FIPS 140-2 Level 2 Security Policy for FlagStone Core (Versions V2.0.1.1, V2.0.1.2, V2.0.1.3, V2.0.2.1, V2.0.2.2, V2.0.2.3, V2.0.3.3, V2.0.3.4, V2.0.4.5, V2.0.5.3, V2.0.5.4, V2.0.5.5)

Issue: 2.0

Contents

Figures

Tables

Glossary

A-A	Auto Authentication
Acct	Account
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
Auth	Authentication
Auto	Automatic
ATA	AT Attachment
C-I	Crypto-Initiator
C-M	Crypto-Migrate
CO	Crypto Officer
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CDI	Connected Drive Interface
CIRNG	Crypto-Initiator's Random Number Generator
CISAV	Crypto-Initiator's Secondary Authentication Value
CIWK	Crypto-Initiator's Wrapping Key
COTS	Commercial Off The Shelf
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DEK	Data Encryption Key
DES	Data Encryption Standard
DP	Datapath
ECB	Electronic Code Book
EECA	Externally Executed Control Application
EHI	External Host Interface
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference

FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HDD	Hard Disk Drive
ISO	International Standards Organization
IV	Initialization Vector
KAT	Known Answer Test
L-U	User – ordinary user with limited management capability
MGR	Manager
N/A	Not Applicable
N-R	No Role
NIST	National Institute of Standards and Technology
NV	Non Volatile
OAVK	Operator Authentication Validation Key
OHP	Operator Host Authentication Parameter
OKAP	Operator Key Port Authentication Parameter
OOB	Out Of Band
OP	Operator/Operational
OPNCISAV	Operational Non Crypto-Initiator's Secondary Authentication Value
OPRNG	Operational Random Number Generator
OPWK	Operational Wrapping Key
PAE	Pre-Authentication Environment
PAEK	PAE Key
PAE-U	PAE Update
PATA	Parallel ATA
PC	Personal Computer
POST	Power on Self-Test(s)
PUB	Publication
RNG	Random Number Generator
SDA	Secure Drive Access
SH	Service Handler
SHS	Secure Hash Standard
SI	System Integrator
SSD	Solid State Device
XOR	eXclusive OR (i.e. bit-wise modulo 2 addition)

Revision History

Issue	Description	Date	Author
1.0	Initial Release to Test House	04/12/08	Tim D. Stone
1.1	Minor updates requested by Test House	19/12/08	Tim D. Stone
1.2	Updated following NIST/CSEC review New Stonewood Group branding adopted	22/04/09	Tim D. Stone
1.3	Added Versions V2.0.2.1, V2.0.2.2 & V2.0.2.3	08/05/09	Tim D. Stone
1.4	Added Versions V2.0.3.3 & V2.0.3.4	12/11/09	Tim D. Stone
1.5	Added Versions V2.0.4.5, V2.0.5.3, V2.0.5.4 & V2.0.5.5	04/02/11	Tim D. Stone
1.6	Updated ANSI X9.31 RNG status	28/03/11	Tim D. Stone
1.7	Removed Versions V2.0.4.5 & V2.0.5.5	14/06/11	Tim D. Stone
1.8	Added Versions V2.0.4.5 & V2.0.5.5	15/06/11	Tim D. Stone
1.9	Updated following NIST/CSEC review ViaSat branding adopted	20/09/11	Tim D. Stone
2.0	Updated following NIST/CSEC review	18/10/11	Tim D. Stone

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] AES Key Wrap Specification (Draft), 16 November 2001, National Institute of Standards and Technology

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

[6] FlagStone Core V2.0.1.x/V2.0.2.x/V2.0.3.x/V2.0.4.x/V2.0.5.x Architecture Specification, ViaSat UK Document Number 3650-RS033

[7] FlagStone (FIPS 140-2) Hardware Design Description (for FlagStone Core V2.0.1.x/V2.0.2.x/V2.0.3.x/V2.0.4.x/V2.0.5.x), ViaSat UK Document Number 3650-DD110

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

[9] Eclypt Freedom (FIPS 140-2) User Guide(s)

[10] Eclypt Nano (FIPS 140-2) User Guide(s)

[11] QP200 Product Development, ViaSat UK Quality Process

[12] QP500 Customer Interface, ViaSat UK Quality Process

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-2 validated cryptographic module deployed within Eclypt 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 twelve physical embodiments, V2.0.1.1, V2.0.1.2, V2.0.1.3, V2.0.2.1, V2.0.2.2, V2.0.2.3, V2.0.3.3, V2.0.3.4, V2.0.4.5, V2.0.5.3, V2.0.5.4 & V2.0.5.5, the security functionality is identical for all twelve. The following table indicates which embodiment is used in each Eclypt Drive.

FlagStone Core	Drive
V2.0.1.1, V2.0.2.1	Eclypt Internal (Parallel ATA Interface)
V2.0.1.2, V2.0.2.2, V2.0.3.4, V2.0.5.4	Eclypt Internal (Serial ATA Interface)
V2.0.1.3, V2.0.2.3, V2.0.3.3, V2.0.5.3	Eclypt Freedom
V2.0.4.5, V2.0.5.5	Eclypt Nano

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

Figure 1 - Eclypt Internal (Parallel ATA)

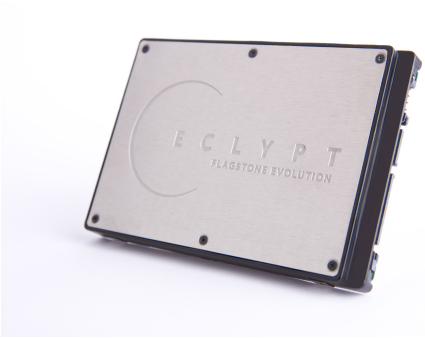

Figure 2 - Eclypt Internal (Serial ATA)

Figure 3 - Eclypt Freedom

Figure 4 - Eclypt Nano

1.2 Security Level

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
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

Table 1 Security Levels

1.3 Related Documents

- Finite State Model, Ref. [6]
- Cryptographic Boundary, Ref. [7]

2 Cryptographic Module Specification

2.1 Overview

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

Figure 5 - FlagStone Core V2.0.1.1, V2.0.2.1

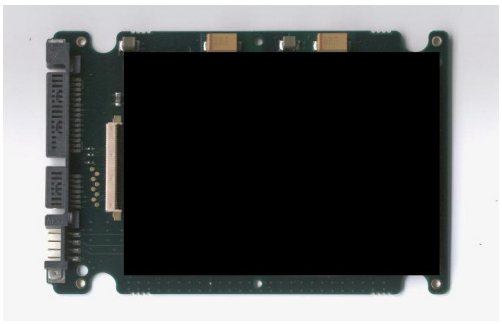

Figure 6 - FlagStone Core V2.0.1.2, V2.0.2.2

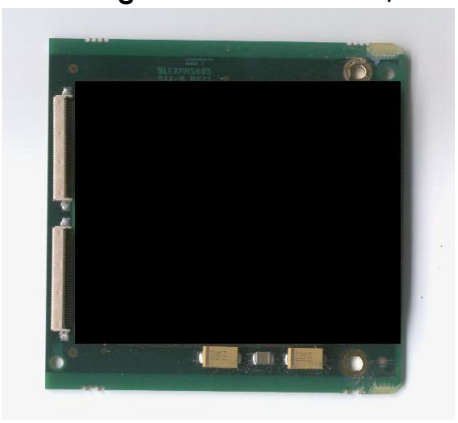

Figure 7 - FlagStone Core V2.0.1.3, V2.0.2.3, V2.0.3.3, V2.0.5.3

Figure 8 - FlagStone Core V2.0.3.4, V2.0.5.4

Figure 9 - FlagStone Core V2.0.4.5, V2.0.5.5

Figure 10 - FlagStone Core Simplified Block Diagram provides a pictorial representation of the FlagStone Core's interfaces and functional blocks. The FlagStone Core consists of two service provision blocks, the Datapath and the Service Handler. Overall control is provided by the Control block, and non-volatile parameter storage (including CSPs) is provided by the NV Store. Since the FlagStone Core is an embedded cryptographic

module, the cryptographic boundary highlighted is not representative of the entire Eclypt device.

