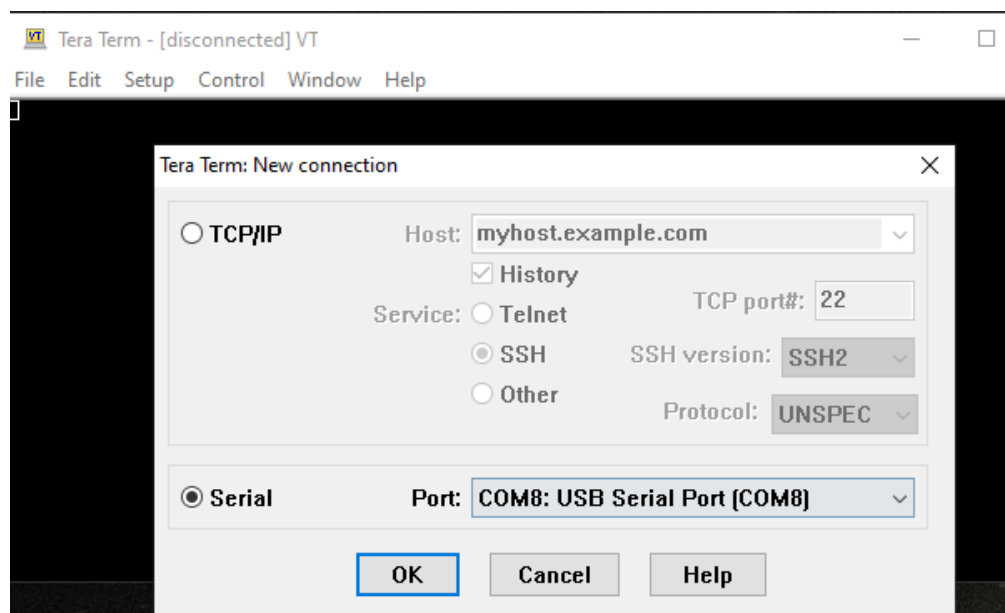
Note: Please contact your Microchip representative for any updated information.

The following step-by-step example shows CEC1736 Serial UART logs after the initial power-up of the development board:

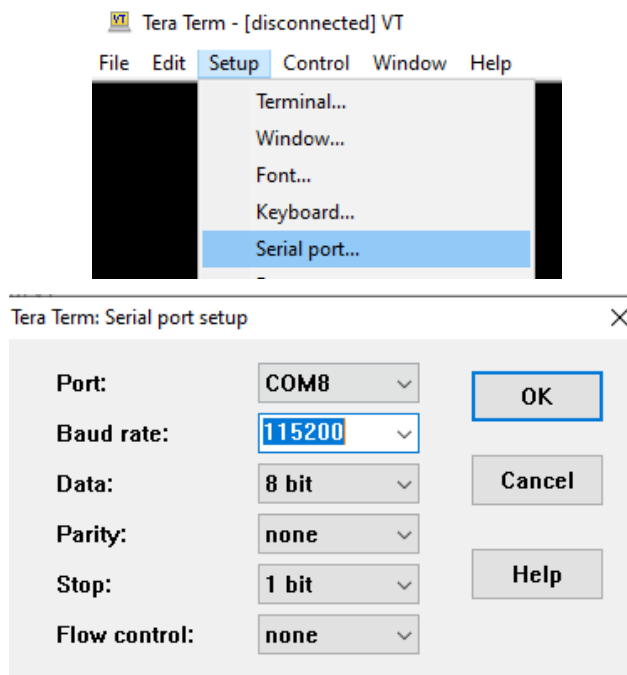
1. Plug-in a Micro-USB Cable from a PC USB Port to CEC1736 Development Board P2 Micro-USB Port for CEC1736, as shown in Chapter 4
2. Plug-in another Micro-USB Cable from a PC USB Port to CEC1736 Development Board P3 Micro-USB Port for MEC1723, as shown in Chapter 4
3. The connected PC Windows Device Manager should have the two USB Serial Ports (ex: COM7, COM8 as shown below) detected.



