

NOT PROTECTIVELY MARKED

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1



MINISTRY OF DEFENCE

Defence Security Division

InfoSy 6
6th Floor Zone B (Mailpoint Zone D), Main Building
Horseguards Avenue
LONDON, SW1A 2HB

Telephone 020 7218 0124
DFTS 9621 80124
Facsimile 020 7218 6825
E-mail DBR-DefSy-InfoSy6@mod.uk



DEFENCE INFOSEC PRODUCT COOPERATION GROUP
(DIPCOG)

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES

for
Stonewood Group
Ecllypt HMG v3.1

Issue 1

26 May 2009

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

INDEX

INDEX 2

1. INTRODUCTION 3

2. HEALTH WARNING 4

3. DATA SHEETS 5

4. PRODUCT DESCRIPTION 6

5. CRYPTOGRAPHIC HANDLING REQUIREMENTS 8

6. KEY MANAGEMENT 11

7. THE SALES APPLICATION PROCESS 12

8. THE KEY MATERIAL APPLICATION PROCESS 13

9. SPECIAL CRYPTOGRAPHIC REQUIREMENTS 13

10. LOSS OR COMPROMISE 13

11. DOS AND DON'TS 14

Appendix 1 - Glossary of Terms and Abbreviations Used within this Document 16

Appendix 2 - Departmental COMSEC Sponsors 18

Appendix 3 - Company Contact Details 19

Appendix 4 – Eclipt HMG System Components 20

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

FOREWORD

(1) These Product Description and Application (PDA) Notes have been submitted by Stonewood Group to support the secure use of Eclipt HMG v3.1. They have been approved by the DIPCOG for use in the Ministry of Defence. These notes may also be of interest and relevance to other HMG Departments.

(2) Users may also refer to the following documents for specific advice on the deployment of Security Products.

Table 1 - Useful Reference Documents		
1	BMD/0001/0002 Leaflets	Published by MOD DCA. Advice contained is intended primarily for the guidance of MOD Users.
2	Security Procedures	Published by CESG. Security Procedures are specific to HMG use of the product.
3	HMG Information Assurance Standard No 4	Published as a Tier 4 document in the Cabinet Office Security Policy Framework (SPF).
4	Eclipt HMG Crypto Officer Guide document no: CI 0013 Eclipt HMG Getting Started document no: CI 0014 Eclipt HMG User Guide document no: CI 0015	Instructions produced by Stonewood Group and included on the Installation and User Guide CD.

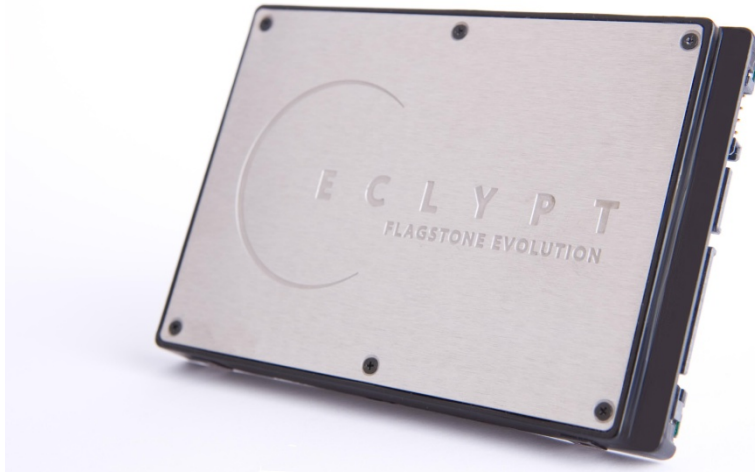
1. INTRODUCTION

1.1 This document summarises security information relevant to Eclipt Baseline, Eclipt Baseline Plus and Eclipt Enhanced, hereafter referred to as Eclipt HMG, and provides a reference for:

- DSOs
- ITSOs
- BSOs
- COMSEC Custodians
- Project and Purchasing Managers
- Users

1.2 Eclipt HMG in the context of this document refers at all times to the UK Government approved version of the product submitted by Stonewood Group (See Appendix 3 for contact details).

