AN2616

Using the ATECC508A to Perform Asymmetric Authentication of a Remote Device

Introduction

This application demonstrates the authentication of a remote device with a host (The Curiosity PIC32MZ EF Development Board and the secure click board using the cryptography module ATECC508A) by using an asymmetric authentication method, where the host verifies the signature from the remote through the public key of the remote. The application allows adding information to the configuration, using the configuration data, and key data to configure a secure click board. The application flow is realized through an interactive user interface through the serial terminal program (Tera term) interfaced through the USB of a computer.

For more information on the features and layout of the Curiosity PIC32MZ EF Development Board, refer to the PIC32MZ EF Curiosity Development Board User's Guide (DS70005282).

For more information on the features of the ATECC508A module, refer to the Product Data Sheet.

1. Required Tools and Applications

The following Microchip development tools are required to run the ATECC508A Asymmetric Authentication demonstration:

- Curiosity PIC32MZ EF Development Board (DM320104), available from Microchip Direct
- Download and install latest version of MPLAB X Integrated Development Environment (IDE)
- Download and install the latest version of MPLAB XC32 C/C++ Compiler
- Optionally download and install the latest version of MPLAB® Harmony Integrated Software Framework

Note:

1. Using the MPLAB Harmony Integrated Software Framework will extend the functionality of this project by adding new modules, software frameworks, and libraries to the project.
2. This application project is developed on the following tools:
   – MPLAB X IDE v4.05
   – MPLAB XC32 C Compiler v1.44
   – MPLAB Harmony v2.05
   – MPLAB X IDE plug-in: MPLAB Harmony Configurator (MHC) v2.0.5.2

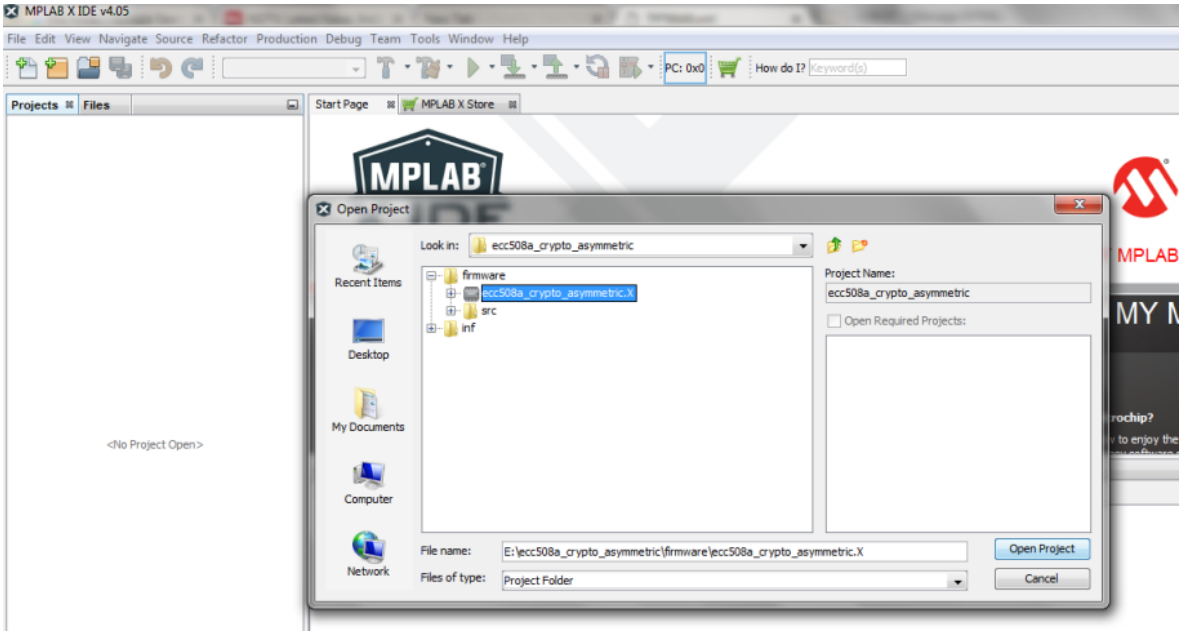
The following click board from Mikroelektronika is used: Secure click board (MIKROE-2522) – 2 Nos.

