Security Policy

Covia Connector Cryptographic Module
Version 2.0

Document Version: 1.6
Revision Date: 09/13/13

Covia Labs, Inc.

TABLE OF CONTENTS

1. MODULE OVERVIEW **3**

2. SECURITY LEVEL **3**

3. MODES OF OPERATION **5**

4. PORTS AND INTERFACES **5**

5. IDENTIFICATION AND AUTHENTICATION POLICY **5**

6. ACCESS CONTROL POLICY **7**

ROLES AND SERVICES 7
DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 8
DEFINITION OF CSPS MODES OF ACCESS 9

7. OPERATIONAL ENVIRONMENT **10**

8. SECURITY RULES **10**

9. PHYSICAL SECURITY **12**

10. MITIGATION OF OTHER ATTACKS POLICY **12**

11. REFERENCES **12**

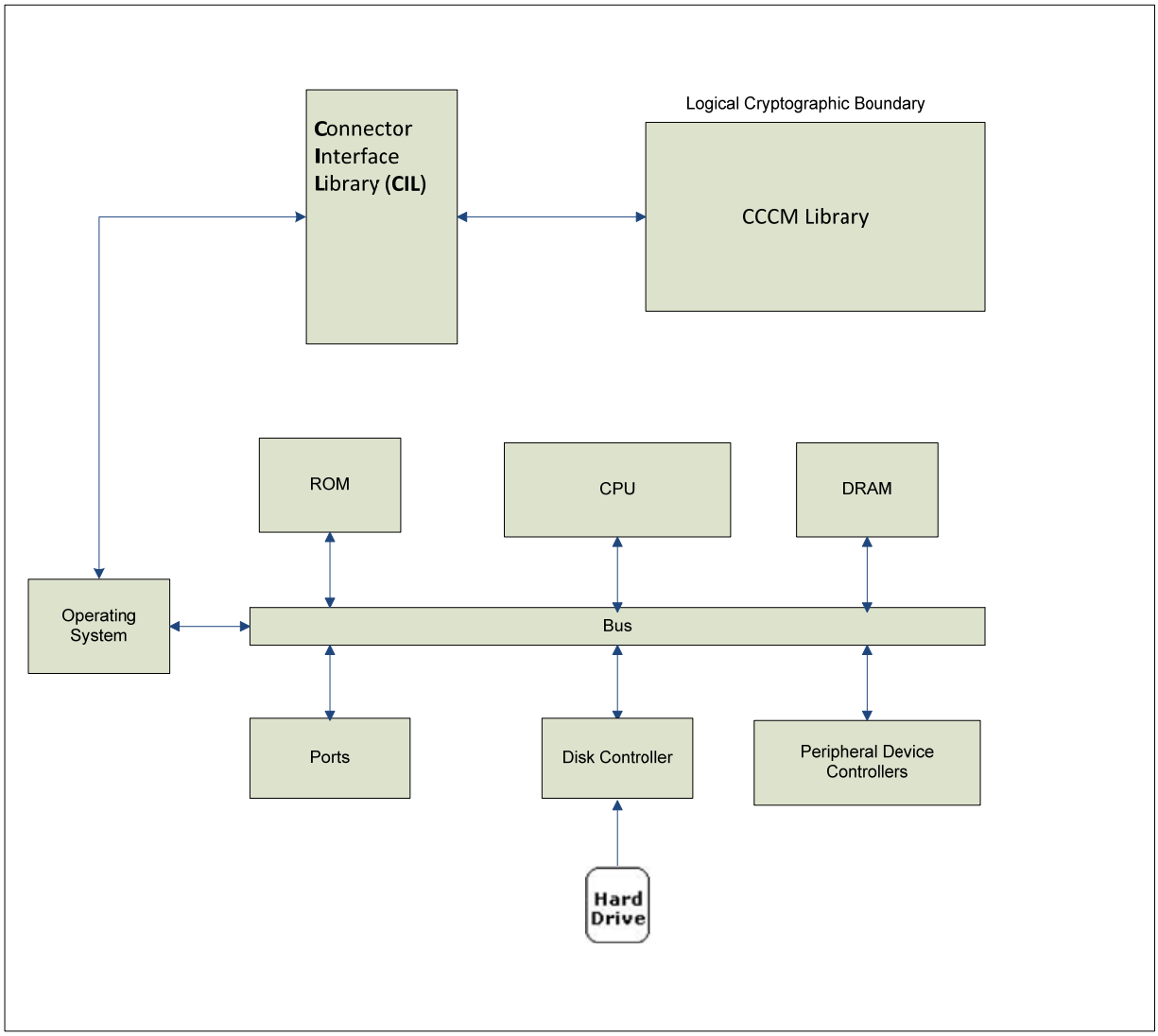
12. DEFINITIONS AND ACRONYMS **12**

1. Module Overview

The **C**ovia **C**onnector **C**ryptographic **M**odule (CCCM) is software only object module that operates on multi-chip standalone general purpose computer (GPC) that runs a general purpose OS. The primary purpose for this module is to provide cryptographic services to calling applications. The physical boundary of the module is defined by the GPC hardware. The logical boundary of the module is the CCCM library.

The cryptographic module was tested on Red Hat Enterprise Linux 5.8.

Figure 1 – Image of the Cryptographic Module



2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The cryptographic module supports FIPS Approved or Allowed algorithms as follows:

Table 2 – FIPS Approved Algorithms Used in Module

Algorithm	Description	Cert #
AES	[FIPS 197] CFB – 128, 192, 256 Encrypt and Decrypt	1896
GCM/GMAC	[SP 800-38D] 128, 192, 256 Encrypt and Decrypt	1896
ECDSA	[FIPS 186-3] Sign/Verify : P-224, P-256, P-384, and P-512	265
DRBG	[SP 800-90] HMAC DRBG –SHA-256, SHA-384, and SHA-512	158
SHA	[FIPS 180-3] SHA 1, SHA 224, SHA 256, SHA 384, and SHA 512	1665
HMAC	[FIPS 198] SHA 1, SHA 224, SHA 256, SHA 384, SHA 512	1136
KAS	[SP 800-56A] ECC DH (Full Unified Model) and concatenation KDF with session key tags generated by applying HMAC SHA-224, SHA-256, SHA-384, and SHA-512. The estimated encryption strength of ECC-DH transport mechanism varies from 112 bits for P-224 to 256 for P-512.	30

Non-Approved but Allowed Cryptographic Algorithms

- AES (Cert. #1896, key wrapping, key establishment methodology provides 128 or 256 bits of encryption strength)

Non-Approved Mode

The module supports a Non-Compliant SP 800-108 KDF. This algorithm shall not be used in FIPS-Approved mode. In addition keys derived using this function shall not be used in FIPS-Approved mode.