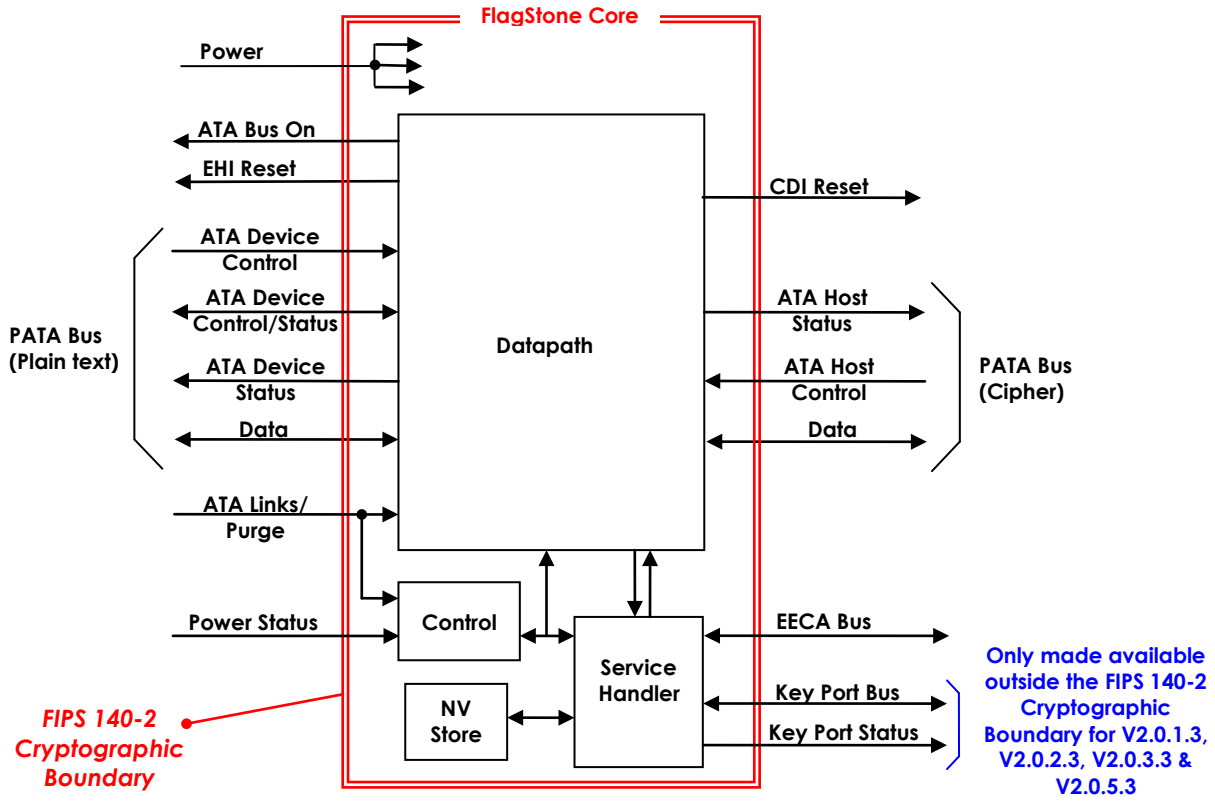

Figure 10 - FlagStone Core Simplified Block Diagram

The PATA Bus (Cipher) provides communication to/from a connected drive, whereas the PATA Bus (Plain Text) provides communication to/from a Host System, e.g. Desktop PC, Laptop.

2.1.1 Datapath

The Datapath of the FlagStone Core, and subsequently the Eclypt Drives utilizing the FlagStone Core, provide data encryption/decryption services to protect the data stored on a connected drive. The connected drive can be any COTS storage device that supports the ATA command protocol, including HDDs (Hard Disk Drives) and SSDs (Solid State Drives). All accessible sectors on a drive connected to a FlagStone Core are encrypted.

These services and security functions can only be accessed through the use of ATA disk reads and ATA disk writes.

In the appropriate Datapath roles, data can be read and written to the connected drive just like a normal drive. Data written to the connected drive is automatically encrypted prior to writing the data to the connected drive; data read from the connected drive is automatically decrypted prior to returning the data to the host.

To provide non-volatile storage for an external application (Section 2.1.3), the Datapath splits the connected drive into two regions. The PAE (Pre-Authentication Environment) region provides storage for the external application, whereas the non-PAE region provides the normal drive data storage region, typically containing the operating system, applications and data. The Datapath ensures that only one of these regions is made available. Following successful POST, the PAE region is made available. Once an operator has successfully authenticated and booted, the non-PAE region is made available.

2.1.2 Service Handler

The Service Handler of the FlagStone Core provides authentication, purge, RNG and management services, including key management, account management, policy management, system control and datapath control.

The Service Handler services can be accessed from the PATA Bus (Plain Text), i.e. the Host, through both the use of ATA Vendor specific commands and the use of ATA disk reads and ATA disk writes targeted to specific sector addresses.

2.1.3 External Applications

With the exception of non-PAE region connected drive access, it is expected that most operators will use an external application to communicate with the FlagStone Core's PATA (Plain Text) interface in order to perform Service Handler and Datapath services.

To avoid the need for users to write their own applications, FlagStone applications are provided with the Eclypt Drives. These FlagStone applications are provided on Optical Media, embedded in hardware within the Eclypt Drives, and/or stored encrypted in the PAE region of the connected drive. 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 Eclypt Drive.

2.2 Modes of Operation

The FlagStone Core can operate in both FIPS 140-2 approved and non-approved modes of operation.

The FlagStone Core implements the following FIPS-approved algorithms:

- 256-bit AES CBC Mode, Cert #922
- 256-bit AES ECB Mode, Cert #923
- ANSI X9.31 AES 256 bit RNG, Cert #531
- 256-bit AES Key Wrap

The FlagStone Core does not implement any non FIPS approved cryptographic algorithms.

The ANSI X9.31 RNG is deprecated (i.e. allowed for use, but the user must accept some risk) from 2011 until 2015, and disallowed after 2015.

In accordance with best practice, directly following any crypto initialization, ViaSat recommends that a Crypto Officer ensures that the FlagStone Core is configured in an approved FIPS 140-2 mode of operation.

2.2.1 Approved FIPS 140-2 Mode of Operation

To operate in an approved FIPS 140-2 mode of operation, a Crypto Officer must ensure that the FlagStone Core is configured as follows.

- IV Diversification must be switched off
- There must be no auto authentication account

The FlagStone Core is supplied from ViaSat with IV Diversification switched off. The IV Diversification process, when switched on, ensures that the IV for every sector on the Drive is unique.

The Get Status – Core service returns the current setting of IV Diversification and indicates whether or not the auto authentication account is present.

Should the auto authentication account be present this can be removed by purging the FlagStone Core.

Further information relating to the use of ViaSat supplied external applications to control the FlagStone Core can be found in the Eclypt User Guides, Refs. [8], [9] & [10].

In accordance with best practice, directly following any crypto initialization, ViaSat recommends that a Crypto Officer ensures that the FlagStone Core is configured in an approved FIPS 140-2 mode of operation.

3 Module Ports and Interfaces

Table 2 provides a brief description of the physical interfaces to the FlagStone Core. The interfaces specified can be seen in Figure 10 - FlagStone Core Simplified Block Diagram. Further details on these interfaces can be found in Ref. [7].

Physical Interface	Description
PATA Bus (Plain text)	The primary interface for the reception of ATA commands, plaintext data and 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 connected drive and the primary interface for the reception of ATA transfer requests and enciphered data from the connected drive.
Power Interface	Provides power to the FlagStone Core.
Power Status	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.
EHI Reset	Provides a status signal to indicate when the FlagStone Core is performing a reset of its PATA Bus (Plain text) interface.
CDI Reset	Provides a status signal to indicate when the FlagStone Core is performing a reset of its PATA Bus (Cipher) interface.
ATA Links/Purge	Provided to allow configuration of the ATA interface within the FlagStone Core including master/slave and cable select options present on Parallel ATA Drives. This interface also provides an external purge input to the FlagStone Core.
Key Port Bus	To support dual port, two factor authentication, this read only interface is provided to allow a token to be read directly by the FlagStone Core. Since dual port, two factor authentication is only available on V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3, this interface is only made available outside the FIPS 140-2 cryptographic boundary for V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3.
Key Port Status	To support dual port, two factor authentication, this interface provides two status signals to indicate status of the Key Port. Since dual port, two factor authentication is only available on V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3, this interface is only made available outside the FIPS 140-2 cryptographic boundary for V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3.
EECA Bus	Provides the interface to the read only EECA Store. The EECA Store contains the Eclypt Drive Identify Device information and External Applications that can be executed on the host.

Table 2 Physical Ports

Table 3 details the mapping of the physical interfaces summarized above to the FIPS 140-2 Logical Interfaces.

FIPS 140-2 Logical Interfaces	Physical Interface
Data Input	PATA Bus (Plain text), PATA Bus (Cipher), Key Port Bus (for V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3 only)
Data Output	PATA Bus (Plain text), PATA Bus (Cipher)
Control Input	PATA Bus (Plain text), PATA Bus (Cipher), Power Status, ATA Links/Purge, Key Port Bus (for V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3 only), EECA Bus
Status Output	PATA Bus (Plain text), PATA Bus (Cipher), ATA Bus On, EHI Reset, CDI Reset, Key Port Bus (for V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3 only), Key Port Status (for V2.0.1.3, V2.0.2.3 & V2.0.3.3 & V2.0.5.3 only), EECA Bus
Power	Power Interface

Table 3 Logical Interfaces

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.

The Key Port Bus provides logical separation between its Data Input, Control Input and Status Output interfaces through the use of its serial data protocol.

The EECA Bus provides logical separation between its Control Input and Status Output interfaces through the use of its serial data protocol.

A description of the ATA command set supported by the FlagStone Core is detailed in Ref. [6]. Details of the ATA protocol can be found in Ref. [5].

4 Roles, Services, and Authentication

The FlagStone Core uses identity-based authentication. There is an account associated with each individual identity (i.e. operator). To facilitate initialization, every FlagStone Core has a single Crypto-Initiator account.

4.1 Roles

The FlagStone Core roles permit authorized access to either Service Handler services or Datapath services, and hence are known as either Service Handler roles or Datapath roles.

The FlagStone Core supports concurrent sessions; however, the maximum number of concurrent sessions is two, and then only when one session has assumed a Service Handler role and the other session has assumed a Datapath role; further details can be found in Section 4.1.3.

An unauthenticated operator cannot assume a Datapath role directly; they must initially assume an appropriate Service Handler role and then assume a Datapath role.

In the event that the FlagStone Core has been unit purged, i.e. all CSPs have been purged, no role (Service Handler or Datapath) can be assumed.

When no operator is assuming an authorized Service Handler role, the Service Handler is deemed to be in No Role. Similarily, when no operator is assuming an authorized Datapath role, the Datapath is deemed to be in No Role.

Under normal operation, the FlagStone Core's Datapath is assuming the SDA role, whilst the Service Handler is not assuming any role (i.e. No Role).

4.1.1 Service Handler Roles

The FlagStone Core's Service Handler supports four roles. The Service Handler only supports a single session; therefore only one of the roles may be active at any given point.

To assume a Service Handler role the operator must successfully authenticate to an account using identity based authentication.

The Crypto Officer, Manager or User roles can be assumed using any operator account whose policy allows the specified role to be assumed, whereas the Crypto-Initiator role can only be assumed by the Crypto-Initiator account.

