AN875

RF4CE GDP ENHANCED SECURITY

This document describes how to use the enhanced security feature of the Generic Device Profile (GDP) in the context of the Generic Device Profile plugin offered by Silicon Labs. It gives an overview of the feature and discusses the specific plugin configuration required to use it.

New in This Revision

Initial release.

Contents

1 Introduction

Enhanced security is an optional feature of the Generic Device Profile (GDP) in ZigBee RF4CE. This feature builds on the standard security mechanism in the RF4CE network stack and provides additional protections against eavesdropping nodes. The enhanced security key negotiation procedure uses an authentication algorithm named AES-CMAC, which uses the Cipher-based Message Authentication Code (CMAC) with the 128-bit Advanced Encryption Standard (AES).

2 Export Restrictions

Implementations of both the AES-CMAC algorithm and the AES-128 cipher are required to enable the enhanced security feature. Silicon Labs provides a source code plugin for the high-level AES-CMAC algorithm in the EmberZNet software. However, AES-128 is classified as strong cryptography and is therefore subject to export restrictions. Because of this, some customers will require additional configuration in order to use enhanced security.

3 System-on-Chip Configuration

Ember ZigBee system-on-chip (SoC) platforms, which are already subject to export control, provide hardware support for AES-128. To utilize enhanced security, customers using SoC platforms must perform the following configuration:

1. Enable the **Generic Device Profile** plugin.
2. Enable the **Enhanced security** option in the Generic Device Profile plugin.
    a. Optionally enable the **Standard shared secret** option in the Generic Device Profile plugin.
    b. Optionally enable the **Vendor-specific shared secrets** option in the Generic Device Profile plugin.
3. Enable the **AES-CMAC** plugin.

No additional configuration is required on SoC platforms.

4 Host Configuration

Customers using host platforms with a network coprocessor, however, must provide their own implementation of AES. Silicon Labs cannot provide a full software implementation of AES for these platforms due to export restrictions. Instead, the EmberZNet software includes a plugin that serves as a wrapper for AES. The wrapper provides the higher-level APIs used by the AES-CMAC plugin. Customers are only required to provide the lower-level APIs to perform AES. In order to minimize the integration burden for customers on host platforms, the wrapper is written to use the Rijndael cipher upon which AES is based. An implementation of Rijndael is in the public domain and is widely available from third parties on the Internet.

To configure enhanced security on a host platform, customers must acquire the Rijndael source and save it in a location on the same drive as the EmberZNet software installation. Implementations of Rijndael generally consist of the following files:

- rijndael-alg-fst.c
- rijndael-alg-fst.h
- rijndael-api-fst.c
- rijndael-api-fst.h

The header files rijndael-alg-fst.h and rijndael-api-fst.h are included in the EmberZNet installer to assist customers in locating the corresponding source files. The following websites provide implementations of Rijndael that are known to be compatible with EmberZNet as of this writing:

- http://www.efgh.com/software/rijndael.zip (md5: cd49617fa6593d2ab67a68f64ede2d78)

Note that these are third-party websites and are not affiliated or controlled by Silicon Labs. Silicon Labs makes no guarantee about the availability of the website or the quality or correctness of the implementation.

Once Rijndael has been acquired, the following steps must be performed to complete the configuration:

1. Enable the **Generic Device Profile** plugin.
2. Enable the **Enhanced security** option in the Generic Device Profile plugin.
    a. Optionally enable the **Standard shared secret** option in the Generic Device Profile plugin.
    b. Optionally enable the **Vendor-specific shared secrets** option in the Generic Device Profile plugin.
3. Enable the **AES-CMAC** plugin.
4. Enable the **AES (Software)** plugin.
5. Set the path for **Rijndael algorithm source** in the AES (Software) plugin to the location of rijndael-alg-fst.c.
6. Set the path for **Rijndael API source** in the AES (Software) plugin to the location of rijndael-api-fst.c.

4.1 Performance

Note that AES operations performed in software may be significantly slower than those performed by dedicated hardware. Because of this, the enhanced security feature may not be suitable for use on all hosts. Customers must test the feature with their target platform to determine whether software AES is capable of meeting the timing constraints of the key exchange procedure.

5 Conclusion

Once the appropriate configuration steps are complete, customers may generate and compile their application. Nodes with enhanced security enabled will advertise support by setting the supportEnhancedSecurity bit of the *aplGDPCapabilities* attribute. The GDP plugin will set this bit based on the enhanced security option in the plugin. The *aplGDPCapabilities* attribute is exchanged during the configuration phase of the binding process. If both the originator and recipient indicate support for enhanced security, the GDP plugin will automatically perform the enhanced security key negotiation procedure after binding.

.

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