4. Ports and Interfaces

The module's physical ports are defined by the ports of the GPC hardware. The module's logical interfaces are defined at the API of the cryptographic module. The API contains all data input, data output, control input, and status output interfaces to and from the module. The API is further described as the logical services provided by the module to a calling application.

5. Identification and Authentication Policy

Assumption of roles

The Module meets all FIPS 140-2 Level 1 requirements for Roles andServices. There are no authentication requirements for Level 1.The cryptographic module shall support two distinct operator roles (User and Cryptographic-Officer). The cryptographic module shall enforce the separation of roles based on the services called. The module does not support authentication of operators.

Table 3 – Roles and Required Identification and Authentication

Role	Description	Type of Authentication	Authentication Data
User	The user role obtains access to all cryptographic operations provided by the module, with the exception of initialization using the RegisterCccmModule() API.	Not Applicable	Not Applicable
Cryptographic-Officer (CO)	The CO role is responsible for installation and initialization of the module using the RegisterCccmModule() API.	Not Applicable	Not Applicable

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Roles	Authorized Services	Description
User	*Key Agreement*	*ECDH key agreement.*
User	*Key Generation*	*Generate Keypairs for ECDH, ECDSA, AES, and HMAC*
User	*Entropy Load*	*Module will load entropy data provided by the calling application.*[1]
User	*Digital Signature Generation/Verification*	*Digital Signature Generation and Verification using ECDSA key pairs.*
User	*AES Block Cipher*	*Employs Key Sizes = 128, 192, 256* *Feedback modes = CFB and GCM with GMAC*
User	*Keyed Hashing*	*HMAC SHA* *SHA block sizes = 512, 384, 256, 224 and 160 for backwards compatibility*
User	*Hashing*	*SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*
User	*Random Number Generation*	*Return random values generated by HMAC-DRBG.*
User	*Key Derivation*	*5.8.1 Concatenation Key Derivation Function (Approved Alternative 1) From NIST SP 800-56A Page 46*
User	*Key Wrap/Unwrap*	*- AES with GCM and GMAC* *-Wrap keys with a 256 bit AES key using GCM and GMAC.* *-Key access and usage control data are output as a plaintext prefix and are protected against compromise of*

