Pure Storage, Inc.

FlashBlade Data Encryption Module

Non-Proprietary FIPS 140-2 Security Policy

Version: 1.1

Date: October 15, 2018

Pure Storage, Inc.

650 Castro Street

Mountain View, CA 94041

800-379-7873

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the FlashBlade Data Encryption Module, hereafter denoted the Module. The Module is a logical soft core within the FPGA that is responsible for performing AES-256 counter mode encryption or decryption. For counter mode, encrypt and decrypt operations are symmetric so the modules are in fact two instances of the same logical block.

Table 1 – Cryptographic Module Configurations

HW P/N and Version	FW Version
Altera ArriaV P/N 09-0001-00	71e841aae4b7bf22
Altera ArriaX P/N 09-0208-00	71e841aae4b7bf22

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated Data Storage. The Module is a single-chip sub-chip cryptographic module as defined in FIPS IG 1.20.

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

1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 2. The Module is a single-chip embodiment with a sub-chip cryptographic subsystem as defined in FIPS IG 1.20. The logical cryptographic boundary is the soft circuity core of the AES algorithm and the physical cryptographic boundary is the single-chip FPGA (see Figure 1).

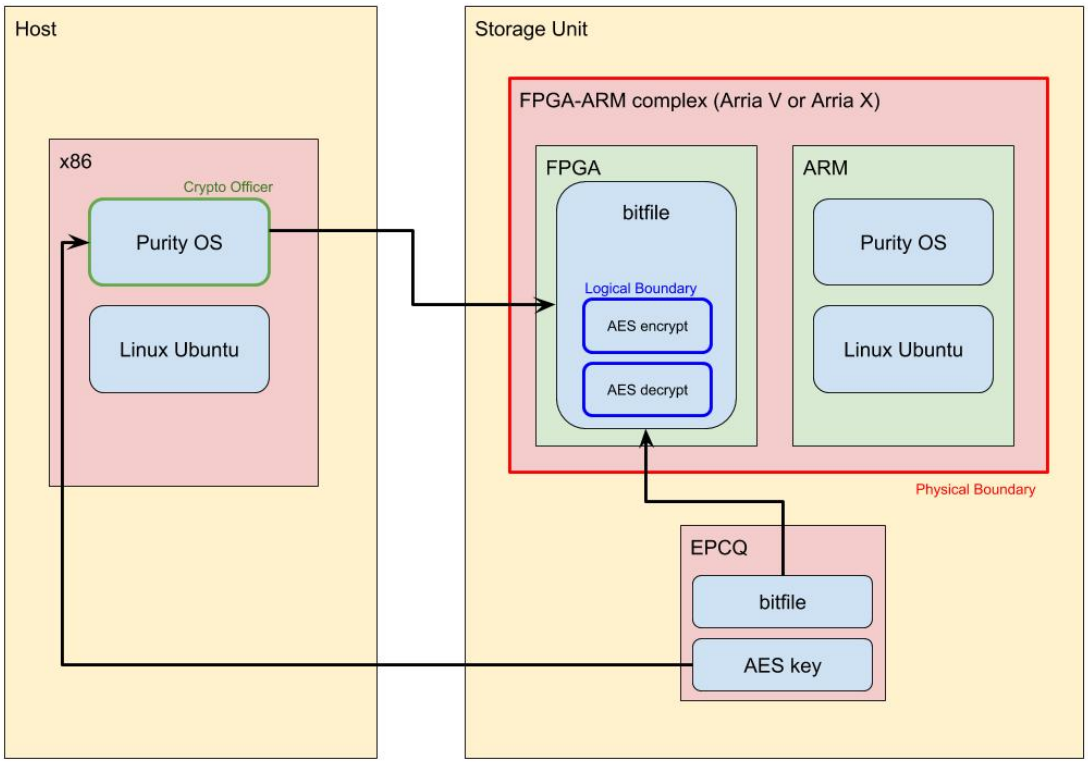

Figure 1 – Logical Boundary in relationship to the Physical Boundary

Figure 2 - Physical Boundary

The Module's ports and associated FIPS defined logical interface categories are listed in Table 3.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
aes_clk;	AES clock.	Control in
aes_reset;	Reset, active high, synchronous to clk_aes.	Control in
aes_key	64 bits; Slice of the 256---bit AES key.	Data in
aes_key_init	Pulse that causes key to be sampled and the key expansion initialization process to begin.	Control in
aes_key_init_sel	Specifies which key expansion is to be initialized.	Control in
aes_key_init_done	Level signal that indicates the key expansion initialization process has completed.	Status out
aes_key_init_reset	Pulse that resets the key init state machine. Allows software to bring the key init back to the initial state.	Control in
key_encrypt_sel	Specifies which key expansion is to be used for encrypting aes_in_valid.	Control in
aes_in_valid	Indicates that the inputs plain_text, counter, aes_in_encrypt, aes_in_sop, and aes_in_eop can all be sampled.	Control in
aes_in_ready	Indicates that the block is ready to accept input data.	Status out
aes_in_sop	Start of packet flag.	Control in
aes_in_eop	End of packet flag.	Control in
plain_text	128 bits; Text to be encrypted.	Data in
counter	128 bits; Counter value.	Data in
aes_out_valid	Indicates that cipher_text can be sampled.	Status out
aes_out_ready	Indicates that the outside world is ready to accept output data.	Control in
aes_out_sop	Start of packet flag.	Status out
aes_out_eop	End of packet flag.	Status out
cipher_text	128 bits; Encrypted data output.	Data out
pkt_hdr_aes_key_sel	Encryption key select for this packet	Control in
aes_address	Register interface address	Control in

Port	Description	Logical Interface Type
aes_writeVld	Register interface write valid	Control In
aes_writeData	Register interface write data	Control In
aes_readVld	Register interface read valid	Control In
aes_readData	Register interface read data	Status out
self_test_active	Indicates that the self-test is active	Status out
