Syn-Tech Systems, Inc.

ProFLEX01-R2

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.4

Date: June 10, 2015

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Syn-Tech Systems, Inc., ProFlex01-R2, hereafter denoted the Module. The Module, validated to FIPS 140-2 overall Level 2, is a multiple-chip embedded module that provides protection for data in transit and data at rest.

The cryptographic boundary is defined as the physical perimeter of the PCB.

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 1 – Security Level of Security Requirements

1.1 Physical Cryptographic Boundary

The Module's physical form is depicted in the images below:

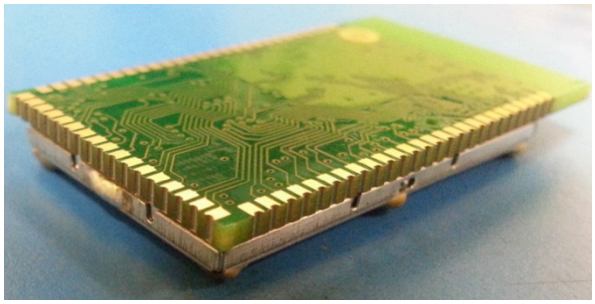

Figure 1 – Module Physical Boundary (bottom side, identical for both PNs)

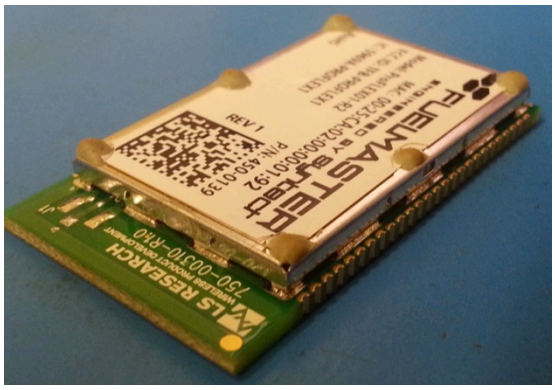

Figure 2 – Module Physical Boundary (top side, PN: 450-0139)

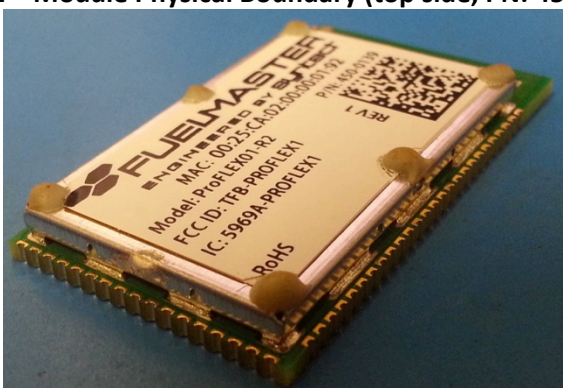

Figure 3 – Module Physical Boundary (top side, PN: 450-0140)

Port	Description	Logical Interface Type
Pins	All logical interfaces are provided by the physical pins of the PCB	Control in, Data in, Data out, Status out, Power In
Antenna	Radio antenna for communication	Control in, Data in, Data out, Status out

Table 2 – Ports and Interfaces

1.2 Logical Cryptographic Boundary

Figure 2 depicts the Module's logical boundary and operational environment.