		their integrity by the GMAC.
User	*Self-tests*	*This service executes the suite of self-tests required by FIPS 140-2 each time the module is loaded.*
User	*Show Status*	*The module provides status at the conclusion of each API call.*
User	*Zeroize*	*The module zeroizes each CSP at the conclusion of its usage.*
User	*Utility Functions*	*These services provide memory allocation and time retrieval functionality.*
CO	*Initialize Module*	*The CO calls the initialization function to begin module operation.*
User	*SP 800-108 Key Derivation (non-compliant)*	*KDF with Feedback described in FIPS SP 800-108*

1. The module generates cryptographic keys whose strengths are modified by available entropy. No assurance of the minimum strength of generated keys.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- *SSPr-EDHK* (**S**tatic **S**ystem **Pr**ivate **E**C**DH K**ey) with key sizes of 256 and 384
- *SS-ECSK* (**S**tatic **S**ystem **E**C **S**ignature **K**ey) with key sizes of 256 or 384

- *ESPr-EDHK* (**E**phemeral **S**ystem **Pr**ivate **E**C**DH K**ey) ECDH Ephemeral keys used to negotiate session keys and shared secrets with peer device.

- *SCD-EK* (**S**ystem **C**rypto **D**ata **E**ncryption **K**ey) 256 bit AES key
- *SCK-EK* (**S**ystem **C**rypto **K**ey **E**ncryption **K**ey) 256 bit AES key
  Key used to wrap/unwrap other keys.
- *CA-KDK* (**C**onnector **A**pplication **K**ey **D**erivation **K**ey) 384 bit HMAC Key
- *CS-KDK* (**C**onnector **S**ystem **K**ey **D**erivation **K**ey) 384 bit HMAC Key
- *DIS* (**D**RBG **I**nternal **S**tate) consists of the K and V state arrays and metadata such as security strength, reseed and counter

- *ECSS* (**EC**DH **S**hared **S**ecret) Master key used to derive session keys.

- *SWK* (**S**ession **W**rite **K**ey) 128 bit key and 256 bit key for encryption and GMAC'ing
- *SRK* (**S**ession **R**ead **K**ey) 128 bit key and 256 bit key for decryption and GMAC verification
- *ISPr-EDHK* (**I**nstance **S**pecific **Pr**ivate **E**C-**DH K**ey) 256 or 384 bit keys
- *IS-ECSK* (**I**nstance **S**pecific **E**C **S**ignature **K**ey) 256 or 384 bit keys

- *MFHAK* (**M**odule **F**ixed **H**MAC **A**uthentication Key) This key is compiled into CCCM library, and used to produce a SHA-512 bit HMAC for integrity checking the CCCM Module.

Definition of Public Keys:

The following are the public keys contained in the module:

SEVK (**S**tatic **E**CDSA **V**erifying **K**ey) Signed with SSPub-EDHK using P-256 or P-384 bit keys.

EPub-EDHK (**E**phemeral **Pub**lic **E**C**DH K**ey) P-256 or P-384 bit keys

SSPub-EDHK (**S**tatic **S**ystem **Pub**lic **E**C**DH K**ey) with key sizes of 256 and 384

IS-EVK (**I**nstance **S**pecific **E**CDSA **V**erifying **K**ey) P-256 or P-384 bit keys

ISPub-EDHK (**I**nstance **S**pecific **P**ublic **E**C**DH V**erifying **K**ey) P-256 or P-384 bit keys

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services.

Table 6 – CSP Access Rights within Roles & Services

Service	**Cryptographic Keys and CSPs Access Operation** **Input = I, Output = O, Zeroize = Z, Generate = G, Execute = E**													
	SSPr-EDHK	SS-ECSK	ESPr-EDHK	SCD-EK	SCK-EK	CA-KDK	CS-KDK	DIS	ECSS	SWK	SRK	ISPr-EDHK	IS-ECSK	MFHAK
Key Agreement	**IE**		**IE**									**IE**		
Key Generation	**G**	**G**	**G**	**G**	**G**	**G**	**G**	**IE**	**G**	**G**	**G**	**G**	**G**	
Entropy Load								**I**						
Access to ECDH Primitives												**IE**		

Digital Signature Generation/Verification		**I E**										**IE**	
AES Block Cipher				**IE**						**I E**	**I E**			
Keyed Hashing													
Hashing													
Random Number Generation								**IE**					
Key Derivation						**I E**	**I E**						
Key Wrapping					**IE**								
Configure Mode of Operation													
Self Tests													**E**
Zeroization of CSPs occur automatically at the conclusion of each service	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	
Show Status													

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable because the cryptographic module operates in a modifiable operational environment.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The cryptographic module does not provide a means to authenticate operators.