self_test_done	Indicates that the self-test has completed	Status out
self_test_passed	Indicates the result of the self-test	Status out
self_test_state	Indicates the self-test state	Status out
Power	Physical port for the FPGA to receive power	Power in

The aes_address, aes_writeVld, and aes_WriteData signals together form a register write interface. To write a register, you put the register address on the wire along with the data to write, while pulsing aes_writeVld high in the same clock cycle. The module supports register writes to the encrypt enable permission register and the encrypt enable register.

Similarly, the aes_address, aes_readVld, and aes_readData signals together form a register read interface. To read a register, you put the register address on the wire and pulse aes_readVld high in the same clock cycle. The data appears on the aes_readData output during the next clock cycle. The module supports register reads from the version register and the encrypt enable register.

1.2 Mode of Operation

The Module only supports an Approved mode of operation. To verify that a module is in the Approved mode of operation and that the FIPS validated version is being used, the operator must check the version output using the Show Status service and compare it against the FIPS certificate.

2 Cryptographic Functionality

The Module implements the FIPS Approved functions listed in the table below.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
5522	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt
		CTR [38A]	Key Sizes: 256	Encrypt/Decrypt

There are no Non-Approved Cryptographic Functions.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) are described in the services detailed in Section 4.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
AES Keys	Two AES 256 bit keys used for encryption/decryption.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using implicit mapping between services and roles.

Table 6 lists all operator roles supported by the module. The Module does not support a maintenance role but does support a bypass capability. The Module does not support concurrent operators.

Table 6 – Roles Description

Role ID	Role Description	Authentication Type
CO	Cryptographic Officer – This role is responsible for loading AES Keys into the Module.	**None – Level 1**
User	User – This role can perform encryption, decryption, or set the bypass flag.	**None – Level 1**

3.2 Services

All services implemented by the Module are listed in the table(s) below.

Table 7 – Authorized Services

Service	Description	CO	U
Key Initialization	Set the AES Keys to be used for encryption/decryption.	X	
Encrypt/Decrypt	Perform AES 256 Bit CTR mode encryption or decryption.		X
Set Bypass	Put the module in bypass mode		X
Bypass	Pass through plaintext data*		X
Reset Module	Resets the module but does not zeroize the CSPs.		X
Show Status	version, KAT pass/fail, bypass status		X
Power Off/Zeroization	Pull power from the module. This zeroizes the CSPs.		X
Power On	Apply power to the module. This runs the power-up self-tests.		X

* Note: The default state of the module upon power-up is to be in bypass. It is the User's responsibility to disable bypass via the Set Bypass service before using the module.

Table 8 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

The module does not Generate (G), Output (O), or Store (S) any CSPs.

