ZyFLEX Crypto Module

ZCM-100

Non-Proprietary Security Policy

Rev. 1.2

ZyFLEX Technologies Inc.

Revisions

Date	**Rev.**	**Author**	**Note**
Jul. 29, 2011	0.1	Nick Tseng	Initial Draft
Aug. 29, 2011	1.0	Nick Tseng	Rev. 1.0 First Release
Nov. 11, 2011	1.1	Nick Tseng	Responses to comments
Feb. 17, 2012	**1.2**	Nick Tseng	Responses to CMVP comments

Contents

Figures

Tables

1. INTRODUCTION

1.1. Document Purpose

This document contains the Security Policy, User Guidance and Crypto Officer Guidance for the ZyFLEX Crypto Module ZCM-100, hereinafter referred to as ZCM-100 or the module.

1.2. Module Overview

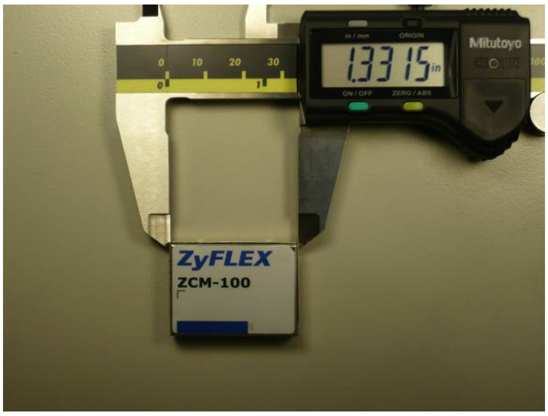
ZCM-100 (Firmware Version: 1.1; Hardware Version: AAM) is a hardware multichip embedded module that targets high speed data link layer (OSI layer 2) secure data transmission applications in an IP-based network.

ZCM-100 implements AES-256 encryption/decryption algorithm and other security functions by using both hardware FPGA circuitry and a 32-bit microcontroller. Its miniaturized size and low power consumption features make ZCM-100 suitably fit in a portable wireless communication device such as a handheld radio.

ZCM-100 is designed to conform to level 3 of FIPS 140-2 standard. Please visit http://csrc.nist.gov/publicationss/fips/fips140-2/fips1402.pdf for details about the standard.

1.3. Module Specification

Figure 1 shows photos of ZCM-100, with all of its interfaces provided through two 20-pin board-to-board connectors J1 & J2. Pin-outs of these connectors are described in section 4.1.



