# Secret Exchange for TrustFLEX Platform

## Overview:

This document explains the steps involved in secret exchange, Certificate signing and creating a support case to track the status of the secure provisioning of the TrustFLEX device selected.

If this document is being followed, then the following steps must have been completed:

- Defined the application and the use case with the Trust Platform Design Suite and ready to order pre-provisioned secure elements from Microchip with "production based crypto keys"
- myMicrochip account has been setup.

This document covers detailed steps that are carried out for Microchip to provision the TrustFLEX devices to the user-defined specifications.

## 1. myMicrochip Account Creation:

- If the account already exists, then you can skip this step.

- Create the myMicorchip account by clicking HERE

- Enter the details and complete the registration.

- There will be email confirming link sent to the email used for the registration.

## 2. Support Case Creation:

- Once the account is created, the next step is to create support case

- Visit the Microchip Case Console. Log in with the email address used to create the myMicrochip account
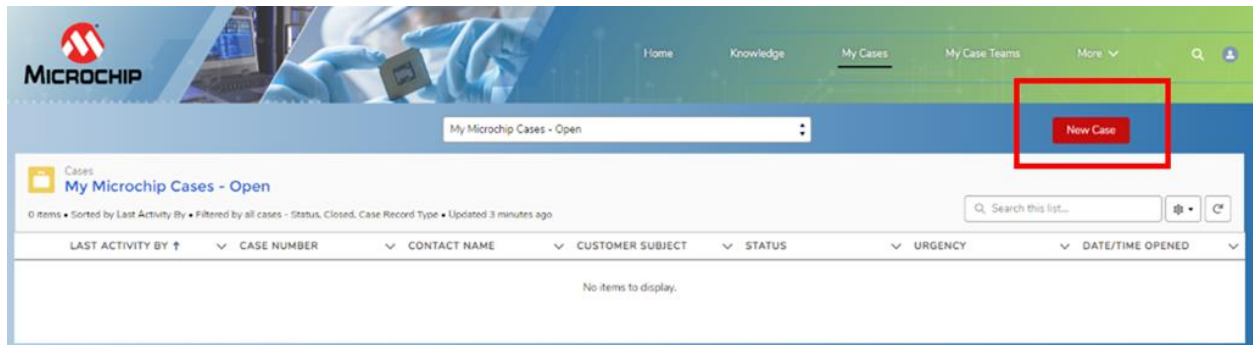
**Note: The URL can also be visited in the later stage to check the support case status.**