When no operator accounts exist, only the Crypto-Initiator role can be assumed. However, when 1 or more operator accounts exist, the Crypto-Initiator role cannot be assumed.

An operator that has assumed the Crypto-Initiator role cannot assume a Datapath role.

Furthermore, once the Service Handler has assumed a role, it must stop assuming this role before a different Service Handler role can be assumed.

Table 4 details the Service Handler roles that can be assumed as a result of a successful authentication.

Role	Description
Crypto-Initiator (C-I)	The Crypto-Initiator role allows the FlagStone Core to be initialized. This role allows the operator to: • Initialize for Operational use • Get Random Numbers • Logout
Crypto Officer (CO)	The Crypto Officer role allows the operator to: • Change the C-I account authentication parameters • Perform key management • Enable migrate access to non-PAE region of the connected drive • Perform operator account management including Creation/Deletion • Enable write access to the PAE region of the connected drive • Configure the FlagStone Core's Drive Policy • Purge the current Operational CSPs • Purge the entire unit (i.e. Unit Purge) • Boot • Get Random Numbers • Logout
Manager (MGR)	The Manager role allows the operator to: • Perform limited management of operator accounts that cannot assume the Crypto Officer role, namely Modify Account Status and Change Authentication Parameters • Purge the current Operational CSPs • Boot • Get Random Numbers • Logout
User (L-U)	The User role allows the operator to: • Boot • Change their own Authentication Parameters • Get Random Numbers • Logout

Table 4 Service Handler Roles

4.1.2 Datapath Roles

The FlagStone Core's Datapath supports three roles.

When operating in a FIPS 140-2 approved mode of operation, Datapath roles can only be assumed by a operator who is a assuming an appropriate Service Handler role; such an operator can assume the Datapath role without the need for further authentication.

The Datapath's Crypto-Migrate and Pre-Authentication Environment Update roles can only be assumed by an operator who is assuming the Service Handler's Crypto Officer role, whereas the Datapath's Secure Drive Access role can be assumed from any Service Handler role except the Crypto-Initiator role.

Furthermore, once the Datapath has assumed a role, it must stop assuming this role before a different Datapath role can be assumed.

Table 5 details the Datapath roles that can be assumed.

Role	Description
Secure Drive Access (SDA)	The Secure Drive Access role provides the operator with read/write access to the non-PAE Region of the connected drive. The Secure Drive Access role allows the operator to: • Encrypt and write data to the connected drive (non PAE region) • Read and decrypt data from the connected drive (non PAE region) • Logout
Crypto-Migrate (C-M)	Whilst in the Crypto-Migrate role, the Datapath is configured to decrypt with the old DEK and to encrypt with the new DEK. This role provides the operator with read/write access to the non-PAE Region of the connected drive, allowing an external application to read then write from / to every non-PAE region sector of the connected drive, thereby re-encrypting the non-PAE region of the connected drive with the new DEK. This role allows the operator to: • Encrypt and write data to the connected drive (non PAE region) • Read and decrypt data from the connected drive (non PAE region) • Logout
Pre-Authentication Environment Update (PAE-U)	The Pre-Authentication Environment Update Role provides the operator with read/write access to the PAE Region of the connected drive. This role allows the operator to: • Encrypt and write to the connected drive (PAE region) • Read and decrypt from the connected drive (PAE region) • Logout

Table 5 Datapath Roles

Notes:

1. *When the Datapath is not assuming a role, the Datapath may provide read only access to the connected drive's PAE region.*

4.1.3 Session Model

Figure 11 summarizes the session model when operating in an approved FIPS 140-2 mode of operation. At power up or following a restart, both the Service Handler (SH) and the Datapath (DP) will not be assuming a role.

When there are no operator accounts, only the Crypto-Initiator can log in using the Log In (C-I) service. Once logged in, the Crypto-Initiator can initialize the FlagStone Core and create a single (Initial) Crypto Officer account, but the Crypto-Initiator cannot assume a Datapath role.

Providing there is at least one operator account, an operator can log in using the Log In (OP) service. Once the operator has completed their activities they can

- simply log out of the Service Handler
- simultaneously assume a Datapath role and stop assuming the Service Handler role (using the Boot service)
- assume a Datapath role whilst continuing to assume the Service Handler role (using the Boot service)
- for the CO role only, continue to assume the Service Handler role and assume a Datapath role (using the Migrate New DEK or Unlock PAE services)

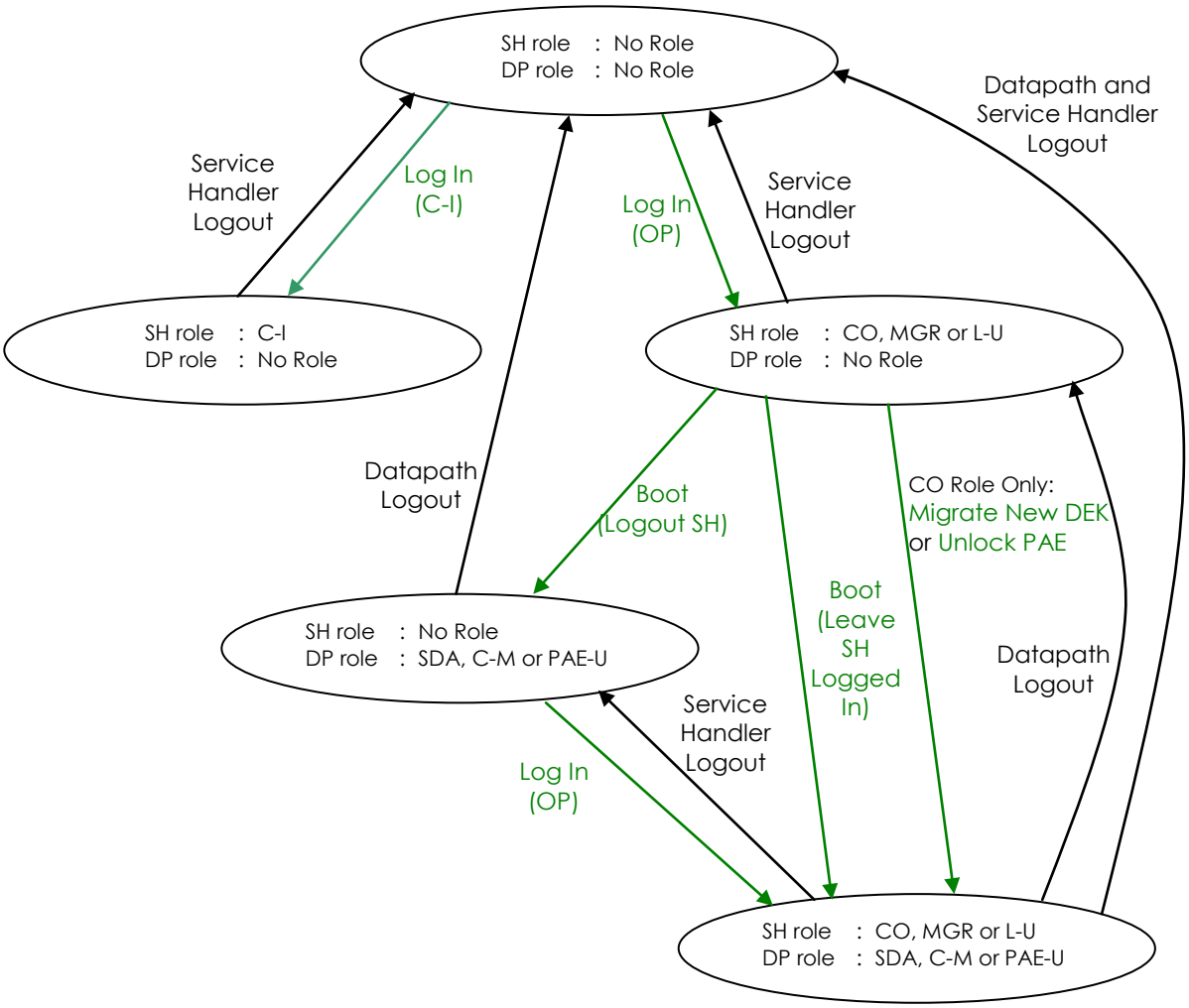

Figure 11 - Session Model (FIPS 140-2 Mode of Operation)

When an authenticated operator has stopped assuming a Service Handler role but has assumed a Datapath role, this authenticated operator or another unauthenticated operator can log in and assume a Service Handler role using the Log In (OP) service.

When an operator is assuming a Datapath role and this operator or another operator is assuming a Service Handler role, no further logins can be performed until the operator assuming the Service Handler role stops assuming this role.

An operator assuming a Service Handler role will stop assuming that role whenever:

- A service that performs a Service Handler log out is invoked
- A FlagStone Core error event occurs

An operator assuming a Datapath role will stop assuming that role whenever:

- A service that performs a Datapath log out is invoked
- A FlagStone Core error event occurs

Notes:

1. *Auto authentication must not be used when operating in a FIPS 140-2 approved mode of operation (see Section 2.2.1); it allows the Datapath's Secure Drive Access role to be assumed without the need for an operator to assume a Service Handler role, i.e. without the need for the operator to supply any authentication parameters.*

4.1.4 Accounts

In addition to the Crypto-Initiator's account, the FlagStone Core supports up to 128 operator accounts. When an account is created for an operator, the Service Handler roles available to that operator are specified through the use of the account type. Table 6 summarizes the accounts and the Service Handler role(s) that the operator can assume.