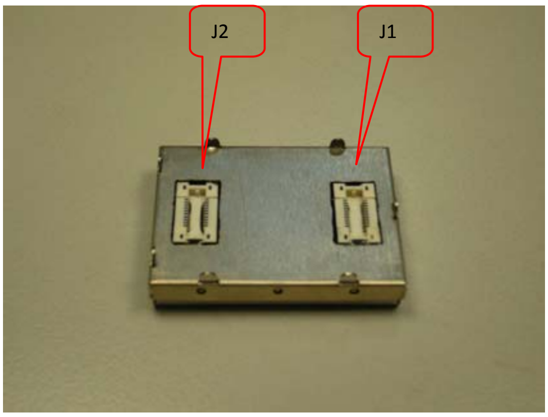


Figure 1: ZCM-100 Photos. Left: Top-view, Right: Bottom-view

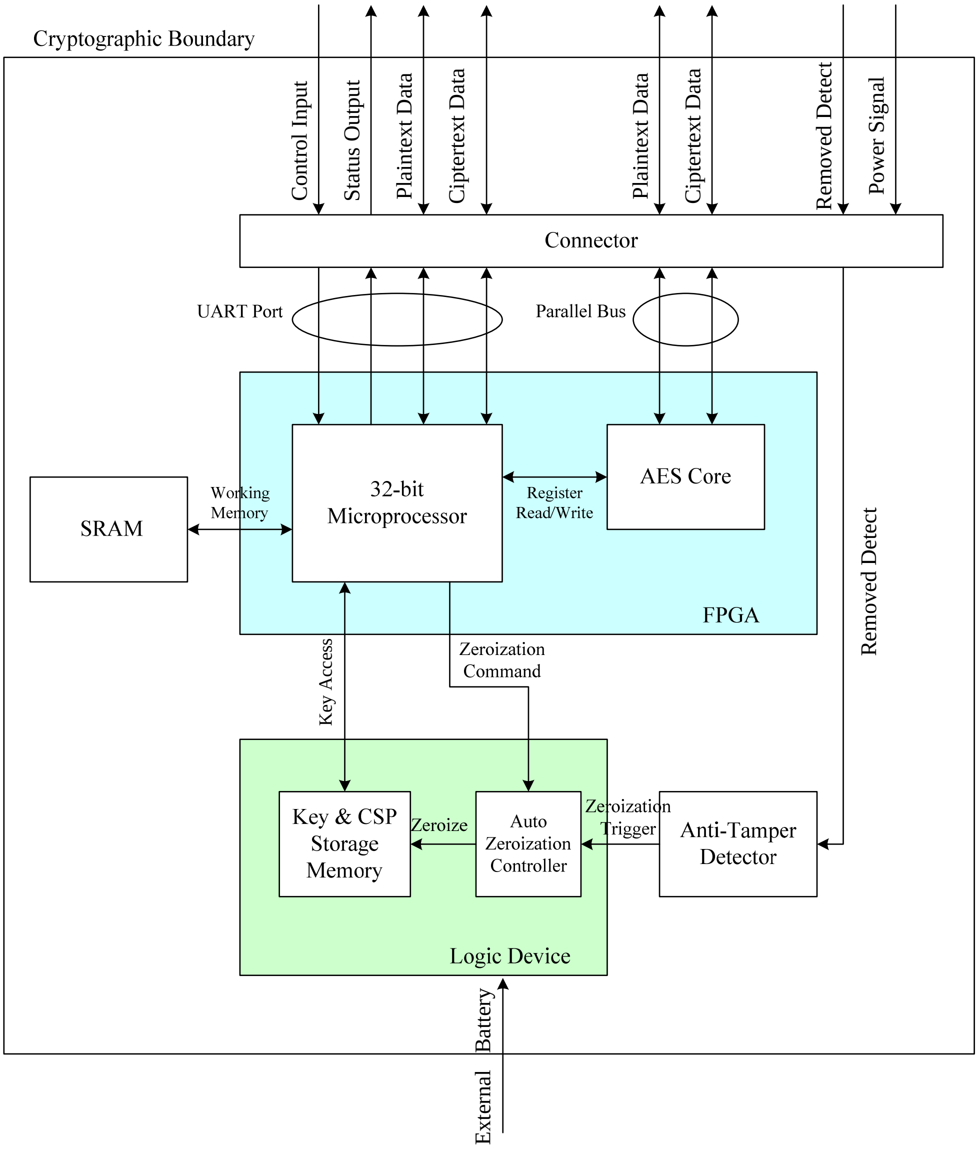


Figure 2: ZCM-100 Hardware Block Diagram

Figure 2 is a hardware block diagram showing ZCM-100's internal circuitry. ZCM-100 needs to be mounted on a host system board where a "host" microprocessor acts as a master device to send control commands as well as plaintext/ciphertext data to ZCM-100. The host system board also provides power inputs (DC3.3V, 1.2V and a battery voltage of 3.3V) to ZCM-100.

ZCM-100 uses an FPGA to implement the AES-256 cryptographic algorithm (the AES Core). Besides, there is a 32-bit microprocessor designed within the FPGA, and this microprocessor acts as a slave device to respond to the host system's commands and provides some other cryptographic services such as:

1. AES 256 encryption & decryption
2. Key storage
3. Signature generation and verification
4. Generation of message digest

The keys and CSPs are stored in the Key & CSP storage memory provided by a logic device, whose power is backed-up by an external battery voltage of 3.3V.

ZCM-100 features a secure tamper detection design: when it is being tried to be removed from the host system board, its tamper detector circuitry will automatically zeroize all the keys stored inside ZCM-100 even when power is cut off.

For physical ports/logical interfaces descriptions of ZCM-100, please refer to sections 4.1 & 4.2.

