EV92R58A

ECC204 mikroBUS™ Evaluation Board User Guide

Introduction

The EV92R58A is an add-on board that demonstrates the capabilities of the Microchip ECC204. The ECC204 is intended for commercial and industrial applications that require asymmetric, custom PKI authentication.

The board is designed to be used with the CryptoAuth Trust Platform and other Microchip development platforms that contain a MikroElektronica mikroBUS™ header. The EV92R58A can also connect to any board that has the XPRO header by using the ATMBUSADAPTER-XPRO to ease development efforts. The on-board Microchip host and accessory devices simplify the development of your authentication system.

The EV92R58A contains the following Microchip devices: ATECC608B-TFLXTLS Host device, ECC204 accessory device with an I^2C interface and ECC204 accessory device using Microchip's proprietary SWI-PWM interface.

Figure 1. EV92R58A Board

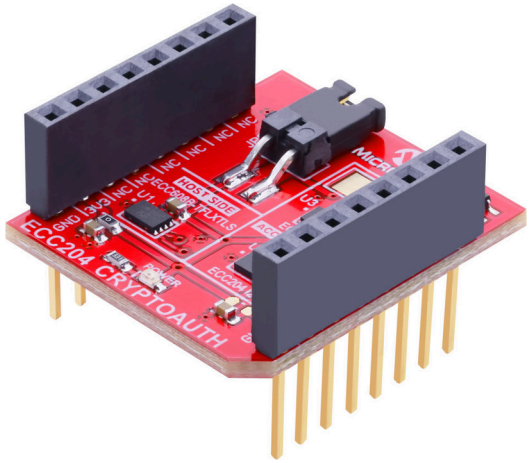


Table of Contents

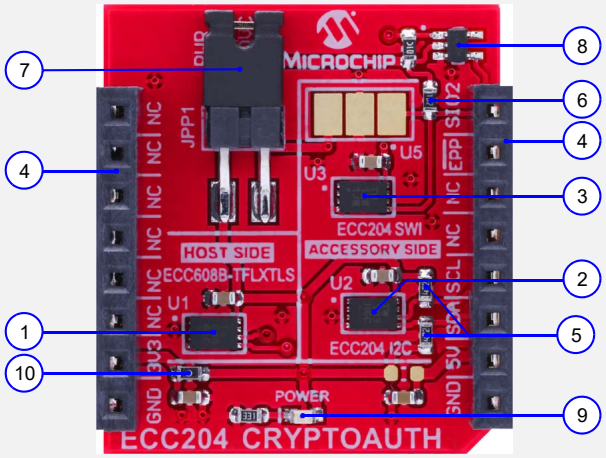
1. Hardware Description

This section details the key features of the EV92R58A and provides detailed board schematics and a list of other useful documentation.

1.1 Key Features

The most important features of the EV92R58A are highlighted in this section.

