SEMTEK
INNOVATIVE SOLUTIONS

Security Policy
for Hardware and Firmware Designs

Cipher Cryptographic Module (Version 1.00)

Document #:	0003
Revision:	20080215
Status:	Released
Author:	Paul Catinella
File Type:	Microsoft Word 2003

Table of Contents

Definitions and Acronyms

AES	Advanced Encryption Standard
AFE	Analog Front End
ASIC	Application Specific Integrated Circuit
CCM	Cipher Cryptographic Module
CO	Cryptographic Officer
CRC	Cyclical Redundancy Check
CSP	Critical Security Parameters
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
F2F	Frequency 2 times base Frequency (Bifrequency modal encoding)
FIPS	Federal Information Processing Standards
I^{2}C	Inter-integrated Circuit
KEK	Key Encryption Key
POR	Power On Reset
RAM	Random Access Memory
RF	Radio Frequency
SRAM	Static Random Access Memory
TDES	Triple Data Encryption Standard (3 DES Encryption)
TECB	Triple Data Encryption Standard Electronic Code Book
TTL	Transistor to Transistor Logic
USB	Universal Serial Bus

Module Overview

The Cipher Cryptographic Module (CCM) Processor (HW P/N: 7000-0008, Version 1.00) is a single-chip ASIC. The primary purpose for this device is to capture point of sale data from commonly used devices (RF card, magnetic strip reader, etc.). The photo and diagrams below illustrate these interfaces as well as defining the cryptographic boundary. The CCM is defined as a single-chip cryptographic module for FIPS 140-2 purposes.

Figure 1a – Image of the CCM FIPS module.

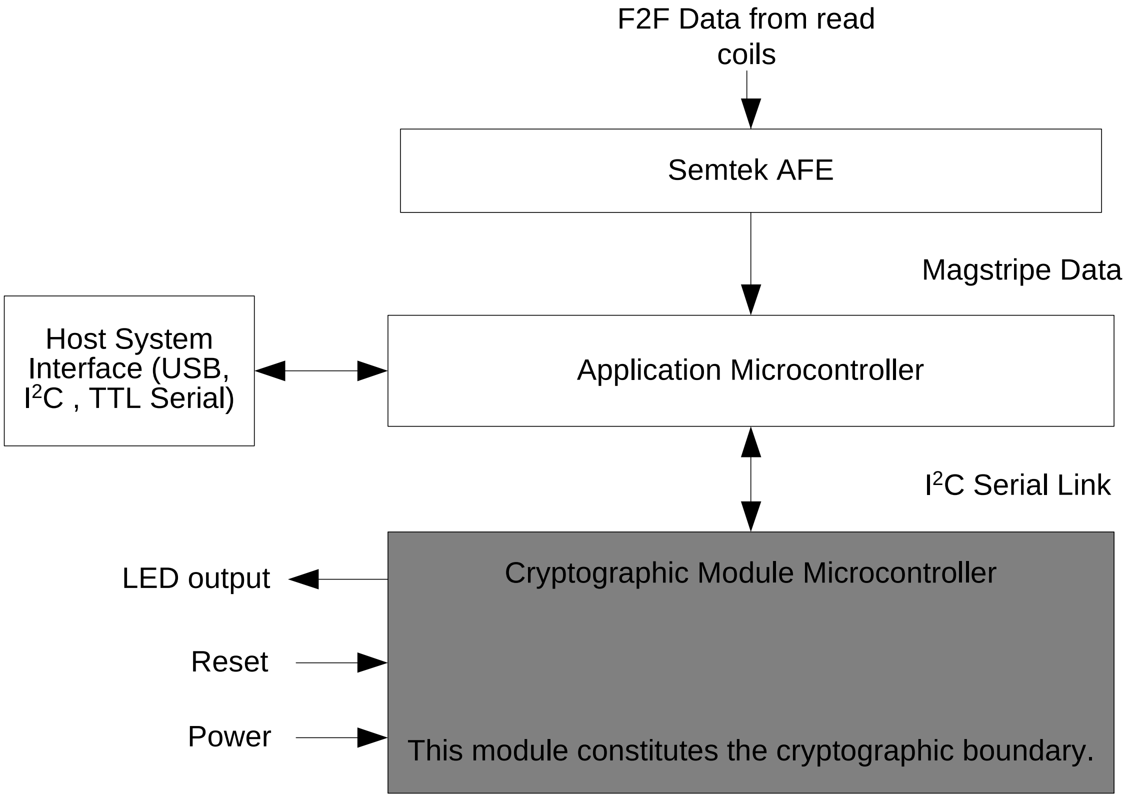
F2F Data from read coils
Semtek AFE
Magstripe Data
Host System Interface (USB, I²C , TTL Serial)
Application Microcontroller
I²C Serial Link
LED output
Reset
Power
Cryptographic Module Microcontroller
This module constitutes the cryptographic boundary.

