ATWINC15X0 Certificates Update from Host via OTA (HTTPS)

Introduction

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client. SSL allows sensitive information to be transmitted securely. SSL certificates are one of the fundamental pieces of public key cryptography. Public key cryptography uses a separate key for encryption and decryption. Anyone can use the encryption key (public key) to encrypt a message. However, decryption keys (private keys) are secret. This way, only the intended receiver can decrypt the message.

Public key is intended to be distributed to anyone to decrypt the information that was encrypted with the private key. SSL/Root certificates are small data files that digitally bind a public key to an organization's details. The SSL certificate to be present on both the server and client for SSL connection establishment. The private key must be kept strictly protected and must only be accessible by the owner of the private key.

When Wi-Fi® Network Controller (WINC) is installed in the field, it is required to renew the existing certificates or required to install new certificates. This document provides the demo procedure for uploading root (server) and local SSL certificates and private keys into ATWINC15x0 SPI flash from Host MCU.

This example project implements getting the certificates and private keys from a remote secure server over secure Wi-Fi link. Certificates are highly confidential files used for secure connection and must be sent securely.

Table of Contents

1. Application Example Objective

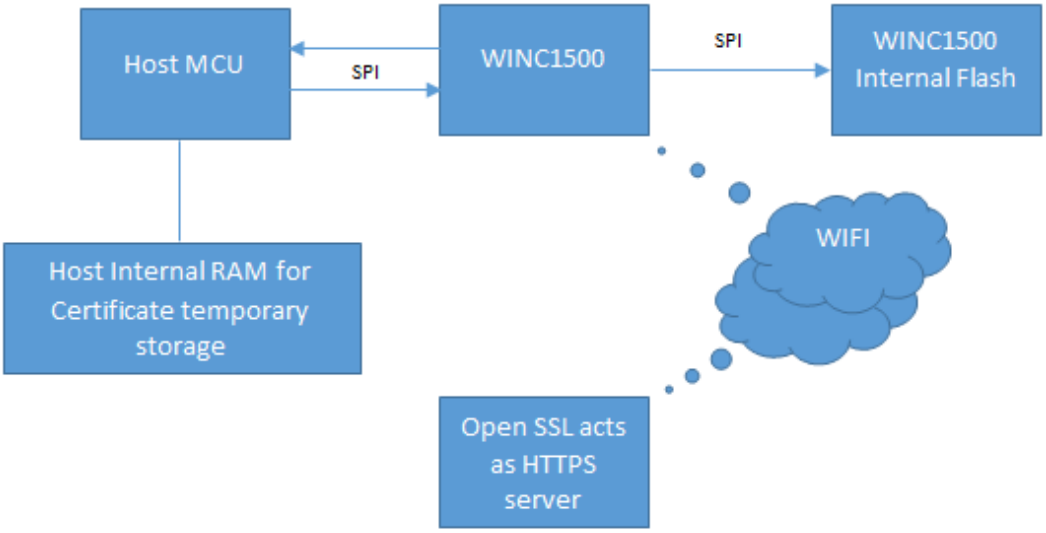
The objectives of the application examples are as follows:

- Receiving the Root/TLS certificates/chain of certificates, private keys over secure HTTPS link on Host MCU
- Updating it on ATWINC15x0 SPI flash through SPI interface between Host MCU and ATWINC15x0

1.1 System Overview

The application is comprised of the following components:

Figure 1-1. Application Overview



1.2 Prerequisites

The following are the hardware and software prerequisites:

Hardware Prerequisites

- SAM D21 Xplained Pro (XPro) Evaluation Kit
- ATWINC1500 extension (for more details, refer to User Guide)
- Micro-USB cable (Micro-A/Micro-B)

Software Prerequisites

- Atmel Studio 7.0 (for more details, refer, User Guide)
- Advanced Software Framework installed as part of Atmel Studio (for more details, refer to Application Note)
- OpenSSL can be downloaded from https://www.openssl.org/source/. Search for Windows downloader at https://slproweb.com/products/Win32OpenSSL.html

Note:

1. OpenSSL is used for demo purposes only. The user can choose their own HTTPS server.
2. The demo is tested with the latest version of Win64 OpenSSL v1.0.2L on the Windows machine.