Figure 1-1. Part Identification

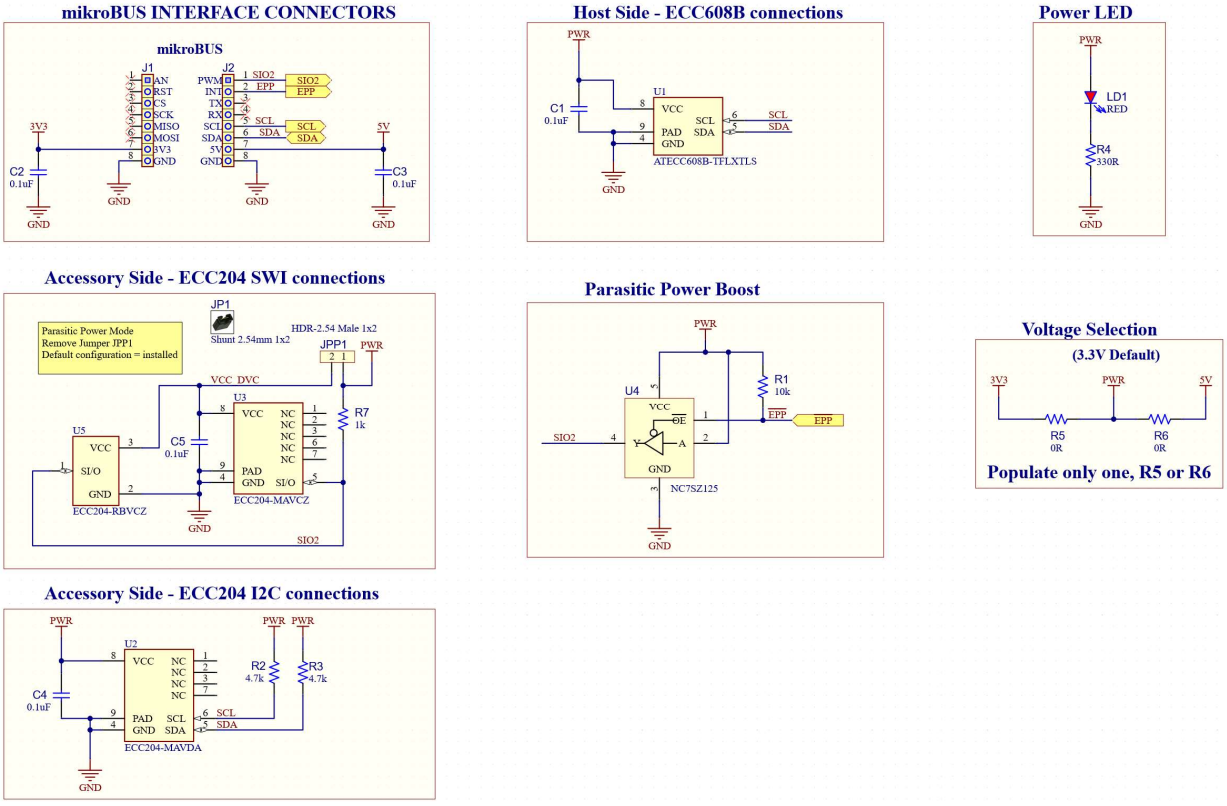


1. One ATECC608B-TFLXTLS Host TrustFLEX Device (U1)
2. One ECC204 I^2C Accessory Device (U2)
3. One ECC204 SWI-PWM Accessory Device (U3)
4. One mikroBUS Connector (J1, J2)
5. On-Board 4.7 kΩ I^2C Pull-Up Resistors (R2, R3)
6. On-Board 1.0 kΩ SWI-PWM Pull-Up Resistor (R7)
7. Jumper to select Parasitic Power mode (JPP1)
8. Parasitic Power boost circuitry (U4)
9. On-Board LED Power Indicator (LD1)
10. Zero-ohm Resistor Jumpers to Select 3.3V or 5V Power (3.3V Enabled by Default via R5)

Note: To enable 5V power, remove R5 and solder a zero-ohm resistor into R6.

1.2 Schematic

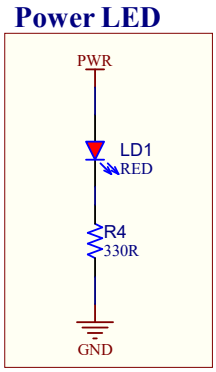
Figure 1-2. Top-Level Schematic



1.2.1 Power Indication

The red LED (LD1) illuminates when power is present on the circuit board.