Figure 1b – Logical diagram showing crypto boundary

Security Level

The Cipher Cryptographic Module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

Modes of Operation

Approved mode of operation

In FIPS mode, the Cipher Cryptographic Module supports FIPS Approved algorithms as follows:

- Triple-DES TECB mode (2-key) with 112 bit keys for encryption / decryption
- AES ECB mode with 128 bit keys for encryption / decryption

The Show Status command may be used to obtain the FIPS Approved mode of operation indicator. The Show Status command returns the module's version number. A version of 1.00 indicates that the module is running in the FIPS Approved mode of operation.

Non-FIPS mode of operation

The Cipher Cryptographic Module does not provide a Non-FIPS mode of operation.

Ports and Interfaces

The Cipher Cryptographic Module provides the following physical ports and logical interfaces:

- I^{2}C data – for data input/output, control input, and status output
- I^{2}C clock – for control input
- LED output – for status output
- RST/C2CK – for control input
- Power port

The chip pins described in Table 2 that are not listed above are non-security related ports and are tied to ground. That is, none of the exposed pins allow programming or debugging access to the chip. Only the four ports listed above are active on the chip; all other ports are disabled by the chip's firmware.

Table 2 -- Pin Definitions

Name	Pin #	Description
VDD	4	Power Supply Voltage. Interface type: power
GND	3	Ground
RST/C2CK	5	Device Reset. Open-drain output of internal POR. An external source can initiate a system reset by driving this pin low for at least 10 µs.
P3.0/C2D	6	Port 3.0. Not used; disabled in firmware.
P0.0/VREF	2	Port 0.0. I^{2}C data. Connected to device using encryption module. Interface type: data input, data output, control input, status output.
P0.1	1	Port 0.1. I^{2}C clock. Connected to device using encryption module. Interface type: control input.
P0.2/XTAL1	24	Port 0.2. Not used; disabled in firmware.
P0.3/XTAL2	23	Port 0.3. Not used; disabled in firmware.
P0.4	22	Port 0.4. Not used; disabled in firmware.
P0.5	21	Port 0.5. Not used; disabled in firmware.
P0.6/CNVSTR	20	Port 0.6. Not used; disabled in firmware.
P0.7	19	Port 0.7. Not used; disabled in firmware.
P1.0	18	Port 1.0. Not used; disabled in firmware.
P1.1	17	Port 1.1. Not used; disabled in firmware.
P1.2	16	Port 1.2. Not used; disabled in firmware.
P1.3	15	Port 1.3. Not used; disabled in firmware.
P1.4	14	Port 1.4. Not used; disabled in firmware.
P1.5	13	Port 1.5. Not used; disabled in firmware.
P2.0	12	Port 2.0. LED output. Interface type: status output.
P2.1	11	Port 2.1. Not used; disabled in firmware.
P2.2	10	Port 2.2. Not used; disabled in firmware.
P2.3	9	Port 2.3. Not used; disabled in firmware.
P2.4	8	Port 2.4. Not used; disabled in firmware.
P2.5	7	Port 2.5. Not used; disabled in firmware.

Identification and Authentication Policy

Assumption of roles

The Cipher Cryptographic Module shall support two distinct operator roles (User and Cryptographic-Officer). The Cipher Cryptographic Module shall enforce the separation of roles using identity-based operator authentication. Upon correct authentication, the service is provided.

The operator's identity is determined by the operator ID value. The authorization for the operator is provided by the operator ID, the operator's secret password, and a counter value provided by the cryptographic module. The 32-bits of authentication data are calculated as follows for each cryptographic service request:

a. An 8-bit operator ID value, a 5-bit secret password for the operator, and the module's current 32-bit counter value are concatenated together and then padded with 32 bits of a known pad.
b. The resulting 128-bit block is encrypted with the AES 128-bit Password Key.
c. The 32 most significant bits of the resulting ciphertext are passed as authentication data to the module.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	The operator ID value provides the identity of the operator. A 32-bit string provides the authentication of the operator.
Cryptographic-Officer	Identity-based operator authentication	The operator ID value provides the identity of the operator. A 32-bit string provides the authentication of the operator.

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
A 32-bit string of authentication data is calculated using an operator ID, the operator's password, a counter, and AES encryption using a shared AES Password Key. (See the description at the start of this section for additional details.)	32 bits of security strength

Secure Operation

The Cipher Cryptographic Module requires no action by the Cryptographic Officer prior to use. The module is delivered pre-configured. No procedures are required for the secure installation, configuration or administration of the module.

