STONEWOOD

FIPS 140-2 Level 2 Security Policy for FlagStone Core (Versions V1.0.1.1a, V1.0.1.2a, V1.0.1.3)

Issue: 1.1

Contents

Figures

Glossary

AES	Advanced Encryption Standard
ATA	AT Attachment
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
C-O	Crypto-Officer
ECB	Electronic Code Book
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
FCC	Federal Communications Commission
FPGA	Field Programmable Gate Array
FIPS	Federal Information Processing Standards
HDD	Hard Disk Drive
IDE	Integrated Drive Electronics
IV	Initialisation Vector
KAT	Known Answer Test
KCC	Key Check Code
MBR	Master Boot Record
N/A	Not Applicable
NV	Non Volatile
OSC	Oscillator
PAC	Personal Authorisation Code
POST	Power on Self-Test(s)
PUB	Publication
RAM	Random Access Memory
RNG	Random Number Generator
SHS	Secure Hash Standard
TBA	To Be Announced
TBC	To Be Confirmed

References

[1] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900

[2] FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900

[3] NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4. Using the 3-Key Triple DES and AES Algorithms, January 31, 2005, Sharon S. Keller

[4] AT Attachment with Packet Interface – 7, Volume 1 – Register Delivered Command Set, Logical Register Set, ANSI NCITS 397-2005 (Vol. 2), American National Standards Institute, Inc., 25 West 43rd Street, New York, NY 10036, USA

[5] FlagStone (Corporate FIPS 140-2) Security Specification, Stonewood Document Number 3600-SS187

[6] FlagStone (FIPS 140-2) Hardware Design Description (for FlagStone Core V1.0.1.x), Stonewood Document Number 3620-DD089

[7] Flagstone Corporate (FIPS 140-2) User Guide(s)

[8] FlagStone Freedom (FIPS 140-2) User Guide(s)

[9] QP200 Product Development, Stonewood Quality Process

[10] QP500 Customer Interface, Stonewood Quality Process

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-2 validated cryptographic module deployed within Flagstone Corporate and FlagStone Freedom Drives referred to as the FlagStone Core. This document has been written based on the requirements specified in Ref. [1].

Whilst the FlagStone Core is provided as three physical embodiments, V1.0.1.1a, V1.0.1.2a & V1.0.1.3, the security functionality is identical for all three. The following table indicates which embodiment is used in each FlagStone Corporate and FlagStone Freedom Drive.

Drive	FlagStone Core
FlagStone Corporate (Parallel ATA Interface)	V1.0.1.1a
FlagStone Corporate (Serial ATA Interface)	V1.0.1.2a
FlagStone Freedom	V1.0.1.3

The following are images of FlagStone Corporate and FlagStone Freedom Drives containing the FIPS 140-2 validated FlagStone Core. Further information on the FlagStone Range can be found on www.flagstonesecure.com

Figure 1 FlagStone Corporate (Parallel ATA)

Figure 2 FlagStone Corporate (Serial ATA)

Figure 3 FlagStone Freedom

1.2 Security Level

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.3 Related Documents

- Finite State Model, Ref. [5]
- Cryptographic Boundary, Ref. [6]
- Supported ATA Commands, Ref. [5]

2 Cryptographic Module Specification

2.1 Overview

The FlagStone Core is a multi-chip embedded cryptographic module used within the FlagStone Corporate and the FlagStone Freedom Drives.

Figure 4 FlagStone Core V1.0.1.1a

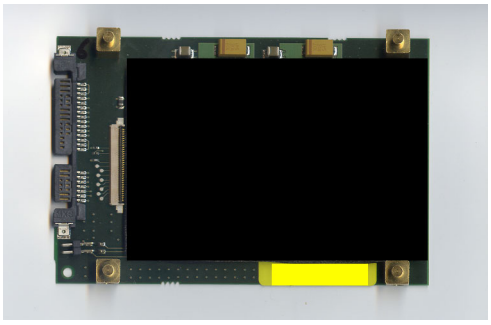

Figure 5 FlagStone Core V1.0.1.2a

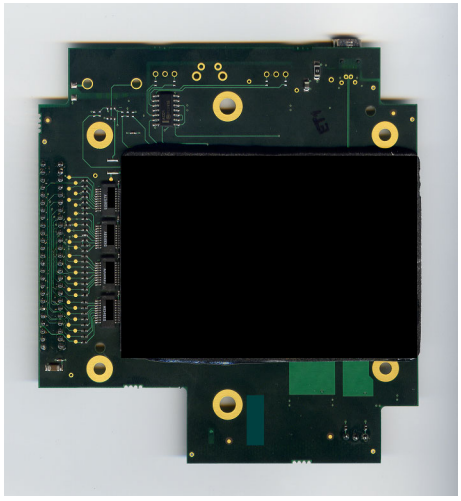

Figure 6 FlagStone Core V1.0.1.3

The FlagStone Core and subsequently the FlagStone Drives utilising the FlagStone Core provide access control and data encryption services to protect access to data stored on a HDD (Hard Disk Drive). All accessible sectors on a HDD connected to a FlagStone Core are encrypted.

The FlagStone Core authentication services and security functions can only be accessed through the use of ATA disk reads and ATA disk writes.