2. SECURITY LEVEL

ZCM-100 meets the overall requirements applicable to FIPS140-2 Security Level 3. In the individual requirement areas of FIPS 140-2 the following Security Level ratings are achieved:

Area	Area Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level per FIPS 140-2 Areas

3. MODES OF OPERATION

3.1. FIPS Approved Mode of Operation

When ZCM-100 powers up, it will execute self-test first; if the self-test passes ZCM-100 will issue a status report indicating that it is entering the login state and operating in the FIPS Approved mode automatically, without any operator's intervention. ZCM-100 only operates in a FIPS Approved mode of operation, comprising all services described in section 6.1.

The module does not implement bypass or maintenance modes.

3.2. FIPS Approved Security Functions

The following table gives the list of FIPS Approved security functions provided by the module.

Security Function	Details	CAVP Cert. #
DSA	FIPS 186-3: SIG(gen) [(1024,160) SHA (1,224,256,384,512);(2048,224) SHA(1,224,256,384,512); (2048,256) SHA(1,224,256,384,512); (3072,256) SHA(1,224,256,384,512)] SIG(ver) [(1024,160) SHA (1,224,256,384,512);(2048,224) SHA(1,224,256,384,512); (2048,256) SHA(1,224,256,384,512); (3072,256) SHA(1,224,256,384,512)] SHS: Val# 1462; RNG: Val# 888	#521
AES	ECB (e/d; 128 , 192 , 256); CBC (e/d; 128 , 192 , 256); CFB128 (e/d; 128, 192, 256); OFB (e/d; 128, 192, 256); CCM (KS: 128, 192, 256) (Assoc. Data Len Range: 0-14) (Payload Length Range: 2-32)(Nonce Length(s): 13) (Tag Length(s): 4 6 8 10 12 14 16)	#1670 #1671
SHS	SHA-1 (BYTE-only); SHA-224 (BYTE-only); SHA-256 (BYTE-only); SHA-384 (BYTE-only); SHA-512 (BYTE-only)	#1462

Security Function	Details	CAVP Cert. #
RNG	ANSI X9.31 [AES-128Key AES-192Key AES-256Key]	#888 #889
RSA	FIPS 186-3: ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver): (1024 SHA(1, 224, 256, 384, 512)) (2048 SHA(1, 224, 256, 384, 512)) (3072 SHA(1,224,256,384,512)) SHS: SHA (Cert. #1462)	#827
HMAC	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS>BS) SHS (Cert. #1462) HMAC-SHA224 (Key Sizes Ranges Tested: KS<BS KS>BS) SHS (Cert. #1462) HMAC-SHA256 (Key Sizes Ranges Tested: KS<BS KS>BS) SHS (Cert. #1462) HMAC-SHA384 (Key Size Ranges Tested: KS<BS) SHS (Cert. #1462) HMAC-SHA512 (Key Size Ranges Tested: KS<BS) SHS (Cert. #1462)	#980

Table 2a – FIPS Approved Security Functions

3.3. Other Allowed Security Functions

The module supports the following non-Approved algorithms which are allowed for use in the FIPS Approved mode of operation.

Security Function	Details
HRNG	Hardware Random Number Generator is composed of 128 bits of on-board CPU’s timer tick. HRNG is used to generate seeds for ANSI X9.31 RNG.
Diffie-Hellman Key Agreement	Used to generate 256 bits session key (i.e., key wrapping key) between ZCM-100 and host system. The functions are implemented following SP800-56A standard, with C(1,1,FFC DH) scheme, that is, host system generates an ephemeral DSA key pair and ZCM-100 uses a static DSA key pair.

Table 2b – Other Allowed Security Functions

4. PORTS AND INTERFACES

4.1. Physical Ports

The ZCM-100 contains two 20-pin board-to-board connectors J1 & J2. Pin-outs of each connector (see Figure 3) are defined in the below tables. (Note that all inputs/outputs are 3.3V LVTTL level, except otherwise mentioned.)