3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests: -

   A. Cryptographic Power-up Self-Test

   - AES CFB - 128, 192, 256 Separate Encrypt and Decrypt KATs
   - AES GCM -128, 192, 256 Separate Generation and Verification KATs
   - ECDSA –P-256, P-384 with private keys' bit lengths equal to the bit length of the underlying P field as per FIPS 186-3 Pairwise Consistency Test
   - DRBG with HMAC –SHA-256 KAT
   - SHA-1 KAT
   - SHA-256 KAT
   - SHA-384 KAT
   - SHA-512 KAT
   - HMAC SHA-1 KAT
   - HMAC SHA-224 KAT
   - HMAC SHA-256 KAT
   - HMAC SHA-384 KAT
   - HMAC SHA-512 KAT
   - SP 800-56A KAS self tests per IG 9.6
     - Concatenation KDF -PRF HMAC SHA-256 and 384.
     - ECDH- ECC schemes: the module shall check Q = dG
     - Tests for P-224, P-384, P-512

   B. Power-up software integrity test:

   - HMAC-SHA512 code

   C. Conditional Tests:

   - Continuous test for HMAC-DRBG output
   - SP 800-KAS Assurance Conditional Tests per IG 9.6
   - SP 800-90 DRBG Section 11.3 Health Checks
   - FIPS 186-3 Section 3.1 ECDSA Assurances per SP 800-89
   - Pair wise consistency tests
     (1) ECDH Ephemeral key pair generation
     (2) EC-DSA key pair generation

5. The module shall return a status indicator of zero upon successful completion of Power-Up self-tests.
6. The module shall not return output during power-up self-tests and error states.
7. At any time the cryptographic module is in an idle state, the operator shall be capable of causing the module to perform the power-up self-test. This requires the unloading and then reloading the module.
8. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.

9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module actively zeroizes each CSP upon termination of its usage.
11. The module acts as a single thread and does not support concurrent operators.

9. Physical Security

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the cryptographic module is software only.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks.

11. References

[1] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*. FIPS 140-2, 25 May, 2001.
[2] National Institute of Standards and Technology, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, Draft, Jan 04, 2011.
[3] FIPS 197 *Advanced Encryption Standard (AES)*
[4] FIPS SP 800-57, *Recommendation for Key Management – Part 1: General*, May, 2006.
[5] FIPS SP 800-38a, *Recommendation for Block Cipher Modes of Operation*, December, 2001.
[6] FIPS SP 800-38d, *Recommendation for Block Cipher Modes of Operation Galois Counter Mode (GCM) and GMAC*, November, 2007.
[7] FIPS 198-1, *Keyed-Hash Message Authentication Code*, July, 2008.
[8] FIPS 180-3, *Secure Hash Standard*, October, 2008.
[9] FIPS 186-3, Digital Signature Standard, June, 2009.
[10] FIPS SP 800-56A *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007.
[11] FIPS 140-2-IG, *Implementation Guidance for FIPS 140-2 and Cryptographic Module Validation Program*, December, 2010.
[12] FIPS SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, October, 2009.

12. Definitions and Acronyms

- HMAC-DRBG = **D**eterministic **R**andom **B**it **G**enerator based on HMAC and SHA
- ECDH = **E**lliptic **C**urve **D**iffie **H**ellman symmetric handshake combining ephemeral and

static keypairs.

- ECDSA = **E**lliptic **C**urve **D**igital **S**tandard **A**lgorithm.
- KDF = **K**ey **D**erivation **F**unction.
- DSSL = **D**art **S**ecure **S**ocket **L**ibrary, a proprietary SSL like communication protocol.
- GCM = **G**alois **C**ounter **M**ode, a cipher feed back mode
- GMAC = **G**alois field based **M**essage **A**uthentication **C**ode
- KAT = Known Answer Test