Account	Type	Service Handler Role				Account Description
		C-I	CO	MGR	L-U	
Crypto-Initiator		✓				This is the default account. There is only one C-I account. It is only available when there are no operator accounts available. This account type supports the Crypto-Initiator.
Operator	Crypto Officer		✓	✓	✓	This account type supports the operators that can assume the Crypto Officer role. Operators using this account type must select the Service Handler Role they wish to assume as part of the Log In process. Having assumed a particular Service Handler role, the operator must logout then re-authenticate to assume a different Service Handler role.
	Initial Crypto Officer		✓	✓	✓	This account type provides all of the functionality available to the CO account type. It differs from a CO account type in that it is the only account that the Crypto-Initiator can create. The FlagStone Core only supports a single Initial Crypto Officer account type.
	Manager			✓	✓	This account type supports the operators that can assume the Manager role. Operators using this account type must select the Service Handler Role they wish to assume as part of the Log In process. Having assumed a particular Service Handler role, the operator must logout then re-authenticate to assume a different Service Handler role.
	User				✓	This account type supports the operators that can only assume the Service Handler's User role.

Table 6 Accounts

Notes:

1. *To support Auto authentication, the FlagStone Core provides a single A-A account. However, auto authentication must not be used when operating in a FIPS 140-2 approved mode of operation (see Section 2.2.1); it allows the Datapath's Secure Drive Access role to be assumed without the need for an operator to assume a Service Handler role, i.e. without the need for the operator to supply any authentication parameters.*

4.2 Services

The FlagStone Core services are provided by the Service Handler (Section 4.2.1) and the Datapath (Section 4.2.2). Further information relating to the services can be found in the Flagstone User Guides (Refs. [8], [9] & [10]).

4.2.1 Service Handler Services

Unless explicitly stated otherwise within the service descriptions, the Service Handler services are invoked from the PATA Bus (Plain Text), i.e. the Host, through both the use of ATA Vendor specific commands and the use of ATA disk reads and ATA disk writes targeted to specific sector addresses.

Table 7 details the Service Handler services and the Service Handler roles that can invoke them. For completeness, the table indicates which services can be invoked when the Service Handler is not assuming a role, i.e. No Role (N-R).

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
System Control Service Group						
Primary (Shutdown)	✓	✓	✓	✓	✓	This service is invoked either as a result of a change in Power Status, or is invoked by another service. The Flagstone Core enters the Shutdown State, power consumption is minimized and the sanitization is performed. The Service Handler and the Datapath assume No Role, i.e. any logged in operators are automatically logged out. (See note 1)
Clear Alarm	✓					Clears the Alarm, then, depending on the supplied parameter, the FlagStone Core is returned to its ready state, or the Restart service is invoked or the Primary (Shutdown) service is invoked.
Clear Error	✓					Clears the Error, then, depending on the supplied parameter, either the Restart service is invoked or the Primary (Shutdown) service is invoked.
Force Shutdown	✓					The Primary (Shutdown) service is invoked.
Restart	✓					The FlagStone Core is restarted. The Service Handler and the Datapath assume No Role, i.e. any logged in operators are automatically logged out. (See note 1) This service is equivalent to powering off then back on the FlagStone Core; as a consequence the Power On Self Tests are invoked.
Clear Response Blocker	✓					When the response blocker is active and the blocker timeout has expired, this service clears the response blocker thereby permitting other services, e.g. Log In, to be invoked.
Status Service Group						
Get Status – Core	✓	✓	✓	✓	✓	Returns the status of the FlagStone Core, including self test results, error status, operator identity & role assumed, & service request status.
Get Status - Drive	✓	✓	✓	✓	✓	Returns the status of the FlagStone Drive, as reported by the ATA Command, Identify Device.

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
EECA Service Group						
Get EECA	✓	✓	✓	✓	✓	This service is only available when the connected Drive's PAE is not available. This service returns the external application stored in the EECA store. In the event that this external application is not available, the Service Handler returns the FlagStone Core's default external application.
C-I Account Service Group						
Get Acct Info (C-I)	✓	✓	✓			Returns account information for the C-I account.
Log In (C-I)	✓					Uses the supplied authentication parameter to log into the C-I account. Only if the authentication is successful will the Service Handler assume the C-I role.
Log Out (C-I)		✓				Logs out the C-I; the Service Handler assumes No Role.
Initialize Operational (Generate) & Logout		✓				This service configures the FlagStone Core for operational use and then automatically logs out the C-I. The configuration involves the import of the operational RNG key (OPRNG), the creation of the initial CO account (using the authentication parameters supplied – see note 2) and the generation of the associated CSPs, including the PAEK.
Initialize Operational (Import) & Logout		✓				This service configures the FlagStone Core for operational use and then automatically logs out the C-I. The configuration involves the import of the operational RNG key (OPRNG) and the operational wrapping key (OPWK), the creation of the initial CO account (using the authentication parameters supplied – see note 2) and the generation of the associated CSPs, including the PAEK.
Operational Account Service Group						
Get Acct Info (Operator)	✓		✓	✓	✓	Returns account information for the operator accounts. If the Service Handler has assumed No Role only the public information is returned. However, if the Service Handler has assumed a role both the public and the private information is returned.
Set Default Acct Info			✓			Changes the default acct record stored within the FlagStone Core.
Get Default Acct Info			✓			Returns the default acct record stored within the FlagStone Core.

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
Operational Account Service Group – continued						
Log In (OP)	✓					Providing the specified operator account exists and it is permitted to assume the specified role, this service uses the supplied authentication parameters (see note 2) to log into the specified operator account. Only if the authentication is successful will the Service Handler assume the specified role.
Log Out (OP)			✓	✓	✓	Logs out the operator currently logged into the Service Handler; the Service Handler assumes No Role.
Open Acct			✓	✓		Providing there is no account open, this service opens the specified operator account for creation/ modification.
Discard Acct			✓	✓		Providing there is an account open, this service unconditionally closes the account; any modifications to the account will be lost.
Save and Close Acct			✓	✓		Providing there is an account open, this service closes the account and updates the account's entry within the NV Store if it has been modified.
Create Acct			✓			Providing there is an empty account open, this service uses the supplied account information and authentication parameters (see note 2) to create an operator account.
Delete Acct			✓			Providing an operator account is open, this service deletes the open account. Note: To complete the deletion, the operator must invoke the Save and Close Acct service.
Modify Acct Policy			✓			Providing there is a non-empty account open, this service updates the account's policy fields.
Modify Acct Status			✓	✓		Providing there is a non-empty account open, this service updates the account's status fields.
Change Auth Parameters			✓	✓		Providing there is a non-empty operator account open, this service updates the operator account using the supplied authentication parameters (see note 2).
Change Own Auth Parameters			✓	✓	✓	Providing there is no account open, this service updates the Service Handler's currently logged in operator's account using the supplied authentication parameters (see note 2). Note: This change takes immediate effect; it does not require the Save and Close Account service to complete the update.
Change C-I Auth Parameters			✓			This service updates the C-I account using the supplied authentication parameter. Note: This change takes immediate effect; it does not require the Save and Close Account service to complete the update.

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
OPWK Management Service Group						
Import New OPWK			✓			This service imports a new operational wrapping key (NewOPWK), and then uses the new OPWK to re-wrap all accessible OPWK protected CSPs. If the operator specified that all accounts are to adopt the new OPWK, the NewOPWK is wrapped using the old OPWK and placed into the NV Store. This enables accounts using the old OPWK to adopt the new OPWK at the next successful account login.
Generate New OPWK			✓			This service generates a new operational wrapping key (NewOPWK), and then uses the new OPWK to re-wrap all accessible OPWK protected CSPs. If the operator specified that all accounts are to adopt the new OPWK, the NewOPWK is wrapped using the old OPWK and placed into the NV Store. This enables accounts using the old OPWK to adopt the new OPWK at the next successful account login.
RNG Management Service Group						
Import New OPRNG			✓			This service, imports the operational RNG key (OPRNG), overwriting any existing OPRNG.
Generate Random Data		✓	✓	✓	✓	Generates 128-bits of random data and stores the data temporarily within the FlagStone Core. To retrieve the random data the operator must use the Get Random Data service.
Get Random Data		✓	✓	✓	✓	Providing the Generate Random Data service has been performed prior to this service, this service will return the random data produced by the last Generate Random Data service.
DEK Management Service Group						
Import New DEK			✓			This service imports a new DEK, wraps the new DEK using the operational wrapping key (OPWK), and then places the wrapped new DEK and into the NV Store.
Generate New DEK			✓			This service generates a new DEK, wraps the new DEK using the operational wrapping key (OPWK), and then places the wrapped new DEK and into the NV Store.

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
DEK Management Service Group - continued						
Migrate New DEK			✓			Providing the Datapath has assumed No Role, this service configures the Datapath for DEK migration. The current DEK is loaded into the Datapath's decrypt path and the new DEK is loaded into the Datapath's encrypt path. The current DEK is replaced with the new DEK, thereby making the new DEK the operational DEK. The wrapped DEKs within the NV Store are updated accordingly. Finally, the Datapath assumes the Crypto-Migrate role and the Service Handler remains in the CO role, i.e. the operator is logged into the Datapath and remains logged into the Service Handler.
Promote New DEK			✓			This service replaces the current DEK with the new DEK, thereby making the new DEK the operational DEK. The wrapped DEKs within the NV Store are updated accordingly.
Remove New DEK			✓			This service updates the FlagStone Core status to indicate that the New DEK is no longer present. The wrapped DEKs within the NV Store are updated accordingly.
Datapath Control Service Group						
Boot			✓	✓	✓	Providing the Datapath has assumed No Role and the connected drive is present and good, this service configures the Datapath for Secure Drive Access, loading the DEK in the process. The Datapath assumes the Secure Drive Access role and, depending whether the supplied parameter indicates logout Service Handler, the Service Handler either assumes No Role (for logout SH) or remains in current role (for no logout SH) , i.e. the operator is logged into the Datapath and may be logged out of the Service Handler.
Log Out (Datapath)	✓	✓	✓	✓	✓	Providing the Datapath is assuming either the SDA or the C-M role, this service forces the Datapath to assume No Role, i.e. the operator logged into the Datapath is logged out. (The Service Handler role is not changed.)
Unlock PAE			✓			Providing the connected drive is present and good, and providing the Datapath has assumed No Role and the PAEK is available, this service enables write access to the PAE region on the connected drive. The Datapath assumes the Pre-Authentication Environment Update role and the Service Handler remains in the CO role, i.e. the operator is logged into the Datapath and remains logged into the Service Handler.