2. Building the Application

To build the application, use the following procedure:

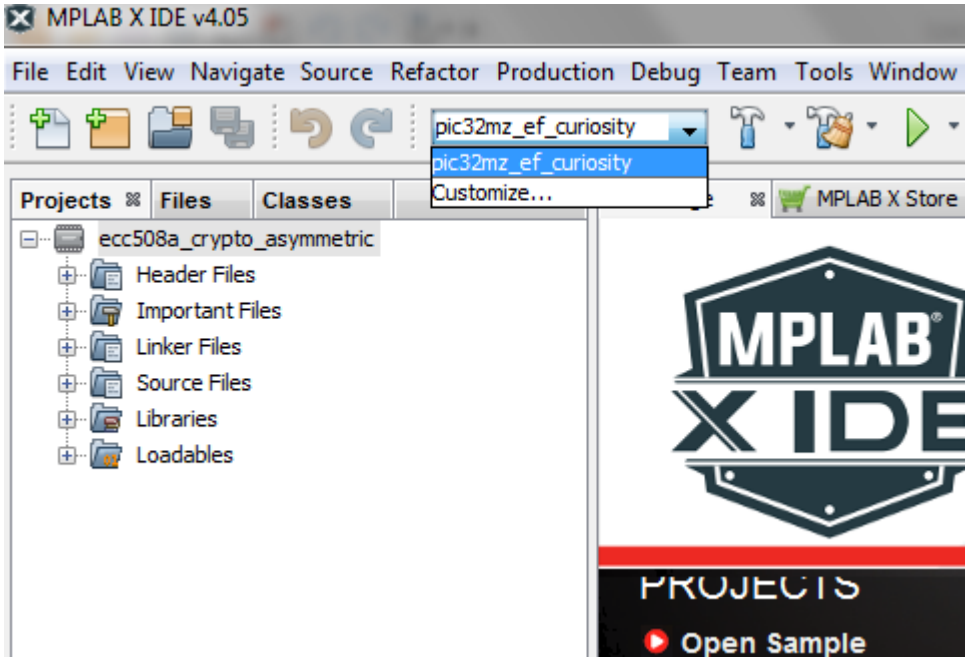
1. Download the *ecc508a_crypto_asymmetric* project to the local computer. This project can be found under the *Curiosity Demo Examples* tab at http://www.microchip.com/Developmenttools/ProductDetails.aspx?PartNO=DM320104.
2. To build the project, in MPLAB X, *File* > *Open Project* then us the `ecc508a_crypto_asymmetric.X` project from *<path-of-project-in-your-pc>/ecc508a_crypto_asymmetric/firmware* in MPLAB X IDE, as shown below.

Figure 2-1. Opening the Project



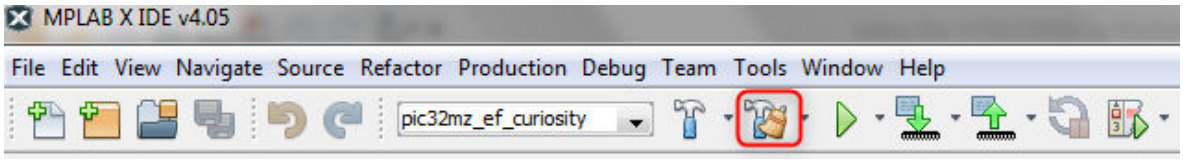
3. The project has only one configuration, *pic32mz_ef_curiosity*, for the Curiosity PIC32MZ EF Development Board. This is the default configuration when the project is open.

Figure 2-2. Choosing the Project Configuration



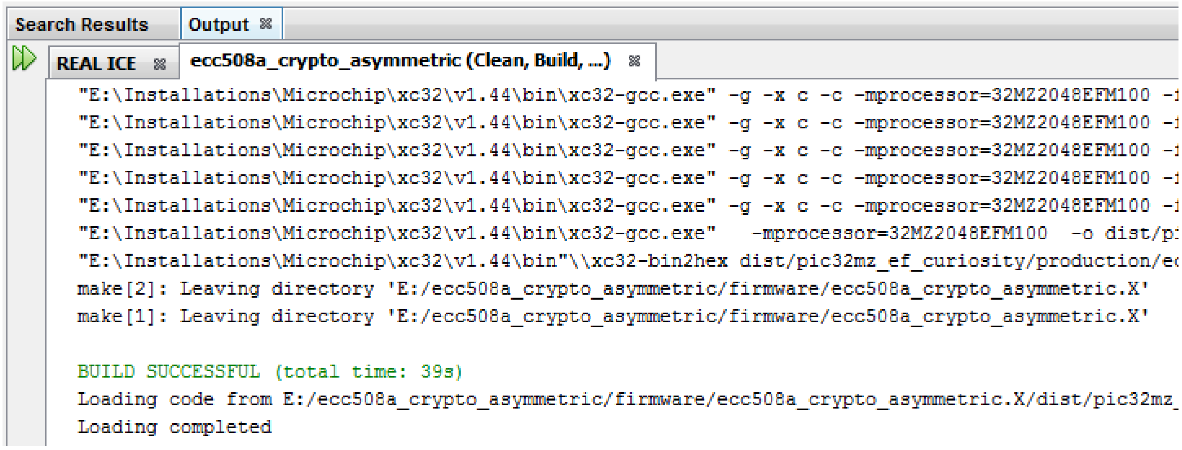
4. The *pic32mz_ef_curiosity* configuration sets up MPLAB X IDE to build and run the demonstration application on the Curiosity PIC32MZ EF Development Board, with the PIC32MZ2048EFM100 microcontroller.
5. The USB CDC class library is configured to enable interactive user interface control.
6. The I^2C driver is configured to use the I^2C1 instance of the peripheral at 100 kHz clock frequency. The application interacts with the ATECC508A (available on the Secure click board) over I^2C1 to implement the host side of the application.
7. The I^2C driver is configured to use the I^2C2 instance of the peripheral at 100 kHz clock frequency. The application interacts with the ATECC508A (available on the Secure click board) over I^2C2 to implement the remote side of the application.
8. Clean and Build the project.