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1



View of 2 1/2" x 9.5mm high ECLYPT HMG Drive

1.3 Eclipt HMG is available in three versions to protect data at rest for different PM:

1.3.1 Eclipt Baseline protects RESTRICTED data, reducing its PM when powered down to NPM.

1.3.2 Eclipt Baseline Plus protects CONFIDENTIAL data, reducing its PM from CONFIDENTIAL to RESTRICTED. It may also be used to protect RESTRICTED DATA, reducing its PM to NPM.

1.3.3 Eclipt Enhanced reduces the PM of data by two levels. Therefore CONFIDENTIAL data becomes NPM, SECRET data becomes RESTRICTED and TOP SECRET data becomes CONFIDENTIAL.

2. HEALTH WARNING

2.1 This document aims to cover requirements for most common modes of operation, but cannot address special circumstances or requirements. Within the spirit of risk management, Departments may use reasonable discretion to interpret the guidance for local circumstances, but in case of doubt should refer the matter to their Departmental COMSEC Sponsor, see Appendix 2.

2.2 It is the responsibility of the purchasing organisation to ensure that the product is appropriate to meet the requirement. Where appropriate, deployment within the declared user community is to be in accordance with the connection policies laid down by the Security Accreditor, and handling policies and security procedures laid down by the Departmental COMSEC Sponsor.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

3. DATA SHEETS

3.1 Summary of Functionality:

Table 2 - Summary of Functionality		
Maximum PM of Data	MOD and OGD	Eclipt Enhanced: TOP SECRET Eclipt Baseline Plus: CONFIDENTIAL Eclipt Baseline: RESTRICTED
Computer Handling Requirements	In Use	PM of Data
	Idle-powered off	See Table 3
Internet Connection Permitted	Only when used in conjunction with appropriate security measures see Para 5.3.4.	
Cryptographic Algorithms	AES-256 in CBC Mode AES-256 Key Wrap LOGFIRE Password Hashing	
Key Material Components	Protective Marking and Handling Descriptor	
Key Material CD-ROM	TOP SECRET/SECRET/CONFIDENTIAL CRYPTO RESTRICTED ACCSEC	
User Token Data CD_ROM (Eclipt Enhanced only)	NPM ACCSEC	
User Tokens (i-Button or KeyStone), when not programmed	NPM	
User Tokens once programmed	NPM ACCSEC	
Keymat Token when not programmed	NPM	
Keymat Token once programmed	TOP SECRET/SECRET/CONFIDENTIAL CRYPTO RESTRICTED ACCSEC (as appropriate to last encryption Key programmed)	
Crypto period of Keys	Lifetime	
Evaluation Status	CAPS	Eclipt Baseline and Baseline Plus: 0934513AEF Eclipt Enhanced: 0934514AEF

3.2 Protective Markings

Table 3 - Protective Markings	
The PM of the Eclipt HMG depends on the level of data that is stored on the device once it has been properly integrated into the PC (desktop/ laptop/ tablet) (including Key load).	
Eclipt Enhanced	
Highest PM of Data when Authenticated	PM of Eclipt Enhanced when NOT Authenticated
TOP SECRET	CONFIDENTIAL
SECRET	RESTRICTED
CONFIDENTIAL	NPM
RESTRICTED	NPM

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Eclypt Baseline Plus	
Highest PM of Data when Authenticated	PM of Ecllypt Baseline Plus when NOT Authenticated
CONFIDENTIAL	RESTRICTED
RESTRICTED	NPM
Eclypt Baseline	
Highest PM of Data when Authenticated	PM of Ecllypt Baseline when NOT Authenticated
RESTRICTED	NPM