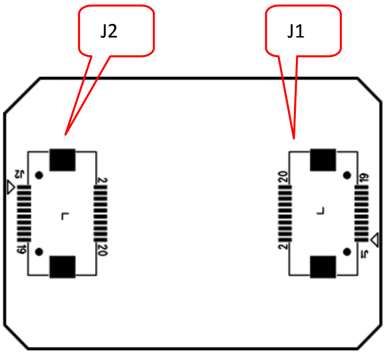


Figure 3: ZCM-100 Connectors

Pin Number	Description
1	Active high, asserted when host system is ready to access the encrypted or decrypted data via DATA_output_dat[3:0]. Part of the parallel data output bus
3	Active high, asserted by ZCM-100 to indicate DATA_output_dat[3:0] validity. Part of the parallel data output bus
4	AES engine clock (1-60Mhz) input. Part of the parallel data bus
5	Active high, asserted by ZCM-100 to indicate start of packet on DATA_output_dat[3:0]. Part of the parallel data output bus
7	Active high, asserted by ZCM-100 to indicate end of packet on DATA_output_dat[3:0]. Part of the parallel data output bus
9	Bit 0 of nibble of the parallel data output bus
11	Bit 1 of nibble of the parallel data output bus
13	Bit 2 of nibble of the parallel data output bus
15	Bit 3 of nibble of the parallel data output bus
19, 20	Ground
Other Pins	Not Connected

Table 3 – Physical Port J1

Pin Number	Description
2	Bit 0 of nibble of the parallel data input bus
4	Bit 1 of nibble of the parallel data input bus
5	ZCM-100 UART port transmit
6	Bit 2 of nibble of the parallel data input bus
7	ZCM-100 UART port receipt
8	Bit 3 of nibble of the parallel data input bus
9	Asserted by ZCM-100 to indicate the AES engine inlet FIFO is available for encryption/decryption. When asserted, plaintext or ciphertext is allowed to be input via DATA_input_dat[3:0]. Part of the parallel data input bus
10	Tied to ground on host system for normal operation. Floating this pin will trigger ZCM-100’s auto-zeroization
11	Active high, asserted by host system to indicate DATA_input_dat[3:0] validity. Part of the parallel data input bus
12	Battery power, ranged 2.5- 3.5V
13	Active high, asserted by host system to indicate start of packet on DATA_input_dat[3:0]. Part of the parallel data input bus
14	3.3V power, 5% tolerance
15	Active high, asserted by host system to indicate end of packet on DATA_input_dat[3:0]. Part of the parallel data input bus
16, 18	1.2V power, 5% tolerance
20	Ground
Other pins	Not Connected

Table 4 – Physical Port J2

4.2. Logical Interfaces

ZCM-100 functions as a slave controller and responds to the commands of the host system. There are five logical interfaces provided by ZCM-100: Data Input、Data Output、Control Input、Status Output and Power.

Table 5 shows the relations between these logical interfaces and physical ports of ZCM-100:

Logical Interface	Physical Ports
Data Input	Parallel Data Bus, UART
Data Output	Parallel Data Bus, UART
Control Input	UART, Zeroization(J2-pin 10)
Status Output	UART
Power	VCC, Ground

Table 5 – Logical Interfaces

The logical interfaces are kept logically separate when sharing a physical port by the protocols used. Information flows of the data input, data output, control input, and status output interfaces are encapsulated into "commands" and "responses". The host system will always act as master and the module as slave. The direction of the transmission is assumed to be known to both the module and the host system. The basic command format will be:

Command/ Response (3 bytes)	Content length (2bytes)	Content (N bytes, N=Content length)

Please refer to ZCM-100 user's manual for detailed descriptions of these commands.

5. IDENTIFICATION AND AUTHENTICATION POLICY

ZCM-100 supports two authorized roles for operators: User and Crypto Officer (CO). ZCM-100 enforces the separation of these roles by using identity-based operator authentication when accessing the module and by restricting the services available to each one. One authentication is allowed per module reset, i.e., an operator must re-authenticate after a power down or reset. There are no concurrent users allowed.

5.1. Crypto Officer (CO) Role

The CO role is responsible for initializing the module and managing the security configuration of ZCM-100. Before issuing a module to a user, the CO initializes the module with keying material and private information. ZCM-100 validates the CO identity using digital signature verification before accepting any initialization commands. This role is also authorized to import keys into ZCM-100, read module status and manage user accounts. The CO cannot be deleted from ZCM-100.

5.2. User Role

The User role is available after the module has been loaded with a user personality. This role is authorized to modify his own access data and use cryptographic services. User role is not authorized to import keys into the module. The module allows at most three different users by checking their individual signatures when accessing ZCM-100.

The module does not implement any maintenance interface, thus there is no maintenance role defined.