2. HTTPS Server Setup

TLS/SSL certificates must be securely sent over a Wi-Fi link. The HTTPS over SSL connection is used to receive the certificates from the remote server. This link ensures that all data passed between the server and client remain private and integral. This example implements HTTP protocol where ATWINC15x0 acts as an HTTPS client. The OpenSSL as HTTPS server is used to send the certificate files to ATWINC15x0.

2.1 Generating Custom Server Certificate

To create an SSL connection, the server and the client require an SSL certificate. The following procedure describes how to create and sign custom certificates using OpenSSL.

1. After installing OpenSSL, open a CMD prompt and navigate to the directory where OpenSSL is installed (for example: `C:\OpenSSL-Win64\bin`).
2. Provide the following command to generate a server private key and public certificate:
   ```
   openssl req -x509 -newkey rsa:2048 -nodes -keyout key.pem -out cert.pem -days 365 -nodes
   ```
   Result: The end of this step generates `key.pem` and `cert.pem` in the OpenSSL directory. In PEM (ASCII) format, `key.pem` is the server private key and `cert.pem` is the server public certificate. These two files need to be available on Server (OpenSSL) and `cert.pem` needs to be available on Client (ATWINC15x0) for an SSL connection between server and client.

2.2 Downloading Server Public Certificate on ATWINC15x0

The generated public certificate `cert.pem` is to be downloaded on ATWINC15x0 for the SSL connection between the ATWINC15x0 (client) and the OpenSSL (server).

The most known encodings for the X.509 digital certificates are PEM and DER formats. The current implementation of the ATWINC15x0 supports only DER format. Perform the following steps to download a server public certificate on ATWINC15x0:

1. If the certificate is not in DER format, it must be converted to DER format using the following command.
   ```
   openssl x509 -outform der -in cert.pem -out cert.cer
   ```
   Note: The root_certificate_downloader script available as part of Firmware Update project is in `.cer` extension.
2. The `cert.cer` is to be uploaded on ATWINC15x0 using Firmware Update Project. Copy and paste `cert.cer` in `src\firmware\Tools\root_certificate_downloader\binary`.
3. Follow the steps mentioned in Integrated Serial Flash Memory Download Procedure.
   Note: If certificate upload fails with “(ERROR) Root Certificate Flash is Full” then the allocated memory in SPI flash on ATWINC15x0 for certificates is full. Try after removing one or more certificates from `src\firmware\Tools\root_certificate_downloader\binary`.
4. Now the ATWINC15x0 is ready for SSL connection with the OpenSSL server for receiving the certificate files.