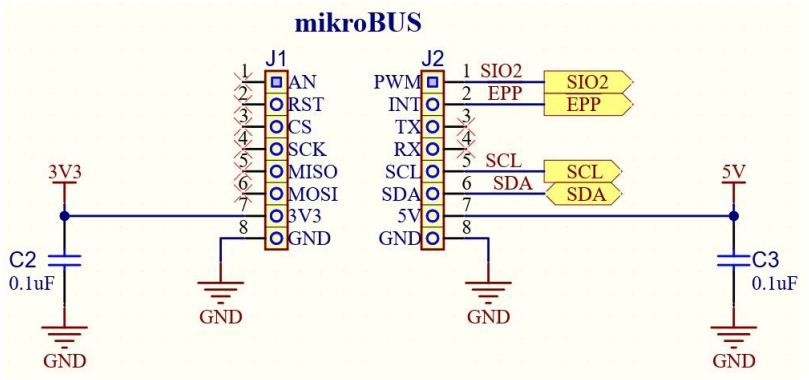
Figure 1-3. Power Indicator Schematic



1.2.2 MikroBUS™ Header

The ECC204 interface uses the standard mikroBUS header, which provides power, I²C and SWI-PWM connections.

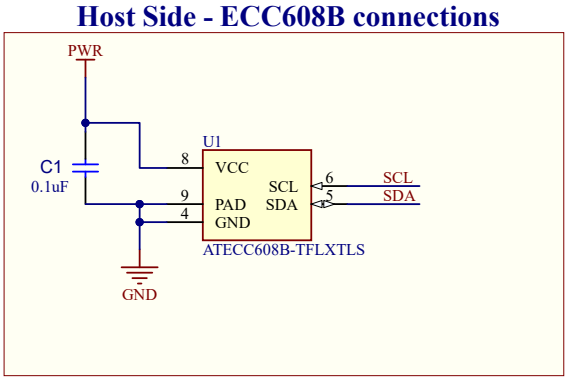
Figure 1-4. mikroBUS™ Header Connection



1.2.3 Host Side Device

The EV92R58A evaluation kit is populated with a Microchip ATECC608B-TFLXTLS host device. It offers pre-architected implementation for accessory authentication, firmware validation, secure boot assistance, key rotation and more. Compatible for AWS IoT, Microsoft Azure, Google Cloud Platform and, in general, any TLS networks with code examples for WolfSSL, mBedTLS, CycloneSSL.

Figure 1-5. Host Side Connection

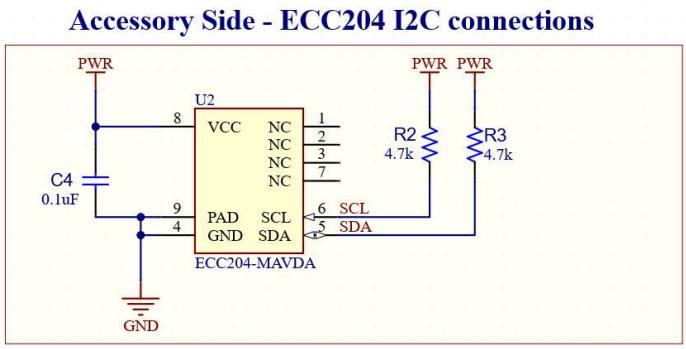


1.2.4 I²C Interface

Communication with the ECC204 and the ATECC608B-TFLXTLS I²C interface will use the standard I²C protocol. The ECC204 I²C interface supports a bit rate of up to 400 Kbps. The ATECC608B-TFLXTLS supports a bit rate of up to 1 Mbps. Both devices are connected to a common I²C interface.

- ATECC608B-TFLXTLS 7-Bit Address 0x36 (Write 0x6C, Read 0x6D)
- ECC204 7-Bit Address 0x33 (Write 0x66, Read 0x67)