Once authenticated, data can be read and written to the connected HDD just like a normal HDD. Data written to the HDD is automatically encrypted prior to writing the data to the HDD; data read from the HDD is automatically decrypted prior to returning the data to the host.

Prior to authentication, ATA disk reads and ATA disk writes are entirely handled internally within the FlagStone Core. Specifically ATA disk reads will return FlagStone Core status information and disk writes, when targeted at the correct sector number, will invoke the authentication services within the FlagStone Core.

It is expected that most users will use an external application to communicate with the FlagStone Core's ATA disk read/write (plain text) interface prior to Authentication. To avoid the need for users to write their own applications, FlagStone applications are provided with the FlagStone Corporate and FlagStone Freedom Drives. Since these applications are not part of the FlagStone Core, they are not covered by this document. Details of these applications can be found in the user guide for the relevant FlagStone Corporate and FlagStone Freedom Drive.

The FlagStone applications are provided on Optical Media and embedded within the FlagStone Corporate and FlagStone Freedom Drives. When embedded, the application itself may be sourced from within the FlagStone Core prior to authentication through the use of ATA disk reads. The reading of the application has no effect on the functionality of the FlagStone Core. Since these applications are not part of the FlagStone Core, they are not covered by this document.

Figure 7 FlagStone Core Interface Diagram provides a pictorial representation of the interfaces to the FlagStone Core. Since the FlagStone Core is an embedded cryptographic module, the cryptographic boundary highlighted is not representative of the entire FlagStone module.

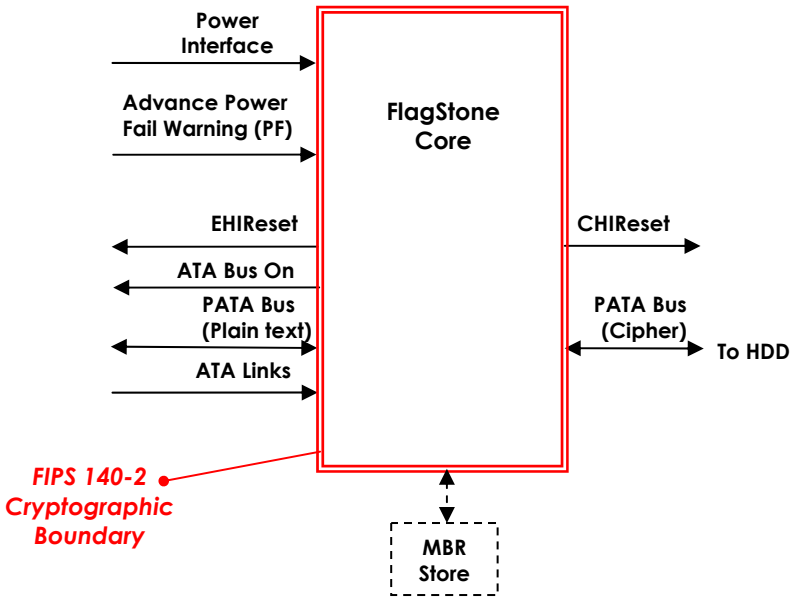

Figure 7 FlagStone Core Interface Diagram

Note: The MBR Store contains an external application that can be executed on a host processor to facilitate communication with the FlagStone Core's ATA disk read/write interface during the authentication process. No part of this application can run on, or alter the configuration of any of the FlagStone Core hardware. This application has no access to any additional port than is accessible by any other software application that can operate on the host processor.

2.2 Modes of Operation

The FlagStone Core can only operate in a FIPS-approved mode of operation.

The FlagStone Core implements the following FIPS-approved algorithms:

- 128-bit AES CBC Mode for full disk data encryption.
- 128-bit AES ECB Mode for Crypto-Officer authentication.
- ANSI X9.31 AES 128 bit RNG for internal Key and IV generation.

The FlagStone Core does not implement any non FIPS -Approved security functions.

3 Module Ports and Interfaces

The following table provides a brief description of the physical interfaces to the FlagStone Core. The interfaces specified can be seen in Figure 7 FlagStone Core Interface Diagram. Further details on these interfaces can be found in Ref. [6].

Physical Interface	Description
PATA Bus (Plain text)	The primary interface for the reception of ATA commands, plaintext data and authentication service requests from the external host ATA controller, and the primary interface for the transmission of data, status information and ATA transfer requests to the external host ATA controller.
PATA Bus (Cipher)	The primary interface for the transmission of ATA commands and enciphered data to the HDD and the primary interface for the reception of ATA transfer requests and enciphered data from the HDD.
Power Interface	Provides power to the FlagStone Core.
Advance Power Fail Warning (PF)	Provides a control signal from the local power supply to indicate the imminent loss of power.
ATA Bus On	Provides a status signal to indicate when the FlagStone Core PATA Bus (Plain text) is available for use.
EHIReset	Provides a status signal to indicate when the FlagStone Core is performing a reset of its PATA Bus (Plain text) interface.
CHIReset	Provides a status signal to indicate when the FlagStone Core is performing a reset of its PATA Bus (Cipher) interface.
ATA Links	Provided to allow configuration of the ATA interface within the FlagStone Core including master / slave and cable select options present on Parallel ATA HDDs.