Figure 2-3. Clean and Build



9. Check the Build log, at the bottom of the MPLAB X IDE interface.

Figure 2-4. Build Log



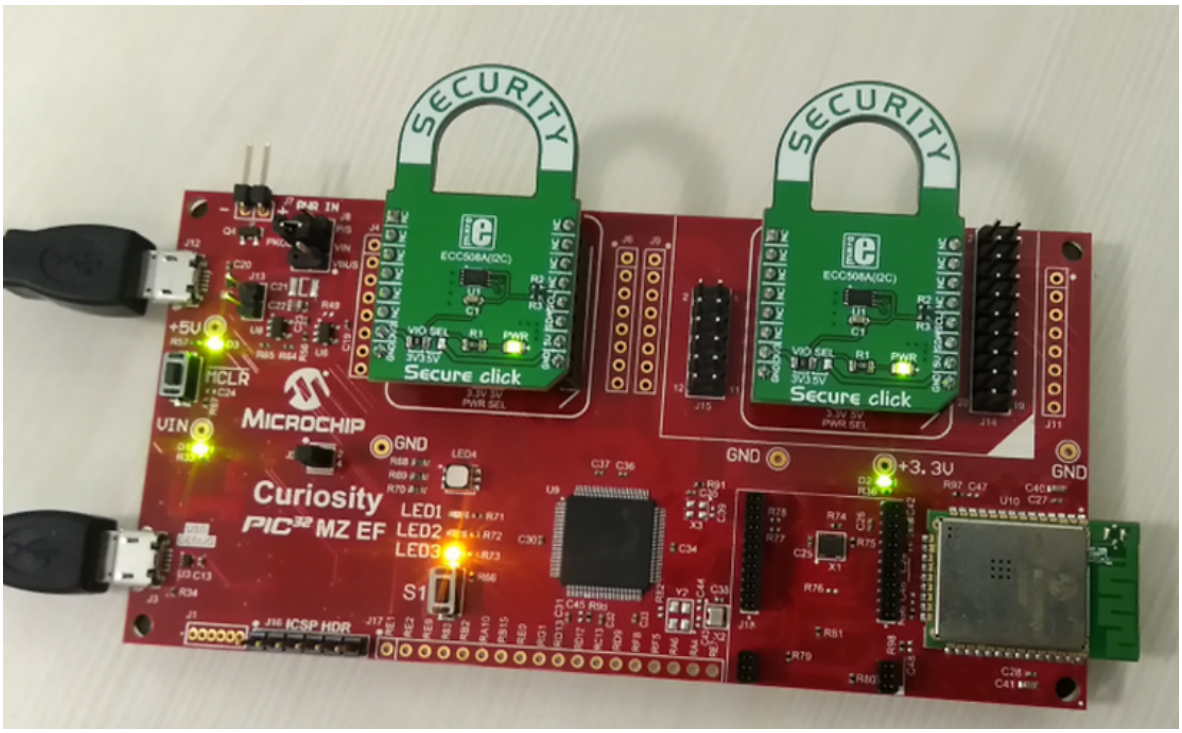
Note: Often a project will not compile on a Windows™ computer due to a limitation in the path length. The Windows operating system has a maximum path length of 260 characters. This limitation causes file paths to be truncated when attempting to compile, which leads to files not being found by the compiler. Try placing the project in the top level directory, usually `C:/`. For more information, refer to the Maximum Path Length Limitation section of the Naming Files, Paths, and Namespaces, which is available on the Microsoft Developer Network site.