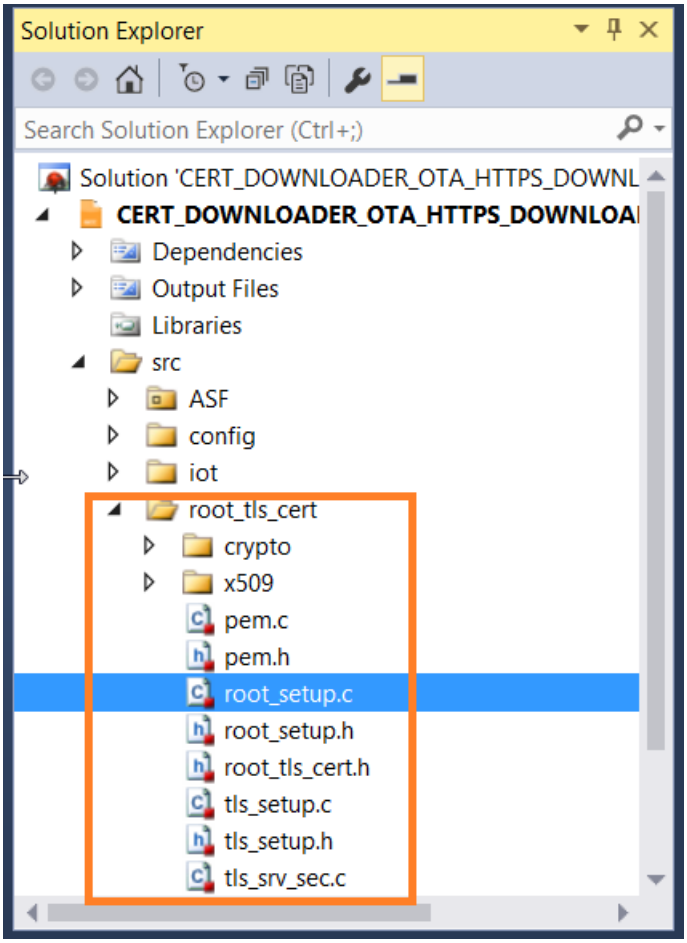
3. Application Flow

ATWINC15x0 SPI Flash stores the root certificates and private keys. The certificate store in SPI flash is divided into two sections. The `M2M_TLS_ROOTCER_FLASH_SIZE` section stores the remote (server) public certificates (or chain of certificates). The `M2M_TLS_SERVER_FLASH_SIZE` section stores local (ATWINC15x0) public certificate (or chain of certificates) private key pairs.

This example implements receiving certificates from a remote server over secure WiFi connection on Host MCU. After receiving the certificates, Host MCU decrypts the certificates and private keys. The unencrypted public certificate and private key are sent over SPI interface to ATWINC15x0 from the Host MCU. The ATWINC15x0 stores the certificates and keys on a specific section of internal SPI flash.

The code implementations are found in the `root_tls_cert folder` as shown in the following figure.

Figure 3-1. Project Folder Structure

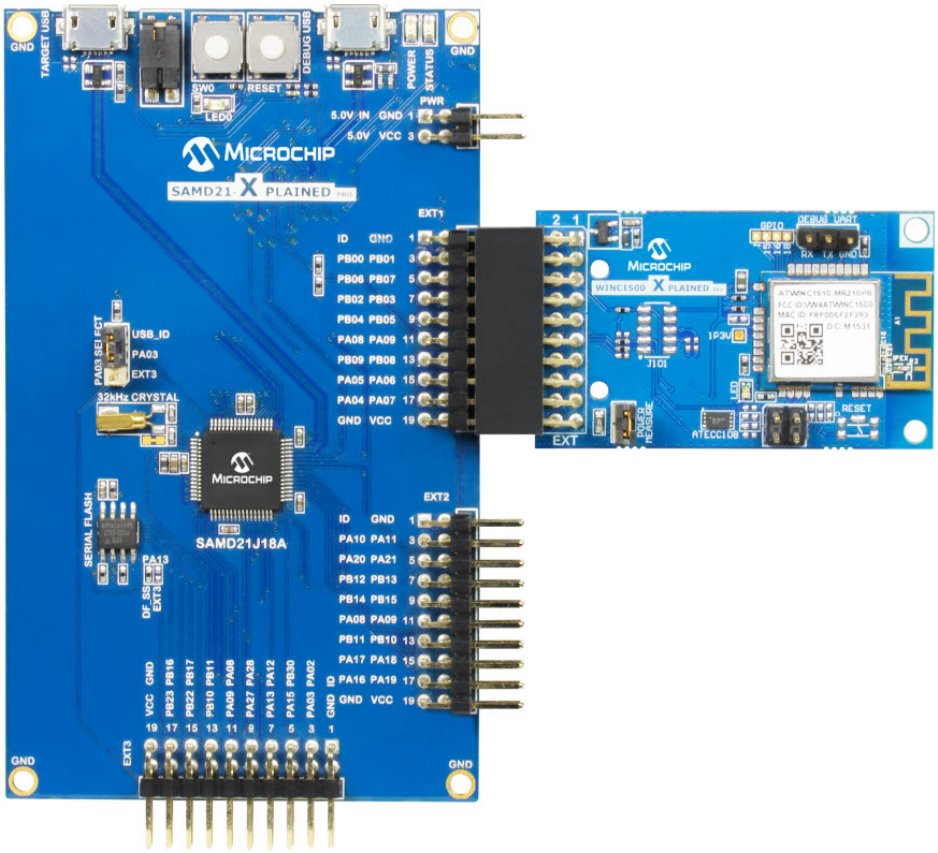


4. Demo Flow

Perform the following steps to run the demo application.