Table 8 – CSP Access by Service

Service	CSPs
	AES Keys
Key Initialization	I
Encrypt/Decrypt	E
Set Bypass	-
Bypass	-
Reset Module	-
Show Status	-
Power Off/Zeroization	Z
Power On	-

4 Self-tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power-up self–tests are available on demand by power cycling the module.

All power-up self-tests must be completed successfully prior to any other use of cryptography by the Module. If the integrity test fails, then the bitfile fails to load and the module effectively does not exist. When this happens, the reconfig_trigger_condition register can be read, and the value will be 0x1 indicating a CRC error during the configuration. If the AES KAT of the test fails, the Module enters the KAT_ERROR error state and outputs status of self_test_active=0, self_test_passed=0, self_test_done=1, self_test_state=TEST_DONE, aes_out_valid=0, and aes_in_ready=0 otherwise it indicates successful completion by self_test_active=0, self_test_passed=1, self_test_done=1, and self_test_state= TEST_DONE.

The Module performs the following power-up self-tests.

- Firmware Integrity: CRC (32 bits for Arria X or 16 bits for Arria V, per configuration frame) of the sub-chip cryptographic boundary performed within the physical boundary over the whole bitfile
- AES-ECB-256 Encrypt KAT (this covers AES CTR encryption/decryption)

The Module performs the following conditional self-tests:

- Bypass test performed when we re-enable encryption.
- Firmware Load Test: N/A per IG 9.7

Upon power-up, a user can read the self-test status register to ensure that the power-up AES KAT has passed. If self_test_active=0, self_test_passed=1, self_test_done=1, and self_test_state=TEST_DONE, then the self-test has passed. When first powered on, the module comes up with encryption disabled. If the User first enables and then disables encryption via the Set Bypass service, the self-test status register will be cleared and reading the self-test status register at this time will be all 0's. When the encryption is again enabled, then the register will be populated with values again when the bypass test AES KAT is run.

The Module performs the following critical functions tests as indicated.

- None

5 Physical Security Policy

The module is compliant with Level 1 only. The module consists of production-grade components that include standard passivation techniques.

6 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Mitigation of Other Attacks Policy

The module does not support mitigation of other attacks.

8 Security Rules and Guidance

This section documents the security rules for the secure operation of the Module to implement the security requirements of FIPS 140-2.

1. Upon powering the module on, the default state is for bypass to be enabled. It is the User's responsibility to disable bypass via the Set Bypass service before using the module.
    a. Write a 1 to the permission register for enabling or disabling encryption.
    b. Write a 0 to the encryption enable register to enable encryption.
2. The module supports an exclusive bypass capability with the following two internal actions to activate bypass:
    a. Write a 1 to the permission register for enabling or disabling encryption.
    b. Write a 0 to the encryption enable register to disable encryption. This will clear the permission register. To re-enable encryption, you do not need to write the permission register first.
3. The Module provides two distinct operator roles: User and Cryptographic Officer.
4. The Module provides no authentication.
5. An operator does not have access to any cryptographic services prior to assuming an authorized role.
6. The Module allows the operator to initiate power-up self-tests by power cycling.
7. Power-up self-tests do not require any operator action.
8. Data output is inhibited during self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. There are no restrictions on which CSPs are zeroized.
11. The module does not support concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support manual key entry.The module does not have any proprietary external input/output devices used for entry/output of data.
14. The module allows entry of plaintext CSPs but does not allow output of plaintext CSPs. The Cryptographic Officer must be present locally with the hardware while using the Key Initialization service to input CSPs. I.e., the keys are manually distributed rather than electronically distributed per IG 7.7.
15. The module does not persistently store any plaintext CSPs.
16. The module does not output intermediate key values.

17. The Crypto Officer is responsible for entering the AES key(s) via the Key Initialization service before enabling encryption. The Crypto Officer should program two separate AES keys, one at a time using the **aes_key**, aes_**key_init**, and aes_**key_init_sel** inputs. Each 256-bit key is programmed in four 64-bit slices. Once initialization has completed this is reflected on the aes_**key_init_done** output signal. Pulsing the **aes_key_init_reset** input will reset the state of the key initialization sequence.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 9 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Table 10 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
CTR	Counter Mode
ECB	Electronic Code Book
EMI / EMC	Electromagnetic Interference / Electromagnetic Compatibility
EPCQ	A programmable NOR flash memory
FIPS	Federal Information Processing Standard
KAT	Known Answer Test