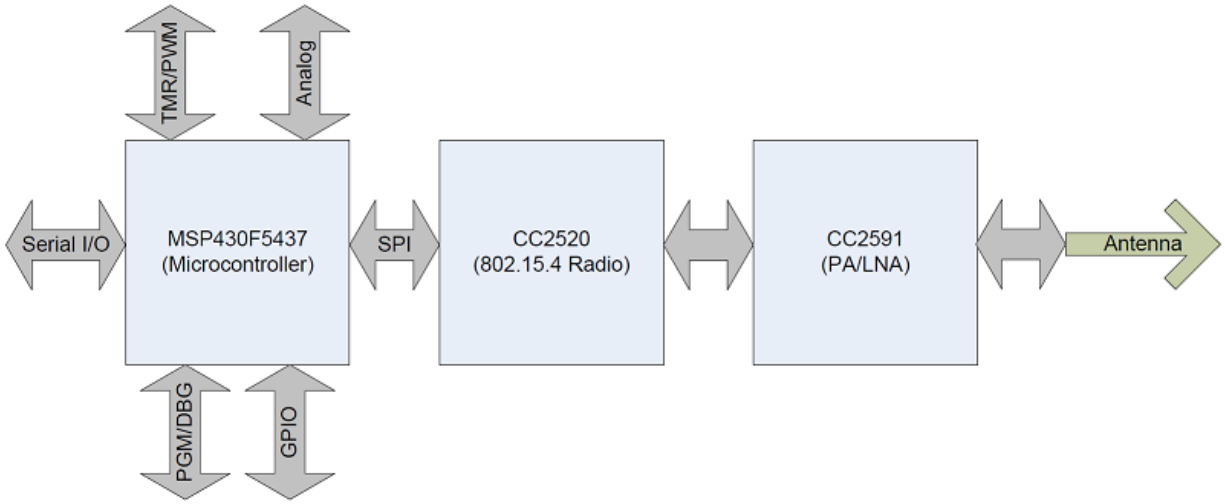

Figure 4 – Module Block Diagram

1.3 Versions and Mode of Operation

	Module	HW P/N and Version	Operating Environment
1	ProFlex01-R2	450-0139, 450-0140, Firmware Version 4.20	N/A

Table 3 – Versions

The two versions of the module differ in antenna type only. P/N 450-0140 includes a U.FL connector for an external antenna, whereas P/N 450-0139 uses a trace antenna. The Module only supports an Approved mode of operation. To verify that the Module is in the Approved mode of operation, the operator must verify they have the FIPS-Approved version of the module, as specified in this Security Policy, and can also review the FIPS Status Register to verify self-tests have passed successfully.

2 Cryptographic Functionality

The Module implements the FIPS Approved cryptographic functions listed in Table 4 and Table 5 below.

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption Modes: ECB Key sizes: 128 bits	3126 3128
AES	[FIPS 197, SP 800-38C] Functions: Encryption, Decryption, Key Wrap Modes: CCM Key sizes: 128 bits	3127 3129

Table 4 –Approved Cryptographic Functions

Note: AES CCM is approved for Key Wrap per SP 800-38F; however, this algorithm is not within the purview of SP 800-38F CAVS testing.

Algorithm	Description
N/A	N/A

Table 5 – Non-Approved but Allowed Cryptographic Functions

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

CSP	Description / Usage
Authentication Encryption Key (AEK)	Advanced Encryption Standard (AES) key used to authenticate operators
Transmission Encryption Key (TEK)	AES key used to protect data in transit
Generic Encryption Keys (GEK)	AES keys used to protect data at rest and transported keys

Table 6 – Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
N/A	N/A

Table 7 – Public Keys

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two operator roles, User and Cryptographic Officer (CO), as described in Table 8. The User and Cryptographic Officer are assumed by the same entity and share the same services. The Module does not support a maintenance role. All previous authenticated states are cleared upon power cycle. Authentication data is never persistently stored within the module and no feedback containing sensitive information is provided to the operator during authentication.

Role ID	Role Description	Authentication Type	Authentication Data
CO	Performs cryptographic operations.	Role-based	Knowledge of a shared secret

Role ID	Role Description	Authentication Type	Authentication Data
User	Performs cryptographic operations.	Role-based	Knowledge of a shared secret

Table 8 – Roles Description

3.2 Authentication Strength

Operators authenticate through proving knowledge of a shared secret. The shared secret is 128-bits in length. As a result, the authentication method has a probability of 1/2^128 that a random authentication attempt by an attacker will succeed, which is less than the 1/1000000 probability required. After three consecutive failed authentication attempts, the Module will block additional attempts for 60 seconds, limiting the number of authentication attempts permitted within a given minute. As a result, the probability that a brute force attack will succeed within a given minute is at most 3/2^128.