5.3. Authentication

Role	Type of Authentication	Authentication Data
User	Identity Based	DSA-signed user ID
Crypto Officer	Identity Based	DSA-signed CO ID

Table 6 – Roles, Identities and Authentication

The identity of each entity performing a role that requires authentication is held within ZCM-100 allowing the identity and authorization of the operator to be validated by checking his signature (DSA).

Authentication Mechanism	Strength of Mechanism
DSA-signed User ID	ZCM-100 uses DSA (L=2,048, N=256) signature to authenticate an operator. The strength depends on the size of the private key space. Therefore the probability of successfully guessing the private key (256-bit) is less than 1 in 1,000,000. (2E255≒10E76) Due to the UART interface speed of ZCM-100 (57,600bps), less than 6,084 authentication attempts could be performed within a one-minute period. Therefore the probability of such a repeated attack within one-minute is still way less than 1 in 100,000. (6,084/10E76≒10E-72)

Table 7 – Strengths of Authentication Mechanism

6. ACCESS CONTROL POLICY AND KEY MANAGEMENT

6.1. Descriptions of Services

ZCM-100 supports the following authenticated services defined in Table 8:

Service Type	Services	Description
User Management	Add User	This service allows crypto officer to add new users to ZCM-100. ZCM-100 supports up to 3 users.
	Delete User	This service allows crypto officer to delete existing users from ZCM-100. CO himself cannot be deleted.
	Modify ID	This service allows operator to modify his own ID.
	Access Request	CO/User login request
Module Management	Read Parameters	This service allows operator to read ZCM-100 parameters such as time of day (ToD) information, module id and network id.
	Write or Modify Parameters	This service allows crypto officer to write ZCM-100 parameters such as ToD information, module id and network id
	Request Self-test	This service allows operator to perform ZCM-100 self-test. Operator may request specific type of self-test.
	Read Status	This service provides the current status of ZCM-100.
	Read Firmware Version	This service returns the firmware version information of ZCM-100.

Service Type	Services	Description
	Read Key-file Version	This service returns the key-file version information of ZCM-100.
Key Management	Key-file Loading	This service allows crypto officer to load key-file into ZCM-100. The key-file loaded is encrypted by AES-256, followed by CRC-16 checksum.
	Key Loading	This service allows crypto officer to load specific keys to ZCM-100. The specific key loaded is encrypted by AES-256.
	Key Zeroization	This service zeroizes all keys and CSPs stored in the volatile and non-volatile memories.
Crypto Service	Generate Device DSA Signature	This service performs device DSA signature generation, based on device DSA private key and module-id stored in the key-file.
	Verify Device DSA Signature	This service performs device DSA signature verification with pre-loaded public key and far end module-id.
	Generate Application DSA Signature	This service performs application DSA signature generation with a pre-loaded private key.
	Verify Application DSA Signature	This service performs application DSA signature verification with a pre-loaded public key.
	Generate Application RSA Signature	This service performs application RSA signature generation with a pre-loaded private key.
	Verify Application RSA Signature	This service performs application RSA signature verification with a pre-loaded public key.
	Generate SHA Digest	This service generates a SHA digest of an operator supplied text-file. There are different options such as SHA-1, SHA-224, SHA-256…etc in ZCM-100. See Table2 for more information.

Service Type	Services	Description
	Generate HMAC Digest	This service generates a HMAC digest of an operator supplied text-file with a pre-loaded secret key. There are different SHA and truncated length options in ZCM-100. See Table2 for more information.
	Plaintext Encryption	This service encrypts operator supplied plaintext with pre-loaded AES key. ZCM-100 supports several AES modes. See Table 2 for more information.
	Ciphertext Decryption	This service decrypts operator supplied ciphertext with pre-loaded AES key. ZCM-100 supports several AES modes. See Table 2 for more information.
	Diffie Hellman Key Agreement	This service generates session key between host system and ZCM-100.

Table 8 – Services

6.2. Roles, Services and Access Rights

Table 9 shows access rights to different services.