The following table details the mapping of the physical interfaces summarised above to the FIPS 140-2 Logical Interfaces.

FIPS 140-2 Logical Interfaces	Physical Interface
Data Input Interface	PATA Bus (Plain text), PATA Bus (Cipher)
Data Output Interface	PATA Bus (Plain text), PATA Bus (Cipher)
Control Input Interface	PATA Bus (Plain text), PATA Bus (Cipher), Advance Power Fail Warning (PF), ATA Links
Status Output Interface	PATA Bus (Plain text), PATA Bus (Cipher), ATA Bus On, EHIReset, CHIReset
Power Port	Power Interface

The PATA Bus (Plain text) provides logical separation between its Data Input, Data Output, Control Input and Status Output interfaces through the use of the ATA Protocol and the Flagstone Core's Finite State Machine.

The PATA Bus (Cipher) provides logical separation between its Data Input, Data Output, Control Input and Status Output interfaces through the use of the ATA Protocol.

A description of the ATA command set supported by the FlagStone Core is detailed in Ref. [5]. Details of the ATA protocol can be found in Ref. [4].

4 Roles, Services, and Authentication

4.1 Roles

The FlagStone Core supports the two roles mandated by FIPS PUB 140-2 (Ref. [1]), namely Crypto-Officer and User. The FlagStone Core only supports a single session, therefore only one of the roles may be active at any given point.

The following table details the roles:

Role	Description
Crypto-Officer	The Crypto-Officer is responsible for User account management. The Crypto-Officer can: • Create a User. • Delete a User. • Recover a User, should a User have been suspended as the result of 5 consecutive failed User authentications. • Change the Recovery and User authentication parameters Completion of User account management always results in the Crypto-Officer being automatically logged out. Furthermore, if a User has been successfully created/recovered, the User is always automatically logged in.
User	The User will utilise the connected HDD for secure data storage. Once a User has been authenticated, the data key is loaded into the encryption / decryption path and the User has access to the data encryption /decryption services. ATA disk read/write data commands will automatically utilise the data encryption/decryption services provided by the FlagStone Core. Furthermore the User is also capable of changing their authentication parameter and logging out from the device.

4.2 Services

The following table details the services offered to valid operators based on their role.

Role	Service	Description
Crypto-Officer	Crypto-Officer Authenticate & Create User	This service allows the Crypto-Officer to authenticate them self, create a User and generate CSPs for the AES Algorithm. Optionally, the Crypto-Officer can also elect to change the User authentication parameter, thus ensuring that the recovery and current User authentication parameters are different. The FlagStone Core will first authenticate the Crypto-Officer. If unsuccessful the FlagStone Core will immediately terminate the service and inhibit any further operation from occurring, until power cycled. If successful, the FlagStone Core will check that there is no User present. If a User is present, an invalid Crypto-Officer Service Request will be reported and the Crypto-Officer will be automatically logged out. If there is no user present, the FlagStone Core will create a User by generating • the User authentication parameter CSPs, (current and recovery) from the User authentication parameter received • the User's Data Key and Initialisation Vector using the FIPS approved RNG, initialised with Date/Time received In the event the FIPS approved RNG reports a Continuous Self-Test error, the Crypto-Officer will be automatically logged out without creating the User. Once the User has been created, if the Crypto-Officer has elected to change the User authentication parameter, the FlagStone Core will regenerate and store the current User authentication parameter CSP using the received updated User authentication parameter. Finally, the FlagStone Core will automatically log out the Crypto-Officer, initialise the AES Algorithm with the Data Key and Initialisation Vector, and log in the User.
	Crypto-Officer Authenticate & Delete User	This service allows the Crypto-Officer to authenticate them self and delete a User. The FlagStone Core will first authenticate the Crypto-Officer. If unsuccessful the FlagStone Core will immediately terminate the service and inhibit any further operation from occurring, until power cycled. If successful, the User will be deleted and the User CSPs will be zeroised. Once completed, the Crypto-Officer will be automatically logged out. Note, this service is available when there is a suspended User present and when there is no User present.

Role	Service	Description
Crypto-Officer	Crypto-Officer Authenticate & Recover User	This service allows the Crypto-Officer to authenticate them self and recover a suspended User. Optionally, the Crypto-Officer can also elect to change the current and/or recovery User authentication parameters. The FlagStone Core will first authenticate the Crypto-Officer. If unsuccessful the FlagStone Core will immediately terminate the service and inhibit any further operation from occurring, until power cycled. If successful, the FlagStone Core will check that there is a suspended User present. If there is no User present, an invalid Crypto-Officer Service Request will be reported and the Crypto-Officer will be automatically logged out. If there is a suspended User present, the FlagStone Core will authenticate the recovery of the User using the User authentication parameter received. In the event the recovery was unsuccessful, the Crypto-Officer will be automatically logged out. Providing the recovery authentication is successful the FlagStone Core will copy the recovery User authentication parameter CSP to the current User authentication parameter CSP. Thereafter, if the Crypto-Officer has elected to change the current and/or recovery User authentication parameter, the FlagStone Core will regenerate and store the appropriate User authentication parameter CSPs using the received updated User authentication parameter. Finally, the FlagStone Core will automatically log out the Crypto-Officer, initialise the AES Algorithm with the Data Key and Initialisation Vector, and log in the (recovered) User. Note, there is a limit to the number of unsuccessful User recovery authentications permitted. After 15 unsuccessful User recovery authentications the User will be automatically deleted and the User CSPs will be automatically zeroised.
	Logout	This is an implicit service that is invoked by removing power.