1. Follow the steps in Generating Customer Server Certificate and Downloading Public Server Certificate on ATWINC15x0 and OpenSSL server's public certificate to download on ATWINC15x0 using Firmware Update Project.
2. Connect the PC Wi-Fi with the Wi-Fi router.
3. Navigate to the directory where OpenSSL is installed (for example: `C:\OpenSSL-Win64\bin`).
4. OpenSSL server certificate and private key generated in Generating Customer Server Certificate, which should be available in the OpenSSL directory.
5. Copy the public certificates, public certificate-private key pairs to be uploaded to OpenSSL directory.
   Note:
   1. The certificates and keys can be generated by following the steps in Generating Customer Server Certificate.
   2. The ATWINC15x0 accepts certificates/keys only in DER format. For converting to DER format, follow the steps in Downloading Public Server Certificate on ATWINC15x0.
6. Open CMD prompt and start OpenSSL as HTTPS server using the following command:
   ```
   openssl s_server -key key.pem -cert cert.pem -accept 4443 -WWW
   ```
   Note:
   1. `key.pem` and `cert.pem` are generated in Generating Customer Server Certificate.
   2. 4443 is the port number.
7. Connect SAM D21 XPro (ATWINC1500 XPRO is connected on the EXT1 header) to the PC using a micro USB cable, as shown in the following figure.

Figure 4-1. SAM D21 XPro connected with ATWINC1500 XPro



8. Open “CERT_DOWNLOADER_OTA_HTTPS_DOWNLOAD_EXAMPLE” application from Atmel Studio through `File > New > Example Project`.
9. This example build procedure is developed using the SAM D21 XPRO board, which is also valid for other supported hardware platforms.
10. Configure the following code in `main.h` for the Access Point (AP) information to be connected.

```
/** Wi-Fi Settings */
#define MAIN_WLAN_SSID "DEMO_AP" /* < Destination SSID */
#define MAIN_WLAN_AUTH M2M_WIFI_SEC_WPA_PSK /* < Security manner */
#define MAIN_WLAN_PSK "12345678" /* < Password for Destination SSID */
```

Note: OpenSSL server and the ATWINC15x0 must be connected to the same network for the OpenSSL server-based demo.

11. Configure the HTTPS Server (OpenSSL) IP address and port number:

```
/** Content URI for download. */
#define MAIN_HTTP_FILE_URL https://192.168.43.34/
#define MAIN_HTTP_PORT_NUMBER (4443)
```

12. Provide certificate/private key file names copied in step 3 along with the total number of certificates/ keys to be downloaded.

```
/** No of certificates to be written to WINC **/
#define NUM_OF_ROOT_TLS_CHAIN_CERTIFICATES 5
/** Root Certificates to be uploaded */
/** Chain of TLS Certificates and private key to be uploaded */
certFileInfo root_tls_certs_name[NUM_OF_ROOT_TLS_CHAIN_CERTIFICATES]=
{{ROOT_CERT,0,(uint8_t*)"PROWL_Root.cer"},
{ROOT_CERT,0,(uint8_t*)"NMA_Root.cer"},
```

```
{TLS_RSA_CERT,2,(uint8_t*)"winc_rsa.key"},
{TLS_RSA_CERT,0,(uint8_t*)"winc_rsa.cer"},
{TLS_RSA_CERT,0,(uint8_t*)"WincRootCA.cer"}
};
```

Note:

1. typedef struct

```
{
cert_type_t cert_type;
uint8_t numOfChainCert;
uint8_t *filename;
} certFileInfo;
```

2. cert_type
   - ROOT_CERT – Remote server certificate stored in `M2M_TLS_ROOTCER_FLASH_SIZE` of flash section starts from `M2M_TLS_ROOTCER_FLASH_OFFSET`. `numOfChainCert` to be 0 for this cert_type. Even if there are chain of certificates, it is provided as individual entry.
   - TLS_RSA_CERT – Local (ATWINC15x0) RSA-based certificate stored in `M2M_TLS_SERVER_FLASH_SIZE` of flash section starts from `M2M_TLS_SERVER_FLASH_OFFSET`. In the array of certificate file names first entry of `TLS_RSA_CERT` is the private key and the following entries are a chain of certificates. Only the first entry must contain the `numOfChainCert`. The `numOfChainCert` in public certificate entries is to be 0. In the above example “2” is `numOfChainCert` where `winc_rsa.cer` and `WincRootCA.cer` are the chain of certificate files.
   - TLS_ECC_CERT – Local (ATWINC15x0) ECC-based certificate stored in `M2M_TLS_SERVER_FLASH_SIZE` of flash section starts from `M2M_TLS_SERVER_FLASH_OFFSET`. In the ECC-based certificates, only the public certificate along with public key is stored in ATWINC15x0. The private key is stored in ECC508 (External Crypto engine). Similar to TLS_RSA_CERT, the first entry must mention `numOfChainCert`. Here, the first entry will be a public certificate as the private key is not stored in ATWINC15x0 for this certificate type.

