DT100104

ATECC608A Trust Development Board User's Guide

Introduction

The ATECC608A Trust Development Board is an add-on board for the CryptoAuth Trust Platform and other Microchip development platforms that contain a MikroElektronika mikroBUS™ header. The board connects to any board that has a host mikroBUS connection. This board provides an alternative to the sample units that require a socket board to perform initial development and testing.

The ATECC608A Trust Development Board contains the ATECC608A-TNGTLS (Trust&GO), ATECC608A-TFLXTLS (TrustFLEX) and ATECC608A-MAHDA (TrustCUSTOM) secure elements. This provides a user the ability to develop solutions with any of these devices based on the requirements of the application. The user's guide provides a physical overview of the connections and switch settings implemented on the board.

Figure 1. Front View

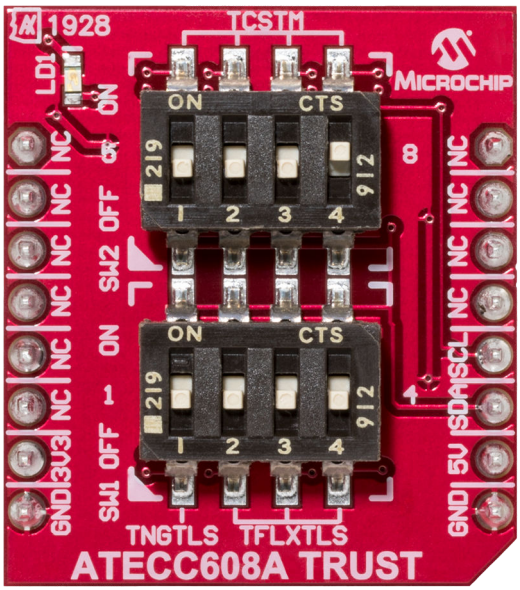


Figure 2. Back View

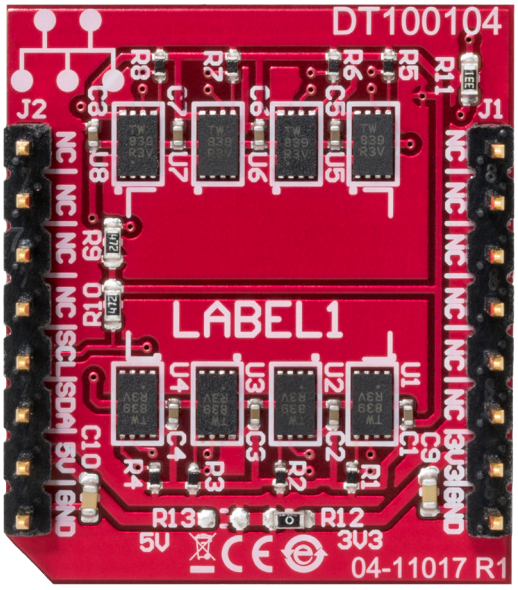


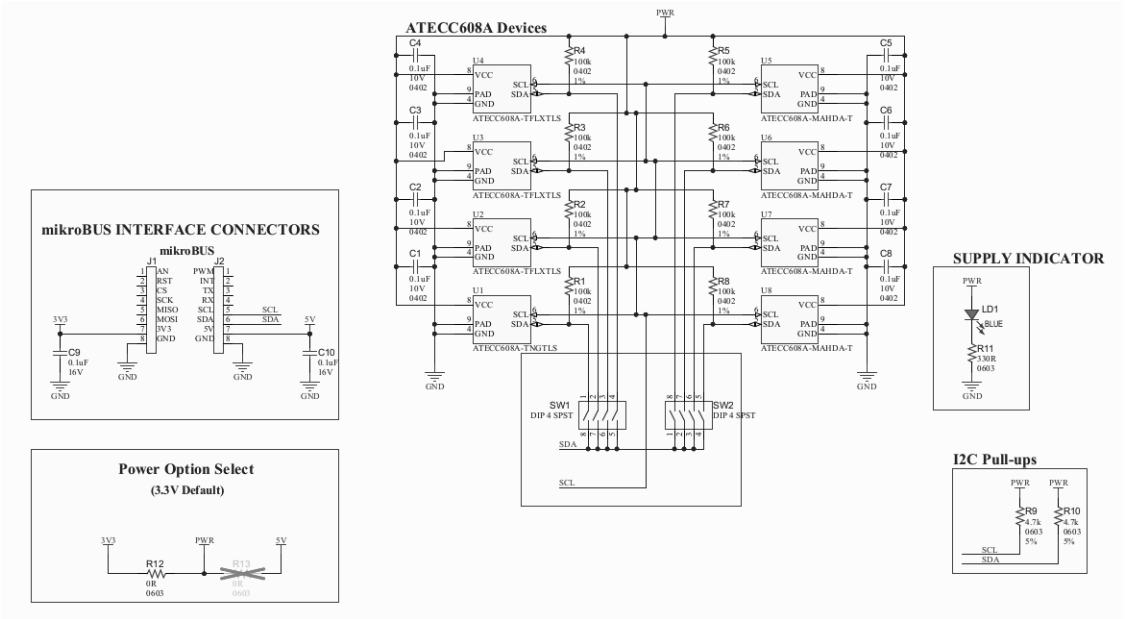
Table of Contents

1. Hardware Description

1.1 Schematic and Key Features

- One ATECC608A-TNGTLS Trust&GO Device (U1)
- Three ATECC608A-TFLXTLS Prototype TrustFLEX Devices (U2, U3, U4)
- Four ATECC608A-MAHDA TrustCUSTOM Devices (U5, U6, U7, U8)
- Two 4-Position SPST DIP Switches for Device Selection (SW1, SW2)
- One mikroBUS Connector (J1, J2)
- On-Board 4.7k I^2C Pull-Up Resistors (R9, R10)
- On-Board LED Power Indicator (LD1)
