2014

C-ACE

FIPS 140-2 Security Policy

Ver. 1.12 - October 20, 2015

Document: 08-2014-001

Table of Contents

Revision History

Revision	Date	Author	Description
1.0	08/14/2014	Andy Lenhart	Initial Version
1.1	08/25/2014	Andy Lenhart	Minor Revision based on Feedback
1.2	09/10/2014	Andy Lenhart	Explicitly State how to Select Modes
1.3	10/21/2014	Andy Lenhart	Error State and RNG Language Cleanup
1.4	11/11/2014	Andy Lenhart	Edited notes regarding Level 1 (now Level 2), added authentication notes
1.5	11/19/2014	Andy Lenhart	Updated concurrent operator note after review
1.6	01/25/2015	Andy Lenhart	Added firmware distribution section
1.7	02/05/2015	Andy Lenhart	Final Cleanup
1.8	02/05/2015	Andy Lenhart	Corrected AES Key Wrap note in Table 4
1.9	02/05/2015	Andy Lenhart	Corrected formatting of I2C acronym
1.10	07/01/2015	Andy Lenhart	Approved mode of operation edits/ clarifications
1.11	08/28/2015	Andy Lenhart	First time initialization, self-test failed return code, and generate IV clarifications
1.12	10/20/2015	Andy Lenhart	Added notes regarding Firmware Update Officer role

1. Introduction

This document defines the Security Policy for the Red Cocoa II Cocoa Advanced Crypto Engine (C-ACE) module, hereafter denoted the module. The module is a single-chip cryptographic engine designed to be implemented in a radio compliant with the APCO Project 25 Over-The-Air Rekeying (OTAR) protocol. The module is a slave device, under the control of the radio's main processor. The module boundary is contiguous, and is defined as the entire chip including packaging. The module meets FIPS 140-2 overall Level 2 requirements.

Table 1 - Cryptographic Module Configurations

	Module	HW Part	Bootloader FW Version	Application FW Version
1	C-ACE	STM32F405OG	0.0.1	1.0.0

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

Table 2 - Security Level of Security Requirements

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

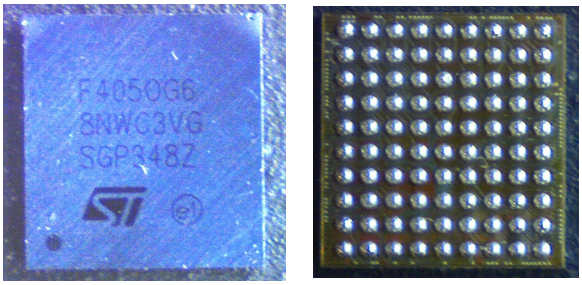
The module implementation is compliant with:

- *Project 25 Digital Over-the-Air Rekeying (OTAR) Protocol*, TIA/EIA 102.AACA
- *Project 25 Digital Land Mobile Radio - Key Fill Device (KFD) Interface Protocol*, TIA/EIA 102.AACD

2. Hardware and Physical Cryptographic Boundary

The physical form of the module is depicted in Figure 1. The figure depicts the contiguous boundary of the entire chip, including packaging. No external memory is used, and all firmware is stored and executed within the boundary.

Figure 1 - Top View and Bottom View of Microcontroller



The module utilizes the ports shown in Table 3. All other pins on the C-ACE module are configured as analog (i.e. disabled) pins.