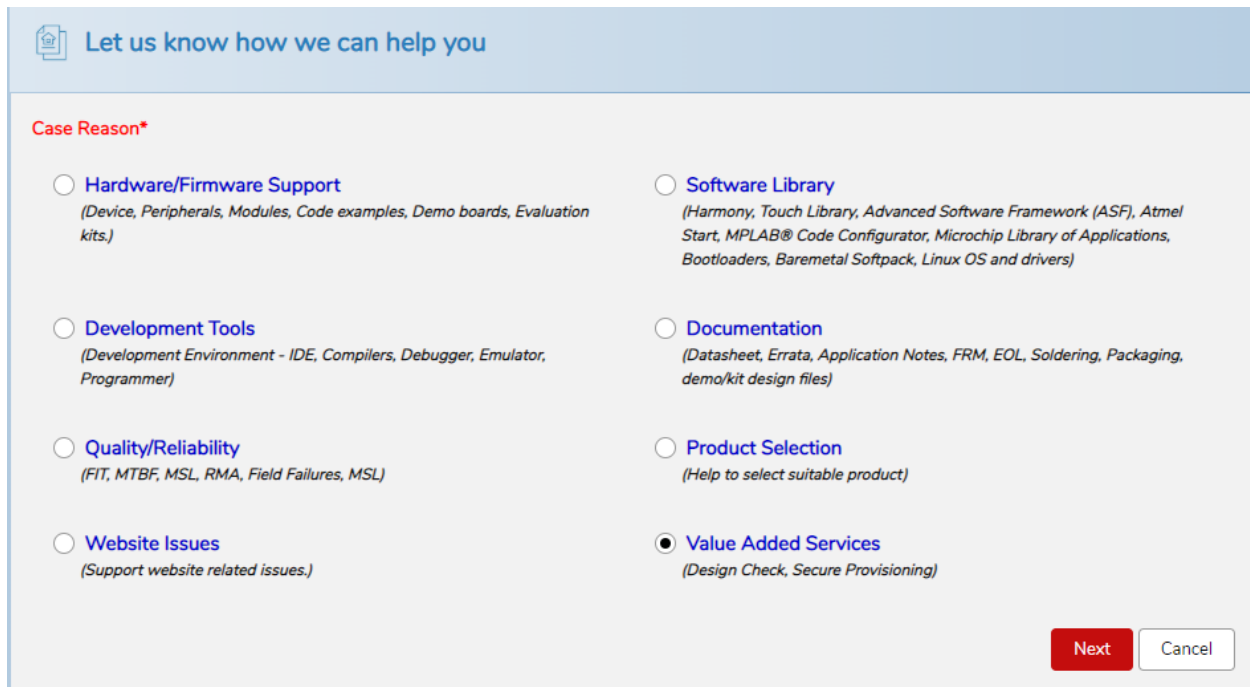Fig 2.1: Login Page for the support case console
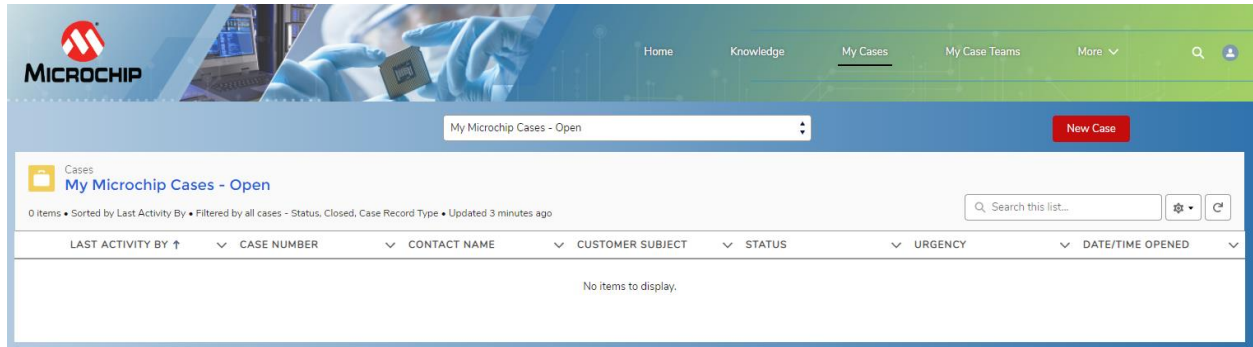


- Click on the "My Cases" tab and select the New Case option present on the top right corner of the page.

Fig 2.2: New Case



- Now select "Value Added Services" and then click on Next.

Fig 2.3: Selecting options



- In the subject line enter the company details, select the target device.

- If the case is being created for the TrustCUSTOM device, enter "ATECC608A-TCSM" as the Target Device, "Provisioning Services" in the Category selection, and "TrustCUSTOM" in Sub-Category as shown below.  Then click Next.

Fig 2.4: Adding details for TrustCUSTOM



- If the case is being created for the TrustFLEX device, enter "ATECC608A-TFLXTLS" as the Target Device, "Provisioning Services" in the Category selection, and "TrustFLEX" in Sub-Category as shown below.  Then click Next.

Fig 2.5: Adding details for TrustFlex



- In the Ticket Description, Enter the following details and click next:
  - **Program Name:** This will be a short name that will help in differentiating the specific TrustFLEX configuration from several other TrustFLEX configurations present.

  - **Version Number:** This will be a short number that will help to differentiate different configurations under the same program name.

  - **Comments:** This is a short description that will be displayed on the E-Commerce portal, that will help describe more about the program.

© 2019 Microchip Technology

- o **MicrochipDirect Email address:** Please provide the email address that is used to register at www.microchipdirect.com  this email address will be used to authorize the purchase of the product that contains the configuration/secrets that will be provided in this ticket portal.

**Note: Please ensure that you provide correct email address(es), as this will be the only account that will be authorized to purchase product with the shared secret.**

Fig 2.6: Adding Description



- The Design Stage and Urgency are default entered. They can be changed as required. Enter any other required information in Application Details option and click on "Submit".

Fig 2.7: Project Information

- Once submitted, if there are any files to be uploaded it can be done now and then click "Done".

Fig 2.8: Final Submitted Page



- Case home page after the case is created.

Fig 2.9: Case Homepage



- Questions and comments can be added by clicking on the "Add Comment" option.

## 3. Secret Exchange:

- In order to begin with the Secret Exchange, user will have to enter their final production based crypto keys in the TrustFlex Configurator Tool that is available in the Trust Platform Design Suite.