- Zero-Ohm Resistor Jumpers to Select a 3.3V or 5V Power (3.3V Enabled by Default via R12)
  Note: To enable a 5V power, remove R12 and solder a zero-ohm resistor into R11.

Figure 1-1. ATECC608A Trust Development Board Schematic



1.2 Device Selection

Devices Hardware Selection

Each secure element has a switch connection that enables the user to select a given device. Slide the DIP switch to the ON state to enable the device selection. Selecting the device connects the corresponding SDA line through the DIP switch. The SCL signals of all eight devices are connected together. A large value pull-up resistor on each SDA line of each device keeps the device in a low-current state when not selected. Note that the switch number shown on the top of the board (***not the number on the switch***) corresponds to the device identifier U# on the back of the board.

Figure 1-2. Device Selection

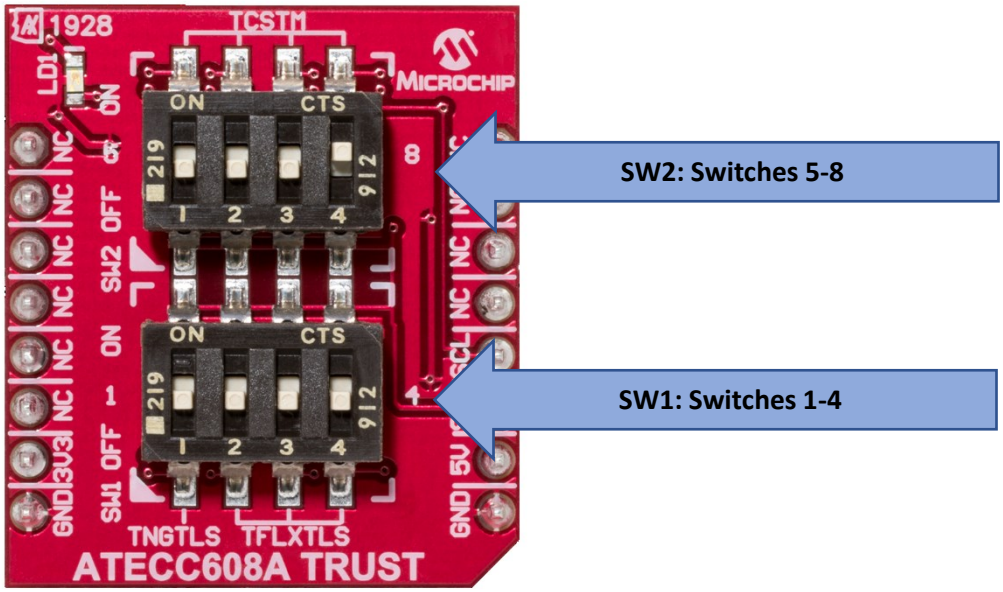


Table 1-1. Device Selection Switches

Switch #	DIP Switch	Secure Element	Trust Element Type
SW1	1	ATECC608A-TNGTLS	Trust&GO
	2, 3, 4	ATECC608A-TFLXTLS	TrustFLEX
SW2	5, 6, 7, 8	ATECC608A-MAHDA	TrustCUSTOM

Devices Software Selection

Once a specific device is selected, a specific I^2C address must be used to address the given device type. While each device is initially programmed with a default I^2C address, it is possible to overwrite this address. See the specific device data sheets for more information.