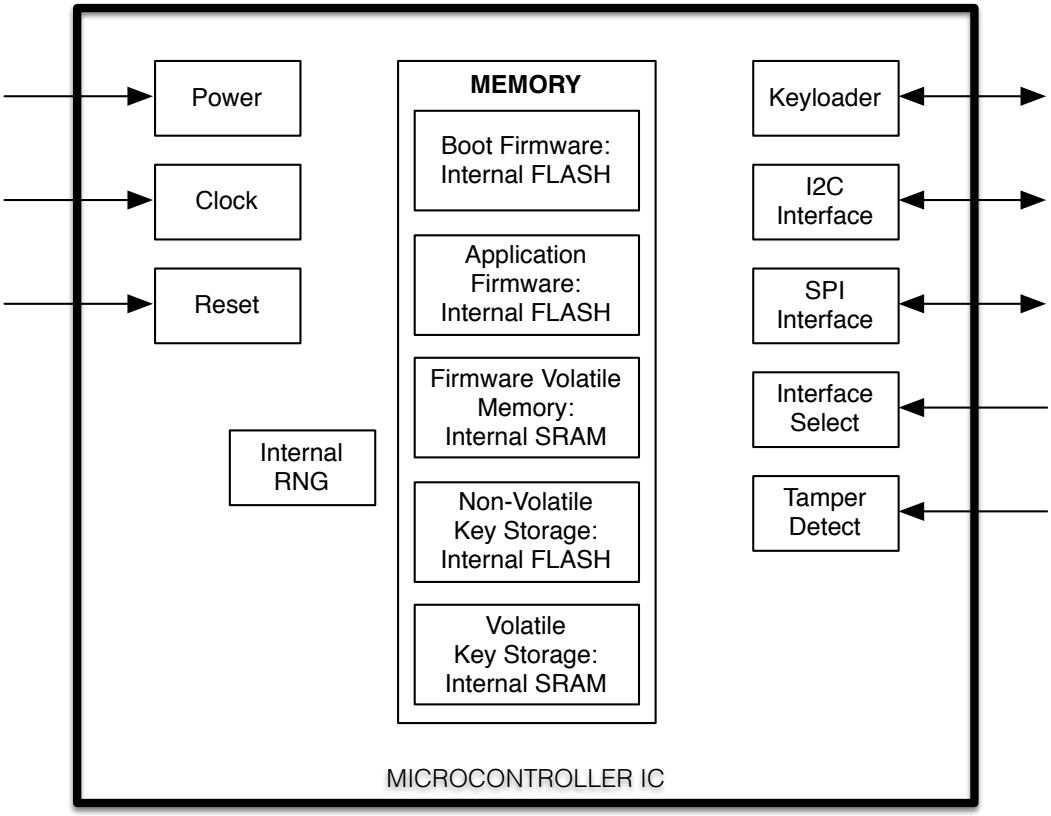
Table 3 - Ports and Interfaces

Port	Description	Logical Interface Type
Serial Peripheral Interface (SPI)	One of the two main ports of the module. In use if the SPI/I2C input is selected to SPI.	Data Input Data Output Control Input Status Output
Inter-Integrated Circuit (I2C)	The second of two main ports of the module. In use if the SPI/I2C input is selected to I2C.	Data Input Data Output Control Input Status Output
Communications Interrupt	An interface to indicate to the host that the C-ACE module has a message to send.	Status Output
Key Variable Loader (KVL)	An interface to provide a connection for use with a Key Variable Loader (KVL).	Data Input Data Output Control Input Status Output
SPI/I2C Select	An interface to indicate to the C-ACE module whether to use I2C or SPI as the communications port.	Control Input
Tamper Indication	An interface to indicate to the C-ACE module that the hardware has been unofficially modified.	Control Input
Clock	An interface to connect an external crystal for faster clock speeds.	Control Input
Reset	An interface to reset the C-ACE module.	Control Input

Port	Description	Logical Interface Type
Power	An interface to power the C-ACE module.	Power Input

Figure 2 shows the C-ACE operational environment.

Figure 2 - Module Block Diagram



3. Modes of Operation

First time initialization is performed by the customer and includes loading the bootloader, then the firmware image. The DSA public key is embedded in the bootloader code. This initialization can only be performed once; once the module has been initialized, it is not possible to return to an uninitialized state and re-perform the initialization.

The C-ACE module supports two Approved modes - the Application mode and the Firmware Updating mode (also called the bootloader). By default, the module powers up into the Application mode of operation after the self-tests for both the Firmware Updating mode and Application mode are run.