- If custom PKI certificate option is selected, the tool will require you to enter MAN ID (Manufacturing ID).
  - You will receive this ID information in the support ticket from MCHP

- Once all crypto keys and details are entered in the TrustFlex Configurator tool, you can click on 'Generate TFLXTLS Provisioning Package' and this will download the XML file along with a few source files that are meant to be integrated into the embedded firmware project.

**Note: The XML file at this stage contains secrets that are still not encrypted, and so special handling of the file is required at this stage**

- Microchip will send RSA encryption keys (typically three different keys) via support ticket portal, which are the public keys for the production HSMs (Hardware Security Module).

- This key should be used along with the XML file in a encryption utility *"MicrochipEncryptionUtility.exe"* that is available in the Trust Platform Design Suite.

- In the utility, click 'Device' and select ATECC608A. Click on 'Load RSA Public Key' and select the public key file that is sent in the support ticket by MCHP

Fig 3.1: Loading RSA Public Key
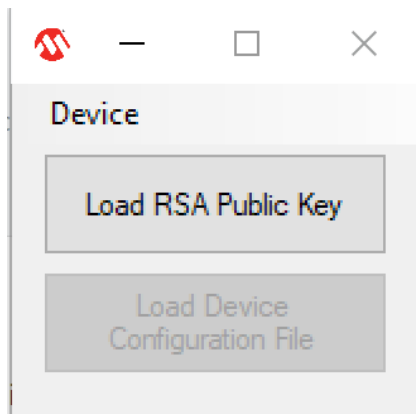


- Select the 'Load Device Configuration File' and browse to the file that is generated by the TrustFlex configurator tool and this step will encrypt the file and a new ATECC608A-TFLXxx_SITE.enc.xml file will be generated and stored.

- The secrets that are entered in the XML file, once encrypted can only be decrypted by our Hardware Security Modules in a protected area and the keys are never exposed.

**Note 1: The unencrypted XML file having the secrets must be stored in a safe and secure location. Microchip does not take responsibility of the un-encrypted XML file.**

**Note 2: Make sure that while uploading the file, it must be encrypted with the RSA keys provided by Microchip that will be shared in the system. Uploading an unencrypted file leads to the probability of exposing the customer`s sensitive data.**

## 4. Signature Exchange:

- Along with secret exchange, signature exchange must also be implemented *if custom certificate option* is selected in the TrustFlex configurator.

**Note: This step is required, if the user selects custom Certificate option in the TFLX configurator**

Fig 4.1:



- This requires a Certificate Authority to be established for the product eco-system.
  - Can be a root certificate authority (with self-sign certificate)
  - Intermediate certificate authority that chains back to the root.

- This certificate authority will be used to sign the Microchip production signers which will sign the device certificates.

- If the own root certificate is established careful security provisions must be observed. Protection of the root private key is of at most importance as it forms the backbone of the entire authentication process.

**Note: Microchip is not responsible for setting up of customer's root certificate and root private key protection.**

- Microchip generates the signer certificates for our production signers to be used for the provisioning of the devices and the Certificate Signing Requests will be sent in the support case

- Once the signer certificates are signed by the root signer they are locked and cannot be modified. These signed certificates will be sent back to Microchip.

## 5. Placing order with Provisioned keys:

- Once MCHP receives the encrypted configuration file (along with signed certificates if 'custom certificate' option is selected), then Microchip support team will respond back on the case to notify the user to proceed with ordering verification samples and the production units.

- Log into the microchipdirect.com account (with the email address provided in the case that is associated with the configuration file) and there will be a screen as shown in Fig 5.1 for all the device configurations registered to your email address.

- Customer will be able to order 20 (default qty) verification samples that will be shipped. If more than 20 samples are needed, user must specify that in the ticket at the time of exchanging the configuration files.