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
Datapath Control Service Group – continued						
Lock PAE			✓			Providing the Datapath has assumed the Pre-Authentication Environment Update role, this service disables write access to the PAE region on the connected drive and results in the Datapath assuming No Role, i.e. the operator is logged out of the Datapath but remains logged into the Service Handler.
FlagStone Drive Policy Management Service Group						
Lock Drive Policy			✓			Locks the FlagStone Drive Policy. Any pending modifications are discarded.
Unlock Drive Policy			✓			Unlocks the FlagStone Drive Policy for modification.
Modify Drive Policy			✓			This service verifies the received FlagStone Drive Policy modifications are in accordance with the current FlagStone Drive Policy. If the verification is successful, a temporary copy of the FlagStone Drive Policy is updated, and modifications are deemed to be pending.
Save Drive Policy & Logout			✓			Providing the FlagStone Drive Policy is unlocked and a modification is pending and the drive policy is valid, then this service writes the modified FlagStone Drive Policy to the NV Store and then automatically invokes the Log Out (OP) service. However, if the FlagStone Drive Policy is locked or has not been modified or it is invalid, an Error is generated (which automatically locks the FlagStone Drive Policy). Note: as soon as the logout has successfully completed, the modified FlagStone Drive Policy comes into effect.
Purge Service Group						
Purge OOB (ATA Links)	✓	✓	✓	✓	✓	When permitted by FlagStone Drive Policy, this service is invoked as a result of a change on the ATA Links/Purge interface. This service purges all copies of the DEK and the operational RNG key (OPRNG), erases the operator accounts and the auto authentication account, and logs out all operators. Both the Service Handler and the Datapath assume No Role, i.e. any logged in operators are automatically logged out.
Purge – Core	✓		✓	✓		When permitted by FlagStone Drive Policy, this service purges all copies of the DEK and the operational RNG key (OPRNG), erases the operator accounts and the auto authentication account, and logs out all operators. Both the Service Handler and the Datapath assume No Role, i.e. any logged in operators are automatically logged out.

Table 7 Service Handler Services

Service	Service Handler Role					Description
	N-R	C-I	CO	MGR	L-U	
Decommissioning Service Group						
Purge Unit – Core	✓		✓			When permitted by FlagStone Drive Policy, this service purges all of the FlagStone Core's CSPs and deletes all accounts. Thereafter, no-one can log into the FlagStone Core. Both the Service Handler and the Datapath assume No Role, i.e. any logged in operators are automatically logged out.

Notes:

1. *When the FlagStone Core is in the Shutdown state, only the Purge OOB (ATA Links) service is available.*

2. *For all operator accounts, should both the FlagStone Drive Policy and the Operator's Account Policy indicate that one of the authentication parameters is sourced from the Key Port, the service will read an authentication parameter from the token connected to the Key port. (The C-I account does not permit authentication parameters to be sourced from the Key Port).*

4.2.2 Datapath Services

The Datapath services are invoked through the use of ATA disk reads and ATA disk writes.

Table 8 details the Datapath services and the Datapath roles that can invoke them. For completeness, the table indicates which services can be invoked when the Datapath is not assuming a role, i.e. No Role (N-R).

Table 8 Datapath Services

Service	Datapath Role				Description
	N-R	SDA	C-M	PAE-U	
ATA Service Group					
Supported ATA Commands – Non FlagStone Core	✓	✓	✓	✓	This service processes the set of ATA commands that are supported by the FlagStone Core but are not associated with FlagStone Core services, e.g. the ATA Set Features command. These commands are processed in accordance with the ATA standards. The responses given are those that would be expected for a standard ATA drive.
Unsupported ATA Commands	✓	✓	✓	✓	This service handles the set of ATA commands that the FlagStone Core does NOT support. In accordance with the ATA Standards, these commands are aborted.
Set ATA Device Number	✓				This service sets the PATA (Plain Text) Bus's ATA Device Number. Any change to the ATA Device number is only recognized during POST.
Secure Drive Access/Crypto-Migrate Service Group					
Read & Decrypt Data		✓	✓		This service returns plaintext by reading the data from the connected drive's non-PAE region and decrypting the data using the DEK loaded when the Datapath role was assumed.
Encrypt & Write Data		✓	✓		This service encrypts the supplied data using the DEK loaded when the Datapath role was assumed. The resulting cipher text is then written to the connected drive's non-PAE region.
Pre-Authentication Environment Service Group					
Read Pre-Authentication Environment	✓			✓	This service returns plaintext by reading the PAE data from the connected drive's PAE region and decrypting the PAE data using the PAEK.
Write Pre-Authentication Environment				✓	This service encrypts the supplied PAE data using the PAEK. The resulting cipher text is then written to the connected drive's PAE region.
Monitor Service Group					
Log Out (Datapath) (Monitor)		✓	✓		When permitted by Drive Policy, this service forces the Datapath to assume No Role. (The Service Handler role is not changed.)
Purge OOB (Monitor)		✓			When permitted by FlagStone Drive Policy, this service purges all copies of the DEK and the operational RNG key (OPRNG), erases the operator accounts and the auto authentication account, and logs out all operators. Both the Service Handler and the Datapath assume No Role, i.e. any logged in operators are automatically logged out.

4.3 Authentication

The FlagStone Core module uses identity-based authentication to facilitate access to cryptographic services.

4.3.1 Mechanism

FlagStone Core V2.0.1.1, V2.0.1.2, V2.0.2.1, V2.0.2.2, V2.0.3.4, V2.0.4.5, V2.0.5.4 & V2.0.5.5 only provide single port authentication, whereas FlagStone Core V2.0.1.3, V2.0.2.3, V2.0.3.3 & V2.0.5.3 can be configured to operate using single or dual port authentication.

Both single and dual port authentication requires the operator to supply a 256 bit authentication value with the service request. Dual port authentication requires the operator to provide a second 256 bit authentication value via the Key Port.

Note: The authentication values described in this document are those 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 Eclypt User Guides (Refs. [8], [9] & [10]).

The authentication mechanism for all roles is as follows:

1. IF this account is configured for dual port authentication,
   THEN XOR the two 256 bit values together to produce a 256 bit Account Validation Key
   ELSE Use the supplied authentication value as the 256 bit Account Validation Key

2. Use the 256 bit Account Validation Key to unwrap the account's Wrapping Key using the AES Key Wrap Algorithm. If the AES Key unwrap's 64 bit check vector fails to validate, then the authentication has failed.

3. Use the account's 256 bit wrapping key (unwrapped in step 2) to unwrap the 256 bit Secondary Authentication Value. If the AES Key unwrap's 64 bit check vector successfully validates, then the authentication has been successful, otherwise the authentication has failed.

Figure 12 provides a pictorial representation of the authentication mechanism.

To successfully authenticate, the authentication mechanism must successfully perform two AES Key unwrap validations using two different wrapping keys.

Re-authentication is required following a power cycle or restart of the FlagStone Core and following operator logout.

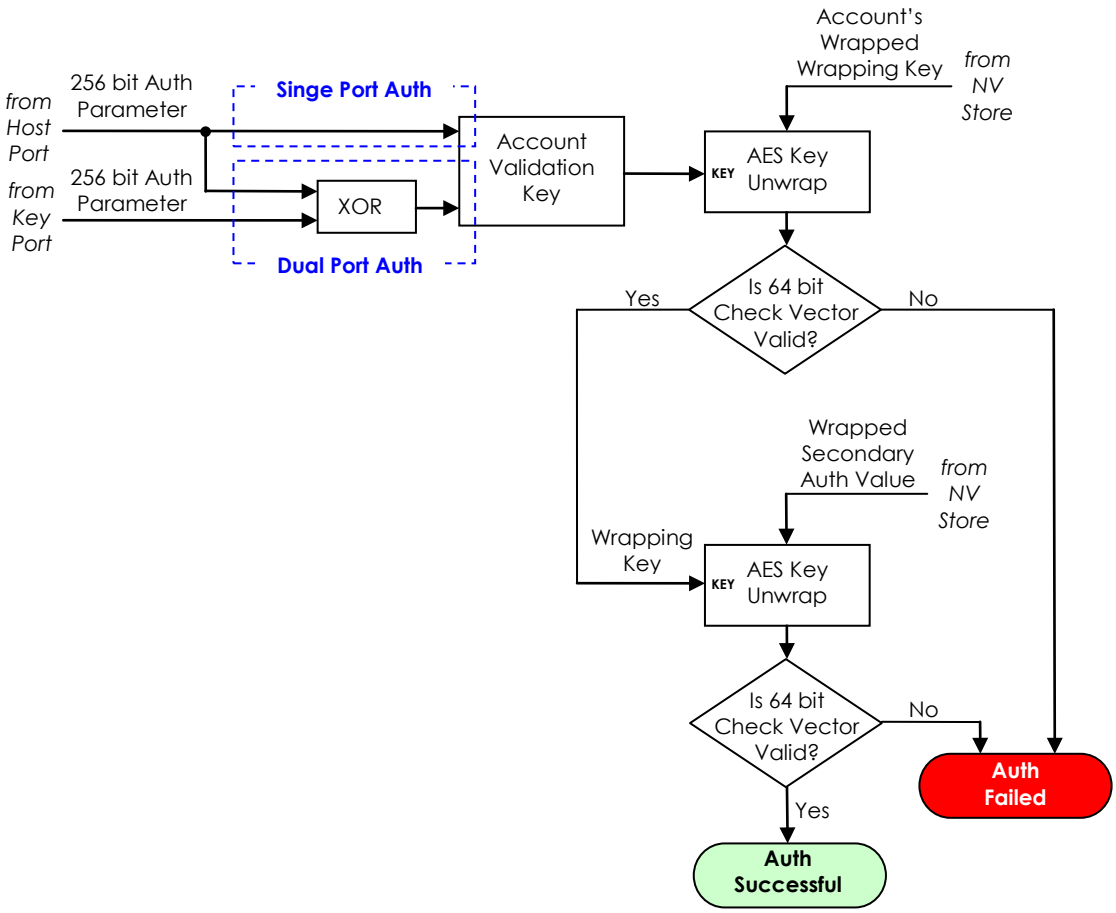

Figure 12 - Authentication Mechanism

4.3.2 Roles Authenticated

Whenever an operator successfully authenticates, they always assume a Service Handler role and they have authenticated the right to assume certain Datapath roles at a later time. The Datapath roles that may be assumed are summarized in Table 9.