4. Open "Tera Term" Terminal and select "Serial" new COM port (ex: COM8).



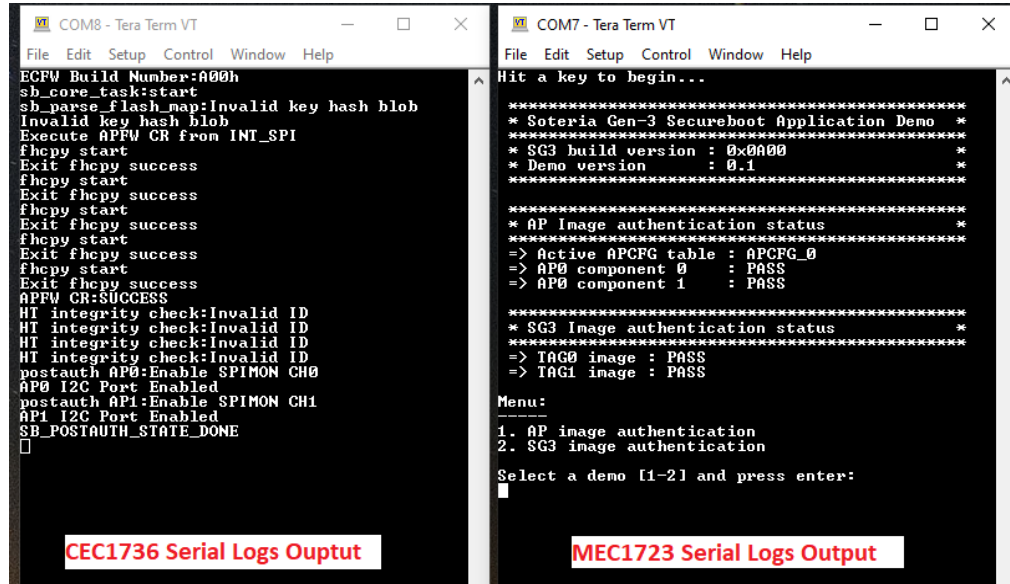
5. Go to "Setup" -> "Serial port", and select "115200-8-n-1-n".



6. Open another Tera Term to set COM7 using the same 115200-8-n-1-n setting.
7. Since the CEC1736 Soteria-G3 firmware has already executed when the board is powered-up, the initial UART logs were missing after the above setup. We can use S1 switch to reset the CEC1736, and the corresponding UART logs will appear as shown in the image below.

Note: Logs below are an example only, the actual results will depend on the test environment and Soteria-G3 firmware release version being used.