3. Configuring the Hardware

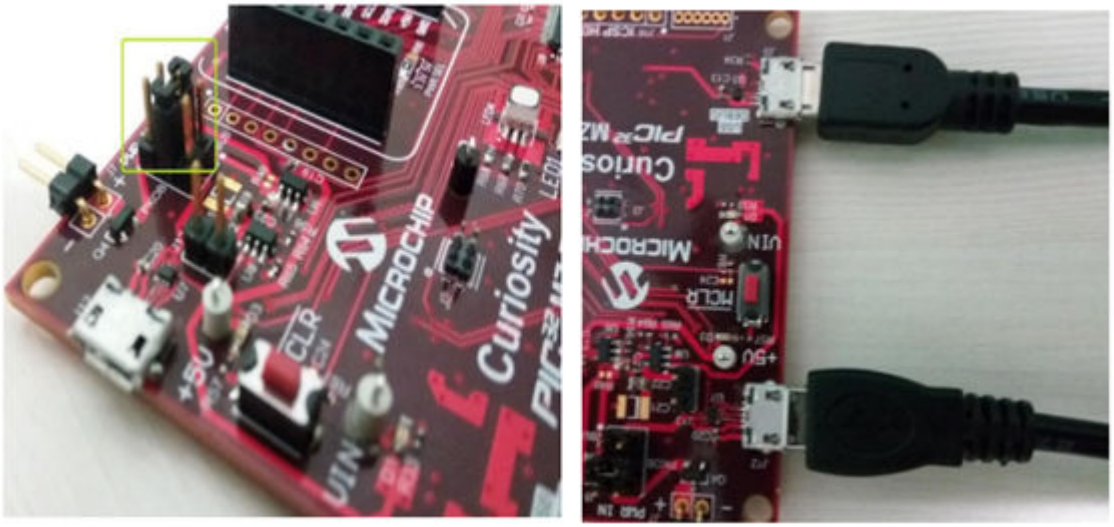
To configure the hardware, use the following steps:

1. For the host operation, mount a Secure click board on the mikroBUS socket J5.
2. For the remote device operation, mount a Secure click board on the mikroBUS socket J10.

Figure 3-1. Hardware Configuration



3. Power the Curiosity PIC32MZ EF Development Board from the host computer through a Type-A male to Micro-B USB cable connected to the Micro-B port (J3). The cable is not included with the kit. Ensure that a jumper is placed in the J8 header (between 4 and 3) to select the supply from the debug USB connector.
4. Ensure that the jumper is not present in the J13 header to use the Curiosity board in Device mode. In Device mode, the board acts as a USB device to the computer. Plug in a USB cable with a Micro-B type connector to Micro-B port (J12), and plug the other end into the computer.



For additional information on the hardware features and configurations, refer to the User's Guide:

PIC32MZ EF Curiosity Development Board User's Guide (DS70005282).

4. Running the Demonstration

This application demonstrates the use of the ATECC508A module to authenticate and verify if the device is secure or not. The authentication method used is Asymmetric.

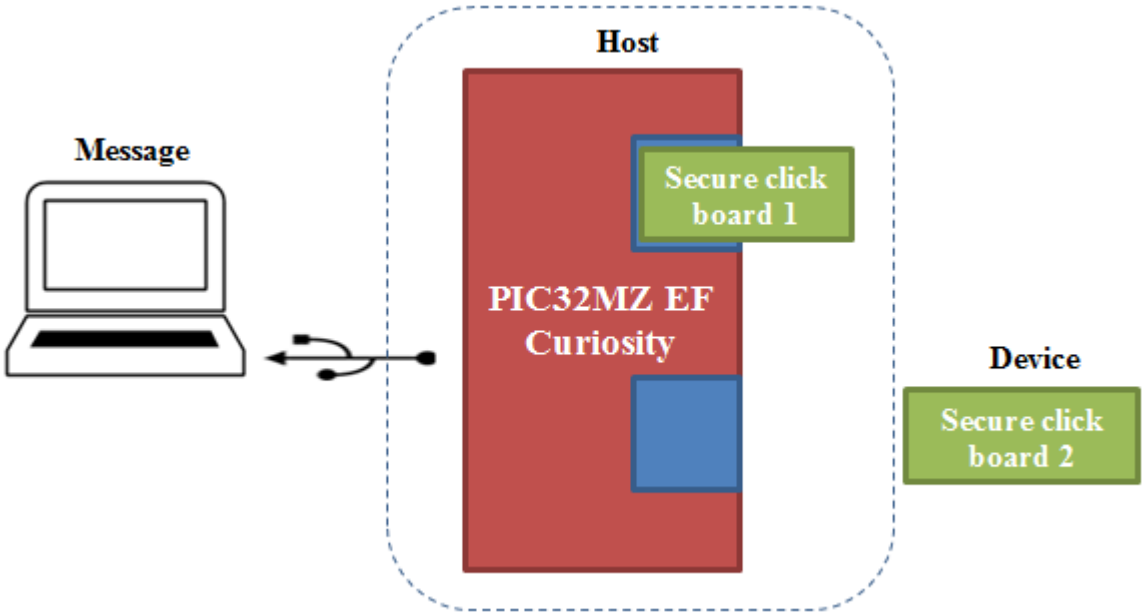
In asymmetric authentication, a verifier checks the authenticity of remote by validating the signature.

Asymmetric authentication is based on the use of two keys. One of the keys needs to be kept secret. This key is called the *Private Key*. The second key is mathematically related to the Private Key and is called the *Public Key*. The public key is openly shared. The key owner will use the Public Key to authenticate the signature.

In this application, a secure hardware key storage device (ATECC508A on a Secure click board) is used to generate a signature by the remote, and the host uses the public key of the remote, and verifies the signature.

The following figure represents the functional block diagram of the application.