Role		Services	CSPs and Keys	Type of Access
Crypto Officer	User			
Y	N	Add User	User(1~3) ID & public key	Write
Y	N	Delete User	User(1~3) ID & public key	Zeroize
Y	Y	Modify ID	Crypto officer ID & public key or user(1~3) ID & public key	Write
Y	Y	Access Request	CO public key or user(1~3) public key	Use
Y	Y	Read Parameters	NA	NA
Y	N	Write or Modify Parameters	Session key	Use
Y	Y	Request Self-test	NA	NA
Y	Y	Read Firmware Version	NA	NA

Role		Services	CSPs and Keys	Type of Access
Crypto Officer	User			
Y	Y	Read Key-file Version	NA	NA
Y	N	Key-file Loading	Session key RNG seed key RNG seed	Use
			Key protection key	Generate
			Crypto officer public key Crypto user(1~3) public key Device DSA public key Device DSA private key Application RSA public key Application RSA private key Application AES key	Write
Y	N	Key Loading	Session key	Use
			Application AES keys or Application DSA key pair or Application RSA key pair or Application HMAC key	Write
Y	Y	Key Zeroization	All keys	Zeroize
Y	Y	Generate Device DSA Signature	Device DSA private key	Use
Y	Y	Verify Device DSA Signature	Device DSA public key	Use
Y	Y	Generate Application DSA Signature	Application DSA private key	Use
Y	Y	Verify Application DSA Signature	Application DSA public key	Use
Y	Y	Generate Application RSA Signature	Application RSA private key	Use
Y	Y	Verify Application RSA Signature	Application RSA public key	Use
Y	Y	Generate SHA Digest	NA	NA
Y	Y	Generate HMAC Digest	Application HMAC key	Use
Y	Y	Plaintext Encryption	Application AES key	Use
Y	Y	Ciphertext Decryption	Application AES key	Use
Y	Y	Diffie Hellman Key Agreement	Session Key	Generate
Y	Y	Read Status	NA	NA

Table 9 Access Rights

6.3. Keys and CSPs Management

The below table shows keys and CSPs used in ZCM-100:

Item	Key/CSP	Description/Usage	Generation	Storage	Entry/ Output	Zeroization
1	Crypto officer public key	2048 bits DSA public key. Used to verify crypto officer's signature while he is logging in.	DSA key pair generated externally	Stored in non-volatile memory in ciphertext form which is encrypted by a 256-bit key protection key	Entry: Either by "Key-file Loading" service or by "Modify ID" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory
2	Users (1~3) public keys	2048 bits DSA public key. Used to verify user's signature while he is logging in.	DSA key pair generated externally	Stored in non-volatile memory in ciphertext form which is encrypted by a 256-bit key protection key	Entry: Either by "Key-file Loading" service or by "Modify ID" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory
3	Device public key	2048 bits DSA public key. Used to verify device signature	Device public key and device private key are DSA key pair and are generated externally	Stored in non-volatile memory in ciphertext form which is encrypted by a 256-bit key protection key	Entry: By "Key-file Loading" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory
4	Device private key	256 bits DSA private key. Used to generate device signature	Device public key and device private key are DSA key pair and are generated externally	Stored in non-volatile memory in ciphertext form which is encrypted by a 256-bit key protection key	Entry: By "Key-file Loading" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory

Item	Key/CSP	Description/Usage	Generation	Storage	Entry/ Output	Zeroization
5	Application AES key	128/ 192/ 256 bits AES key. Used to encrypt/decrypt application data when external applications issue encryption or decryption service request.	Generated externally	Stored in non-volatile memory in ciphertext form which is encrypted by a 256- bit key protection key	Entry: By "Key-file Loading" service or by "Key Loading" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory
6	Application DSA public key	1024/ 2048/ 3072 bits DSA public key. Used to verify application DSA signature when external applications issue DSA signature verification service request.	Generated externally.	Stored in volatile SRAM temporarily in plaintext form	Entry: By "Key Loading" service Output: NA	Cleared after each reset cycle
7	Application DSA private key	160/ 224/ 256 bits DSA private key. Used to generate application DSA signature when external applications issue DSA signature generation service request.	Generated externally.	Stored in volatile SRAM temporarily in plaintext form	Entry: By "Key Loading" service Output: NA	Cleared after each reset cycle
8	Application RSA public key	1024/ 2048/ 3072 bits Used to verify application RSA signature when external applications issue RSA signature verification service requests.	Generated externally.	Stored in non-volatile memory in ciphertext form which is encrypted by 256-bit key protection key.	Entry: By "Key-file Loading" service or by "Key Loading" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory
9	Application RSA private key	1024/ 2048/ 3072 bits Used to generate application RSA signature when external applications issue RSA signature generation service request.	Generated externally.	Stored in non-volatile memory in ciphertext form which is encrypted by 256-bit key protection key.	Entry: By "Key-file Loading" service or by "Key Loading" service Output: NA	Tamper detection and "Key Zeroization" service will delete all keys and CSPs stored in the non-volatile memory