Role	Service	Description
User	User Authenticate	This service allows the user to authenticate them self. The FlagStone Core will attempt to authenticate the User. If successful the FlagStone Core will initialise the AES Algorithm with the Data Key and Initialisation Vector and log in the User.
	User Authenticate & Change Authentication Parameter	This service allows the user to authenticate them self and change their authentication parameter. The FlagStone Core will attempt to authenticate the User. If successful the FlagStone Core will regenerate and store the current User authentication parameter CSP using the received updated User authentication parameter, initialise the AES Algorithm with the Data Key and Initialisation Vector and log in the User.
	Encrypt & Write Data to HDD	Given a block of data, this service encrypts the data with AES-128 in CBC mode using the User's Data Key and Initialisation Vector. The resulting cipher text is then written to the HDD using an ATA disk write. This service is initiated by the host performing an ATA disk write. This service is available only after authentication.
	Read & Decrypt Data from HDD	This service returns plaintext from the enciphered HDD by performing an ATA disk read from the HDD, and decrypting the retrieved (cipher text) data with AES-128 in CBC mode using the User's Data Key and Initialisation Vector. The service is initiated by the host PC performing an ATA disk read. The resulting plaintext is returned to the host using the appropriate ATA response. This service is available only after authentication.
	Logout	This is an implicit service that is invoked by removing power.

The following table details the services that do not require the authentication of an operator:

Service	Description
Read MBR Store	Prior to authentication, ATA disk reads to specific sectors will return a buffer of data sourced from the FlagStone Core's MBR store. This service will provide an application that can be executed externally on the host connected to the FlagStone Core. This application can be used to allow users to communicate with the FlagStone Core's ATA disk read/write interface prior to Authentication.
Supported ATA commands – non crypto	This service processes the set of ATA commands that are supported by the FlagStone Core but do not involve cryptographic/access control operations. These commands are processed in accordance with Ref. [4]. The responses given are those that would be expected for a standard HDD. These commands do not output user data.
Unsupported ATA commands	This service handles the set of ATA commands that the FlagStone Core does NOT support. In accordance with Ref. [4], these commands are aborted.
Run Self-Test	Following power up the FlagStone Core will perform a number of Self-Tests to ensure correct operation of the device. The service is invoked automatically by the power-up of the FlagStone Core.
Get Status	This service provides the current status of the FlagStone Core, including the results of self-tests. Status data is output as a sector of data prior to authentication and can be read using an ATA disk read.
Suspend User	This service is an implicit service that is invoked by deliberately performing 5 consecutive user authentications using an incorrect User Authentication Parameter.
Purge Unit	This service zeroises all CSPs from the FlagStone Core including those injected during manufacture. Following the activation of this service neither the Crypto-Officer nor User will be able to authenticate with the FlagStone Core. This service can be invoked by performing 5 consecutive invalid Crypto-Officer authentication attempts.

4.3 Authentication

The FlagStone Core module uses role-based authentication to facilitate access to cryptographic services. Re-authentication is required following a power cycle of the FlagStone Core module. The following table summarises the authentication inputs.

Role	Mechanism
Crypto-Officer	128 bit factory programmed value
User	Generation of a CRC32 from the received 256-bit user authentication parameter, followed by an equality test of the generated CRC32 and the Current User Authentication Parameter KCC stored within the FlagStone Core.

Note: The values described in this document are the authentication parameters received by the FlagStone Core. It is expected that most users will use an external application to capture and collate these parameters. The FlagStone Range provides a selection of external applications that users may use to facilitate capture of these parameters. Further details can be found in the respective Flagstone User Guides (Refs. [7] & [8]).

4.3.1 Crypto-Officer Authentication

The FlagStone Core limits the number of consecutive failed Crypto-Officer authentication attempts. Following each failed attempt the FlagStone Core requires power cycling before another attempt to authenticate can be made.

The Crypto-Officer is authenticated by using the Crypto-Officer PAC as the input to a 128bit AES Known Answer Test; the probability of a false acceptance is therefore 1 in 2^{128}.

Probability of false accept
1 in 3.40×10^{38}

The FlagStone Core limits the number of Crypto-Officer authentication attempts to five, see Security Rules section 13 for details. All five attempts may be completed within one minute; on the 5th failure the purge unit service is automatically invoked.

Probability of false accept in 1 minute
1 in 6.81×10^{37}

4.3.2 User Authentication

User authentication is performed by generating a CRC32 from the received user authentication parameter, followed by an equality test of the generated CRC32 and the Current User Authentication Parameter KCC. Since false acceptance of a User is based on a comparison of a 32-bit CRC, the probability of a false acceptance is therefore 1 in 2^{32}.

Probability of false accept
1 in 4.29×10^9

The FlagStone Core limits the number of User authentication attempts to five, see Security Rules section 13 for details. Following this only Crypto-Officer authentication is offered, where by the Crypto-Officer PAC needs to be entered. In the worst case scenario, the Crypto-Officer PAC is known enabling 15 attempts to recover the user.