Figure 4-1. Functional Block Diagram

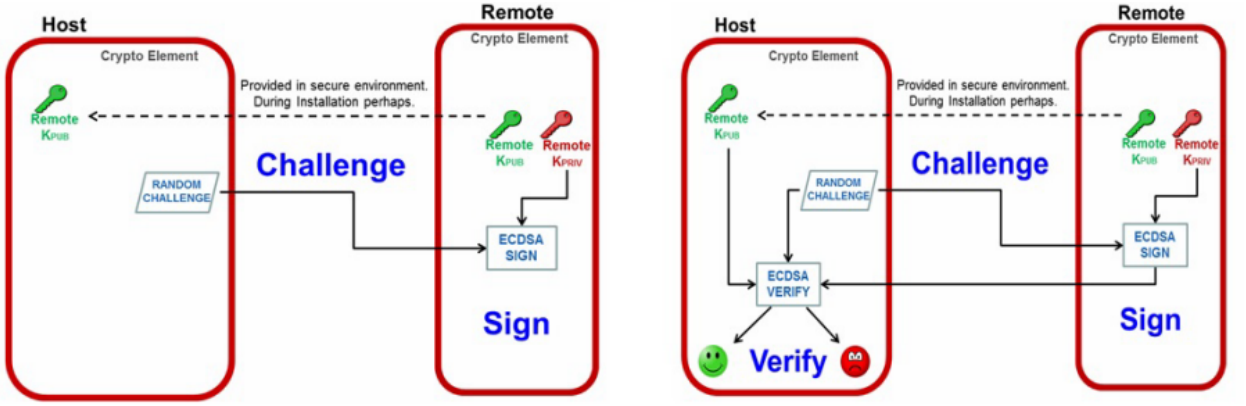


Note: The *Secure click board 1* and *Secure click board 2* house the ATECC508A module and interface with the Curiosity PIC32MZ EF Development Board microcontroller over I^2C interface.

Authentication Process

The host sends a random challenge to the remote device. The remote device responds with a signature. However, the host only needs the public key from the remote (not a secret key) to verify the signature on the challenge.

Figure 4-2. Authentication Process

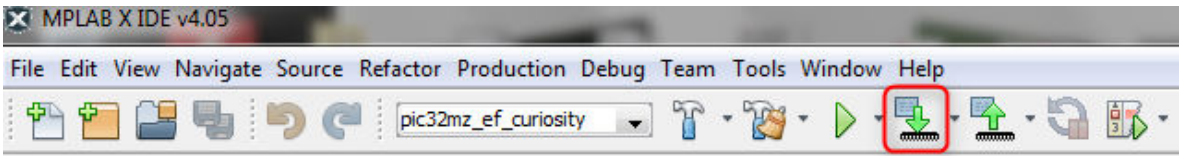


If the signature verification matches, then the remote device has successfully responded to the challenge and the host can trust the remote device.

The following steps are used to run the demonstration:

1. Open the project in MPLAB X IDE and select the pic32mz_ef_curiosity project configuration.
2. Build the code and program the device by clicking on the program button as shown below.