3.3 Technical Specifications

Table 4 - Technical Specifications		
Operating Systems Supported		Operating System independent
Minimum System Requirements	RAM	N/A
	Processor	Any Intel x386 type equivalent and later versions.
	Hard Drive Space	N/A
	Floppy Drive / CD-ROM	Not required See Para 4.2.2
Interfaces Supported		Serial ATA (SATA) Parallel ATA (PATA)
Communications Protocols Supported		PATA variants 2/3/4/5/6/7 SATA variants 7
Dimensions		2.5" HDD – 69.85 x 100.0 x 9.5mm 2.5" HDD – 69.85 x 100.0 x 11.5mm
Electrical Safety		CE, UL
EMC		CE, FCC Class B
Environmental	Temperature	5°C to 55°C (Operating)
	Humidity	8% to 90% non-condensing
	Air Pressure	Altitude: -300 to 3000m (Operating) -400 to 12500m (Non-Operating)
Power Requirements		Taken from host via interface connector

4. PRODUCT DESCRIPTION

4.1 Overview.

4.1.1 Ecllypt products are hardware-based full disk encryptors securing data at rest up to and including TOP SECRET stored on magnetic or solid state (flash) media. The stored data can be handled at a lower PM when powered down. Ecllypt HMG replaces the existing hard disk drive in a Personal Computer providing encryption and authentication

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

to restrict access to the contents of the hard disk. Eclipt has evolved from the FlagStone product range.

4.1.2 This document applies to 3 Eclipt HMG products:

- a. Eclipt Enhanced, version 3.1
- b. Eclipt Baseline Plus, version 3.1
- c. Eclipt Baseline, version 3.1

Each of these Eclipt products is available with either magnetic or solid state (flash) storage.

4.1.3 Eclipt HMG is a sector level hardware-based disk encryptor with pre-boot authentication. All authentication verification and key decryption occurs within the hardware boundary and cannot be read or modified on the hard disk drive.

4.1.4 Eclipt HMG:

4.1.4.1 Uses AES-256 Hardware Data Encryption in CBC Mode

4.1.4.2 Uses the LOGFIRE algorithm for authentication parameter hashing and KEK formation.

4.1.4.3 Encrypts all the data on the storage medium independent of any operating system, application, service pack or software patch.

4.1.4.4 Allows up to 128 operator accounts with 3 account types:

- a. Crypto Officer including the initial account - the Initial Crypto Officer account.
- b. User Manager.
- c. User.

4.1.4.5 Provides a pre-boot management console, the Command Line Interface (CLI) Management Application, which is independent of the operating system.

4.1.4.6 Is sealed in a tamper-evident enclosure, where KEKs and account status values are stored.

4.1.4.7 Provides encryption in hibernation mode.

4.1.5 Eclipt System Components. See Table 6 at Appendix 4.

4.2 Installation Host.

4.2.1 Eclipt products will run on any x386 or greater host and runs independent of operating system.

4.2.2 COMSEC Custodians require a standalone Windows PC for Key Material programming, with a CD-ROM drive for Key Material transfer.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

4.3 Encryption/Decryption Process.

4.3.1 The process is one of hardware based on-the-fly encryption transparent to the end user. Every sector stored on the integral Hard Disk Drive is encrypted using AES-256 in CBC mode; there is no plain text data on the drive. Each and every HDD sector is encrypted as it is written and decrypted as it is read.

4.3.2 There is no mechanism for either the host or the device to write plaintext data to the integral drive.

4.4 Authentication Process.

4.4.1 Authentication depends on the security grade of the Eclipt. Eclipt Enhanced utilises two factor authentication consisting of a username, password and a token. The password is nine characters long and in CLEARVIEW format. Eclipt Baseline and Eclipt Baseline Plus utilise single factor authentication mechanisms, requiring entry of a username and password. Initially Eclipt Baseline generates a 14 character password, whilst Eclipt Baseline Plus generates a 15 character password.

4.4.2 Eclipt HMG provides the option to alter the password length between 9 and 16 characters.

4.5 Tamper Events and Alarms.

4.5.1 There are no electronic tamper events or alarms on Eclipt HMG. However the product is supplied with tamper evident labels which must be applied to all access covers to the hard-drive bay and host electronics in which the Eclipt is fitted before Key Material is loaded. The tamper labels must be inspected on each use to ensure that no damage is evident (see also Paragraph 10.2.1). Replacement Tamper Evident Labels may be obtained from Stonewood Group.