In order to switch to the Firmware Updating mode, the Firmware Update Officer can invoke the Firmware Update service, which includes a restart of the module. On restart, the module will

power up into the Firmware Updating mode. The self-tests for the Firmware Updating mode are run. In order to switch back to the Application mode, the module must be reset. On reset, the module will automatically power up into the Application mode as described above. Switching modes requires the module to be restarted, so all self-tests for the mode are automatically run. To verify that the module is in an approved mode of operation, the Show Status command can be used to query the module for its state. If the returned state value indicates 0xA0, the module is in the Application mode of operation. If the returned state value indicates 0xA3, the module is in the Firmware Updating mode of operation.

For a list of self-tests run in each mode, see Tables 8 and 9. For a list of services available for each mode, see Tables 6 and 7. For a list of algorithms used in each mode, see Table 4. For a list of CSPs used in each mode, see Section 6.

Table 4 - FIPS 140-2 Approved Operation Mode Security Functions

Approved Security Functions		**Application Mode**	**Firmware Updating Mode**
AES-128 ECB	FIPS 197, Certification #3137	✓	
AES-256 ECB	FIPS 197, Certification #3137	✓	
AES-256 CBC	FIPS 197, Certification #3137	✓	
AES-256 OFB	FIPS 197, Certification #3137	✓	
SHA-256	FIPS 180-4, Certification #2605	✓	✓
DSA Signature Verification (SHA-256, 3072-bit key)	FIPS 186-4, Certification #908		✓
Non-approved Security Functions (allowed for use in FIPS 140-2 Approved Mode)		**Application Mode**	**Firmware Updating Mode**
AES Key Wrap using 256-bit key size (provides 256 bits of strength)		✓	
AES CBC-MAC (P25 OTAR)	TIA-102.AACA, FIPS 197, Certification #3137, vendor affirmed	✓	
NDRNG		✓	

4. Authentication

Three operator roles, User, Cryptographic Officer and Firmware Update Officer, are supported by the C-ACE module. Prior to using certain services, authentication must take place.

- PIN Based Authentication (User and Cryptographic Officer roles): Either role can utilize an eight-character alphanumeric PIN (‘A’-‘Z’, ‘a’-‘z’, ‘0’-‘9’). Authentication is not persistent and must occur each time the module is powered. An eight-character PIN provides a false acceptance rate of $1/62^8$. A log in attempt takes > 1 ms to occur regardless of the interface chosen for communication, thus the false acceptance within a minute probability is 1/3,639,001,760.
- DSA Signature Based Authentication (Firmware Update Officer role only): During firmware updates, the Firmware Update Officer role is authenticated using a DSA 3072-bit digital signature. Authentication is not persistent and must occur each firmware update. A DSA digital signature provides a false acceptance rate of $1/2^{128}$. Each firmware update attempt takes approximately 3 seconds in the best case scenario, thus the false acceptance within a minute probability is $1/(1.7 \times 10^{38})$.

5. Roles

As stated, three roles are supported in the C-ACE module: User, Cryptographic Officer and Firmware Update Officer. While a brief overview is given in Table 5, a full overview of services is provided in Table 6.

Table 5 - Roles Description

Role	Description
User	Role for services that encrypt or decrypt voice or data
Cryptographic Officer	Role for services that load or zeroize keys and update the firmware of the C-ACE module.
Firmware Update Officer	Role for service that updates the firmware of the C-ACE module.

6. Critical Security Parameters and Keys

The C-ACE module stores symmetric keys for AES. Both traffic encryption keys (TEK) and key encryption keys (KEK) are stored in plaintext form in the flash and RAM within the cryptographic boundary. No asymmetric private keys are used or stored.

The following Critical Security Parameters (CSPs) are used with the C-ACE module in the Application mode of operation:

- Traffic Encryption Key (TEK): A 256-bit AES key used for data and voice encryption. TEKs will be input either in plaintext (via a key variable loader) or encrypted (via P25 OTAR). AES TEKs will not be an output from the module.
- Key Encryption Key (KEK): A 256-bit AES key used to encrypt other keys. KEKs will be input either in plaintext (via a key variable loader) or encrypted (via P25 OTAR). AES KEKs will not be an output from the module.
- P25 Authentication Key: A 128-bit AES key used to generate an authentication response. Authentication keys will be input in plaintext via a key variable loader. Authentication keys will not be an output from the module.
- Role PIN: An 8-character alphanumeric PIN is stored for both the User and Cryptographic Officer role. PINs will be input in plaintext via an I2C/SPI command. PINs will not be output from the module.