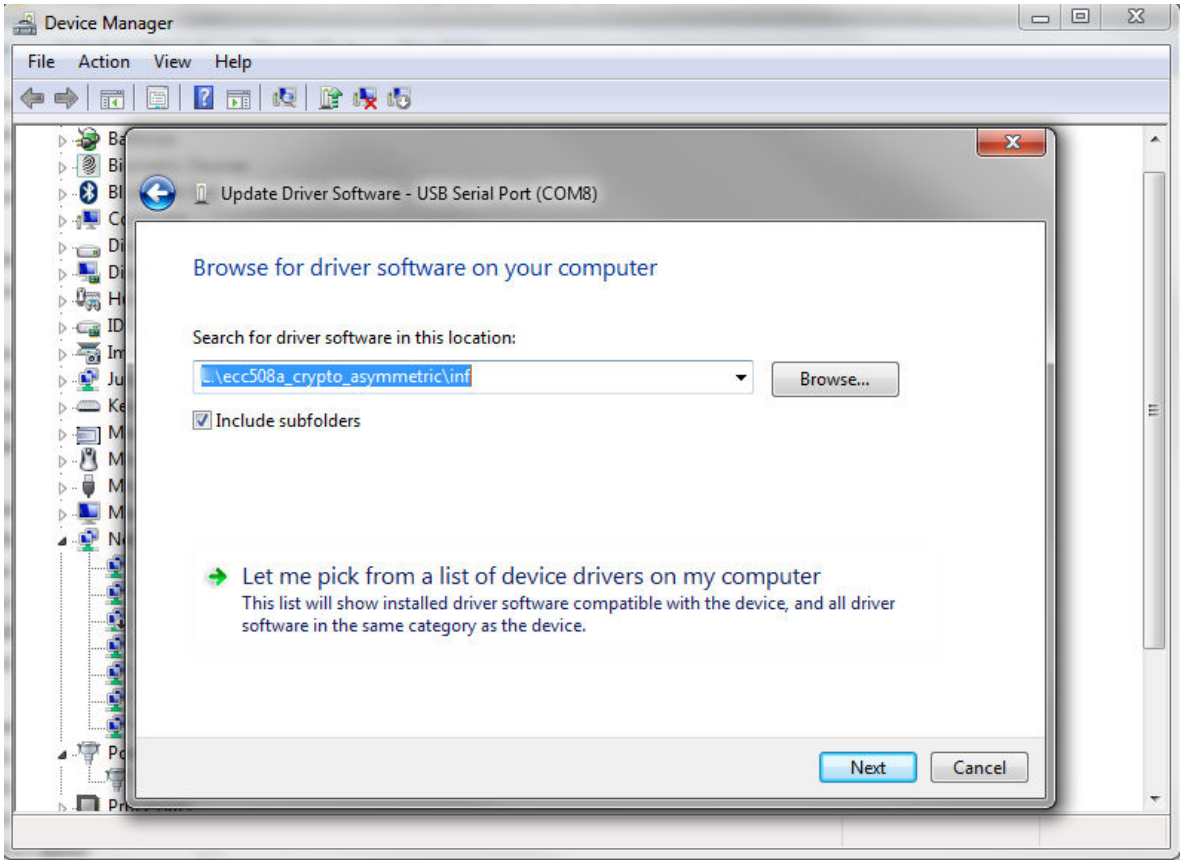
   Figure 4-3. Build and Program

3. After power up, the demonstration is active. This is indicated by a yellow LED (LED3) on the board.
4. Plug in a USB cable with a Micro-B type connector to the Micro-B port (J12) of the Curiosity board, and plug the other end into the computer.
5. If this is the first time using this device with a personal computer, there may be a prompt for a .inf file.
6. Select the *Install from a list or specific location (Advanced)* option. Specify the path *from / ecc508a_crypto_asymmetric/inf directory*.

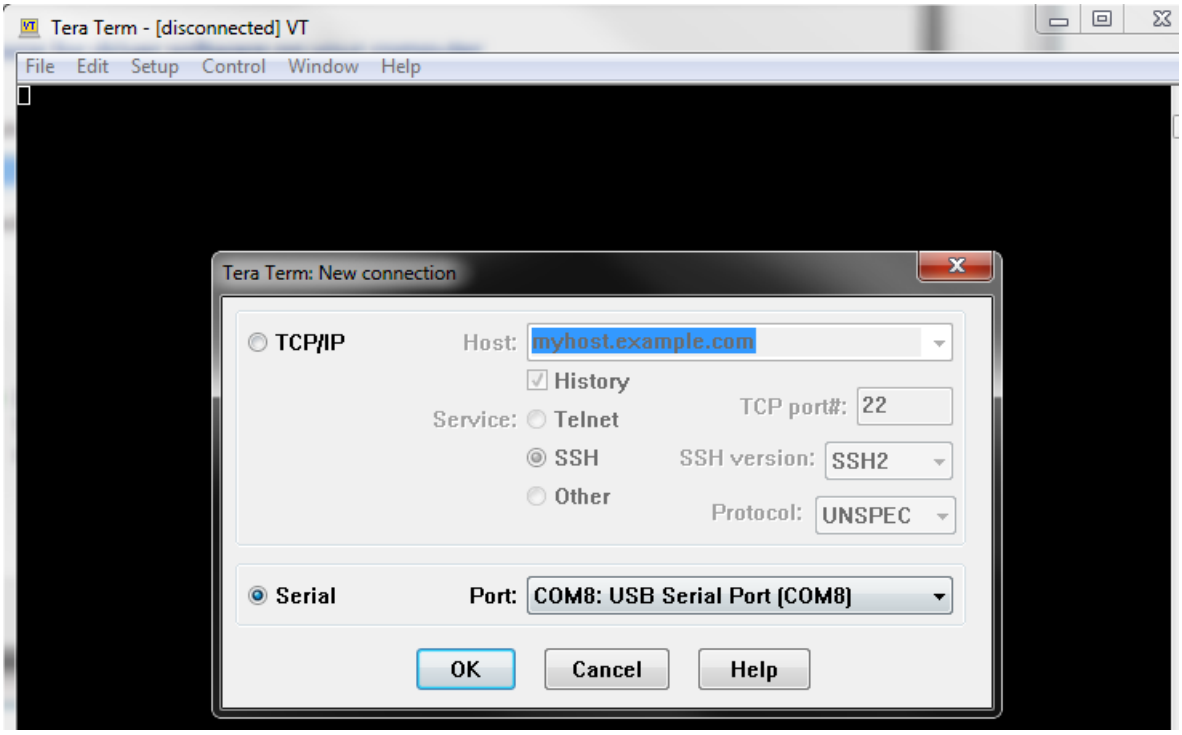
   Note: Optionally, to specify the driver, open the device manager and expand the Ports (COM & LPT) tab, then right click on *Update Driver Software*.