4.5.2 In accordance with ACCSEC procedures, the tamper labels must be formally inspected by the System Administrator / COMSEC Custodian every 12 months.

4.6 Auditing. There are no audit functions associated with this product.

5. CRYPTOGRAPHIC HANDLING REQUIREMENTS

5.1 Storage. The Key Material CD-ROM for Eclipt HMG is accountable and must be stored, handled and transported in accordance with Departmental COMSEC procedures. This disk may not be moved without the authority of the COMSEC Custodian. If transportation is authorised, then it must be in accordance with approved COMSEC procedures issued by the COMSEC Custodian.

5.2 Warning on Carriage of Cryptographic Products Overseas. The movement of any cryptographic device or system to certain countries is forbidden. The movement of many cryptographic devices or systems to other countries, even for personal use, is carefully prescribed. If in any doubt users should take advice from Departmental Standing Security Instructions, or from Security or COMSEC Staffs, before taking cryptographic products outside the UK.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

5.3 Deployment.

5.3.1 Deployment of Eclipt HMG will be dictated by the requirements of the owning business unit. Standard security requirements for the transportation and use of devices containing PM data will apply. Further advice may be obtained from the System Accreditor, Departmental COMSEC Sponsor, or Agent of Supply Sales Office. Before computers/systems with Eclipt HMG installed are deployed, a recognizable security policy and/or security procedures must be in place.

5.3.2 System Configuration

5.3.2.1 The COMSEC Custodian must ensure that the unit and supporting software has been received from its expected source and can be tracked.

5.3.2.2 Prior to fitting the tamper-evident labels to the host PC or laptop, the COMSEC Custodian must inspect the unit to ensure that it has not been modified or tampered with.

5.3.2.3 The Eclipt HMG unit is delivered in "Unprotected mode". This means that it can be used as a normal disk drive prior to loading Key Material. However, it must not be used for PM data until the Key Material is loaded.

5.3.2.4 If not already fitted, the COMSEC Custodian should fit the Eclipt HMG into the host PC or laptop, following the manufacturer's guidance. The COMSEC Custodian must then apply the tamper-evident labels to all points of access to the Eclipt HMG and electronics in the host PC or laptop, so that it shall be impossible to remove or modify them without removing or damaging the tamper-evident labels.

5.3.2.5 The COMSEC Custodian must adjust the host PC or laptop BIOS settings to ensure that access to the BIOS is password controlled. This is important to prevent use of the "temporary boot device" option and to ensure that unauthorized personnel shall not be able to change the configuration that the host will always boot from the Eclipt HMG prior to any other device. A 9-character Clearview password is recommended. Note that there is no requirement to use a BIOS password for booting the system.

5.3.2.6 Configure the BIOS to disable Standby and Suspend modes. Hibernation is fully supported by Eclipt HMG.

5.3.2.7 Refer to the Eclipt HMG Crypto Officer Guide to complete software installation and configuration of the Eclipt HMG.

5.3.2.8 Following the user guidance for the installed Operating System, disable Operating System Standby and Suspend modes. If the operating system supports it, Hibernation mode can be used securely with Eclipt HMG.

5.3.3 Key Load.

5.3.3.1 Key Material is copied onto a Keymat Token using the Token Programmer in the Key Management Kit available from Stonewood Group. The

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Token Programmer must be loaded onto a standalone computer that is accredited to the highest PM of Key to be programmed.

5.3.3.2 Eclipt Enhanced units additionally require the programming of User i-Button or KeyStone Tokens. User Token data is ordered from the UKKPA and is transferred onto User Tokens using the Eclipt Token Programmer.

5.3.3.3 Once programmed the Keymat Token is connected to the Eclipt HMG device for the Key load process. Refer to the Eclipt HMG Crypto Officer Guide for more information on this process.

