Palm Solutions Group

Security Policy

Version 2.52

1 Purpose and Scope

This document has been created as part of the process of submitting Palm Crypto Manager v2.0 to the FIPS-140-2 validation process. Crypto Manager is a software library that designed to make available cryptography services to applications written for Palm handhelds. Crypto Manager provides services such as encryption, decryption, key generation, pseudo-random number generation, and message authentication and digests. Crypto manager is designed so that any application for the Palm OS could potentially take advantage of its features.

This document helps to guide the design and implementation of the module, and aids in the evaluation of the module by providing an unambiguous definition of the set of rules (security policy) that govern the external behavior of the module.

Hereinafter, Crypto Manager will be referred to by its development name, FCCM, (FIPS Compliant Cryptographic Module).

2 Table of Contents

3 Module Objectives and Security Rules

This section describes the module objectives and security rules for the FCCM. All security rules listed are enforced by the module.

The security objectives of the FCCM are listed below.

- The functionality, documentation and testing of the FCCM is designed to meet the FIPS-140-2 Level 1 criterion.
- The FCCM will be validated on Palm device model i705 SW Version 2.0, Palm OS 4.1.
- The FCCM will support AES, SHA1, HMAC-SHA1, and FIPS approved algorithms for key generation (FIPS-186-2 Appendix 3.1 using SHA1), pseudo random number generation (PRNG) (FIPS-186-2 Appendix 3.1 using SHA1), and key transport (AES-CBC).
- The FCCM will support two types of AES keys: Data Encrypting Keys (DEK) and Key Encrypting Keys (KEK). Only the DEK keys can encrypt and decrypt data, and only the KEK keys can wrap and unwrap DEK keys for transport.
- The KEK and DEK keys can be either 128-bits or 256-bits long.
- The seed keys for the random byte generation algorithm will be 256-bits long.
- The seed keys for the DEK key generation algorithm will be 256-bits long.

The objectives are refined into the following detailed security rules.

1 The FCCM will be evaluated as a "multi-chip standalone" system.

1.1 The FCCM only has one mode of operation, which is the FIPS-140 mode. No operator action is required to enter this mode.

1.2 The FCCM does not support any non-approved security functions.

1.3 The physical boundary of the module is the same as the physical boundary of the Palm i705 device. The FCCM is entirely contained within a hard plastic production-grade enclosure that does not have a removable cover.

1.4 The Palm i705 device uses standard quality ICs.

1.5 The logical boundary of the module is the FCCM software library.

1.6 The operating environment for the FCCM is a "general purpose operational environment".

2 The FCCM does not support multiple concurrent operators.

3 The length of the KEK key must be greater than or equal to the length of the DEK key it is used to wrapping or unwrapping.

4 The FCCM supports the SHA1 algorithm

5 The FCCM supports the HMAC-SHA1 algorithm

6 The DEK key generation service and the PRNG generation service use the PRNG algorithm specified in Appendix 3.1 of FIPS-186-2

6.1 The seed key and state (XKEY) for the DEK generator and the PRNG generator are 256-bits long.

6.2 When generating output values, the generator can take optional seed bytes, which are digests with SHA1 to produce a 160-bit XSEED value.

7 The DEK keys are imported into and exported from the FCCM as ciphertext.

7.1 The DEK keys cannot be used to wrap and unwrap DEK keys.

7.2 The DEK keys cannot be used to wrap and unwrap KEK keys.

7.3 The DEK keys can be used with the data encrypt and decrypt services.

7.4 The DEK keys can be used with the HMAC-SHA1 service.

7.5 The DEK keys can be either 128-bits or 256-bits long.

8 There will be two types of operator roles: User role and Crypto Officer role.

9 The FCCM has one error state called Alarm.

9.1 The operator can invoke the self-tests explicitly.

9.1.1 The self-tests include known answer tests for all cryptographic algorithms. See section 7 for details.

9.1.2 The self-tests include a software integrity check that uses HMAC-SHA1.

9.1.3 There are no critical functions, and thus no critical function tests.

9.2 The operator obtains the "status output" by calling a Show Status service.

10 The module supports a Zeroize service that zeroizes all active keys and the software integrity check key, which is a KEK key used with the HMAC service.

3.1 Security Levels

This table specifies which security level we are pursuing for each area of FIPS 140-2:

Cryptographic Module Specification:	Level 1
Module Ports and Interfaces:	Level 1
Roles, Services, and Authentication:	Level 1
Finite State Model:	Level 1
Physical Security:	Level 1
Operational Environment:	Level 1
Cryptographic Key Management:	Level 1

EMI/EMC	Level 1
Self-Tests:	Level 1
Design Assurance:	Level 1
Mitigation of Other Attacks:	N/A

4 Operator Roles

The FCCM supports a User role and a Crypto Officer role. The security services available to each role are specified in a later section. Basically, the User role provides the basic services to process data (encryption, decryption and integrity checking), whereas the Crypto Officer role provides the services to manage keys.

The FCCM does NOT support a Maintenance role.

5 Cryptographic Keys and Management

The FCCM supports two kinds of keys: Data Encryption Keys (DEK) and Key Encryption Keys (KEK). The following subsections address all the FIPS-140-2 key management areas.

5.1 Random Number Generators

The KEK keys are generated outside the FCCM so there is no issue with random number generation for these keys.

5.2 Key Generation

The KEK keys are generated outside the FCCM so there is no issue with generation for these keys.

The DEK keys (both 128-bit and 256-bit) can be generated by the FCCM. The keys are generated using the FIPS approved algorithm (described in Appendix 3.1 of FIPS-186-2).

