AN714

SMART ENERGY ECC-ENABLED DEVICE SETUP PROCESS

(Formerly document 120-5070-000)

This document describes how to set up a device with the security resources required to support Smart Energy (SE) security, which is based on certificate-based key establishment (CBKE) using Elliptic-Curve Cryptography (ECC). This includes the ECC 163k1 curve used by Smart Energy 1.0 and 1.1, as well as the ECC 283k1 curve used by Smart Energy 1.2.

These steps involve obtaining a certificate and installation code, programming them onto the device, setting up unique security keys for incoming devices, and joining new devices with this unique security information. While these security resources (which also include Certicom's ECC library, available upon request from Silicon Labs' support team) are not necessary for testing SE networks, any devices wishing to participate in or host a ZigBee-compliant, production-grade (non-test) SE network must implement these features. Readers of this document should be familiar with the ZigBee Smart Energy Application profile (available from the http://www.zigbee.org website in the Standards section) and have basic familiarity with the Silicon Labs' graphical and command-line-based tools. This document also assumes that the user already has access to the Certicom ECC library (or an ECC-enabled network coprocessor image, for EZSP-based platforms) for their target Ember® platform; for access to this content, please contact the Silicon Labs ZigBee support team.

New in This Revision

Smart Energy 1.2 Certificate support.

Contents

1 Introduction 3
1.1 ECC Curves and Certificates 3
2 Test Certification Generation 3
3 Certificate File Modification 4
3.1 Combined Certificate File 4
3.2 Smart Energy 1.0 4
3.3 Smart Energy 1.2 5
3.4 EM3xx Platform 5
4 Installation Code Generation 6
5 Installation Code Programming 6
5.1 EM3xx Platform 6
6 Application Setup (Build Time) 6
6.1 System on Chip 6
6.2 Network Coprocessor 7
7 Application Setup (Run Time) Prior to Joining a New Device to the HAN 7

7.1 Procedure for Development Prototypes / Debugging 7
7.2 Procedure for Production/Field Deployments 8
8 Joining Process for New Device 9
9 Network Analyzer Capture Setup 9

1 Introduction

The processes described in this application note are all those required to set up Smart Energy (SE) elliptic curve cryptography (ECC)-enabled devices. The processes include the following:

- Test certificate generation
- Certificate file manipulation
- Certificate file programming (for EM3xx platforms)
- Installation code generation
- Installation code programming (for EM3xx platforms)
- Application setup (build time)
- Application setup (run time) if using unique link keys
- Joining a new device
- Ember Network Analyzer capture setup

1.1 ECC Curves and Certificates

Smart Energy 1.0 utilized an ECC 163k1 curve with a 48-byte certificate format. All certified devices are required to support this. Smart Energy 1.2 introduces a new curve ECC 283k1, and a 74-byte certificate format. Smart Energy 1.2 devices must support the existing 163k1 ECC curve and may also support the new 283k1 curve. (The requirements for what devices **must** support the 238k1 ECC curve is spelled out in the ZigBee Smart Energy specification.)

The certificates and libraries are **not** interoperable. In order to support both curves two sets of certificates, private keys, and CA public keys must be installed.

2 Test Certification Generation

1) Register for an account (for test certificate generation) at http://www.certicom.com/index.php/gencertregister. This registration is valid for a limited time.
2) Log in to the test certificate generation site with your account login:
   a) http://www.certicom.com/index.php/devicelogin
3) Go to the certificate generation page:
   a) Smart Energy 1.0 Certificates: http://www.certicom.com/index.php/smartenergydevicecertificateservice
   b) Smart Energy 1.2 Certificates: http://www.certicom.com/index.php/smartenergydevicecertificateservice1dot2
4) In the **Subject ID** field, enter the MAC address (EUI64) of the target device where the certificate will reside (MSB order, such as 000D6F... for Ember EUI64s). This can be different than your target node's current EUI64, but if the address differs, the current one will generally be overwritten during programming.
5) Smart Energy 1.0 Certificates
   a) In the **Profile Attribute Data** field, enter any custom hex data you want associated with this device. (The recommended format is profile ID [0109] + cert type [1 for test] + 16-bit ZigBee Manufacturer Code + optional customer data of any length.)
   b) Leave the **Public Key** field empty!
6) Smart Energy 1.2 Certificates
   a) Leave the Lifetime field empty
   b) Check the **Key Agreement** checkbox
   c) Leave the Override Certificate Attributes field empty.
   d) Leave the Public Key Contribution field empty.