There is a single public key used in the C-ACE module which is used in the Firmware Updating mode of operation:

- DSA Verification Key: A 3072-bit public key is used by DSA to verify the downloaded firmware. The key is loaded during module initialization as a hard-coded value and will not be output from the module.

The modes of access to the CSPs and the services that the C-ACE module offers are as follows:

- Check Key: Validates a key (TEK or KEK) is present in the keyspace
- Delete Key: Remove a key (TEK, KEK or P25 Authentication) from the keyspace
- Load Key: Loads a key (TEK or KEK) to a specified stream
- Store Key: Store a key (TEK, KEK, P25 Authentication) in the keyspace
- TEK Decrypt: Decrypt a data buffer using a TEK
- TEK Encrypt: Encrypt a data buffer using a TEK
- Unwrap: Decrypt a key using a KEK
- Verify Signature: Verify the provided signature with DSA
- Load PIN: Store a new User or Cryptographic Officer role PIN
- Verify PIN: Validate a User or Cryptographic Officer role PIN

7. Services

Table 6 - Normal Mode Services

Service	Description	CO	U	FUO	Auth Req	CSP Mode of Access
Encrypt Data	Encrypt a data buffer using the loaded TEK for the stream	✓	✓		✓	TEK Encrypt
Decrypt Data	Decrypt a data buffer using the loaded TEK for the stream	✓	✓		✓	TEK Encrypt
Keyset Select	Change the active keyset	✓	✓		✓	Load Key (TEK)
Key Check	Check whether a TEK or KEK exists	✓	✓		✓	Check Key (TEK or KEK)
Key Select	Load the TEK for encryption operations for a given stream	✓	✓		✓	Load Key (TEK and KEK)
Show Status	Gets the C-ACE module state	✓	✓			N/A
Generate Initialization Vector	Generates a 64-bit random number for use as an initialization vector, which is output in plaintext for use by the main processor.	✓	✓		✓	N/A
Zeroize/Delete Key	Either a single key or all keys can be deleted	✓	✓		✓ (Single)	Delete Key (TEK or KEK)
Run Self Test	Accomplished via a reset	✓	✓			N/A
Key Load Using Keyloader	Load, change or delete key and OTAR information via a keyloader	✓			✓	Store Key (TEK or KEK)
Key Load Using OTAR	Load, change or delete key and OTAR information using P25 Over-the-Air Rekeying	✓			✓	Unwrap Store Key (TEK)
P25 Authentication	Load keys and encrypt blocks for P25 authentication services	✓			✓	Store Key (P25 Auth) TEK Encrypt Delete Key (P25 Auth)
Load Role PIN	Stores a new user or cryptographic officer PIN	✓	✓		✓	Load PIN Verify PIN
Verify Role PIN	Activates a user or cryptographic officer role	✓	✓			Verify PIN

Table 7 - Firmware Update Mode Services

Service	Description	CO	U	FUO	Auth Req	CSP Mode of Access
Show Status	Gets the C-ACE module state	✓	✓			N/A
Run Self Test	Accomplished via a reset	✓	✓			N/A
Firmware Update	Update the module firmware			✓	✓	Verify Signature (DSA Public Key)

8. Self Tests

Every time that the C-ACE module is powered up, it will test the algorithms that it uses to verify proper operation. The self tests can be run at any time by resetting the module. If a power up or conditional self-test fails, notification will be provided through return codes per the module's API. A self-test error is indicated by a return code of 0xA1 for the application and 0xA4 for the bootloader.