5.3.3.4 A programmed the Keymat Token must be handled according to the PM of the Key Material. The Eclipt Token Programmer may be used to securely erase Keymat Tokens and therefore decrease the PM of the token after use.

5.3.3.5 Once Key Material is loaded, host machines may be deployed as required, within the parameters set out above, but handled as detailed in Table 3.

5.3.4 Connections to the Internet.

5.3.4.1 Host PCs and laptops utilising Eclipt HMG must only be connected to systems that are of the same PM as the data being stored on the unit.

5.3.4.2 All computers must be protected against malware in accordance with Departmental instructions.

5.3.4.3 Computers holding TOP SECRET/ SECRET data are not to be connected directly to the Internet. Connection over insecure networks, such as the Internet, through a CESG High Grade encryption device to other systems at the same PM is permitted.

5.3.4.4 Computers holding CONFIDENTIAL or RESTRICTED data are not to be connected directly to the Internet. If they are using a MOD approved COMSEC encryption product, such as Baron McCann X-Kryptor or AEP Networks ED Net Remote, they may be connected over insecure networks, such as the Internet, to other systems at the same PM.

5.3.4.5 Computers holding PROTECT or NPM data may be connected to the Internet, but care should be taken over what PROTECT information is transmitted over the Internet.

5.4 Disposal.

5.4.1 Purging of Key Material. The Eclipt HMG shall be purged of Key Material before re-use, disposal or repair. The Purge Core facility should be used; it can be invoked from either the pre-boot or Windows management applications. The Purge Core mechanism is automatically invoked when all user accounts have been locked or deleted.

5.4.2 Disposal of Equipment at End of Life. The Purge Disposal facility, which electrically destroys the electronics, must be used before disposal at end of life. Following the Purge Disposal purge, the unit must be degaussed or physically destroyed, using methods approved by Information Assurance Standard No 5.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

5.4.3 Disposal of Key Material. Media, which are COMSEC accountable, are to be destroyed in accordance with BMD/0001/0001, Defence Cryptosecurity Operating Instructions.

6. KEY MANAGEMENT

6.1 Delivery, Storage and Accounting.

6.1.1 Key Material is ordered in accord with the PM of the data to be protected. Key Material is delivered through COMSEC channels to an approved CRYPTO or ACCSEC Custodian (depending on the PM) and remains a fully accountable cryptographic item throughout its life. When issued by the CRYPTO or ACCSEC Custodian to user level, it must be handled by authorized persons only and stored in accordance with the instructions advised by the CRYPTO or ACCSEC Custodian. Loss or compromise is a reportable event.

6.2 Key Structure.

6.2.1 Key Material and Token Programming.

6.2.1.1 Key Material is supplied by CESG and must be transferred to a Keymat Token for use with Eclipt HMG. The Eclipt Token Programmer software must be used for this purpose.

6.2.1.2 The Key Material CD-ROM contains the Key data for each of the Eclipt HMG units ordered. Each Key Material file contains the data for a single Eclipt HMG.

6.2.1.3 For Eclipt Enhanced Only. The User Token data CD-ROM contains the data¹ to be transferred on to the User Token issued to each user of Eclipt Enhanced. Each user file contains 16 records which can be used to periodically change a user's User Token, if desired.

6.2.1.4 Transferring the Key Material into each Eclipt HMG unit is by a Keymat Token which is physically and electrically different from the User Token. Keymat Tokens are reusable and are only filled with the Key Material for each Eclipt HMG for as long as it takes to transfer the Key Material from the CD-ROM on to the Keymat Token and then into the Eclipt HMG drive. After that the Keymat Token may be either securely erased (and stored awaiting re-use) or filled with a new Key for the next Eclipt HMG drive to be loaded with Key Material. Key Material is loaded into the Eclipt drive, when prompted during initialisation, using the i-Button User Token Interface Cable, which is supplied in the Key Management Kit.