Fig 5.1: MicrochipDirect – Trust Platform Page for registered accounts
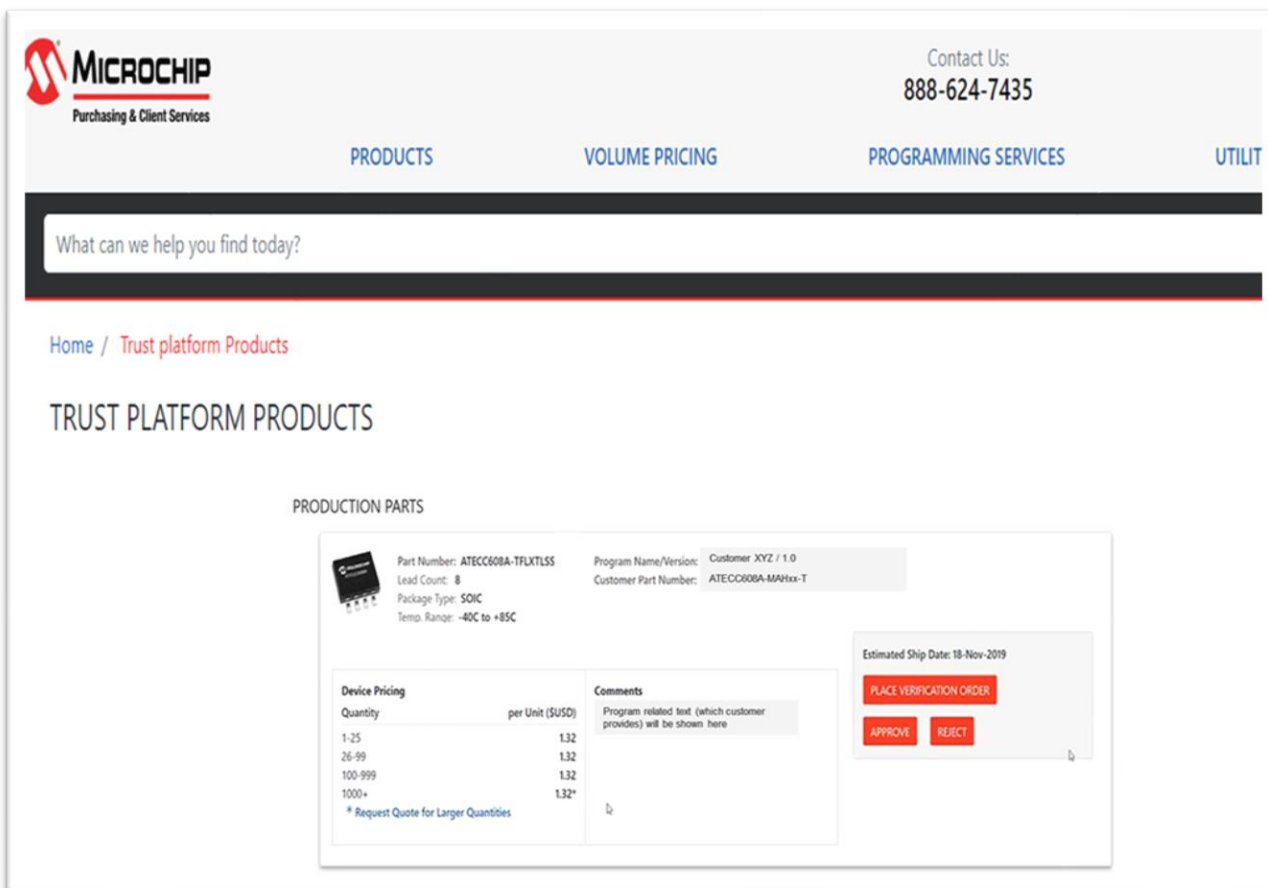
If the user logs into MicrochipDirect account with the email account that is **unregistered** (Log-in email address not sent in the ticket support portal where the secret exchange steps are handled), user will not be able to see the specific configuration and instead will see a page similar to below:

Fig 5.2: MicrochipDirect – Trust Platform Page for unregistered accounts



　　　　　　　　　　　　　　　　　　　　© 2019 Microchip Technology
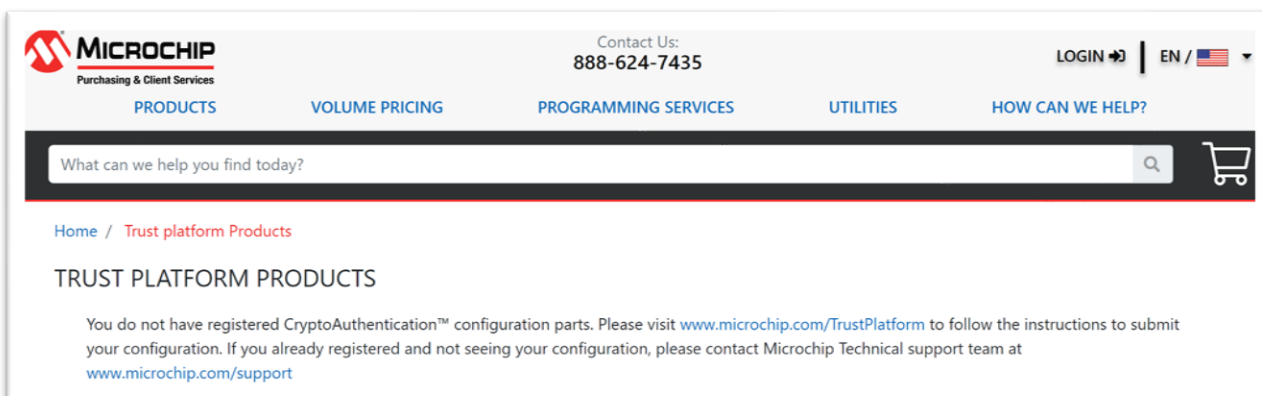
- For registered account, By clicking on the "Place verification order" button, the verification parts can be ordered so that the user can verify if the parts work for their application and have been provisioned correctly with the shared secrets.

- Once the parts are tested and they are successfully working with the application, then log back to MicrochipDirect and click on Approve or Reject the verification samples.

    o If approved is selected, then there will be screen as shown below where the production orders can be placed.

**Note: For the TrustFLEX devices the minimum order quantity is 2000 units. Each order can contain any number of units above 2000. There will be MoQ limit for every order.**

Fig 5.3: Ordering Production Parts



- Once the parts are ordered and are shipped by Microchip, user can log back into MicrochipDirect and view the "Order History" tab to find the option to "Download Manifest" for shipped parts.

- Manifest file format details can be found in the Trust Platform Design Suite

Fig 5.3: Download the Manifest file

| Order Date | PO Number | Order Status | Web Order Number | Recipient Name | Order Total (USD) |
|---|---|---|---|---|---|

Part Number: **ATECC608A-TFLXTLS**
Customer Part Number: **N/A**

**BUY IT AGAIN**    **Cancel or Return**

**Download Manifest**

Quantity: **10**
Unit Price:
Line Total: :

Line Status: **Invoiced**
Request Arrival Date: **09-Sep-2019**
Estimated Ship Date: **18-Sep-2019**
Delivery Date:  **21-Sep-2019**
Shipping Method: **FedEx Thailand to USA or US to USA**
Tracking Number:
Invoice Number:

## The Microchip Web Site

Microchip provides online support via our web site at http://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 (FAQ), 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

## 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 http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

## 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

## 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, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, 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, 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, motorBench, 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.

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.