User recovery authentication is performed by generating a CRC32 from the received user authentication parameter, followed by an equality test of the generated CRC32 and the Recovery User Authentication Parameter KCC. Since this is based on a comparison of a 32-bit CRC, the probability of a false acceptance is 1 in 2^{32}, i.e. the same as for User authentication.

Consequently, in this worst case scenario this provides a total of 20 attempts (5 user plus 15 recovery authentication attempts), all of which can be completed within one minute.

Probability of false accept in 1 minute
1 in 2.15×10^8

5 Finite State Model

The Finite State Model for the FlagStone Core is specified in Ref. [5].

All states required for a FIPS 140-2 validation, including Power On / Off states, Crypto Officer states, CSP Entry states, User states, Self-Test states and Error states have been included in the Finite State Model.

The FlagStone Core contains no Bypass States and no Maintenance States.

6 Physical Security

The FlagStone Core is a multi-chip embedded cryptographic module that meets FIPS 140-2 Level 3 for physical security. The FlagStone Core is potted with a hard epoxy resin that is opaque within the visible spectrum.

There are no access points to the FlagStone Core and there is no maintenance mode.

Damage to the epoxy resin is indicative of a potential violation of the physical security of the FlagStone Core. Damage to the FlagStone Core may be recognised as serious scratching, filing or drilling into the epoxy resin. Visibility of the circuit-board or any chips within the potted boundary may also be indicative of an unauthorised attempt at physical access or a unit not suitable for use.

Use of the epoxy resin ensures that attempts to penetrate the FlagStone Core will cause serious damage to the module and it will cease to function correctly, therefore an unauthorised attempt at physical access may also be determined if the module begins functioning abnormally, Power On Self-Tests fail, Continuous RNG Self-Test fails or it is Unusable.

Stonewood recommends that customers ensure themselves that the FlagStone Drive has not been tampered with when they first receive it. If the FlagStone Drive is received embedded within a host (e.g. a laptop or PC) the user is recommended to remove the FlagStone Drive and inspect it prior to first use.

Furthermore, Stonewood recommends that customers inspect the Flagstone Drive if it is suspected that it may have been in the possession of an unauthorised individual, e.g. if the FlagStone Drive is lost and subsequently found.

7 Operational Environment

The FlagStone Core module does not contain a modifiable operational environment and thus the Operational Environment requirements of FIPS PUB 140-2 (Ref. [1]) are not applicable.

8 Cryptographic Key Management

8.1 Critical Security Parameters

8.1.1 FlagStone™ID

The FlagStone™ID is generated using a FIPS validated SHS based RNG from FIPS 186-2, and injected into the FlagStone Core NV Store during unit manufacture.

The FlagStone™ID is used for authentication of the Crypto-Officer PAC, and is a fixed value.

Type: AES-128 Key
Storage: FlagStone Core NV Store (Constants)
Zeroisation: Purge Unit service

8.1.2 FlagStone™ID Schedule

The FlagStone™ID Schedule is a set of AES Round Keys computed from the FlagStone™ID CSP during the Crypto-Officer Authenticate & Create User service, the Crypto-Officer Authenticate & Delete User service and the Crypto-Officer Authenticate & Recover User service. These values are computed in accordance with the key schedule computation specified in the FIPS 197 *Advanced Encryption Standard (AES)*.

The FlagStone™ID Schedule is used by the AES Algorithm to authenticate the Crypto-Officer (section 4.3.1).

Type: AES-128 Round Keys
Storage: FPGA-RAM
Zeroisation: Logout service

8.1.3 Data Key

The Data Key is generated during the Crypto-Officer Authenticate & Create User service using the FlagStone Core FIPS approved RNG. The result of the operation is stored in the FlagStone Core NV Store.

The Data Key is used to generate the Data Key Schedule used for encrypting/decrypting data to/from the connected HDD during the Encrypt & Write Data to HDD service and the Read & Decrypt Data from HDD service.

Type: AES-128 Key
Storage: FlagStone Core NV Store (Variables)
Zeroisation: Purge Unit service and immediately following User deletion

8.1.4 Data Key Schedule

The Data Key Schedule is a set of AES Round Keys computed from the Data Key CSP, during the Crypto-Officer Authenticate & Create User service, the Crypto-Officer Authenticate & Recover User service, the User Authenticate service and the User Authenticate & Change Authentication Parameter service. These values are computed in accordance with the key schedule computation specified in the FIPS 197 *Advanced Encryption Standard (AES)*.

The Data Key Schedule is used by the AES Algorithm to encrypt/decrypt data to/from the connected HDD during the Encrypt & Write Data to HDD service and the Read & Decrypt Data from HDD service.

Type: AES-128 Round Keys
Storage: FPGA-RAM
Zeroisation: Logout service

8.1.5 Recovery User Authentication Parameter KCC

The Recovery User Authentication Parameter KCC is generated from the User Authentication Parameter during the Crypto-Officer Authenticate & Create User service and can be generated from the Updated User Authentication Parameter during the Crypto-Officer Authenticate & Recover User service. It is the result of a CRC32 calculation of the appropriate User authentication parameter and is stored in the FlagStone Core NV Store.