7) Click the **Generate** button.
8) Highlight and copy the text in the HTML table on the resulting page.
9) Open a text editor and paste the contents of the table into the text file; save the file.

3 Certificate File Modification

3.1 Combined Certificate File

If you intend to install both certificates onto a device you may combine the contents of the certificate files into a single file.

Note: This portion of the process is subject to change if Certicom's certificate generation web page alters its output format. Silicon Labs is working with Certicom in the hope of achieving a more consistent output format in the future, one which would require less manual editing before programming.

3.2 Smart Energy 1.0

At the beginning of this process, the certificate text file you created in the previous step should look something like this (with different hex numbers in the fields):

```
CA Pub Key: 0200fde8a7f3d1084224962a4e7c54e69ac3f04da6b8
Device Implicit Cert: 02040e92886475999701a626a75be9cfb9ccb0ee7481
000d6f000092e0475445535453454341010910 83d1bbd1bbd1bb
Device Private Key: 00ea5606dec9ec8f85a5f53405b67b2988b74bcd73
Device Public Key: 0202f25c9e4aaf910d6bbc16f444715d39962e3a5500
```

1. (optional) Remove "Device Public Key" line from the certificate text file, as our tools do not need it. If you do not remove this line, it is ignored.
2. Remove extra line breaks in the hex string following "Device Implicit Cert:" so that all characters are on one line.
3. Change "CA Pub Key" to "CA Public Key"
4. Make sure that only a single blank space is between the ":" and the hex string of each line (no tabs or extra white space).
5. Remove the extra blank space at the end of each line before the line return.

At the end of the process, the certificate text file should look like the following, with the Device Implicit Cert line on a single line:

```
CA Public Key: 0200fde8a7f3d1084224962a4e7c54e69ac3f04da6b8
Device Implicit Cert:
02040e92886475999701a626a75be9cfb9ccb0ee7481000d6f000092e0475445535453454341010910 83d1bbd1bbd1
bb
Device Private Key: 00ea5606dec9ec8f85a5f53405b67b2988b74bcd73
```

3.3 Smart Energy 1.2

At the beginning of this process the certificate text file you created in the previous step should look something like this (with different hex numbers in the fields):

```
CA Pub Key:  0207a445022d9f39f49bdc38380026a27a9e0a1799313ab28c5c1a1c6b605154db1dff6752
Device Implicit Cert:
      00e4d6197cf4b7b87e0d08111213141516171800532 0b5f6ffffffff000000000000000900
0200849946d913e09111970ff24bac05605fecaf258dfc1c586de5690de8b8d11b393a1b69
Device Private Key:
      01817e7b640c0833c3daa12cf57284e959551455246a0cbcf876955c4492a0416350255d
Device Public Key:  02064af594acdee3c5cc41086c3f72f5b3ef6197cee9726e98d78227b4e0401cf08df0781d
```

1. Remove "Device Public Key" line from the certificate text file, as our tools do not need it.
2. Remove extra line breaks in the hex string following "Device Implicit Cert:" so that all characters are on one line.
3. Change "CA Pub Key" to "CA Public Key (283k1)"
4. Change “Device Implicit Cert” to “Device Implicit Cert (283k1)”
5. Change “Device Private Key” to “Device Private Key (283k1)”
6. Make sure that only a single blank space is between the ":" and the hex string of each line (no tabs or extra white space).
7. Remove the extra blank space at the end of each line before the line return.

```
CA Public Key (283k1):
0207a445022d9f39f49bdc38380026a27a9e0a1799313ab28c5c1a1c6b605154db1dff6752
Device Implicit Cert (283k1):
00e4d6197cf4b7b87e0d08111213141516171800532 0b5f6ffffffff000000000000000900020084994 6d913e09111
970ff24bac05605fecaf258dfc1c586de5690de8b8d11b393a1b69
Device Private Key (283k1):
01817e7b640c0833c3daa12cf57284e959551455246a0cbcf876955c4492a0416350255d
```