Access Control Policy

Roles and Services

Table 5 – Services Authorized for Roles

Role	Authorized Services
User:	• AES Encryption: encrypts data using AES algorithm • AES Decryption: decrypts data using AES algorithm • TDES Encryption: encrypts data using Triple DES algorithm • TDES Decryption: decrypts data using Triple DES algorithm • Show Status: shows current status information for module including counter value • Zeroize Service: overwrites all plaintext CSPs
Cryptographic-Officer:	• Unwrap Key: decrypts or unwraps any key or CSP to be replaced in the module • Show Status: shows current status information for module • Zeroize Service: overwrites all plaintext CSPs

Unauthenticated Services

The following services do not require operator authentication:

- On Demand Self-Tests – may be run at any time by cycling power to the module
- Show Status – shows the current status information for the module
- Zeroize Service – actively overwrites all plaintext CSPs

Table 6 – Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
AES Encryption	AES Encryption command code	Plaintext data to be encrypted	Resultant ciphertext data	Success / Error code
AES Decryption	AES Decryption command code	Ciphertext data to be decrypted	Resultant plaintext data	Success / Error code
TDES Encryption	TDES Encryption command code	Plaintext data to be encrypted	Resultant ciphertext data	Success / Error code
TDES Decryption	TDES Decryption command code	Ciphertext data to be decrypted	Resultant plaintext data	Success / Error code
Unwrap Key	Unwrap Key command code	Ciphertext data to be unwrapped	None	Success / Error code
Show Status	Show Status command code	None	None	Success / Error code
Zeroize Service	Zeroize Service command code	None	None	Success / Error code

Definition of Critical Security Parameters (CSPs)

Table 7 – Critical Security Parameters

Key Name	Description/ Usage	Generation	Storage	Entry/ Output	Destruction
KEK_MASTER	Master Key Encrypting Key; AES 128-bit key used for unwrapping keys and CSPs	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: Injected at manufacture. A new key may be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service
Password Key	AES 128-bit key for verifying passwords	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: Injected at manufacture. A new key may be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service
CO Operator ID	8-bit value for the CO operator ID	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: Injected at manufacture. A new value may be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service
CO Password	56-bit value for the CO password	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: Injected at manufacture. A new value may be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service

Key Name	Description/ Usage	Generation	Storage	Entry/ Output	Destruction
User Operator ID	8-bit value for the User operator ID	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: Injected at manufacture. A new value may be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service
User Password	56-bit value for the User password	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: Injected at manufacture. A new value may be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service
User AES Key	AES 128-bit key for encrypting/ decrypting data	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: May be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service
User TDES Key	TDES 112-bit key for encrypting/ decrypting data	Generated externally	Stored as plaintext in flash and SRAM	*Entry*: May be entered AES encrypted or AES wrapped *Output*: Never output	Zeroized after use in SRAM. Zeroized in flash memory by the zeroize service

Definition of CSPs Modes of Access

Table 8 defines the type of access to the CSPs in the module for every service.

Table 8 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
	X	AES Encryption	User AES Key: Read Password Key: Read User Operator ID: Read User Password: Read
	X	AES Decryption	User AES Key: Read Password Key: Read User Operator ID: Read User Password: Read
	X	TDES Encryption	User TDES Key: Read Password Key: Read User Operator ID: Read User Password: Read
	X	TDES Decryption	User TDES Key: Read Password Key: Read User Operator ID: Read User Password: Read
X		Unwrap Key	KEK_MASTER: Read, Write Password Key: Read, Write CO Operator ID: Read, Write CO Password: Read, Write User Operator ID: Write User Password: Write User AES Key: Write User TDES Key: Write
X	X	Show Status	None
X	X	Run Zeroize Service	Destroy all keys

Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Cipher Cryptographic Module does not contain a modifiable operational environment.

Security Rules

The Cipher Cryptographic Module's design corresponds to the Cipher Cryptographic Module's security rules.

FIPS 140-2 Level 3 module requirements

This section documents the security rules enforced by the CCM to implement the security requirements of this FIPS 140-2 Level 3 module.

Security rules are derived from the security requirements of FIPS 140-2 and any additional security requirements imposed by the manufacturer.

1. The Cipher Cryptographic Module shall provide two distinct operator roles. These are the User role and the Cryptographic-Officer role.
2. The Cipher Cryptographic Module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The Cipher Cryptographic Module shall encrypt sensitive parameters using the TDES or AES algorithms.
5. The Cipher Cryptographic Module shall perform the following tests:

   Power up Self-Tests:

   1. Cryptographic algorithm tests:
      a. TDES Encrypt/Decrypt Known Answer Tests
      b. AES Encrypt/Decrypt Known Answer Tests
   2. Firmware Integrity Test (16 bit CRC)
   3. Critical Functions Tests: N/A

   Conditional Self-Tests:
   None.

6. At any time the operator shall be capable of commanding the module to perform the power-up self-tests by recycling power to the module.
7. Data output shall be inhibited during self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module shall not support concurrent operators.
10. The module is available for cryptographic services after the self-tests have completed.
11. The cryptographic module shall not support a maintenance role or maintenance interface.
12. The cryptographic module shall not support a bypass mode.

Physical Security Policy

Physical Security Mechanisms

The single-chip embedded Cipher Cryptographic Module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque coating.
- Hard potting material encapsulation of chip circuitry enclosure with removal/penetration attempts causing serious damage.

Operator Required Actions

No inspection is required by Operator.

Mitigation of Other Attacks Policy

The module has not been designed to mitigate other attacks.

Table 9 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A