6 Security Services by Role

This section describes which services can be accessed by which roles. It begins with a description of the services and then presents an access matrix.

6.1 Brief Description of Services

The FCCM supports the following security services. There are no Critical Operations and there are Conditional Tests supported by the FCCM module. In the list below "DEK" is an acronym for "Data Encryption Key" and "KEK" is an acronym for "Key Encrypting Key."

- Encrypt/Decrypt data with AES and a DEK key.
- Integrity check data with HMAC-SHA1 with a DEK or KEK key.
- Digest data with SHA1.
- Load/Zeroize KEK key.
- Key Entry/Output (Wrap/Unwrap DEK key with KEK key).
- Load seed key for DEK Generator.
- Generate/Zeroize DEK key.
- Load seed key for PRNG Generator.
- Generate random bytes.
- Show status.
  This service allows the operator to find out the status of the device. It will be one of Uninitialized, Idle, Busy or Alarm.
- Perform self-tests.
  The module performs the following Power-up self-tests:
  - Cryptographic algorithm tests:
    - AES (CBC mode)
    - HMAC with SHA-1
    - PRNG
  - Software/Firmware Integrity Check:
    - HMAC
- Reset alarm.

- Zeroize module.
  The FCCM is a software library, so the FIPS-140-2 concept of "power-on" needs to be mapped into the operations that "load" the library into the address space of the application that will use it. The FIPS-140-2 self-tests are performed during "load," which involves calling a standard PalmOS library function called "open". The "load" happens when a application that is using the FCCM is launched (activated) by the user. It does not happen automatically when the device is turned on. The library can also be "unloaded" by the application, which matches the FIPS-140-2 concept of "power off." This action will cause the FCCM module to zeroize any security relevant data items that remain within the module, which is performed by a PalmOS standard library function called "close". The "unload" happens when the user launches (activates) a new application or when they terminate the application explicitly.

6.2 Service Access Matrix

The following three matrices define the security services that are available to each role. Notice that each service is available to only one role, thus it is possible to identify the operator role from the service being used.

Table 1. Role vs. Services Matrix 1 of 3

Role	Encrypt/Decrypt	HMAC	Digest	Load KEK	Key Transport
User	Y	Y	Y		Y
Crypto Officer				Y	

Table 2. Role vs. Services Matrix 2 of 3

Role	Load DEK Seed	Generate DEK	Load PRNG Seed	Generate Rand.
User		Y		Y
Crypto Officer	Y		Y	

Table 3. Role vs. Services Matrix 3 of 3

Role	Show Status	Perform Tests	Reset Alarm	Zeroize Module
User				
Crypto Officer	Y	Y	Y	Y

The FCCM includes both an approved generation method and a random byte generator that use the same FIPS approved algorithm (FIPS-186-1 Appendix 3.1) that is based on the compression function of the SHA1 digest algorithm. The FCCM has two generators to make it easier to ensure that Keys and Initialization Vectors are computed from different seed keys.

7 Critical Security Parameters

The Critical Security Parameters (CSP) for the FCCM are:

- KEK keys
- DEK Keys
- DEK generator seed keys
- PRNG generator seed keys

The following matrices show how the CSP are used by the different services.

Notice that there are no CSPs associated with the "Show Status", "Perform Self-Tests", and "Reset Alarm" services.

Table 4. Services vs. CSP Matrix 1 of 2

Service	KEK Key	DEK Key	DEK Gen Seed
Encrypt/Decrypt		Y	
HMAC Data	Y	Y	
Digest Data			
Load/Zeroize KEK	Y		
Key Transport	Y	Y	
Load DEK Gen Seed			Y
Gen/Zero DEK		Y	
Load PRNG Seed			
Gen Random			
Show Status			
Perform Self Tests			
Reset Alarm			
Zeroize Module	Y	Y	Y

Table 5. Services vs. CSP Matrix 2 of 2

Service	PRNG Seed
Encrypt/Decrypt	
HMAC Data	
Digest Data	
Load/Zeroize KEK	
Key Transport	
Load DEK Gen Seed	
Gen/Zero DEK	
Load PRNG Seed	Y
Gen Random	
Show Status	
Perform Self Tests	
Reset Alarm	
Zeroize Module	Y

8 Access Policy

This section defines which CSP can be accessed by different roles performing different services. The FCCM access policy is simplified by making each service useable by only one role, thus the access matrix can be defined separately for the User role and the Crypto Officer role. Each service can only be accessed by one role, and that role is implicitly identified by the act of call the service routine.

Each CSP can be accessed in four modes: Create, Read, Update, Zero. The Create mode means allocating and writing an item for the first time. The Update mode implies being able to read and write the item. The Zero mode means zeroize and deallocate the item.

Notice that there are no CSPs associated with the "Show Status", "Perform Self-Tests", and "Reset Alarm" services.

Table 6. CSP vs. Services in User Role Matrix

CSP	Encrypt / Decrypt	HMAC	Digest	Key Transport	Gen Random	Gen / Zero DEK
KEK Key		Read		Read		
DEK Key	Read	Read		Read		Create/Zero
DEK Gen. Seed						
PRNG Seed						

Table 7. CSP vs. Services in Crypto Officer Role Matrix 1 of 2

CSP	Load KEK	Load DEK Seed	Load PRNG Seed	Show Status	Perform Self Tests
KEK Key	Create				
DEK Key					
DEK Gen. Seed		Read			
PRNG Seed			Read		

Table 8. CSP vs. Services in Crypto Officer Role Matrix 2 of 2

CSP	Reset Alarm	Zeroize Module
KEK Key		Zero
DEK Key		Zero
DEK Gen. Seed		Zero
PRNG Seed		Zero