6.2.1.5 Programming of the User Tokens uses the same software program as for the loading of Key Material.

¹ This data is one part of the authentication data set; it is not a Key.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

6.2.1.6 The COMSEC Custodian must record the issue of Eclipt HMG, Key Material (Key File Reference) and User Token(s) to each protected PC.

6.2.2 Eclipt Key Management Kit

6.2.2.1 A standalone PC is required for hosting the Eclipt Key Management Kit application software for programming Eclipt HMG tokens. This standalone PC must be accredited to the same PM as the tokens it will be used to programme.

6.2.2.2 Prior to the use of the Eclipt Key Management Kit it must be confirmed that the Eclipt Key Management Kit is genuine and has not been tampered with. Local procedures must be used to determine the provenance of Eclipt Key Management Kit.

Key Material Purpose	Short Title	Supplied Medium	Remarks
Eclipt Baseline v3.1	***/7586/XXXX	CD-ROM	RESTRICTED ACCSEC
Eclipt Baseline Plus v3.1	***/7586/XXXX	CD-ROM	CONFIDENTIAL CRYPTO
Eclipt Enhanced	***/7586/3/XXXX	CD-ROM	PM of data to be protected plus CRYPTO
Eclipt Enhanced User Token data	***/7586U/3/XXXX	CD-ROM	NPM ACCSEC

In the above table:

*** denotes a 3-letter trigraph identifying the Departmental COMSEC Sponsor/Controlling Authority.

7586 identifies the Key Material as for Eclipt HMG: this is the same for Eclipt Freedom HMG.

XXXX is the incremental number allocated by UKKPA to signify a particular community of users within a Department.

7. THE SALES APPLICATION PROCESS

7.1 Stonewood Group holds sole production and distribution rights for Eclipt HMG. All MOD users should purchase via the IA Section of the MOD ICS Catalogue and an appointed Agent of Supply. Other Government Departments and Government Agencies should purchase Eclipt HMG through GCat approved resellers. List X companies should purchase direct from Stonewood Group.

7.2 As with other commercially developed products incorporating CESG-designed or approved algorithms, Eclipt HMG is subject to formal sales approval procedures. It should be noted that CESG Sales Approval covers only Eclipt Encrypted Replacement Drives and the initial supply of Key Management Kits: all other items at Appendix 4 are freely available from Agents of Supply.

7.2.1 The MOD ICS Catalogue Agent of Supply/Government Security Specialist will provide the purchaser with a set of “Application to Purchase Products Incorporating

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

CESG Cryptography” forms, customised for Eclipt HMG, for completion by the purchaser, noting those parts that are for completion by other than the purchaser.

7.2.2 When the Purchaser has completed the relevant parts, these forms should be despatched to the Departmental COMSEC Sponsor, who will validate them before sending them to CESG for sales approval and for the provisioning of Key Material.

7.2.3 After sales approval CESG will distribute the forms to the Departmental COMSEC Sponsor, Agent of Supply/Government Security Specialist, and Purchaser.

8. THE KEY MATERIAL APPLICATION PROCESS

8.1 It is the responsibility of the administrator/purchaser, to determine the use of the product, and hence the quantity and delivery requirements for the Key Material. Guidance is given in the following sub-paragraphs.

8.1.1 Key Material for Eclipt HMG is produced by CESG using the root 7586 for Eclipt Baseline and Baseline Plus, 7586/3 for Eclipt Enhanced and for MOD users will be delivered via UKNDA; the format is described in more detail under Section 6 Key Management. CESG charges for Key Material; whether or not this charge is passed on to the purchaser is determined by arrangements currently in place between sponsoring organisations and CESG. For further information, contact the Departmental COMSEC Sponsor.

8.1.2 The production and provisioning of Key Material is inherent in completion of the Application to Purchase form set and will be provided automatically, provided the form set is completed correctly and dispatched to the correct authority.