Table 8 - Power Up Self Tests (Bootload Mode)

Test Target	Description
SHA-256	SHA-256 KAT
DSA	Signature verification KAT
Bootloader Integrity	32-bit checksum over bootloader space
Application Integrity	SHA-256 value over application space

Table 9 - Power Up Self Tests (Application Mode)

Test Target	Description
AES	AES-128 ECB encrypt/decrypt KAT, AES-256 OFB and AES-256 CBC encrypt/decrypt KAT
SHA-256	SHA-256 KAT

Table 10 - Conditional Self Tests

Test Target	Description
Firmware Load	DSA signature verification before finalizing code update
Non-approved NDRNG	Continuous RNG self test
Application Integrity	SHA-256 value over application space

9. Security Rules and Guidance

- The C-ACE module supports the following roles: User, Cryptographic Officer and Firmware Update Officer. Authentication is required in order for certain services to be used.
- The C-ACE module prevents all data transfers during self tests, zeroization, and error states. The only transfer that is allowed is the module state query while the module is in an error state, so as to satisfy the status indication requirement.
- Status information does not contain any CSPs.
- Zeroization allows for the deletion of all secret keys and PINs.
- The C-ACE module does support concurrent operators, but only a single Cryptographic Officer, a single User, and a single Firmware Update Officer.
- The C-ACE module does not support manual key entry or key generation.
- The C-ACE module stores keys (TEKs and KEKs) and PINs in plaintext form in flash within the cryptographic boundary.
- A non-FIPS Approved random number generator is employed to generate 64-bit random numbers for use as initialization vectors. A 64-bit random number is achieved by combining two 32-bit random numbers from the NDRNG.
- The C-ACE module supports two approved modes - Application mode for normal operations (AES and SHA-256 functionality) and Firmware Updating mode, called the bootloader. The module always powers up into the bootloader and if no firmware updating is to take place, advances automatically to application operation. During application operation, the Firmware Update Officer can request that the module return to the bootloader for a firmware update.

10. Firmware Distribution

The C-ACE module's firmware will be distributed digitally via email. In order to be securely distributed, the SHA-256 hash value of the image will be provided in the email.

11. Physical Security Policy

The C-ACE module is a single chip of commercial grade and uses standard passivation. It meets FIPS 140-2 Security Level 2 requirements for opacity and tamper evidence.

12. Mitigation of Other Attacks Policy

The C-ACE module is not designed to mitigate against attacks outside of the scope of FIPS 140-2.

13. References

- *APCO Project 25 System and Standards Definition*, TSB 102-A, November 1995
- *Project 25 FDMA Common Air Interface*, TIA/EIA 102.BAAA, May 1998
- *Project 25 Digital Radio Over-the-Air Rekeying (OTAR) Protocol*, TIA/EIA 102.AACA, April 2001
- *Project 25 Digital Land Mobile Radio - Key Fill Device (KFD) Interface Protocol*, TIA/EIA 102.AACD, February 2005
- *Data Encryption Standard*, NIST, FIPS Publication 46-3, October 1999
- *Advanced Encryption Standard*, NIST, FIPS Publication 197, November 2001
- *Digital Signature Standard (DSS)*, NIST, FIPS 186-4, July 2013
- *Secure Hash Standard (SHS)*, NIST, FIPS 180-4, March 2012
- *Security Requirements for Cryptographic Modules*, NIST, FIPS 140-2, May 2001

14. Definitions and Acronyms

The following list contains the acronyms used in this document and their meaning.

- AES: Advanced Encryption Standard
- C-ACE: Cocoa Advanced Crypto Engine
- CBC: Cipher Block Chaining
- CSP: Critical Security Parameter
- DSA: Digital Signature Algorithm
- ECB: Electronic Codebook
- EMC: Electromagnetic Compatibility
- EMI: Electromagnetic Interference
- FIPS: Federal Information Processing Standard
- IV: Initialization Vector
- KAT: Known Answer Test
- KEK: Key Encryption Key
- MAC: Message Authentication Code
- NIST: National Institute of Standards and Technology

- OFB: Output Feedback
- OTAR: Over-the-Air Rekeying
- SHA: Secure Hash Algorithm
- SHS: Secure Hash Standard
- TEK: Traffic Encryption Key
- TIA: Telecommunications Industry Association

red-cocoa.com • 8200 Cody Drive, Suite G2, Lincoln, NE 68512 • mnispel@red-cocoa.com