13. Build the program and download it into the SAM D21 XPRO board.
14. Start the application.
15. ATWINC15x0 starts receiving the certificate files one by one and sends them to Host MCU.
16. After receiving all the certificates, the Host uploads on the ATWINC15x0 SPI flash.

Note:

1. To write the certificates into ATWINC15x0, it is required to put ATWINC15x0 into downloader mode. This halts any running ATWINC15x0 firmware. After the certificate download is completed, ATWINC15x0 has to be re-initialized to start the Wi-Fi operations.
2. If the certificates upload fail with “(ERROR) Root Certificate Flash is Full” print message on console, which shows the allocated memory (`M2M_TLS_ROOTCER_FLASH_SIZE`) is full. For more details, refer to Erasing of Certificate Flash Section.
3. The verification of received certificates with the stored certificates can be enabled by defining

```
#define ENABLE_VERIFICATION
```

   This reads back the certificates from the ATWINC15x0 SPI flash and compares with the received certificates. This requires `FLASH_SECTOR_SZ` (4 KB) of the Host MCU RAM for comparison. Therefore, this is disabled by default in the demo application. After ensuring sufficient RAM in Host MCU, this verification can be enabled.

Figure 4-2. Demo Console Log Server Side

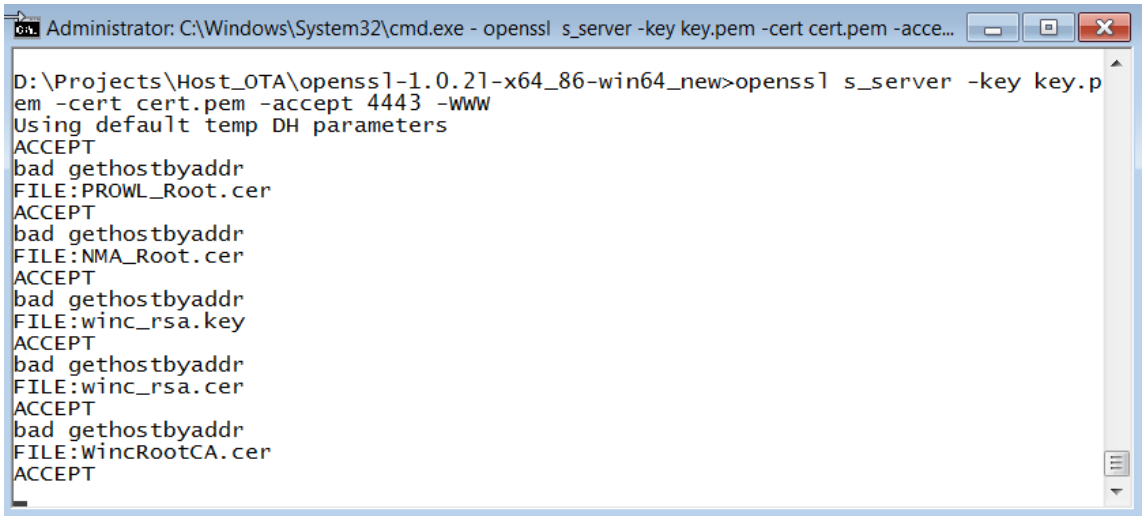
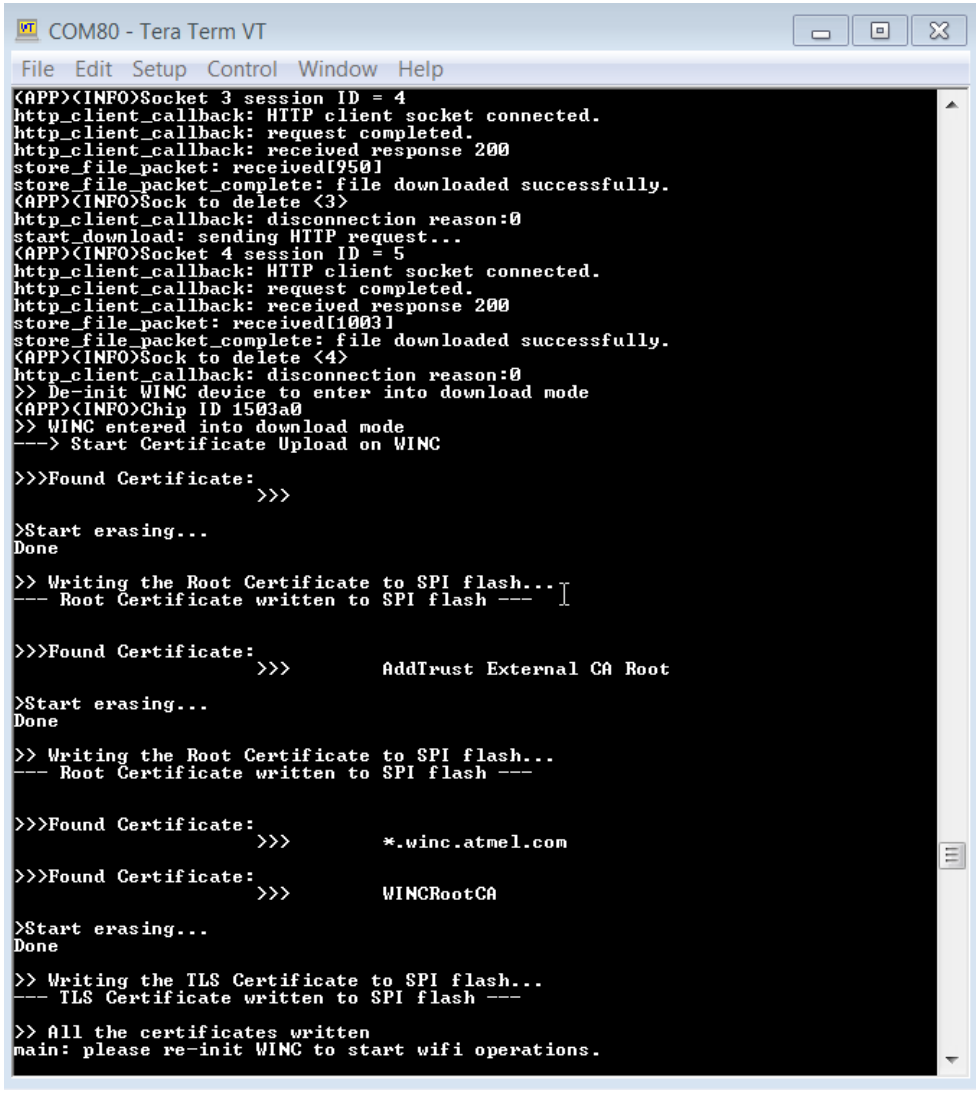


Figure 4-3. Demo Console Log ATWINC15x0 Side



5. Erasing of Certificate Flash Section

The demo application adds the new certificates in the free space and replaces the same certificate location in case of certificate renewal. Certificates that already exist are not erased. This is implemented to retain all the previously used certificates, so that they can be used in future.

The customer must have the knowledge of allocated memory for certificate storage and expected size of the certificates in field. The following APIs are used to erase the complete certificate storage flash section.

- For erasing M2M_TLS_ROOTCER_FLASH_SIZE section – `programmer_erase_root_cert();`
- For erasing M2M_TLS_SERVER_FLASH_SIZE section – `programmer_erase_tls_cert_store();`

These APIs need to be called before `burn_certificates()` to erase the complete certificate Flash section. If these APIs are called, then all the stored certificates in Flash will be erased. Only the new certificates received over-the-air will be stored when `burn_certificates()` is called.

6. Document Revision History

Rev A - 11/2017

Section	Changes
Document	Initial release

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

Trademarks

ISBN: 978-1-5224-2371-3

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 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	**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: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820