Figure 4-4. Update Driver Software



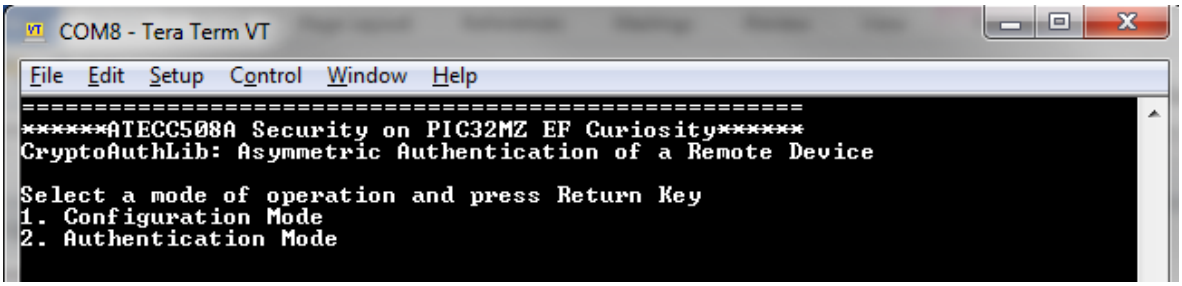
7. Once the device is installed, open a terminal program, such as *Tera Term* or *HyperTerminal*. Select the appropriate COM port for the terminal. The following figure shows the COM port selection for the Tera Term terminal program.

Figure 4-5. COM Port Selection



8. Once the Tera Term screen is displayed, Press the *Enter key*. The following modes of operation will be displayed.

Figure 4-6. Mode of Operation Menu



9. The application demonstration offers the following two modes of operation.
   - **Configuration Mode**: This mode is used to configure a blank ATECC508A module with the configuration data and keys to be stored. A blank ATECC508A device is in an unlocked state. This operation performs a lock on the Configuration Zone and Data Zones on the ATECC508A device. The locking operation is a one time operation and is irreversible.
   - **Authentication Mode:** This mode performs the secured authentication of the Remote ATECC508A device.
10. **Selecting Option 1 - Configuration Mode**
    - The display prompts the user to perform an action

Figure 4-7. Configuration Mode

– When the Secure click board is plugged-in, the application enters into Configuration Write mode, and prints the existing or default configuration
Note: The existing or default configuration may be different from what is shown in the following figure.

Figure 4-8. Writing Configuration

– If the plugged-in board is a brand new Secure click board, the application will write the new configuration to the configuration zone and lock it. The application will display the following messages:
  - **Configuration Write Complete**
  - **Locking Configuration Zone..**
  - **Configuration Zone Lock Complete**
– This would be followed by the writing of the new data (data slot contents and new keys) to the data zone and locking it. It would display the following messages:
  - **Writing Data Zone**
  - **Data Zone Write Complete**
  - **Locking Data Zone..**
  - **Data Zone Lock Complete**
  - ****Host board Configuration Done****
– If the plugged-in board is already configured, the application displays the following message: ATCA already configured.
– Once the host configuration is completed, The display prompts the user to choose an action: Plug in remote Secure Click board in Mikro Bus Interface 2 and press S1.
– When the Secure click board is plugged-in, the application enters the configuration write mode and prints the existing or default configuration
Note: The existing or default configuration could be different from what is shown in the following figure.

Figure 4-9. Default Configuration

- If the plugged-in board is a brand new Secure click board, the application will write the new configuration to the configuration zone and lock it. It will display the following messages:
  - **Configuration Write Complete**
  - **Locking Configuration Zone..**
  - **Configuration Zone Lock Complete**
- This would be followed by writing of the new data (data slot contents and new keys) to the data zone and locking it. It would display the following messages:
  - **Writing Data Zone**
  - **Data Zone Write Complete**
  - **Locking Data Zone..**
  - **Data Zone Lock Complete**
  - ****Remote board Configuration Done****
- If the plugged-in board is already configured, the application displays the following message: ATCA already configured.
- The application provides a user the option to return to main menu: Press a key followed by 'enter' key to return to Options Menu.

11. **Selecting option 2 - Authentication Mode**
    - **Fail Case:**
      - By default, if the application fails to authenticate the Remote Secure click (plugged in J10), it will be indicated by a red LED (LED1) on the board.

Figure 4-10. Fail Case

– The Remote Secure click fails to authenticate when the host does not have the public key for the remote in its database. The host will verify only those remote devices whose public key it possesses.

```
if(key_found)
{
    status = atcab_verify_extern((const uint8_t*)&nonce,
                                 (const uint8_t*)&signature,
                                 (const uint8_t*)key_store[i].pub_key,
                                 &verify);
}
else
{
    SYS_PRINT("Remote's Public Key not found in Host's Database \r\n\r\n");
}
```

– *Pass Case:* To verify the signature of the remote, place the Disposable Public Key of the remote in the database of the host. Copy the Remote Disposable Public Key from the previous figure and paste the key into the array key_store[] in *ecc508a_crpyto_asymmetric_app.c file* as shown in the following figure.