Figure 1-6. I²C Connection

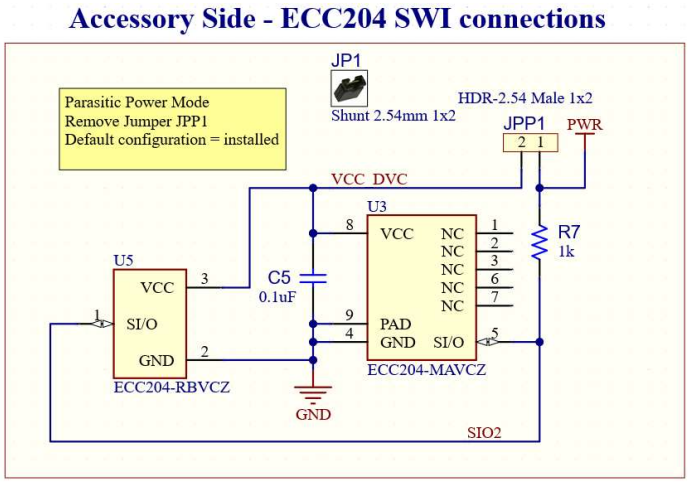


1.2.5 SWI-PWM Interface

Communication with Microchip's ECC204 in SWI-PWM mode is at 125 Kbps.

- ECC204 7-Bit Address 0x33 (Write 0x66, Read 0x67)

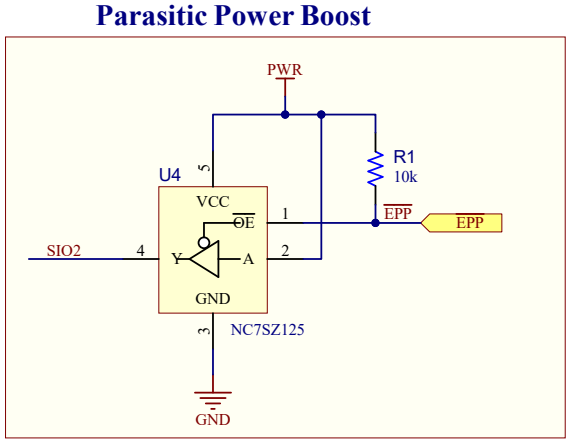
Figure 1-7. SWI-PWM Connection



1.2.5.1 Parasitic Power

The ECC204 has the capability to use parasitic power on the SWI-PWM device. The Parasitic Power mode removes the need for a dedicated power source to the crypto device. Power is supplied to the device by capacitor C5. The capacitor is charged when SIO_2 (SIO-PWM mode) is higher than VCC_DVC. For proper operation, VCC_DVC must always be greater than the minimum supply operating voltage of the device. See the specific device data sheet for more details and recommendations.

Figure 1-8. Parasitic Power Boost Circuitry



Follow these guidelines for proper circuitry usage:

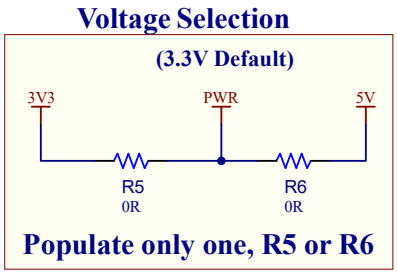
1. The device must be in Parasitic Power mode (remove jumper JPP1).
2. The EPP# signal must be initially asserted HIGH.
3. Issue a cryptography command.
4. Assert the EPP# signal LOW for the duration of the command.
5. Assert the EPP# signal HIGH.
6. Read back the command response.

Tip: The Parasitic Power Boost circuitry in general will not be needed. It is recommended that the EPP# signal be driven HIGH or allowed to float to disable the parasitic power circuitry if present. Special software will need to be written to incorporate control of the boost circuitry. This circuitry, in general, will be depopulated on the board.

1.2.6 Voltage Selection

The EV92R58A features the capability to choose the voltage for the board (3.3V or 5V) by installing the correct resistor configuration in the R5 or R6 positions. By default, R5 is installed for 3.3V power.

Figure 1-9. Voltage Selection



Note: Populate only one resistor, either R5 or R6, to select the input voltage for the board (3.3V or 5V).

1.3 Hardware Documentation

Additional documentation for the kit can be found on the Microchip website for the ECC204 Crypto Authentication (EV92R58A) development kit.