The Recovery User Authentication Parameter KCC is used during the Crypto-Officer Authenticate & Recover User service for authenticating the User's recovery authentication parameter.

Type: 32-bit CRC
Storage: FlagStone Core NV Store (Variables)
Zeroisation: Purge Unit service and immediately following User deletion

8.1.6 Current User Authentication Parameter KCC

The Current User Authentication Parameter KCC is generated from the User Authentication Parameter during the Crypto-Officer Authenticate & Create User service, is generated from the Updated User Authentication Parameter during the User Authenticate & Change Authentication Parameter service and can also be generated from the Updated User Authentication Parameter during the Crypto-Officer Authenticate & Recover User service. It is the result of a CRC32 calculation of the appropriate User authentication parameter and is stored in the FlagStone Core NV Store.

The Current User Authentication Parameter KCC is used during the User Authenticate service and the User Authenticate & Change Authentication Parameter service for authenticating the User's authentication parameter.

Type: 32-bit CRC
Storage: FlagStone Core NV Store (Variables)
Zeroisation: Purge Unit service and immediately following User deletion

8.1.7 RNG Seed

The RNG Seed is generated at the same time as the RNG Seed Key, see Section 8.1.8, using a FIPS validated SHS based RNG from FIPS 186-2, and injected into the FlagStone Core NV Store during unit manufacture. Prior to injection, the generating software compares the RNG Seed and the RNG Seed Key and verifies that they are not the same.

The RNG Seed is used by FlagStone Core's FIPS approved RNG and is a fixed value.

Type: 128-bit value
Storage: FlagStone Core NV Store (Constants)
Zeroisation: Purge Unit service

8.1.8 RNG Seed Key

The RNG Seed Key is generated at the same time as the RNG Seed, see Section 8.1.7, using a FIPS validated SHS based RNG from FIPS 186-2, and injected into the FlagStone Core NV Store during unit manufacture. Prior to injection, the generating software compares the RNG Seed and the RNG Seed Key and verifies that they are not the same.

The RNG Seed Key is used by FlagStone Core's FIPS approved RNG and is a fixed value.

Type: AES-128 Key
Storage: FlagStone Core NV Store (Constants)
Zeroisation: Purge Unit service

8.1.9 RNG Seed Key Schedule

The RNG Key Schedule is a set of AES Round Keys computed from the RNG Seed Key CSP once a Crypto-Officer has been authenticated during the Crypto-Officer Authenticate & Create User service. These values are computed in accordance with the key schedule computation specified in the FIPS 197 *Advanced Encryption Standard (AES)*.

The RNG Key Schedule is used by the RNG's AES Algorithm when generating random numbers.

Type: AES-128 Round Keys
Storage: FPGA-RAM
Zeroisation: Logout service and immediately following successful User creation

8.1.10 User Authentication Parameter

An externally sourced value used during the Crypto-Officer Authenticate & Create User service, the Crypto-Officer Authenticate & Recover User service, the User Authenticate service and the User Authenticate & Change Authentication Parameter service.

This is a transient value and is never persistently stored within the FlagStone Core.

Type: 256-bit value
Storage: FPGA-RAM (during authentication only)
Zeroisation: N/A

8.1.11 Updated User Authentication Parameter

An externally sourced value used during the Crypto-Officer Authenticate & Create User service, the Crypto-Officer Authenticate & Recover User service, and the User Authenticate & Change Authentication Parameter service.

This is a transient value and is never persistently stored within the FlagStone Core.

Type: 256-bit value
Storage: FPGA-RAM (during authentication only)
Zeroisation: N/A

8.1.12 Crypto-Officer PAC

An externally sourced value used during the Crypto-Officer Authenticate & Create User service, the Crypto-Officer Authenticate & Delete User service, and the Crypto-Officer Authenticate & Recover User service.

The Crypto-Officer PAC is a transient value and is never persistently stored in the FlagStone Core.

Type: 128-bit value
Storage: FPGA-RAM (during authentication only)
Zeroisation: N/A

8.2 Non Critical Security Parameters

8.2.1 Initialisation Vector

The Initialisation Vector is generated during the Crypto-Officer Authenticate & Create User service using the FlagStone Core FIPS approved RNG. The result of the operation is stored in the FlagStone Core NV Store.

The Initialisation Vector is used by the AES Algorithm for CBC encrypting/decrypting data to/from the connected HDD during the Encrypt & Write Data to HDD service and the Read & Decrypt Data from HDD service.

Type: 128-bit value
Storage: FlagStone Core NV Store (Variables)
Zeroisation: Purge Unit service and immediately following User deletion

8.2.2 RNG Date/Time

An externally sourced value used during the Crypto-Officer Authenticate & Create User service.

The RNG Date/Time is a transient value and is never persistently stored in the FlagStone Core.