Figure 4-11. Pass Case

```
asymm_public_key_t key_store[4] =
{
    0x07, 0x8c, 0xe2, 0x2c, 0x19, 0xbc, 0xf4, 0x09,
    0x4c, 0x56, 0xcb, 0x9a, 0x3c, 0xa0, 0x93, 0x74,
    0xc7, 0xc2, 0xd2, 0x2d, 0x15, 0x76, 0x74, 0x9d,
    0xdd, 0x8a, 0x6a, 0x22, 0xae, 0x67, 0xee, 0xc3,
    0x97, 0x90, 0x73, 0xa2, 0x39, 0x72, 0x68, 0x30,
    0x7e, 0xdf, 0x21, 0xa0, 0x37, 0xad, 0xcc, 0x2d,
    0x7a, 0x0b, 0xa5, 0xd6, 0xac, 0x64, 0xab, 0x01,
    0x00, 0xbc, 0x8b, 0xe5, 0x8a, 0xa1, 0x1e, 0xba,
}; //cut and paste in remote public key
```

– Build and program the code. Repeat the user actions to select Authentication mode. The application now passes to verify the signature from the Remote Secure click (plugged in J10). This is indicated by a green LED (LED2) on the board.

Figure 4-12. Authentication Verification

```
------In Authentication Mode------
Random from host
0xe4, 0x46, 0x63, 0x22, 0xd3, 0x2a, 0x88, 0x40,
0x69, 0xef, 0xdb, 0x0d, 0x42, 0xd0, 0x01, 0x53,
0xfb, 0x1a, 0x61, 0xd0, 0x1a, 0x08, 0xcc, 0x72,
0x81, 0xdd, 0x4d, 0x64, 0x36, 0x05, 0xa8, 0x86,

Signature from remote
0x3e, 0x73, 0x77, 0x25, 0xb3, 0xc8, 0x0d, 0xe7,
0xb1, 0xe0, 0xb4, 0xb5, 0xca, 0x11, 0x53, 0xe9,
0x99, 0xf9, 0xc5, 0x33, 0x64, 0x8c, 0xb2, 0x3a,
0x12, 0xc2, 0xc7, 0x67, 0xa8, 0xb7, 0x13, 0x50,
0xf9, 0x2c, 0x7f, 0xaf, 0x8d, 0x95, 0x9c, 0x42,
0xca, 0xde, 0x1f, 0xb4, 0x92, 0x9b, 0x86, 0x61,
0x8f, 0xb3, 0x6c, 0x8b, 0x93, 0xc0, 0x6a, 0x9a,
0xb9, 0x0e, 0x96, 0x8f, 0x81, 0xf2, 0x52, 0xca,

Remote disposable public key
0x07, 0x8c, 0xe2, 0x2c, 0x19, 0xbc, 0xf4, 0x09,
0x4c, 0x56, 0xcb, 0x9a, 0x3c, 0xa0, 0x93, 0x74,
0xc7, 0xc2, 0xd2, 0x2d, 0x15, 0x76, 0x74, 0x9d,
0xdd, 0x8a, 0x6a, 0x22, 0xae, 0x67, 0xee, 0xc3,
0x97, 0x90, 0x73, 0xa2, 0x39, 0x72, 0x68, 0x30,
0x7e, 0xdf, 0x21, 0xa0, 0x37, 0xad, 0xcc, 0x2d,
0x7a, 0x0b, 0xa5, 0xd6, 0xac, 0x64, 0xab, 0x01,
0x00, 0xbc, 0x8b, 0xe5, 0x8a, 0xa1, 0x1e, 0xba,

Verified Signature - Authentication Successful!
```

– The signature of the Remote Secure click is successfully verified as the remote had generated the signature using its private key and the random challenge from the host, while the host verified the signature by authenticating it against the public key of the remote.

– The application provides the following option to return to the main menu: Press a key followed by 'enter' key to return to Options Menu.

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

Product Identification System

To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.

PART NO. [X](1) –X /XX

Device — Tape and Reel — Temperature Range — Package

Device:	Device A, Feature A, (Package A) Device B, Feature B, (Package B)	
Tape & Reel Option:	Blank	= Tube
	T	= Tape & Reel
Temperature Range:	I	= -40°C to +85°C (Industrial)
	E	= -40°C to +125°C (Extended)
Package:	AA	= Package AA
	BB	= Package BB

Examples:

- MCPXXXXXAT-E/AA: Tape and Reel, Extended temperature, XAA package
- MCPXXXXXBT-E/BB: Tape and Reel Extended temperature, XBB package

Note:

1. Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.
2. Small form-factor packaging options may be available. Please check http://www.microchip.com/packaging for small-form factor package availability, or contact your local Sales Office.

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: 978-1-5224-2548-9

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