Service Handler Role assumed	Datapath Roles authenticated for assumption at a later time		
	SDA	C-M	PAE-U
C-I			
CO	✓	✓	✓
MGR	✓		
L-U	✓		

Table 9 Service Handler and Datapath Roles Authenticated by Operator Login

4.3.3 Probability of False Accept

The authentication mechanism is described in Section 4.3.1 and Figure 12. In order to achieve a false accept the authentication value(s) must be guessed and the guess must either be correct or cause the authentication mechanism to deem them to be correct.

For single port authentication the probability of correctly guessing the 256 bit authentication value is 1 in 1.16×10^{77}.

For dual port authentication, the two 256 bit authentication values are XORed to form a single 256 bit Account Validation Key; as a consequence, whilst two 256 authentication values need to be guessed, the guess need only find a pair that produces the correct Account Validation Key. Since the Account Validation Key is 256 bits, the probability of guessing a suitable pair of authentication values is 1 in 1.16×10^{77}.

The AES Key Wrap Algorithm uses a 64 bit check vector to validate the AES Key unwrap; therefore the probability of a AES Key unwrap validating using an incorrect key is 1 in 1.84×10^{19}.

The authentication mechanism performs two AES Key unwrap validations using two different wrapping keys; consequently the probability of a single false accept is:

$$(1 \text{ in } 1.84 \times 10^{19}) \times (1 \text{ in } 1.84 \times 10^{19}) = 1 \text{ in } 3.40 \times 10^{38}$$

Since the probability of guessing the authentication value for single port authentication is the same as the probability of guessing a valid pair of authentication values for dual port authentication, the probability of a false accept is the same for both single port and dual port authentication.

Since the authentication mechanism's probability of a single false accept is many orders of magnitude more likely that the probability of guessing the authentication value(s), the probability of guessing the correct authentication value(s) can be ignored. As a consequence, the probability of a single false accept is 1 in 3.40×10^{38}.

Crypto Officers can limit the number of consecutive failed authentication attempts on each operator account. Furthermore, the FlagStone Core's response blocker can slow down the rate at which authentication requests are processed. Crypto Officers can configure the FlagStone Core to permit up to 640 failed authentication requests to be processed before the response blocker slows down the rate at which authentication requests are processed.

In the worst case, the number of authentication attempts that can be performed in one minute is 648. Consequently, the probability of a false accept within one minute is:

$$648 \text{ in } 3.40 \times 10^{38} = 1 \text{ in } 5.25 \times 10^{35}$$

Table 10 summarizes the probability of a false accept against specific criteria.

Criteria	Probability
Single False Accept	1 in 3.40×10^{38}
Within 1 minute	1 in 5.25×10^{35}

Table 10 Probability of False Accept

5 Finite State Model

The Finite State Model for the FlagStone Core is specified in Ref. [6].

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's Finite State Model has 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. The FIPS 140-2 validation testing was performed at 25°C; no assurance is provided for Level 3 hardness conformance at any other temperature.

There are no physical access interfaces to the FlagStone Core and no maintenance services.

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 recognized 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 unauthorized 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 unauthorized attempt at physical access may also be determined if the module begins functioning abnormally, Power On Self-Tests fail, any Continuous Self-Test fails or it is Unusable.

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

Furthermore, ViaSat recommends that customers inspect the Eclypt Drive if it is suspected that it may have been in the possession of an unauthorized individual, e.g. if the Eclypt 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

The Flagstone Core does not allow the export/output of CSPs.

Table 11 details the CSPs provided to support FIPS 140-2 approved mode of operation.

Table 11 Critical Security Parameters

CSP	Type	Generation/ Input	Storage	Erasure (note 5)	Use
Datapath CSPs					
OPDEK	Datapath Operational DEK – 256 bit AES Key	• Imported from host; **or** • Generated internally using FIPS 140-2 RNG.	Transient within FPGA	Sanitize, Purge & Purge Unit	Datapath's Operational DEK used for read/write access to the non-PAE region of the connected drive.
			Stored AES Key Wrapped (as wDEK) within NV Store	Purge & Purge Unit	
NewDEK	Datapath NewDEK – 256 bit AES Key	• Imported from host; **or** • Generated internally using FIPS 140-2 RNG.	Transient within FPGA	Sanitize, Purge & Purge Unit	Datapath's New DEK used for write access to the non-PAE region of the connected drive.
			Stored AES Key Wrapped (as wNewDEK) within NV Store	Migrate/ Promote/ Remove New DEK services, Purge & Purge Unit	
PAEK	Datapath PAE Key – 256 bit AES Key	• Generated internally using FIPS 140-2 RNG	Transient within FPGA	Sanitize, Purge & Purge Unit	Datapath's Encryption/ Decryption Key for the PAE region of the connected drive.
			Stored in plain text within NV Store	Purge & Purge Unit	
RNG CSPs					
CIRNG	RNG_Key – 256 bit AES KEY	• Injected during manufacture (see note 2)	Transient within FPGA	Sanitize, Purge, Purge Unit	Crypto-Initiator's RNG parameters.
			Stored in plain text within NV Store	Purge Unit	
	RNG_Seed – 128-bit	• Injected during manufacture (see note 2) • Updated following each RNG use.	Transient within FPGA	Sanitize, Purge, Purge Unit	
			Stored in plain text within NV Store	Purge Unit	
OPRNG	RNG_Key – 256 bit AES Key	• Imported from host.	Transient within FPGA	Sanitize, Purge & Purge Unit	Operational RNG parameters.
			Stored AES Key Wrapped (as wRNG_Key) within NV Store	Purge & Purge Unit	
	RNG_Seed – 128-bit	• Imported from host. • Updated following each RNG use.	Transient within FPGA	Sanitize, Purge & Purge Unit	
			Stored in plain text within NV Store	Purge & Purge Unit	

Table 11 Critical Security Parameters

CSP	Type	Generation/ Input	Storage	Erasure (note 5)	Use
Operator CSPs					
OHP[Acct]	Operator's Host Auth Parameter – 256 bits	• Input supplied by operator (on PATA Bus (Plain Text))	Transient within FPGA	Overwritten by next service request & Sanitize	Mandatory Operator Authentication Parameter for the specified operator account.
OKAP[Acct]	Operator's Key Port Auth Parameter – 256 bits	• Input supplied by operator (on Key Port Bus)	Transient within FPGA	Sanitize, Purge & Purge Unit	Optional Operator Authentication Parameter for the specified operator account.
OAVK[Acct]	Operator's Auth Validation Key – 256 bit Wrapping Key	• Internal copy of OHP[Acct]; **or** • The XOR of OHP[Acct] & OKAP[Acct]	Transient within FPGA	Sanitize, Purge & Purge Unit	Key for the first stage of operator authentication for the specified operator account.
OPWK	Operational Wrapping Key - 256 bit Wrapping Key	• Imported from host; **or** • Generated internally using FIPS 140-2 RNG.	Transient within FPGA	Sanitize, Purge & Purge Unit	Wrapping Key for OPDEK, NewDEK, OPRNG and NewOPWK, and the key for the second stage of operator authentication for operator accounts. The wrapped version of this CSP is unwrapped during operator authentication (for operator accounts that have not been migrated to the NewOPWK).
			Stored AES Key Wrapped (as wOPWK[Acct]) within NV Store (one for each operator acct that has not been migrated to NewOPWK)	Acct deleting services (note 6), Purge & Purge Unit	
OPNCISAV	Operational Non C-I Secondary Auth Value - 256 bit	• Generated internally using FIPS 140-2 RNG.	Transient within FPGA	Sanitize, Purge & Purge Unit	Never used – discarded output from the second stage of operator authentication for operator accounts.
			Stored AES Key Wrapped (as wOPNCISAV) within NV Store	Purge & Purge Unit	
NewOPWK	New Operational Wrapping Key - 256 bit Wrapping Key	• Imported from host; **or** • Generated internally using FIPS 140-2 RNG.	Transient within FPGA	Sanitize, Purge & Purge Unit	New Wrapping Key for OPDEK, NewDEK and OPRNG, and the key for the second stage of operator authentication for operator accounts that have already been migrated to the NewOPWK. The wrapped version of this CSP is unwrapped during operator authentication (for operator accounts that are being migrated to or already have been migrated to the NewOPWK).
			Stored AES Key Wrapped (as wNewOPWK) within NV Store	Login (Op) service, Import/ Generate NewOPWK services, Purge & Purge Unit	
			Stored AES Key Wrapped (as wOPWK[Acct]) within NV Store (one for each operator acct already using NewOPWK)	Acct deleting services (note 6), Purge & Purge Unit	
Crypto-Initiator CSPs					
OHP[C-I]	C-I's Host Auth Parameter – 256 bits	• Input supplied by operator (on PATA Bus (Plain Text))	Transient within FPGA	Overwritten by next service request & Sanitize	Mandatory Operator Authentication Parameter for the C-I account
OAVK[C-I]	C-I's Auth Validation Key – 256 bit Wrapping Key	• Internal copy of OHP[C-I]	Transient within FPGA	Sanitize, Purge & Purge Unit	The key for the first stage of operator authentication for the C-I account.