This includes:

- EV92R58A-Design-Documentation: Includes Schematics, BOM and 3D-Views
- EV92R58A-Gerber-files: Includes Gerber Files and Assembly Information Files
- ECC204 CryptoAuthentication Board User's Guide

Other useful documentation can be found at:

- CryptoAuth Trust Platform (DM320118)
- Crypto Authentication Starter Kit (DM320109)

2. Connecting the Board

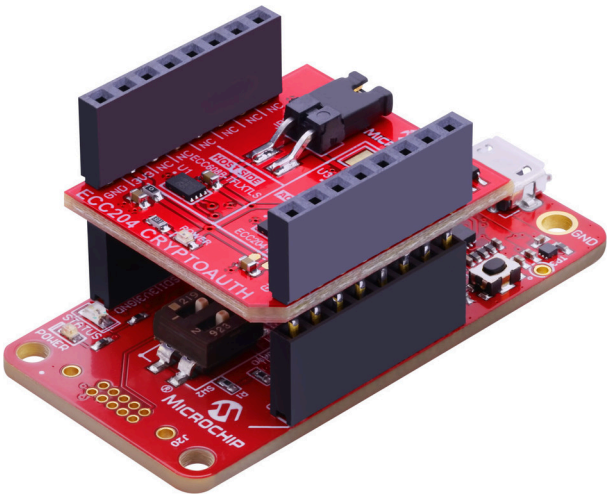
The form factor of the EV92R58A is consistent with Microchip's adoption of the mikroBUS connector on host boards. Many of Microchip's development platforms will support one or more mikroBUS interfaces. These include:

- Microchip Explorer 16/32 Development Board
- MPLAB® Xpress Evaluation Board
- Automotive Networking Development Board
- PIC Curiosity Boards
- PIC Curiosity Nano Boards
- AVR Curiosity Boards

2.1 mikroBUS Header

The EV92R58A development board has an I^2C interface and the SWI-PWM connection through the mikroBUS header. This enables communication to the host present on the Trust Platform or any of the PIC/AVR/SAM MCU host development boards with a mikroBUS header. Microchip's DM320118 Trust Platform board is designed to be a host platform to ease development for the EV92R58A. Using the USB port, the user can write host applications using Python scripts and access debug information. The DM320118 comes pre-loaded with Microchip's kit protocol. Additional documentation for the DM320118 kit can be found on the Microchip Website (DM320118).

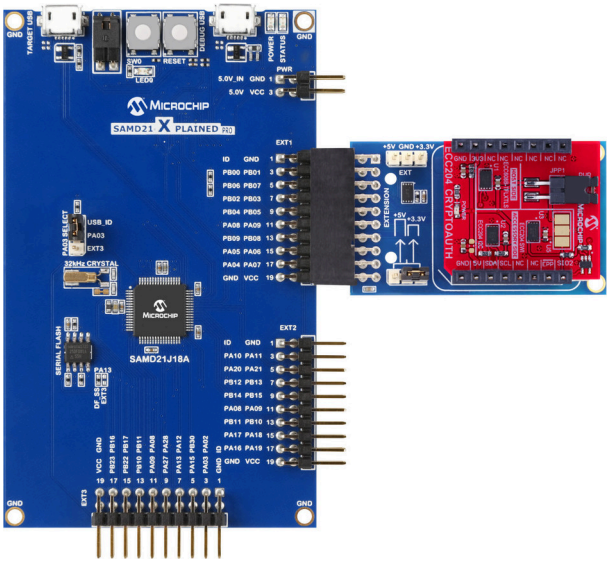
Figure 2-1. The EV92R58A Connected to the DM320118



2.2 Xplained Pro Connections

Some Microchip development boards support only the Xplained Pro extension headers. By using Microchip's ATMBUSADAPTER-XPRO adapter board, the EV92R58A can be connected to any development board that has the XPRO header. Microchip's DM320109 Starter kit provides the easiest way for configuring and using the EV92R58A. The on-board SAMD21-XPRO is pre-programmed with Microchip's Security Products Group (SPG) kit protocol. This protocol handles the communication between the CryptoAuthentication devices and the host system regardless of the device interface. The data transfer between the kit and the PC is indicated by the Status LED on the SAMD21 board. Additional documentation for the DM320109 kit can be found on the Microchip Website (DM320109).