Item	Key/CSP	Description/Usage	Generation	Storage	Entry/ Output	Zeroization
10	Application HMAC key	Used to generate HMAC digest	Generated externally.	Stored in volatile SRAM temporarily in plaintext form	Entry: By “Key Loading” service Output: NA	Cleared after each reset cycle
11	RNG seed	128 bits. Used to generate random number	Time information, generated from ZCM-100 local timer counter (hardware RNG)	Stored in volatile SRAM temporarily in plaintext form	Entry: NA Output: NA	Cleared after each reset cycle
12	RNG seed key	256 bits. Used to generate random number	Computed and generated based on ZCM-100 local timer counter (hardware RNG)	Stored in volatile SRAM temporarily in plaintext form	Entry: NA Output: NA	Cleared after each reset cycle
13	System default public key	2048 bits DSA public key. Used to login ZCM-100 for 1st time initialization	Hardcoded in ZCM-100 program	Hardcoded in ZCM-100 program in plaintext form	Entry: NA Output: NA	Cannot be zeroized
14	CO & Users ID	Used to login ZCM-100	Generated externally (CO & User defined, 16 characters each)	Stored in non-volatile memory in plaintext form	Entry: By ”Add User” service or by “Modify ID” service Output: NA	Tamper detection and “Key Zeroization” service will delete all keys and CSPs stored in the non-volatile memory
15	Key protection key	256-bit AES key. Used to encrypt /decrypt non-volatile CSP block	Generated internally via random number generation service	Stored in non-volatile memory in plaintext form	Entry: NA Output: NA	Tamper detection and “Key Zeroization” service will delete all keys and CSPs stored in the non-volatile memory

Item	Key/CSP	Description/Usage	Generation	Storage	Entry/ Output	Zeroization
16	Diffie Hellman static key pair	2048-bit public key and 256-bit private key. Used to generate session key	Hardcoded in ZCM-100 program	Hardcoded in ZCM-100 program in plaintext form	Entry: NA Output: NA	Cannot be zeroized
17	Diffie Hellman ephemeral key pair	2048-bit public key and 256-bit private key. Used to generate session key	Generated externally by host system	Ephemeral public key stored in SRAM temporarily in plaintext form	Entry: Ephemeral public key entered in "Diffie Hellman Key Agreement" service Output: NA	Cleared after each reset cycle
18	Session key (i.e., key wrapping key)	256-bits AES key. Used to establish secure session communication channel with host system	Generated during session establishment by D-H process	Stored in volatile SRAM temporarily in plaintext form	Entry: NA Output: NA	Cleared after session closed.

Table 10 Keys and CSPs Management

6.4. Zeroizations

As shown in Table 10, there are two occasions that the keys and CSPs stored inside of ZCM-100 would be zeroized:

1. When tamper detected, ZCM-100 will automatically zeroize the keys stored inside the module's non-volatile memory.
2. Crypto officer and user can send commands via control interface to ask ZCM-100 to zeroize the keys stored in the non-volatile memory.

In addition, all keys held in the SRAM of ZCM-100 will be cleared after power shuts down.

7. PHYSICAL SECURITY POLICY

ZCM-100 is housed in a metal case, with its PCB encapsulated in black epoxy within the metal case. The metal case as well as the epoxy cover are resistant to probing and are opaque within the visible spectrum. The cryptographic boundary of ZCM-100 contains the metal case, the PCB assembly and the epoxy cover. ZCM-100 uses production-grade components.

In a typical application the ZCM-100 metal case will be soldered onto the host system board for normal operation. This gives extra protection of ZCM-100 while operating.

Once ZCM-100 is being removed from the host system board, the tamper detection will be triggered and the ZCM-100 will automatically zeroize the keys stored inside.

Operators should regularly (once a day) check ZCM-100 internal log file or perform self-tests to ensure that physical security is maintained. The operator shall also check the appearance of ZCM-100's metal case (once half-year), whether the module is physically intact.