3.4 EM3xx Platform

1. Ensure that the Debug Adapter (ISA3) Utilities (version 1.0.2 or higher) are installed. If you want to verify, you can check your computer’s Programs list for “Ember ISA3 Utilities”.
2. Change to the directory where the certificate text file is stored.
3. Determine the IP address of the target node's Debug Adapter (ISA3). You can use the Network Analyzer adapter properties window to view the IP address and other Debug Adapter (ISA3)/node details.
4. Run the following command to apply the certificate (shown for IP address 192.168.0.1 and certificate filename cert_001.txt):

   ```
   em3xx_load --ip 192.168.0.1 --cibtokenspatch cert_001.txt
   ```

Note: If you are overriding previously written certificate data, you may need to add an "--Override" flag before the "--cibtokenspatch" flag. However, use this option with caution, as it can permanently corrupt your device if the flash-writing process is terminated unexpectedly.

5. Optionally, verify written certificate data with a command like the following:

```
em3xx_load --ip 192.168.0.1 --cibtokensprint
```

4 Installation Code Generation

1. Pick a random hex string of 6, 8, 12, or 16 bytes. You can generate this programmatically with a random number generate if you wish.
2. Open a text editor and enter this string (as ASCII) in a file by itself, preceded by the string "Install Code: ". Note the single whitespace character following the colon.
3. Save this file for later use.

5 Installation Code Programming

Note: This is not necessary for devices that only form SE networks (like an Energy Services Interface (ESI), which is typically the Trust Center for the network) rather than join them.

5.1 EM3xx Platform

1. Change to the directory where the installation code file is stored.
2. Determine the IP address of the target node's Debug Adapter (ISA3). You can use Network Analyzer's adapter properties window to view the IP address and other Debug Adapter (ISA3)/node details.
3. Run the following command to apply the installation code (shown for IP address 192.168.0.1 and installation code filename inst_001.txt):

```
em3xx_load --ip 192.168.0.1 --cibtokenspatch inst_001.txt
```

Note: If you are overriding previously written installation code data, you may need to add an "--Override" flag before the "--cibtokenspatch" flag. However, use this option with caution, as it can permanently corrupt your device if the flash-writing process is terminated unexpectedly.

4. Optionally, verify written installation code data with command like the following:

```
em3xx_load --ip 192.168.0.1 --cibtokensprint
```

6 Application Setup (Build Time)

6.1 System on Chip

Ensure that you have the ECC library for your SoC platform. Access is granted by Silicon Labs Support upon request.

1) Create a new Ember AppBuilder configuration from Ember AppBuilder's File | New | Application Configuration menu.
2) In Ember AppBuilder configuration, on the Stack Configuration tab, perform the following settings:
3) If you are using unique, per-device link keys (as should be the case for production deployments), set the **Security** option to "Smart Energy Security full (compliant)".

If you are using a single, global link key for all devices (often used in development/testing scenarios to reduce complexity), set the **Security** option to "Smart Energy Security test".

4) Check the **Use ECC 163k1** is enabled (checked).

5) In the **Library path** text entry box next to the **Use ECC 163k1** checkbox enter the filepath to the location of your ECC library file (*.xap for EM250 or *.a for EM35x).

6) If you intend to use the 283k1 ECC Curve (Smart Energy 1.2), then check the **Use ECC 283k1** checkbox.

    1. In the **Library path** text entry box next to the **Use ECC 283k1** checkbox enter the filepath to the location of your ECC library file (*.a for EM35x).