Type: 128-bit value
Storage: FPGA-RAM (during authentication only)
Zeroisation: N/A

8.3 Access Privileges to Critical Security Parameters

CSP	Role	Service	Access
FlagStone™ID	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read
		Crypto-Officer Authenticate & Delete User	Read
		Crypto-Officer Authenticate & Recover User	Read
	No Role	Purge Unit	Zeroise
FlagStone™ID Schedule	Crypto-Officer	Crypto-Officer Authenticate & Create User	Write
		Crypto-Officer Authenticate & Delete User	Write
		Crypto-Officer Authenticate & Recover User	Write
		Logout	Zeroise
Data Key	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read/Write
		Crypto-Officer Authenticate & Delete User	Zeroise
		Crypto-Officer Authenticate & Recover User	Read
	User	User Authenticate	Read
		User Authenticate & Change Authentication Parameter	Read
	No Role	Purge Unit	Zeroise
Data Key Schedule	Crypto-Officer	Crypto-Officer Authenticate & Create User	Write
		Crypto-Officer Authenticate & Recover User	Write
		Logout	Zeroise
	User	User Authenticate	Write
		User Authenticate & Change Authentication Parameter	Write
		Encrypt & Write Data to HDD	Read
		Read & Decrypt Data from HDD	Read
		Logout	Zeroise
Recovery User Authentication KCC	Crypto-Officer	Crypto-Officer Authenticate & Create User	Write
		Crypto-Officer Authenticate & Delete User	Zeroise
		Crypto-Officer Authenticate & Recover User	Read/Write
	No Role	Purge Unit	Zeroise
Current User Authentication KCC	Crypto-Officer	Crypto-Officer Authenticate & Create User	Write
		Crypto-Officer Authenticate & Delete User	Zeroise
		Crypto-Officer Authenticate & Recover User	Write
	User	User Authenticate	Read
		User Authenticate & Change Authentication Parameter	Read/Write
	No Role	Purge Unit	Zeroise
RNG Seed	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read
	No Role	Purge Unit	Zeroise
RNG Seed Key	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read
	No Role	Purge Unit	Zeroise
RNG Seed Key Schedule	Crypto-Officer	Crypto-Officer Authenticate & Create User	Write/Zeroise
		Logout	Zeroise
User Authentication Parameter	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read
		Crypto-Officer Authenticate & Recover User	Read
	User	User Authenticate	Read
		User Authenticate & Change Authentication Parameter	Read

CSP	Role	Service	Access
Updated User Authentication Parameter	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read
		Crypto-Officer Authenticate & Recover User	Read
	User	User Authenticate & Change Authentication Parameter	Read
Crypto-Officer PAC	Crypto-Officer	Crypto-Officer Authenticate & Create User	Read
		Crypto-Officer Authenticate & Delete User	Read
		Crypto-Officer Authenticate & Recover User	Read

8.4 Random Number Generator

The FlagStone Core contains a FIPS approved Deterministic Random Number Generator based on ANSI X9.31 Appendix A.2.4 Using the AES 128 bit Algorithm, Ref. [3]. The Seed and Seed Key are held secret and are never released from the FlagStone Core.

8.5 Key Derivation

There are no Key Derivation techniques employed by the FlagStone Core.

8.6 Key Generation

The FlagStone Core contains an approved AES security function that requires a single key, the Data Key, which is generated each time a User is created. The FlagStone Core uses a FIPS 140-2 approved internal key generation technique to generate the key using the random number generator detailed in section 8.4.

8.7 Key Entry and Output

No keys are entered into the FlagStone Core after manufacture. Only the date/time and the authentication CSPs can be entered from an external source once the FlagStone Core has been potted in the hard opaque epoxy resin.

All CSPs are loaded into the FlagStone Core in plaintext form, both during manufacture and during normal operation.

Keys cannot be exported from the FlagStone Core in any form.

8.8 Initialisation Vector Generation

The FlagStone Core contains an approved AES security function that requires a single IV, the Initialisation Vector, which is generated each time a User is created. The FlagStone Core uses a FIPS 140-2 approved internal IV generation technique to generate the IV using the random number generator detailed in section 8.4.

8.9 Key Storage

The FlagStone Core stores all keys in plain text form.

9 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The FlagStone Core has been tested and meets applicable Federal Communications Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, (Class B for home use).

10 Self-Tests

The FlagStone Core performs self-tests during its power-on sequence and on demand to ensure all security critical functions are functioning correctly. Two types are implemented, Power On Self-Tests (section 10.1), which are performed when the FlagStone Core is powered up, and Conditional Self-Tests (section 10.2), which are performed when ever the relevant security function is invoked.

The status of Self-Tests can be retrieved, via the status output interface, using the Get Status service. This service returns a set of Self-Test Boolean Flags, as shown in the table below, which indicates whether the Self-Test(s) have passed or failed. A Self-Test Flag that represents more than one Self-Test result, e.g. Red ATA Controller, will indicate passed only if all Self-Tests grouped for that particular Self-Test Flag have passed.

Self-Test Boolean Flag	Self-Test Type	Reports overall result for:
Red ATA Controller	Power On Self-Test	1. ATA Bus On Signal Test 2. Status Input Test
Non Volatile Store	Power On Self-Test	1. Non-volatile store variable Test 2. Non-volatile store constants Test
Key Manager	Power On Self-Test	1. Cryptographic Algorithm Test 2. RNG KAT Test
Black ATA Controller	Power On Self-Test	1. Hardware Integrity Check
RNG Status	Conditional Self-Test	1. Continuous RNG Test

In addition to the Self-Test Flags, the Get Status service will return a general boolean "Error" flag. This "Error" flag is set to error state when any Self-Test has failed else it is set to no error state.