8.1.3 Lead Times and Routine Re-supply of Key Material. The unique Key Material provided by CESG takes at least 12 **weeks**² from point of order to delivery to user. Key Material is valid for the life of the product. Additions to or deletions from Key Material sets can be arranged at any time on request to the Departmental COMSEC Sponsor. However, the above note concerning charging also applies.

8.2 All enquiries relating to the supply of Key Material should be directed to the Departmental COMSEC Sponsor (see Appendix 2)

9. SPECIAL CRYPTOGRAPHIC REQUIREMENTS

9.1 There are no special cryptographic requirements for Eclipt HMG.

10. LOSS OR COMPROMISE

10.1 Any loss or compromise of Key Material, or of a keyed element of a cryptographic system, is a reportable event and must be brought in the first instance to the attention of the COMSEC Custodian. Loss solely of an encrypted Eclipt HMG, including its host, shall be treated as an Information Security Incident in accordance with JSP 541. All other cases of

2 Based on 8-12 weeks for Key production and 2-4 weeks for Key delivery.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

loss, compromise or tampering shall be treated as a COMSEC Incident in accordance with Chapter 6 of BMD/0001/0001, Defence Cryptosecurity Operating Instructions.

10.2 Host Desktop, Laptop or Tablet PC

10.2.1 If evidence of tampering is found on the host PC or laptop, all elements of the system including the host PC or laptop, User Token (if applicable) and Eclipt HMG unit must immediately be handled at the same PM as the data on the drive.

10.2.2 If the host PC or laptop is lost or stolen, all remaining elements must be handled at the same PM as the data on the drive.

10.3 Key Material. If Key Material is lost or stolen, all Eclipt HMG units using a lost Key must be handled at the highest PM of the data on the drive until such time that the units can be rekeyed.

10.4 User Token Data

10.4.1 If User Token data is lost, all user accounts across all Eclipt HMG machines that are using the lost data must be changed to a new User Token. Refer to the Eclipt User Guide for instructions on this process.

10.4.2 Until the compromise is rectified all effected units and remaining parameters must be handled according to the PM of the data on the drive.

10.5 Eclipt Software CD. If the Eclipt Software CD is lost, it may be replaced. If its integrity can no longer be guaranteed, the CD must be destroyed and replaced with an authentic version. Replacement CDs can be purchased from Stonewood Group.

10.6 Eclipt Key Management Kit. If the Token Programmer CD is lost, it may be replaced. If its integrity can no longer be guaranteed, the CD must be destroyed and replaced with an authentic version. Replacement CDs can be purchased from Stonewood Group.

11. DOS AND DON'TS

Table 6 - Dos and Don'ts	
DO	DO NOT
Ensure all users of Eclipt HMG are trained in its use.	
Fully power down the host prior to removing the host from a secure environment.	
Carry User Tokens separately from the host.	
Ensure that power saving modes such as Standby, Sleep and Suspend are disabled.	
Remember that passwords are PM the same as the information on the host.	

NOT PROTECTIVELY MARKED
PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Appendices:

1. Glossary of Terms and Abbreviations Used within this Document.
2. Departmental COMSEC Sponsors.
3. Company Contact Details.
4. Eclipt System Components.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Appendix 1 - Glossary of Terms and Abbreviations Used within this Document

ACCSEC	ACCCountable and SECure
AES	The Advanced Encryption Standard Cipher
BIOS	Basic Input Output System
BSO	Branch Security Officer
CBC	Cipher-block chaining – Encryption of a block is dependent on the previous block
CAPS	CESG Assisted Products Service
CESG	UK National Technical Authority for Information Assurance
CLI	Command Line Interface – that provides a pre-boot Eclipt Management Console.
COMSEC	Communication Security
DefSy	Defence Security Division of MOD
DE&S ISS	Defence Equipment and Support Information Systems and Services
DCA	Defence Cryptosecurity Authority
DIPCOG	Defence Infosec Product Co-Operation Group
DSO	Departmental Security Officer
Eclipt HMG	The generic name for Eclipt Baseline, Eclipt Baseline Plus and Eclipt Enhanced.
EMC	Electromagnetic Compatibility
GCAT	Government Catalogue
HDD	Hard Disk Drive
Hibernate	Hibernate copies the RAM to the Eclipt's encrypted internal drive (into a file such as C:\hiberfil.sys) and then shuts down the host PC removing power from the Eclipt Encrypted Replacement Drive.
ITSO	Information Technology (IT) Security Officer
KEK	Key Encryption Key
Keymat	Abbreviation for Key Material, applicable to the Stonewood Token used to load Key Material
KeyStone User Token	A USB User Token. It combines the functions of an i-Button User Token and a Token Interface Cable with a USB connector
List X	UK Companies authorised to hold and process UK PM information at CONFIDENTIAL and above
MOD	Ministry of Defence
NPM	Not Protectively Marked