Note: Some versions of Ember Desktop don't support white space in the ECC library path, so you may need to relocate these files to satisfy this requirement.

7) Set up the remaining SE device configuration as appropriate, and generate the project.
8) Populate callbacks in the generated project as necessary, then build and load to the target device (after the certificate and installation codes have been programmed as described above).

6.2 Network Coprocessor

There are different versions of the network coprocessor with and without ECC support compiled in. Access to the ECC version is granted by Silicon Labs Support upon request.

The ECC version of the network coprocessor firmware contains support for both Smart Energy 1.0 and Smart Energy 1.2 curves. However which curves can be utilized depends on the certificates that are installed on the coprocessor.

7 Application Setup (Run Time) Prior to Joining a New Device to the HAN

Note: This process is only required if you are using installation codes to generate unique, per-device link keys, such as when "Smart Energy Security (full)" is selected as the security model for your application configuration in Ember AppBuilder.) If you are using a global link key for joining, such as when using Ember AppBuilder's "Smart Energy Security (test)" security model, skip this section.

This section describes the process of setting up the Trust Center device (the network coordinator) for the SE network to accept an incoming SE device into its home area network (HAN). It also describes the process of setting up a new HAN device prior to joining the HAN created by this Trust Center.

7.1 Procedure for Development Prototypes / Debugging

This process relies on the serial command line interface (CLI) to the Ember application framework. If the CLI is no longer supported or accessible on your network's Trust Center or incoming HAN device, please refer to the "Procedure for Production/Field Deployments" later in this section.

1. Before joining a HAN device to the SE network, determine its installation code string, including its 16-bit CRC (in LSB order), as well as its EUI64 (MAC address). In a development/debugging environment, you can do this using the em3xx_load tools with the appropriate "print" option to output the installation code data. See the "Installation Code Programming" section for more information.

2. Use the MMO hash algorithm to compute the device-specific link key from the installation code. Devices running EmberZNet PRO 4.3.0 and later can perform an AES MMO hash operation using the emberAesHashSimple() method provided on SoC platforms or the ezspAesMmoHash() API provided on EZSP host platforms. Devices running EmberZNet PRO 4.7.0 and later can utilize the “option install-code …” CLI command at the Trust Center device as an alternative during the development/debugging phase. The application framework then verifies the CRC for the provided installation code, computes the device-specific link key from this code, and then adds the hashed key result to the specified key table index on the Trust Center for the specified EUI64, thereby allowing you to skip step 3.
3. (Skip this step if using the “option install-code ...” CLI command method described in Step 2.) Once you have the EUI64 and device-specific link key, access the trust center for this HAN and register the key into the key table using the "option link ..." CLI command. This command takes a table index, an EUI64 specified in MSB order (or LSB if using EmberZNet PRO versions older than 4.3), and a key (in MSB order, just as it is printed by "keys print") for that device. For example, for EUI64 0x000D6F0011223344 and key 0x00112233445566778899AABBCCDDEEFF (shown with EUI in MSB as expected in newer stack versions):

```
option link 0 {44 33 22 11 00 GF 0D 00} {00 11 22 33 44 55 66 77 88 99 AA BB
CC DD EE FF}
```

4. Confirm that the proper key table entry now exists and is displayed in the output of the "keys print" command at the trust center.

