Release Notes

Product: Application Framework for EmberZNet 5.9.2
Release Date: April 7, 2017

1 Overview

This release contains the GA release of Application Framework for use with EmberZNet 5.9 for the EFR32 and EM3xx platforms. This release must be used with Silicon Labs Simplicity Studio 4.0. The Application Framework is installed along with the EmberZNet stack. For more information on software installation and support, see QSG106, Getting Started with EmberZNet."

2 The 5.9 Release

This release includes a number of new features, improvements, and bug fixes. Customers upgrading from previous releases are strongly encouraged to carefully review this section. It is important to become with familiar with the changes in this release before attempting to migrate applications.

Version 5.9.0

2.1 New Features

2.1.1 Secure EZSP protocol

The Secure EZSP protocol encrypts EZSP frames between the host and NCP. Security key is set by the host, followed by the security parameters. The protocol uses HMAC with AES-MMO for authentication and AES-CCM with 128-bit key for encryption. The security key is not permanent and can be reset through an API.

2.1.2 Switched Multiprotocol

The Switched Multiprotocol feature allows the device to receive commissioning commands through Multiprotocol Stack Interface (MPSI) messages. A new MPSI plugin, along with its message configuration window, allow an application to send and receive MPSI messages. This feature is used in conjunction with the storage Gecko bootloader to achieve Switched Multiprotocol, where one application commissions network parameters for another app that is then bootloaded.

2.2 Configuration Changes

One configuration change was made in this release.

2.2.1 EZSP Protocol Version 5

The host now uses EZSP protocol version 5 when communicating with the NCP. The NCP image must be updated along with the host application. A version mismatch will cause the host to assert at startup.

2.3 Removed APIs

No APIs were removed in this release.

2.4 Removed Callbacks

No callbacks were removed in this release.

2.5 Removed CLI Commands

No CLI commands were removed in this release.

2.6 Removed Plugins

No plugins were removed in this release.

2.7 Removed Sample Applications

No sample applications were removed in this release.

2.8 Changed APIs

No APIs changed in this release.

2.9 Changed Callbacks

No callbacks changed in this release.

2.10 Changed CLI Commands

No CLI commands changed in this release.

2.11 Changed Plugins

One plugin changed in this release.

2.11.1 Device Table

The function `emberAfPluginDeviceTableMessageSentStatus` in the Device Table plugin has changed. Additional parameters for the profile id and cluster id were added. The call to `emberAfPluginDeviceTableMessageSentStatus` from the HA Gateway sample application has been updated to reflect the new parameters. Customers who use the Device Table plugin directly will need to update any calls to `emberAfPluginDeviceTableMessageSentStatus`.

2.11.2 EZSP Common

The EZSP Common plugin now requires either the EZSP Secure Protocol or EZSP Secure Protocol Stub plugin. AppBuilder will automatically enable the EZSP Secure Protocol Stub plugin in existing applications. Customers who want to use the secure protocol should enable the EZSP Secure Protocol plugin. These plugins are described in section 2.21.1.

The callbacks `emberAfGenerateRandomKey` and `emberAfGenerateRandomData` were added to the EZSP Common plugin. These functions allow the application to generate random keys on the host, instead of on the NCP. The default implementation will use the NCP as in previous releases. The new Security Support plugin, described in section 2.21.2 can be used to generate random keys on Unix-like operating systems. Customers who want to generate keys themselves can implement these functions directly.

2.11.3 EZSP SPI

The generated makefile for applications that use the EZSP SPI plugins will now link the pthread library automatically. Previously, the pthread library needed to be manually linked.

2.12 Changed Sample Applications

No sample applications changed in this release.

2.13 Deprecated APIs

No APIs were deprecated in this release.

2.14 Deprecated Callbacks

No callbacks were deprecated in this release.

2.15 Deprecated CLI Commands

No CLI commands were deprecated in this release.

2.16 Deprecated Plugins

No plugins were deprecated in this release.

2.17 Deprecated Sample Applications

No sample applications were deprecated in this release.

2.18 New APIs

One new API was added in this release.

2.18.1 emberAfMainInit

Initialization code was moved from `emberAfMain` to the new `emberAfMainInit` function. `emberAfMainInit` must be called prior to `emberAfMain`. The Simple Main plugin has been updated for this change. Customers who do not use the plugin must call `emberAfMainInit` directly.

2.19 New Callbacks

No callbacks were added in this release.

2.20 New CLI Commands

No CLI commands were added in this release.

2.21 New Plugins

Four new plugins were added in this release.

2.21.1 EZSP Secure Protocol and EZSP Secure Protocol Stub

The EZSP Secure Protocol plugin provides an implementation of the Secure EZSP protocol. The Secure EZSP protocol encrypts EZSP frames between the host and NCP. Both the host and the NCP must support Secure EZSP commands, and customers must manually build the NCP image with Secure EZSP plugin to use the feature.

AppBuilder will automatically include the EZSP Secure Protocol Stub plugin when upgrading existing applications

2.21.2 Security Support

The Security Support plugin provides support features for security, such as random number generation, on Unix-like hosts. Customers who want to generate random keys on host, instead of the NCP, should include this plugin.

2.21.3 Unix Library

The Unix Library plugin provides common functionality for Unix hosts. It includes functionality that was automatically included in host applications in previous releases. Customers developing host applications should include the Unix Library plugin in their application or implement the equivalent functionality themselves. AppBuilder will automatically include this plugin when upgrading existing applications

2.22 New Sample Applications

Three new sample application were added in this release.