Table 1-2. Default I^2C Addresses

Device	Default 7-bit I^2C Address	8-bit Programmed I^2C Address Value(1)
ATECC608A-TNGTLS	0x35	0x6A
ATECC608A-TFLXTLS	0x36	0x6C
ATECC608A-MAHDA	0x60	0xC0

Note:

1. This is the I2C_Address byte value programmed into the ATECC608A device.

Note that multiple devices can be enabled provided they have different I^2C addresses. If multiple devices with the same address are selected, a failure occurs due to a conflict on the I^2C bus.

1.3 Hardware Documentation

Additional documentation for the kit can be found on the Microchip website for the ATECC608A Trust (DT100104) development kit.

This includes:

1. Board design documentation including schematics/3D views.
2. Gerber files.
3. ATECC608A Trust Development Board User's Guide.

2. Connecting the Board

The form factor of the ATECC608A Trust Development Board was chosen because Microchip has heavily adopted the use 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 Nano Boards

2.1 CryptoAuth Trust Platform Connections

The ATECC608A Trust Development Board has an I^2C connection through the mikroBUS header that enables it to connect to the mikroBUS host header present on the Trust Platform, or any of the PIC/AVR/SAM MCU host development boards that have a mikroBUS header.

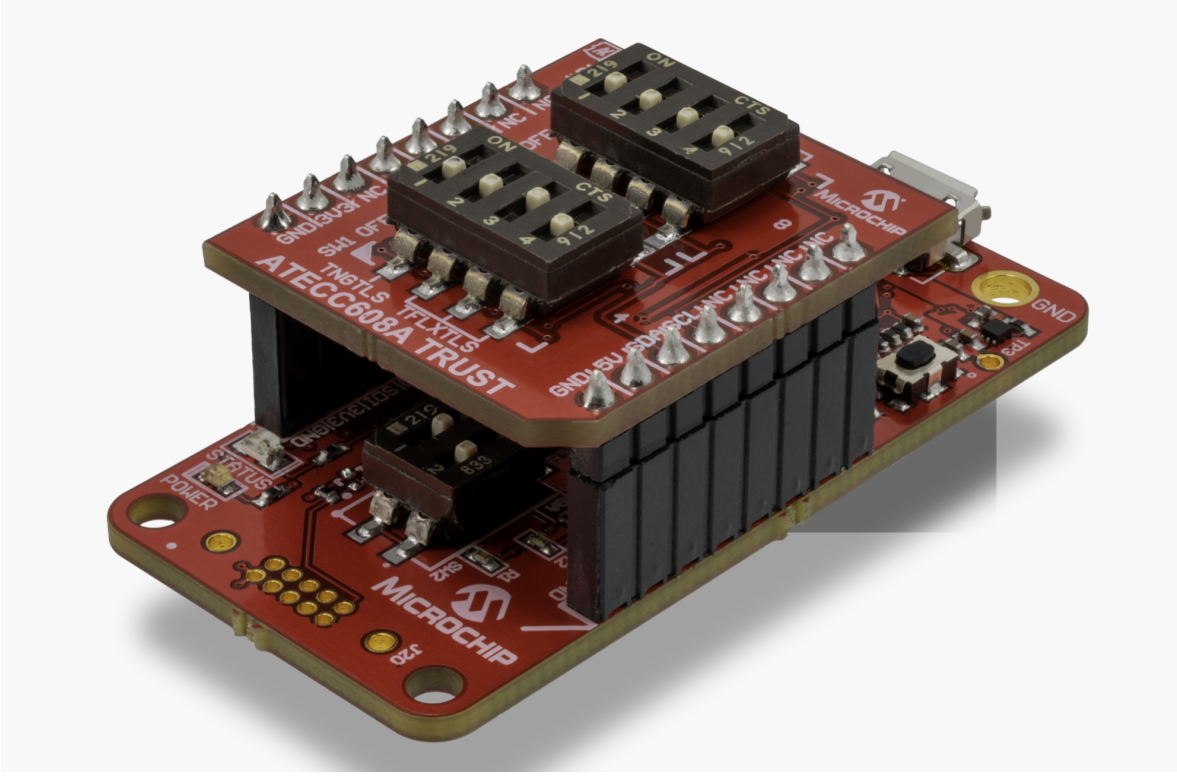
Connecting the ATECC608A Trust Development Board to the CryptoAuth Trust Platform