7.2 Procedure for Production/Field Deployments

1. Before joining a HAN device to the SE network, determine its installation code string, including its 16-bit CRC (in LSB order), as well as its EUI64 (MAC address); these byte values are meant to be published externally with the device for use during installation.
2. Using some out-of-band (non-ZigBee) method, such as verbally or through some proprietary communications interface, convey the HAN device's installation code to the ESI for the HAN, its trust center device (if different from the ESI), or some head-end device in the utility's backhaul network that has access to the HAN's ESI.
3. Have the ESI (or the utility’s head-end) sanity-check the provided installation code by computing the CRC of those hex bytes (less the final two, which are the provided CRC16 from the installer) using the CRC16 algorithm described in the "CRC Algorithm Information" section (section 5.4.8.1.1.1 in the current [r15] version) of the ZigBee Smart Energy Application Profile Specification (ZigBee document 075356). The computed CRC (when converted into LSB order) for the 6/8/12/16-digit code should match the last 4 digits of the provided installation code string.
4. Once the installation code string (variable-length code + 2-byte CRC16 in LSB order) has been verified, have the ESI or its head-end compute the device-specific initial link key by performing an AES MMO hash function against the entire 8/10/14/18-byte string, using the algorithm described in the "MMO Hash Code Example" section (section 5.4.8.1.2.1 in the current [r15] version) of the ZigBee Smart Energy Application Profile Specification (ZigBee document 075356). Devices running EmberZNet PRO 4.3.0 and later can perform this AES MMO hash operation using the emberAesHashSimple() method provided on SoC platforms or the ezspAesMmoHash() API provided on EZSP host platforms, as demonstrated by the optionInstallCodeCommand() routine found in app/framework/cli/option-cli.c in EmberZNet PRO 4.7.0 and later.
5. Once this key has been determined for the incoming HAN device, install a link key table entry in the HAN’s trust center by using the emberSetLinkKeyTableEntry() ir emberAddOrUpdateKeyTableEntry() function with the device-specific key and EUI-64.

8 Joining Process for New Device

If you are using installation codes to create unique keys, the application setup process discussed in the previous section “Application Setup (Run Time) Prior to Joining a New Device to the HAN” should have been performed.

1. Join the new HAN device to the ESI's HAN (using the Button Form/Join Plugin or "network join ..." CLI command or emberAfStartSearchForJoinableNetwork API function, for example).
2. The ESI (as Trust Center) will trigger its emberAfTrustCenterJoinCallback() to indicate the outcome of the initial joining process. If successful, the joining device should begin CBKE (certificate-based key establishment).
3. If both the ESI and HAN devices support CBKE and ECC and have valid certificates issued by the same authority, CBKE should succeed, and the HAN device should move on to registration (asking the ESI to bind to it on specific clusters). When the SE registration process completes, the HAN device will trigger its emberAfRegistrationCallback() to notify the application.
4. After the SE registration completes successfully, the HAN device can now send/receive messages to/from the ESI using its CBKE-authorized link key.

9 Network Analyzer Capture Setup

To capture the initial joining process before CBKE, first determine the device's preconfigured link key (either the unique one generated from the installation code as described in the section “Application Setup (Run Time) Prior to Joining a New Device to the HAN” or the global one if using SE Security Test mode). Enter this code into Network Analyzer using either of the two methods described below before attempting to join the HAN.

To capture the encrypted SE traffic after CBKE/registration has been performed, determine the CBKE-authorized link key by querying either the HAN device or the ESI. If the serial CLI is still available, you can use the "keys print" command. If you are using the stack API directly, use the emberGetKey() API. Enter the discovered key into Network Analyzer (see the two methods below) after CBKE completes; remember that this key is unique for each instance of CBKE, even for the same pair of devices.

You can enter the key into Network Analyzer in either of two ways:

1. Through the main list of keys at File: Preferences: Decoding: Security Keys. This data entry method is more flexible, but keys must be entered here before beginning a capture session, else they won't be used for decryption.
2. Through the live capture keys menu at Edit: Live Capture Security Keys. This has a very basic data entry method but the keys are applied to decryption of future events right away, even in already open (or still-capturing) logs. The traffic captured before entering this key won't be decrypted unless you save and re-open the capture session.

CONTACT INFORMATION

Silicon Laboratories Inc.

400 West Cesar Chavez
Austin, TX 78701
Tel: 1+(512) 416-8500
Fax: 1+(512) 416-9669
Toll Free: 1+(877) 444-3032

Please visit the Silicon Labs Technical Support web page for ZigBee products:
www.silabs.com/zigbee-support and register to submit a technical support request