Running Out-of-Box (OOB) Demo Code



The image shows two terminal windows side-by-side. The left window, titled 'COM8 - Tera Term VT', displays a series of boot logs for CEC1736. The right window, titled 'COM7 - Tera Term VT', displays boot logs for MEC1723, including a menu for selecting a demo.

```
COM8 - Tera Term VT
File Edit Setup Control Window Help
ECFW Build Number:A00h
sb_core_task:start
sb_parse_flash_map:Invalid key hash blob
Invalid key hash blob
Execute APFW CR from INT_SPI
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
APFW CR:SUCCESS
HT integrity check:Invalid ID
HT integrity check:Invalid ID
HT integrity check:Invalid ID
HT integrity check:Invalid ID
postauth AP0:Enable SPIMON CH0
AP0 I2C Port Enabled
postauth AP1:Enable SPIMON CH1
AP1 I2C Port Enabled
SB_POSTAUTH_STATE_DONE
□

CEC1736 Serial Logs Ouptut
```

```
COM7 - Tera Term VT
File Edit Setup Control Window Help
Hit a key to begin...

*****
* Soteria Gen-3 Secureboot Application Demo *
*****
* SG3 build version : 0x0A00 *
* Demo version : 0.1 *
*****

*****
* AP Image authentication status *
*****
=> Active APCFG table : APCFG_0
=> AP0 component 0 : PASS
=> AP0 component 1 : PASS

*****
* SG3 Image authentication status *
*****
=> TAG0 image : PASS
=> TAG1 image : PASS

Menu:
-----
1. AP image authentication
2. SG3 image authentication

Select a demo [1-2] and press enter:
█

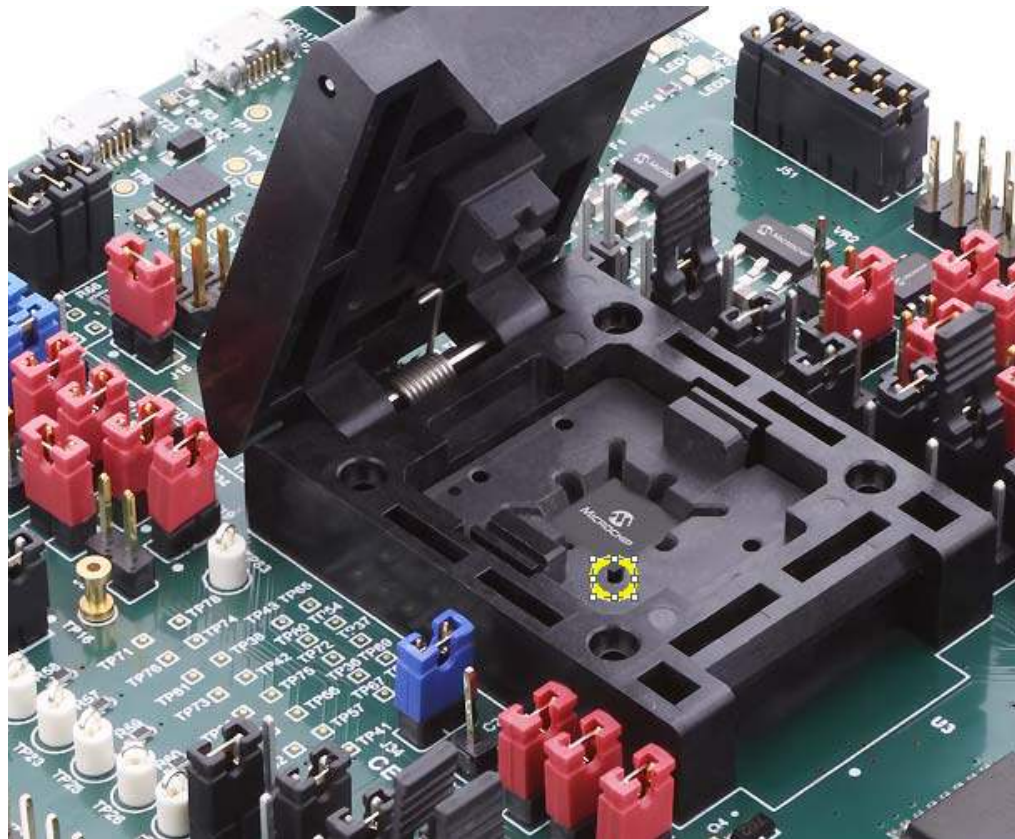
MEC1723 Serial Logs Output
```

Chapter 7. Getting Ready for Development

After the demonstration and evaluation stages, users may use this development board to customize their security features.

Firstly, users will need to create their own QTP package to request a production version of CEC1736-S0-I/2ZW (84-pin package) device(s) order.

Users will then be able to swap the new custom CEC1736 into the Development Board socket. Please make sure the small black dot on the device is pointing to the socket Pin 1 as shown in yellow mark below.



- Please refer to the Microchip Trust Platform Design Suite (TPDS) w/ CEC1736 enabled version package for the rest of the development steps and operations details.
- Please refer to Trust Platform Design Suite Quick Start Guide to learn about using the tools to provision the CEC1736.
- Please refer to MPLAB Harmony v3 User Guide to learn about using the tools to develop and customize CEC1736 peripherals such as UART, SPI, LEDs, PWM, etc.
- Please contact your local Microchip representative to access the Trust Platform Design Suite (TPDS), MPLAB Harmony v3 and related user guides. A Non-Disclosure Agreement (NDA) is needed.

7.1 EVALUATING CEC1736 WITH USER'S SYSTEM

Users may consider connecting the CEC1736 Development Board to the system for further evaluation and product development.

The CEC1736 development board has designed the way that we can disable the MEC1723 by changing the followings:

- Remove J65 to disconnect the CEC1736 AP0_RESET# to MEC1723 RESET_IN# pin
- Jumper the J43 and J44 to hold the MEC1723 in reset, and all the connected pins will be at input mode and tri-stated.
- Connect P4 (BMC Host Header) to the Platform AP0 interface
 - CEC1736 QSPI0_IN bus to AP0 QMSPI bus
 - CEC1736 AP0_RESET# to the AP0 reset pin
 - CEC1736 I2C channel to AP0 I2C channel
 - Other optional feature signals that required in the design
- If dual channels are used, connect P5 (CPU Host Header) to the Platform AP1 interface
 - CEC1736 QSPI1_IN bus to AP1 QMSPI bus
 - CEC1736 AP1_RESET# to the AP1 reset pin
 - Other optional feature signals that required in the design



MICROCHIP

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

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

ASIA/PACIFIC

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

EUROPE

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: 47-7288-4388

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