## 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.

# Worldwide Sales and Service

| AMERICAS | ASIA/PACIFIC | ASIA/PACIFIC | EUROPE |
|---|---|---|---|
| **Corporate Office**<br>2355 West Chandler Blvd.<br>Chandler, AZ 85224-6199<br>Tel: 480-792-7200<br>Fax: 480-792-7277<br>Technical Support:<br>http://www.microchip.com/<br>support<br>Web Address:<br>www.microchip.com<br>**Atlanta**<br>Duluth, GA<br>Tel: 678-957-9614<br>Fax: 678-957-1455<br>**Austin, TX**<br>Tel: 512-257-3370<br>**Boston**<br>Westborough, MA<br>Tel: 774-760-0087<br>Fax: 774-760-0088<br>**Chicago**<br>Itasca, IL<br>Tel: 630-285-0071<br>Fax: 630-285-0075<br>**Dallas**<br>Addison, TX<br>Tel: 972-818-7423<br>Fax: 972-818-2924<br>**Detroit**<br>Novi, MI<br>Tel: 248-848-4000<br>**Houston, TX**<br>Tel: 281-894-5983<br>**Indianapolis**<br>Noblesville, IN<br>Tel: 317-773-8323<br>Fax: 317-773-5453<br>Tel: 317-536-2380<br>**Los Angeles**<br>Mission Viejo, CA<br>Tel: 949-462-9523<br>Fax: 949-462-9608<br>Tel: 951-273-7800<br>**Raleigh, NC**<br>Tel: 919-844-7510<br>**New York, NY**<br>Tel: 631-435-6000<br>**San Jose, CA**<br>Tel: 408-735-9110<br>Tel: 408-436-4270<br>**Canada - Toronto**<br>Tel: 905-695-1980<br>Fax: 905-695-2078 | **Australia - Sydney**<br>Tel: 61-2-9868-6733<br>**China - Beijing**<br>Tel: 86-10-8569-7000<br>**China - Chengdu**<br>Tel: 86-28-8665-5511<br>**China - Chongqing**<br>Tel: 86-23-8980-9588<br>**China - Dongguan**<br>Tel: 86-769-8702-9880<br>**China - Guangzhou**<br>Tel: 86-20-8755-8029<br>**China - Hangzhou**<br>Tel: 86-571-8792-8115<br>**China - Hong Kong SAR**<br>Tel: 852-2943-5100<br>**China - Nanjing**<br>Tel: 86-25-8473-2460<br>**China - Qingdao**<br>Tel: 86-532-8502-7355<br>**China - Shanghai**<br>Tel: 86-21-3326-8000<br>**China - Shenyang**<br>Tel: 86-24-2334-2829<br>**China - Shenzhen**<br>Tel: 86-755-8864-2200<br>**China - Suzhou**<br>Tel: 86-186-6233-1526<br>**China - Wuhan**<br>Tel: 86-27-5980-5300<br>**China - Xian**<br>Tel: 86-29-8833-7252<br>**China - Xiamen**<br>Tel: 86-592-2388138<br>**China - Zhuhai**<br>Tel: 86-756-3210040 | **India - Bangalore**<br>Tel: 91-80-3090-4444<br>**India - New Delhi**<br>Tel: 91-11-4160-8631<br>**India - Pune**<br>Tel: 91-20-4121-0141<br>**Japan - Osaka**<br>Tel: 81-6-6152-7160<br>**Japan - Tokyo**<br>Tel: 81-3-6880- 3770<br>**Korea - Daegu**<br>Tel: 82-53-744-4301<br>**Korea - Seoul**<br>Tel: 82-2-554-7200<br>**Malaysia - Kuala Lumpur**<br>Tel: 60-3-7651-7906<br>**Malaysia - Penang**<br>Tel: 60-4-227-8870<br>**Philippines - Manila**<br>Tel: 63-2-634-9065<br>**Singapore**<br>Tel: 65-6334-8870<br>**Taiwan - Hsin Chu**<br>Tel: 886-3-577-8366<br>**Taiwan - Kaohsiung**<br>Tel: 886-7-213-7830<br>**Taiwan - Taipei**<br>Tel: 886-2-2508-8600<br>**Thailand - Bangkok**<br>Tel: 66-2-694-1351<br>**Vietnam - Ho Chi Minh**<br>Tel: 84-28-5448-2100 | **Austria - Wels**<br>Tel: 43-7242-2244-39<br>Fax: 43-7242-2244-393<br>**Denmark - Copenhagen**<br>Tel: 45-4450-2828<br>Fax: 45-4485-2829<br>**Finland - Espoo**<br>Tel: 358-9-4520-820<br>**France - Paris**<br>Tel: 33-1-69-53-63-20<br>Fax: 33-1-69-30-90-79<br>**France - Saint Cloud**<br>Tel: 33-1-30-60-70-00<br>**Germany - Garching**<br>Tel: 49-8931-9700<br>**Germany - Haan**<br>Tel: 49-2129-3766400<br>**Germany - Heilbronn**<br>Tel: 49-7131-67-3636<br>**Germany - Karlsruhe**<br>Tel: 49-721-625370<br>**Germany - Munich**<br>Tel: 49-89-627-144-0<br>Fax: 49-89-627-144-44<br>**Germany - Rosenheim**<br>Tel: 49-8031-354-560<br>**Israel - Ra'anana**<br>Tel: 972-9-744-7705<br>**Italy - Milan**<br>Tel: 39-0331-742611<br>Fax: 39-0331-466781<br>**Italy - Padova**<br>Tel: 39-049-7625286<br>**Netherlands - Drunen**<br>Tel: 31-416-690399<br>Fax: 31-416-690340<br>**Norway - Trondheim**<br>Tel: 47-7289-7561<br>**Poland - Warsaw**<br>Tel: 48-22-3325737<br>**Romania - Bucharest**<br>Tel: 40-21-407-87-50<br>**Spain - Madrid**<br>Tel: 34-91-708-08-90<br>Fax: 34-91-708-08-91<br>**Sweden - Gothenberg**<br>Tel: 46-31-704-60-40<br>**Sweden - Stockholm**<br>Tel: 46-8-5090-4654<br>**UK - Wokingham**<br>Tel: 44-118-921-5800<br>Fax: 44-118-921-5820 |