3.3 Services

All services implemented by the Module are listed in Table 9 and Table 10 below. Each service description also describes all usage of CSPs by the service.

Table 9 describes all authenticated services provided by the Module.

Service	Description	CO	U
Authenticate	Authenticate the operator to perform cryptographic services	X	X
Zeroize	Destroys all CSPs	X	X
Toggle Bypass	Enable or disable data protection and confidentiality for data in transit	X	X
Load Key	Decrypt a key and load it into a key storage register.	X	X
Set Key	Specify the encryption key to be used	X	X
Store Data	Save data at rest (encryption optional)	X	X
Read Data	Read data at rest (decryption optional)	X	X
Settings	Configure radio options	X	X
Send/Receive	Send and Receive Data Packets	X	X

Table 9 – Authenticated Services

Table 10 describes all unauthenticated services provided by the Module.

Service	Description
Self-Tests	Performs the Power-On Self-Tests and is invoked by power cycling the module

Service	Description
Get Status	Read the FIPS Status Register (which specifies the Bypass mode status, self-test status, and authentication status) and the FW version
Reset	Power cycle

Table 10 – Unauthenticated Services

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Service	CSPs		
	AEK	TEK	GEK
Authenticate	RE		
Zeroize	Z	Z	Z
Toggle Bypass			
Load Key	RWE	RWE	RWE
Set Key		RE	RE
Store Data		RE	RE
Read Data		RE	RE
Settings		RE	RE
Send/Receive		RE	RE
Get Status			
Reset			
Self-Tests			

Table 11 – CSP Access Rights within Services

4 Self-test

4.1 Power-On Self-Tests

Each time the Module is powered up it tests that the cryptographic algorithm is operating correctly. Power-On Self–Tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 12 below. The KAT must be completed successfully prior to any services being offered by the Module. If the KAT fails, the Module enters the error state and only status services will be made available. FIPS Status Bit 3 will be set to "0" for a firmware integrity error and FIPS Status Bit 1 will be set to "0" for a KAT failure.

Test Target	Description
Firmware Integrity	16-bit CRC
AES	KAT: Encryption Modes: CCM Key sizes: 128 bits

Table 12 – Power Up Self-tests

4.2 Conditional Self-tests

Test Target	Description
Bypass	Exclusive Bypass Test ensures the cryptographic engine is functioning appropriately prior to exiting bypass mode. In addition, the module performs two independent internal actions prior to entering bypass mode.

Table 13 – Conditional Self-tests

4.3 Critical Function Tests

Test Target	Description
N/A	N/A.

Table 14 – Critical Function Tests

5 Physical Security Policy

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Label and Epoxy (applied during manufacturing)	Every three months	Inspect for attempts to remove the label or epoxy
Tamper Resistant Enclosure	Every three months	Inspect for tamper evidence

Table 15 – Physical Security Policy

If the Label, Epoxy, and/or Enclosure show signs of tampering, contact your system administrator.

6 Operational Environment

The Module is non-modifiable and as such, the requirements of FIPS 140-2, Area 6, are not applicable.

7 Mitigation of Other Attacks Policy

N/A. The Module is not designed to mitigate any attacks beyond the scope of FIPS 140-2 requirements.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The module provides two operator roles: User and Cryptographic Officer.
2. The module provides role-based authentication.
3. The module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The operator is capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power-up self-tests do not require any operator action.
7. Data output is inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not support key generation.
13. The module does not enter or output plaintext CSPs.
14. The module does not output intermediate key values.

9 References

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001

Table 16 – References

10 Acronyms and Definitions

Acronym	Definition
AEK	Authentication Encryption Key
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
DRNG	Deterministic Random Number Generator
FIPS	Federal Information Processing Standards
GEK	General Encryption Key
POST	Power On Self-Tests
TEK	Transmission Encryption Key

Table 17 – Acronyms and Definitions