Figure 2-2. The EV92R58A Connected to an Xplained Pro Development Platform (DM320109)



3. Software Requirements

The EV92R58A development board does not have a microcontroller on board and, therefore, does not require firmware. The board was, however, defined and developed in conjunction with other Microchip development boards that do have firmware requirements. The specific boards highlighted in 2. Connecting the Board define those boards that can be used with this development board. Other boards may also be capable of being used with the EV92R58A development kit.

Additional software tools were also created by Microchip and are made available either for free or under NDA. These include C-language libraries, Python libraries and the Trust Platform Design Suite (TPDS) of tools for rapid application development.

3.1 Firmware Requirements

For each new device type added to Microchip's family of secure products, the firmware of the host application board or boards that it is used with must be updated. This firmware is typically referred to as “Kit Protocol” and allows for identification of the device or devices on the board. It provides the basic infrastructure to communicate to the boards with higher-level software tools.

It is recommended that the host application boards be kept up-to-date with the latest version of the firmware to take advantage of any enhancements or bug fixes that may have been implemented. The latest version of the software can be downloaded from the kit website along with the procedure on how to upgrade the Kit Protocol firmware on the board.

Firmware Requirements

- DM320118 – Trust Platform Development Board
  - Firmware Revision: 3.0.8 or Higher
- DM32109 – CryptoAuthentication Starter Kit
  - Firmware Revision: 3.0.8 or Higher

3.2 Software Tools

Microchip provides additional software tools that aid in the rapid development of applications. These include software libraries, development tools and example applications. Whenever new versions of CryptoAuthentication devices are developed, the library has to be upgraded to implement the new capabilities of the device. It is recommended that the latest version of these tools always be downloaded and implemented to take advantage of any enhancements and bug features.

CryptoAuthLibrary (CAL) – C Language

CryptoAuthLib is a software support library for the majority of Microchip security devices, including the ECC204 devices, written in C code. It is a portable, extensible, powerful and easy-to-use library for working with devices in the CryptoAuthentication device families by providing common APIs and command structures.

The library is designed with a Hardware Abstraction Layer (HAL) so that it can be readily ported for use with both Microchip and non-Microchip microcontrollers. The library can be readily included into MPLAB X or Microchip Studio projects and is integrated into the MPLAB Harmony framework.

Important: CAL Requirements:

- ECC204 requires CAL Version: 3.4.1 or Higher

CryptoAuthLibrary (CAL) – Python

A Python version of CAL is also available to allow for the development of system-level applications from a PC environment without having to reprogram a microcontroller. Applications can, thus, be developed in a generic way

prior to porting to a specific microcontroller. The python version of the library has all the capabilities of the C-version of the library and the commands were made syntax-consistent with the C-version of the library.

Important: CAL Python Requirements:

- ECC204 requires Python CAL Version: cryptoauthlib 20221114 or higher.
- Python Version 3.8 or higher is recommended

Trust Platform Design Suite

To simplify the implementation process, Microchip offers the web-based Trust Platform Design Suite (TPDS) tools that will allow developers to go from concept to production via a guided flow. The Trust Platform tools allow you to develop and construct the transaction diagrams and code necessary to implement a particular application within the constraints of the configuration and defined access policies. Specific Trust variants of the ECC204 will be developed over time. The ECC204 devices on this board are generic devices. The ECC608-TFLXTLS host device on this board is compatible with the TPDS tools.

More information on these tools can be found under Microchip's Security ICs section of the webpage Security ICs.

4. Revision History

Revision A (November 2022)

- Initial release of this document

Microchip Information

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.

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, 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, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, 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, Clockstudio, 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, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, 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, Trusted Time, 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, and Symmcom 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.

ISBN: 978-1-6683-0992-6

Quality Management System

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

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