Table 11 Critical Security Parameters

CSP	Type	Generation/ Input	Storage	Erasure (note 5)	Use
Crypto-Initiator CSPs (continued)					
CIWK	C-I Wrapping Key - 256 bit Wrapping Key	• Injected wrapped during manufacture (see note 3) • Imported from host when C-I auth parameter is changed	Transient within FPGA Stored AES Key Wrapped (as wCIWK) within NV Store	Sanitize, Purge & Purge Unit Purge Unit	The key for the second stage of operator authentication for the C-I account. The wrapped version of this CSP is unwrapped during Crypto-Initiator authentication
CISAV	C-I Secondary Auth Value - 256 bit	• Injected wrapped during manufacture (see note 4) • Generated internally using FIPS 140-2 RNG when C-I auth parameter is changed	Transient within FPGA Stored AES Key Wrapped (as wCISAV) within NV Store	Sanitize, Purge & Purge Unit Purge Unit	Never used – discarded output from the second stage of operator authentication for the C-I account.

Notes:

1. *The prefix "w" on a parameter within the NV Store indicates that it is AES Key Wrapped, i.e. it is encrypted.*
2. *Prior to injection during manufacture, both the RNG_Key and the RNG_Seed for CIRNG are generated using a CAVP validated SHS based RNG from FIPS 186-2.*
3. *Prior to injection during manufacture, the CIWK is generated using a CAVP validated SHS based RNG from FIPS 186-2 and is then AES Key Wrapped, using the factory determined OAVK[C-I] as the key, to form wCIWK.*
4. *Prior to injection during manufacture, the CISAV is generated using a CAVP validated SHS based RNG from FIPS 186-2 and is then AES Key Wrapped, using the CIWK generated in note 3 above as the key, to form wCISAV.*
5. *When the number of active operator accounts falls to zero, a Purge is automatically invoked.*
6. *Remember, since it is the Save and Close Account service that completes the account deletion, it is this service that performs the erasure.*

8.2 Access Privileges to FIPS 140-2 Critical Security Parameters

Table 12 details the four types of access to the CSPs.

Access Type	Description
R – Read	This access type can read the CSP value, but cannot change the CSP value.
W- Write	This access type can change the CSP value, but cannot read the CSP value.
S – Sanitize	This access type positively erases this CSP's transient storage within the FPGA.
E – Erase	This access type positively erases this CSP's non-volatile storage within the NV Store.

Table 12 CSP Access Types

8.2.1 Role Access Privileges to CSPs

When operating in an approved FIPS 140-2 mode of operation, Table 13 details the access privileges to the FIPS140-2 CSPs for the Service Handler roles and the Datapath roles.

Critical Security Parameter		Service Handler Role					Datapath Role			
		N-R	C-I	CO	MGR	L-U	N-R	SDA	C-M	PAE-U
OPDEK		SE		RWSE	RSE	RSE		RSE	RS	
NewDEK		SE		RWSE	SE	SE		SE	RS	
PAEK		SE	RWSE	SE	SE	SE	R	SE		R
CIRNG	RNG_Key	SE	RS	RSE				S		
	RNG_Seed	SE	RWS	RWSE				S		
OPRNG	RNG_Key	SE	RWSE	RWSE	RSE	RSE		SE		
	RNG_Seed	SE	RWSE	RWSE	RWSE	RWSE		SE		
OHP[Acct]	*(Own account only)*	RWS		RWS	RWS	RWS		S		
	(Accounts that cannot assume CO role)	RWS		RWS	RWS					
	(Accounts that can assume CO role)	RWS		RWS						
	(Initial CO account during initialization)		RWS							
OKAP[Acct]	*(Own account only)*	RWS		RWS	RWS	RWS		S		
	(Accounts that cannot assume CO role)	RWS		RWS	RWS					
	(Accounts that can assume CO role)	RWS		RWS						
	(Initial CO account during initialization)		RWS							
OAVK[Acct]	*(Own account only)*	RWS		RWS	RWS	RWS		S		
	(Accounts that cannot assume CO role)	RWS		RWS	RWS					
	(Accounts that can assume CO role)	RWS		RWS						
	(Initial CO account during initialization)		RWS							
OPWK		RSE	RWSE	RWSE	RWSE	RWSE		SE		
OPNCISAV		RSE	RWSE	RWSE	SE	SE		SE		
NewOPWK		RSE		RWSE	RSE	RSE		SE		
OHP[C-I]		RWS	S	RWS				S		
OAVK[C-I]		RWS	S	RWS				S		
CIWK		RSE	S	RWSE				S		
CISAV		RSE	S	RWSE				S		

Table 13 Role Privileges Rights to CSPs

8.2.2 Service Access Privileges to CSPs

When operating in an approved FIPS 140-2 mode of operation, Table 14 lists the access privileges to the FIPS140-2 CSPs for the Service Handler services and the Datapath services.

Table 14 Service Access Privileges to CSPs

Service - *Conditions*	Datapath CSPs			RNG CSPs				Operator CSPs						Crypto-Initiator CSPs			
				CIRNG		OPRNG											
	OPDEK	NewDEK	PAEK	RNG_Key	RNG_Seed	RNG_Key	RNG_Seed	OHP[Acct]	OKAP[Acct]	OAVK[Acct]	OPWK	OPNCISAV	NewOPWK	OHP[C-I]	OAVK[C-I]	CIWK	CISAV
Service Handler Services (Table 7) – no error occurred																	
Primary (Shutdown)	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Clear Alarm – *Shutdown selected*	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Clear Alarm – *Restart selected*	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Clear Alarm – *Return to Ready selected*																	
Clear Error – *Shutdown selected*	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Clear Error – *Restart selected*	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Force Shutdown	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Restart	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Clear Response Blocker																	
Get Status – Core																	
Get Status – Drive																	
Get EECA																	
Get Acct Info (C-I)																	
Log In (C-I)														RW	RW	R	R
Log Out (C-I)				S	S									S	S	S	S
Initialize Operational (Generate) & Logout *- Initial Crypto Officer Account Only*			RW	S	S	RWS	RWS	RWS	RWS	RWS	RWS	RWS		S	S	S	S
Initialize Operational (Import) & Logout *- Initial Crypto Officer Account Only*			RW	S	S	RWS	RWS	RWS	RWS	RWS	RWS	RWS		S	S	S	S
Get Acct Info (Operator)																	
Set Default Acct Info																	

Table 14 Service Access Privileges to CSPs

Service - *Conditions*	Datapath CSPs			RNG CSPs				Operator CSPs						Crypto-Initiator CSPs			
				CIRNG		OPRNG											
	OPDEK	NewDEK	PAEK	RNG_Key	RNG_Seed	RNG_Key	RNG_Seed	OHP[Acct]	OKAP[Acct]	OAVK[Acct]	OPWK	OPNCISAV	NewOPWK	OHP[C-I]	OAVK[C-I]	CIWK	CISAV
Service Handler Services (Table 7) – no error occurred– (continued)																	
Get Default Acct Info																	
Log In (OP) - *Active operator accts remain present* **See note 1**								RW	RW	RW	RW	R	RE				
Log In (OP) *- Number of active operator accts falls to zero*	SE	SE	SE			E	E	RWS	RWS	RWS	RSE	RSE	RSE				
Log Out (OP) - *Service Handler Role is CO*				S	S	S	S	S	S	S	S	S	S	S	S	S	S
Log Out (OP) - *Service Handler Role is MGR or L-U*						S	S	S	S	S	S	S	S				
Open Acct																	
Discard Acct																	
Save and Close Acct *- Active operator accts remain present*																	
Save and Close Acct - *Service Handler Role is CO & Number of active operator accts falls to zero*	SE	SE	SE	S	S	SE	SE	S	S	S	SE	SE	SE	S	S	S	S
Save and Close Acct - *Service Handler Role is MGR & Number of active operator accts falls to zero*	SE	SE	SE			SE	SE	S	S	S	SE	SE	SE				
Create Acct								RW	RW	RW	R		R				
Delete Acct																	
Modify Acct Policy																	
Modify Acct Status																	
Change Auth Parameters *– Acct currently open only*								RW	RW	RW	R		R				
Change Own Auth Parameters *– Acct logged into Service Handler*								RW	RW	RW	R		R				
Change C-I Auth Parameters				R	RW									RW	RW	RW	RW
Import New OPWK – *OPWK migration completed*	R					R	RW			R	RW	RW	RWE				
Import New OPWK – *allow further OPWK migration*	R					R	RW			R	R	RW	RW				
Generate New OPWK – *OPWK migration completed*	R					R	RW			R	RW	RW	RWE				
Generate New OPWK– *allow further OPWK migration*	R					R	RW			R	R	RW	RW				
Import New OPRNG						RW	W				R		R				
Generate Random Data *- Service Handler Role is C-I*				R	RW												