1. Set the switches on the CryptoAuth Trust Platform to enable the mikroBUS header and disable the on-board devices. This setting is highlighted in Bold and Italic below:

Switch Settings		What is Enabled	
SW2_1	**SW2_2**	**mikroBUS™ Header**	**On-Board Devices**
ON	ON	Yes	Yes
OFF	ON	No	Yes
ON	***OFF***	***Yes***	***No***
OFF	OFF	No	No

2. Connect the two boards as shown in Figure 2-1.

Figure 2-1. ATECC608A Trust Connected to a CryptoAuth Trust Platform Development Board



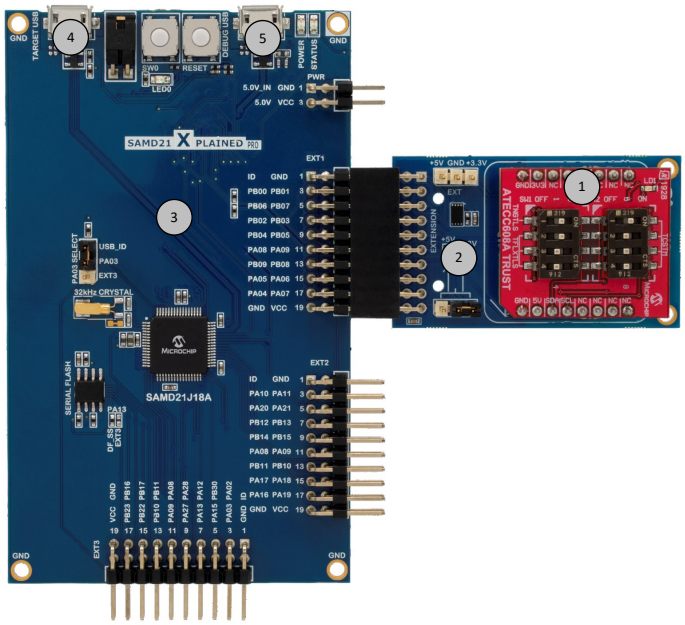
Attention: The angled notch on the ATECC608A Trust Development Board must be aligned with the angled line on the silk screen near the mikroBUS connector.

3. Select the device that you want to connect to the host via the DIP switches shown on the ATECC608A Trust Development Board. Switch 3 is on and all others are off. This selects an ATECC608A-TFLXTLS device.
4. Connect a USB cable between the CryptoAuth Trust Platform on the host system where the software is developed.
5. Invoke the software tools for the given application or the use case that is being developed.

2.2 Xplained Pro Connections

Some Microchip development boards support only the Xplained Pro extension headers. Through use of an adapter board, the ATECC608A Trust Development Board can still be used. Figure 2-2 shows the full assembly of the ATECC608A Trust Development Board, the ATMBUSADAPTER-XPRO and an ATSAMD21-XPRO Development Board.

Figure 2-2. Connections to an Xplained Pro Development Platform



1. ATECC608A Trust Development Board
2. ATMBUSADAPTER-XPRO
3. ATSAMD21-XPRO Development Board
4. TARGET USB Port
5. DEBUG USB Port

How to Connect the ATECC608A Trust Development Board to an Xplained Pro Host Board

1. Connect the ATMBUSADAPTER to the ATECC608A Trust Development Board as shown in Figure 2-2.
2. Connect the combined ATMBUSADAPTER and ATECC608A Trust Development Board to one of the XPRO extension connectors on the host board. EXT1 has been used in Figure 2-2.
3. Set the switch or switches on the ATECC608A Trust Development Board to enable the device you want to connect to.
   Note: The switch settings, as shown, enable one each of the ATECC608A-TNGTLS, ATECC608A-TFLXTLS and ATECC608A-MAHDA TrustCUSTOM devices. This is legal because all the I^2C addresses for the selected devices are unique. In general, only one device will be selected.
4. Connect the USB cables to the TARGET USB Port and the DEBUG USB Port and the host system.
5. Invoke the appropriate software development tools for the application.

3. Document Revision History

Revision A (September 2019)

- Initial release of this document

The Microchip Website

Microchip provides online support via our website at http://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 http://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: http://www.microchip.com/support

Microchip Devices Code Protection Feature

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.

Legal Notice

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

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, Vite, 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, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, 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, 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.

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: 978-1-5224-5087-0

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit http://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: http://www.microchip.com/support Web Address: http://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: 45-4450-2828 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 **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

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Microchip:
DT100104