ZCM-100 is designed to meet FIPS 140-2 physical security level 3.

Note: The module hardness testing was only performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

8. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 Operational Environment requirements do not apply to the module in this validation because the module does not contain a modifiable operational environment.

9. SELF-TESTS

ZCM-100 self-tests include power-up test and conditional test. These tests are conducted automatically and do not require any operator intervention. All data output via the output interface is inhibited while any power-up and conditional test are running.

ZCM-100 also provides test-on-demand commands to CO and users. (See section 6.2)

Self-tests failure turns ZCM-100 into error state. Under such circumstance operator can send a command to ask ZCM-100 to return to factory default and power it up again. If the error still remains, ZCM-100 must be returned to ZyFLEX for repair.

9.1. Power-Up Test

There are three test items for power-up test:

1. Code Integrity Test: Checking ZCM-100 program code by CRC-32.

2. Cryptographic Algorithm Test: Known Answer Tests (KATs) are conducted for cryptographic algorithm including: SHA, HMAC, RSA, AES, and RNG.. DSA is tested using a pair-wise consistency test.

3. Key Integrity Test: Calculating SHA-256 digest of keys and CSPs stored in the non-volatile memory, then comparing it with the stored SHA-256 digest.

9.2. Conditional Test

ZCM-100 will perform continuous random number generator test. The RNG value will be compared with the previously generated value and they should not equal. If the continuous test fails, ZCM-100 will go into error state.

ZCM-100 will also perform continuous random number generation test on HRNG, which is used to generate RNG seed according to ANSI X9.31 Appendix A2.4.

10. DESIGN ASSURANCE

Inside ZCM-100, the FPGA implementation is written in Verilog language, and the microprocessor code is written in C. ZyFLEX uses Subversion to perform code and documentation versioning and management.

ZyFLEX uses Product Document Management (PDM), a custom-made software program, to control hardware design versions.

11. MITIGATION OF OTHER ATTACKS POLICY

The module has not been designed to mitigate specific attacks beyond the scope the FIPS 140-2 requirements.

12. CRYPTO OFFICER AND USER GUIDANCE

12.1. User Guidance

1. ZCM-100 feeds on three external power inputs: 3.3V, 1.2V, and a battery voltage of 3.3V (used to maintain key storage inside ZCM-100). Once the power inputs and external battery voltage are cut off, (say, when the ZCM-100 is removed from the host system board) the keys stored inside ZCM-100 will be automatically zeroized.
2. ZCM-100 works as a half-duplex encryption/decryption module, and its high-speed parallel data bus throughput depends on the external clock fed from the host system. For a typical application, an external clock of 25MHz is suggested, and the throughput is around 20Mbps (encryption or decryption). The external clock rate range is 1-60MHz.
3. ZCM-100 should be hand-soldered onto the host system board. For ZCM-100's dimension and layout suggestion, please contact ZyFLEX.
4. If ZCM-100 is in error state, please remove it from host system board and send it back to ZyFLEX for repair/exchange service.

12.2. Crypto Officer Guidance

1. Please refer to User Guidance.
2. For first-time initialization of ZCM-100, it must be done by the CO.
3. CO can add/delete/modify users. The CO cannot be deleted.
4. When the keys and CSPs are zeroized, ZCM-100 will go back to factory-default. CO must then re-initialize ZCM-100 before it can go into normal operation again.

13. REFERENCES & ACRONYMS

1. FIPS PUB 140-2 Security Requirements For Cryptographic Modules
2. Annex A: Approved Security Functions for FIPS PUB 140-2
3. Annex C: Approved Random Number Generators for FIPS PUB 140-2
4. Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2
5. Derived Test Requirements for FIPS PUB 140-2
6. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

Acronyms	Descriptions
AES	Advanced Encryption Standard
CCM	Counter with Cipher block chaining-Message authentication code
CSP	Critical Security Parameters
DSA	Digital Signature Algorithm
FPGA	Field Programmable Gate Array
HRNG	Hardware Random Number Generator
IV	Initialization Vector
KAT	Known Answer Test
RSA	Rivest Shamir and Adleman public key algorithm
SRAM	Static Random Access Memory
UART	Universal Asynchronous Receiver/Transmitter