Table 14 Service Access Privileges to CSPs

Service - *Conditions*	Datapath CSPs			RNG CSPs				Operator CSPs						Crypto-Initiator CSPs			
				CIRNG		OPRNG											
	OPDEK	NewDEK	PAEK	RNG_Key	RNG_Seed	RNG_Key	RNG_Seed	OHP[Acct]	OKAP[Acct]	OAVK[Acct]	OPWK	OPNCISAV	NewOPWK	OHP[C-I]	OAVK[C-I]	CIWK	CISAV
Service Handler Services (Table 7) – no error occurred– (continued)																	
Generate Random Data *- Service Handler Role is CO, MGR or L-U*						R	RW				R		R				
Get Random Data																	
Import New DEK		RW									R		R				
Generate New DEK		RW				R	RW				R		R				
Migrate New DEK	RW	RE									R		R				
Promote New DEK	W	RE															
Remove New DEK		E															
Boot – *Service Handler remains logged in*	R										R		R				
Boot – *Service Handler logs out CO role*	R			S	S	S	S	S	S	S	RS	S	RS	S	S	S	S
Boot – *Service Handler logs out MGR or L-U role*	R					S	S	S	S	S	RS	S	RS				
Log Out (Datapath)	S	S															
Unlock PAE																	
Lock PAE																	
Lock Drive Policy																	
Unlock Drive Policy																	
Modify Drive Policy																	
Save Drive Policy and Logout				S	S	S	S	S	S	S	S	S	S	S	S	S	S
Purge OOB (ATA Links)	SE	SE	SE	S	S	SE	SE	S	S	S	SE	SE	SE	S	S	S	S
Purge – Core	SE	SE	SE	S	S	SE	SE	S	S	S	SE	SE	SE	S	S	S	S
Purge Unit – Core	SE	SE	SE	SE	SE	SE	SE	S	S	S	SE	SE	SE	S	S	SE	SE
Service Handler Services (Table 7) – error occurred																	
Any Service – *Service Handler Role is C-I*				S	S	S	S	S	S	S	S	S		S	S	S	S
Any Service – *Service Handler Role is CO* *& Active operator accts remain present*				S	S	S	S	S	S	S	S	S	S	S	S	S	S
Any Service – *Service Handler Role is MGR or L-U* *& Active operator accts remain present*						S	S	S	S	S	S	S	S				
Any Service – *Service Handler Role is N-R* *& Active operator accts remain present*								S	S	S	S	S	S				
Any Service *– Number of active operator accts falls to zero*	SE	SE	SE	S	S	SE	SE	S	S	S	SE	SE	SE	S	S	S	S

Table 14 Service Access Privileges to CSPs

Service - *Conditions*	Datapath CSPs			RNG CSPs				Operator CSPs						Crypto-Initiator CSPs			
				CIRNG		OPRNG											
	OPDEK	NewDEK	PAEK	RNG_Key	RNG_Seed	RNG_Key	RNG_Seed	OHP[Acct]	OKAP[Acct]	OAVK[Acct]	OPWK	OPNCISAV	NewOPWK	OHP[C-I]	OAVK[C-I]	CIWK	CISAV
Datapath Services (Table 8)																	
Supported ATA Commands – Non FlagStone Core																	
Unsupported ATA Commands																	
Set ATA Device Number																	
Read & Decrypt Data	R																
Encrypt & Write Data *– Datapath Role is SDA and no errors*	R																
Encrypt & Write Data *– Datapath Role is C-M and no errors*		R															
Encrypt & Write Data *– Datapath Role is SDA and error occurred*	RS			S	S	S	S	S	S	S	S	S	S	S	S	S	S
Encrypt & Write Data *– Datapath Role is C-M and error occurred*	S	RS		S	S	S	S	S	S	S	S	S	S	S	S	S	S
Read Pre-Authentication Environment			R														
Write Pre-Authentication Environment			R														
Log Out (Datapath) (Monitor)	S	S															
Purge OOB (Monitor)	SE	SE	SE	S	S	SE	SE	S	S	S	SE	SE	SE	S	S	S	S

Notes:

1. *The Write access to the OPWK and the Erase access to NewOPWK can only occur after the operator has been successfully authenticated.*

8.3 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 256 bit Algorithm, Ref. [3]. The RNG can operate from two different sets of Seed Key and Seed, depending on the Service Handler role adopted.

RNG Key and RNG Seed used to support the Service Handler's Crypto-Initiator role are held secret and are never released from the FlagStone Core.

RNG Key and RNG Seed used to support the Service Handler's Crypto Officer, Manager and User roles are imported in plain text; however they cannot be exported from the FlagStone Core. ViaSat recommends that the RNG Keys and Seeds that are imported into the FlagStone Core are generated or established using a FIPS 140-2 approved or a FIPS 140-2 allowed method. At the time of import of an RNG Key and an RNG Seed, the host shall not be connected to a network.

8.4 Key Derivation

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

8.5 Key Generation

The FlagStone Core uses a FIPS 140-2 approved internal key generation technique to generate keys using the random number generator detailed in Section 8.3.

8.6 Key Entry and Output

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

During manufacture, both plain text and AES key wrapped keys are injected into the FlagStone Core.

Once manufacturing has been completed, the FlagStone Core only permits the entry of plain text keys. It does not permit the entry of encrypted keys or key components. ViaSat recommends that all such keys that are imported into the FlagStone Core are generated or established using a FIPS 140-2 approved or a FIPS 140-2 allowed method. At the time of import of a key, the host shall not be connected to a network.

8.7 Initialization Vector Generation

The Initialization Vector is injected into the FlagStone Core during manufacture; this Initialization Vector is generated using a CAVP validated SHS based RNG from FIPS 186-2.

A replacement Initialization Vector can be imported in plain text. ViaSat recommends that all replacement Initialization Vectors that are imported into the FlagStone Core are generated or established using a FIPS 140-2 approved or a FIPS 140-2 allowed method.

8.8 Key Storage

The FlagStone Core stores the following keys and RNG seeds in plain text:

- CIRNG - RNG_Key and RNG_Seed
- OPRNG - RNG_Seed
- PAEK

For all other keys, the FlagStone Core uses a FIPS 140-2 approved key wrapping technique, AES Key Wrap (Ref. [4]) to encrypt the keys prior to storage.

In order to state that the keys are FIPS 140-2 encrypted, FIPS 140-2 requires that the key used for the AES Key Wrap Algorithm is generated or established using a FIPS 140-2 approved or a FIPS 140-2 allowed method.

ViaSat recommends that all keys that are imported into the FlagStone Core are generated or established using a FIPS 140-2 approved or a FIPS 140-2 allowed method. At the time of import of a key, the host shall not be connected to a network.

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 to ensure all security critical functions are functioning correctly. Two types are implemented:

- Power On Self-Tests (Section 10.1), which are automatically performed when the FlagStone Core is powered up and can be performed again at the request of an Operator.
- Conditional Self-Tests (Section 10.2), which are performed whenever the relevant security function is invoked.

The status of Self-Tests can be retrieved, via the status output interface, using the Get Status – Core service. This service returns the overall Power On Self Test status, and the results of individual tests.

The overall Power On Self Test status can indicate one of two values as detailed in Table 15.

Value	Description
Passed	The Power On Self Tests have been completed and none of them have failed
Failed	The Power On Self Tests have been completed and one or more of the Power On Self Tests have failed

Table 15 Power On Self Test Status

In addition to the Self-Test results, the Get Status service will return the general boolean flags, "Error" and "Alarm". The "Error" flag is set whenever an error has occurred, including any self test failures. The "Alarm" flag is set whenever an alarm has occurred; an alarm is any event that results in a purge being performed.

If an external application supplied with the Eclypt/Eclypt Freedom Drive 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. [8], [9] & [10], for further information).

10.1 Power On Self-Tests

Table 16 details the tests performed by the FlagStone Core during the power-on sequence. The Power On Self-Tests can be initiated on demand through the use of the Restart, Clear Error and Clear Alarm services.

Power On Self-Test	Description
ATA Bus On Control Test	Ensures that the ATA Bus On signal can be controlled correctly.
NV Store Integrity Test	Ensures that communication can occur between the FlagStone Core and the NV-Store device by verifying that all data regions pass their relevant checksum tests.
EECA integrity Test	Ensures that communication can occur between the FlagStone Core and the EECA device by performing a CRC-32 based KAT.
Connected Drive Integrity Test	Ensures that communication can occur between the FlagStone Core and the Connected Drive. In the event the connected drive is not present, this test will pass indicating that the connected drive is not present.
Service Handler Crypto Function Test	Performs known answer tests (KATs) to verify the following Service Handler Cryptographic Functions are operating correctly. • AES Wrap • AES Unwrap • RNG
Datapath Crypto Function Test	Performs known answer tests (KATs) to verify the following Datapath Cryptographic Functions are operating correctly. • Encrypt Path of the AES Algorithm • Decrypt Path of the AES Algorithm
Datapath Key Store Integrity Test	Ensures that the key storage can be zeroized and controlled correctly.

Table 16 Power On Self Tests

10.2 Conditional Self-Tests

Table 17 details the conditional tests performed by the FlagStone Core; the associated test 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.

Table 17 Conditional Self Tests

11 Design Assurance

11.1 Configuration Management

All elements of the FlagStone Core, including hardware, FPGA code and documentation, are revision controlled according to ViaSat UK ISO 9001:2000 accredited quality management systems.

All documents are assigned unique document numbers and subsequently version controlled using issue numbers of the form: 4560-TN123 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: LF123456-P78 Issue A. All FPGA images are assigned individual part numbers and issue characters of the form: 876543-P21 Issue B.

FlagStone Cores are assigned a Version Number of the form: Vu.w.y.x, where u is the major version number, w is the minor version number, y is the FPGA variant number and x is the hardware variant number.

Details of the ViaSat UK Quality Process for product development are documented in Ref. [11].

11.2 Delivery and Operation

The FlagStone Core is manufactured and integrated into Eclypt 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 Eclypt Drive, it will be shipped via courier. The delivery process is detailed in the ViaSat UK ISO 9001:2008 accredited Quality Management System and documented in Ref. [12].

11.3 Development

All elements of the FlagStone Core are developed in accordance with the ViaSat UK ISO 9001:2000 accredited Quality Management System and documented in Ref. [11].

All documentation required for the FIPS validation of the FlagStone Core has been submitted, including PCB layouts, schematics, source code and specifications. Ref. [6] 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 User Guides (Ref. [8] for Eclypt, Ref. [9] for Eclypt Freedom and Ref. [10] for Eclypt Nano) and this document provide all the guidance for the management and usage of the FlagStone Core. This Security Policy and the relevant user guides will be supplied on the 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.