The Self-Tests results will be available once all the Power On Self-Test routines have been completed.

If an external application supplied with FlagStone/FlagStone Freedom is being used, then retrieval of the Self-Test results using the Get Status service is performed automatically. When an error is detected the external application will display an error message with the appropriate error code (refer to the relevant User Guides, Refs. [7] & [8], for further information).

10.1 Power On Self-Tests

The following table details the tests performed by the FlagStone Core during the power-on sequence. The Power On Self-Tests can only be initiated on demand by power cycling.

Power On Self-Test	Description
ATA Bus On Signal	Ensures that the ATA Bus On signal can be switched on and off.
Non-volatile store variable Test	The FlagStone Core NV Store holds two copies of variable data to ensure that if a power-down event occurs during an update at least one copy is valid. This test fails if both the primary and secondary copies fail CRC32 verification. A failure of this kind will render the unit permanently in-operable by automatically invoking the Purge Unit service, see section 4.2 for service details.
Non-volatile store constants Test	This test fails if the system constants fail a CRC32 verification.
Cryptographic Algorithm Test	Performs a 128-bit KAT test on the encrypt and decrypt path of the AES Algorithm.
RNG KAT Test	Performs a KAT test on the X9.31 AES 128 bit RNG.
Hardware Integrity Check	Ensures that communications can occur between the FlagStone Core and the connected HDD and ensures that the HDD has passed its own Self-Test.
Static Input Test	This ensures that the static input configuration pins have been configured correctly.

10.2 Conditional Self-Tests

The following table details the conditional test performed by the FlagStone Core; it is performed each time the security function is invoked.

Conditional Self-Test	Description
Continuous RNG Test	This conditional Self-Test ensures that the RNG security function does not generate two identical numbers in succession. In the event this conditional test fails, the FlagStone Core will inhibit all authentication services and security functions until power is cycled.

11 Design Assurance

11.1 Configuration Management

All elements of the FlagStone Core, including hardware and documentation are revision controlled according to Stonewood Electronics Ltd ISO 9001:2000 accredited quality management system.

All documents are assigned unique document numbers and subsequently version controlled using issues numbers of the form: 3600-SP189 Issue 1.0. Document numbers are formed by the project code, followed by the document type and a unique one-up value for the remainder of the document number.

All hardware components are assigned individual part numbers and issue characters of the form: 600051-P12 Issue A.

Details of the Stonewood Electronics Quality Process for product development are documented in Ref. [9].

11.2 Delivery and Operation

The FlagStone Core is manufactured and integrated into FlagStone Corporate and FlagStone Freedom Drives within the same secure environment and does not leave the secure environment prior to the FlagStone Core being potted in the hard opaque epoxy resin.

Once integrated into the FlagStone Drive, it will be shipped via courier. The delivery process is detailed in the Stonewood Electronics Ltd ISO 9001:2000 accredited Quality Management System and documented in Ref. [10].

11.3 Development

All elements of the FlagStone Core are developed in accordance with the Stonewood Electronics Ltd. ISO 9001:2000 accredited Quality Management System and documented in Ref. [9].

All documentation required for the FIPS accreditation of the FlagStone Core has been submitted for FIPS validation including PCB layouts, schematics, source code and specifications. Ref. [5] provides the functional specification of the FlagStone Core.

All FPGA code has been written in a high-level description language.

11.4 Guidance Documents

A combination of the relevant FlagStone User Guides (Ref. [7] for FlagStone Corporate and Ref. [8] for FlagStone Freedom) and this document provide all the guidance required for a Crypto-Officer and a User of the FlagStone Core. This Security Policy and the relevant user guide will be supplied on CD supplied with the end-product.

12 Mitigation of Other Attacks Policy

The FlagStone Core does not mitigate against other attacks beyond the scope of the FIPS 140-2 requirements.

13 Security Rules

13.1 Authentication Attempt Counters

The FlagStone Core limits the number of consecutively failed authentication attempts for both the User and the Crypto-Officer through the use of two attempt counters stored in the FlagStone Core NV Store.

Whilst the unit has a valid User created, failure to authenticate with the unit will result in the User authentication counter being decremented. Once the counter reaches zero the User will be suspended. The User can be recovered using the Crypto-Officer Authenticate & Recover User service.

If no valid users are present in the unit, failure to provide the valid Crypto-Officer PAC code will result in the Crypto-Officer authentication counter being decremented. Once the counter reaches zero the Purge Unit service will be automatically invoked.

At any point, if a successful authentication attempt is made the respective counter will be reset to its maximum value.

The current number of authentication attempts remaining can be determined using the Get Status service.

13.2 Recovery Attempt Counter

The FlagStone Core limits the number of failed recovery attempts within the Crypto-Officer Authenticate & Recover User service by maintaining a recovery attempt counter, which is decremented if the Crypto-Officer is authenticated but User Recovery is not. Once the counter reaches zero, the User is deleted. Whenever a user is created or recovered then this counter will be reset to its maximum value.

The current number of recovery attempts remaining can be determined by using the Get Status service.