2.22.1 SecureEzsp

The SecureEzsp sample application demonstrates the host communicating with an NCP application using Secure EZSP protocol. This host application is meant to be used with the NCP sample application SecureEzspNcp.

2.22.2 SwitchedMultiprotocolJoiningDevice

The SwitchedMultiprotocolJoiningDevice sample application is new in this release. The SwitchedMultiprotocolJoiningDevice application receives commissioning commands as Multiprotocol Stack Interface (MPSI) messages, which are retrieved from storage on the device. Note that the application requires that these messages be written into storage before the SwitchedMultiprotocolJoiningDevice is booted by another application. A typical use of this application is to first have a BLE image run on the joining device. The BLE application receives MPSI messages from some source, saves them in storage, and then switches to the SwitchedMultiprotocolJoiningDevice application, which attempts to join a network based on the received MPSI configuration. For the purpose of the SwitchedMultiprotocolTrustCenter and SwitchedMultiprotocolJoiningDevice sample applications, the EUI and install code of the SwitchedMultiprotocolJoiningDevice should be sent to the SwitchedMultiprotocolTrustCenter via MPSI messages. The SwitchedMultiprotocolJoiningDevice application and SwitchedMultiprotocolTrustCenter application should then be instructed to join and form a network (respectively) to demonstrate a switched multiprotocol joining procedure.

2.22.3 SwitchedMultiprotocolTrustCenter

The SwitchedMultiprotocolTrustCenter sample application is new in this release. The role of the SwitchedMultiprotocolTrustCenter application is to form a network and wait for Multiprotocol Stack Interface (MPSI) messages. These MPSI messages may instruct the SwitchedMultiprotocolTrustCenter application to add a joining device's EUI and install code into the transient key table or open the network for joining. The intended scenario is for a BLE trust center application, which runs on the same host as the SwitchedMultiprotocolTrustCenter, to feed the SwitchedMultiprotocolTrustCenter application with MPSI messages that originate from some source. For the purpose of the SwitchedMultiprotocolTrustCenter and SwitchedMultiprotocolJoiningDevice sample applications, the EUI and install code of the SwitchedMultiprotocolJoiningDevice should be sent to the SwitchedMultiprotocolTrustCenter via MPSI messages. The SwitchedMultiprotocolJoiningDevice application and SwitchedMultiprotocolTrustCenter application should then be instructed to join and form a network (respectively) to demonstrate a switched multiprotocol joining procedure.

3 Known/Fixed Issues

3.1 Fixed Issues

3.1.1 Fixed Issues in EmberZNet 5.9.0

- Issue 238768: The "device masserase" command does not erase the upper half of flash for EFR32xG12, EFM32JG12, and EFM32PG12 parts, regardless of flash size.

- Issue 191014: All board headers will now default to defining EMDRV_RTCDRV_USE_LFRCO, ensuring that both SoC and NCP builds will default to LFRCO.

3.2 Known Issues

- Issue 159611: ZCL attribute tokens creator codes likely to change if you add or remove one or more attributes. For instance, if you add an attribute whose cluster ID or attribute ID is not the largest numerically, then this attribute gets inserted into a list of creator codes and makes all creator codes after it to be different (shifted).

- Issue 136274: Node State Cache incorrectly indicates no nodes in trace file.

- Issue 110166: Extended Ember Desktop Decoder's events window to be customizable

- Issue 92566: APS Alarm message always decodes to say missing packets

- Issue 65929: Global channel change via Sniffer Settings dialog doesn't impact EM35x sniffers

- Issue 65898: ISD cannot find JRE on some 64-bit Windows 7 machines

- Issue 65687: Console view renders ASCII 0x81 character incorrectly

- Issue 213424: Problem with ZLL Devices responding to a multicast addScene when they should not.

- Issue 205394: In situations where a concentrator doesn't use the NCP-based concentrator-util-library code to manage source routing, a route error will trigger an MTORR from the Conc Support plugin, but the new source route may not be known for a long time. The ZigBee NCP firmware concentrator-util solves this problem by doing a ZDO Network Address Request for the target device. For SoC, until that functionality is added to the Conc Support plugin code, it needs to be implemented manually.

- Issue 201417: Adding GPIO Sensor Interface plugin to an EM358x project results in error: "identifier "GPIO_SENSOR_IRQ" is undefined".

- Issue 146795: Added Alarm Cluster functionality to IAS Zone Plugin.

- Issue 126087: Sleepy end device would return NO_LOCAL_RESOURCES when a coordinator initiates key establishment with it in Multi-networking.

- Issue 123399: Non-sleepy endpoint does not always keep correct network parameters on reset in multi-networking.

- Issue 121707: Reporting does not send to a group address.

- Issue 119828: ota-client.c does not use the server EUI64 in Partner Link Key Exchange.

- Issue 101644: Add a callback to the check-in interval for poll control.

- Issue 92147: ZLL Scan Response Should Be Sent at Power 0 rather than last-used power level

- Issue 83798: Image Integrity Tag generation in image builder for an OTA file

- Issue 66944: Duplicate Key Confirm Response message can lock up KE plugin state machine

- Issue 66786: "zcl ota server reload" doesn't properly reload image info when using OTA Simple Storage plugin

- Issue 66785: Messaging Client plugin should differentiate between Cancel Msg command and timed out / replaced message

- Issue 66508: Framework should avoid sending unicast loopback messages with APS security since stack doesn't support this