NOT PROTECTIVELY MARKED

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

OGD	Other Government Department
PATA	Parallel ATA also known as IDE
PC	Any Intel x386 type equivalent or later version, including desktop, laptop, tablet and other computers.
PDA Notes	Product Description and Application Notes
PM	Protectively Marked (formerly Classified) or Protective Marking
Purge Core	Removes the Key from the Eclipt drive but does not destroy it. The data on the Eclipt can be recovered by loading the same key that was originally used to encrypt the data onto the Eclipt drive.
Purge Disposal	Electronically destroys the Eclipt Electronics. This is irreversible.
SATA	Serial ATA the connection between the Eclipt Hard Drive and the computer
UKKPA	United Kingdom Key Production Authority (part of CESG)
UKNDA	United Kingdom National Distribution Agency

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Appendix 2 - Departmental COMSEC Sponsors

For MOD Military Users, MOD, Centre TLB, Agencies, List X:

For advice on products:

Defence Equipment and Support Information Systems and Services
DE&S ISS DCA Proc10a1
Building 009, Basil Hill Site, Corsham, Wiltshire, SN13 9NR

Tel: 01225 815902

Fax: 01225 815814

Internal Email: DESDCA-Proc10a1

Internet Email: DESDCA-Proc10a1@mod.uk

For Key Material Ordering:

Defence Equipment and Support Information Systems and Services
DE&S ISS DCA Key Order CAPS
Building 009, Basil Hill Site, Corsham, Wiltshire, SN13 9NR

Tel: 01225 818608

Fax: 01225 815882

Internal Email: DESDCA-Ops-Req2

Internet Email: DESDCA-Ops-Req2@mod.uk

For CESG and OGD sponsored users:

CESG Assisted Products Scheme (CAPS)
A2H, CESG, Hubble Road, Cheltenham, GL51 0EX

Tel: 01242 221491 Ext 34130

Fax: 01242-236742

Email: caps@cesg.gsi.gov.uk

CESG, UKKPA

A1-D7-4, CESG, Hubble Road, Cheltenham, GL51 0EX

Tel: 01242 221491 Ext 31950

Fax: 01242-709196 (non-secure)

Email: keymat@cesg.gsi.gov.uk



PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Appendix 3 - Company Contact Details

Vendor Name		Stonewood Group
Vendor Address		Stonewood Group Sandford Lane Wareham Dorset BH20 4DY
Vendor WWW Site Address		www.eclipt.com
Sales Contact	Name	Stonewood Group
	Telephone	01929 554400
	E-Mail	sales@stonewood.co.uk
	Facsimile	01929 552525
	Address	See vendor address
Technical Contact	Company	Stonewood Support
	Telephone	08450 66 44 00
	E-Mail	support@eclipt.com
	Facsimile	01929 552525
	Address	Stonewood Group Sandford Lane Wareham Dorset BH20 4DY
Point of Contact for Maintenance		See Technical Contact details

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT HMG V3.1

Appendix 4 – Eclipt HMG System Components

Table 7 - Eclipt System Components		Supplied By	Required for Eclipt		
			Baseline	Baseline Plus	Enhanced
Each Eclipt HMG Comprises					
Eclipt Encrypted Replacement (magnetic or solid state (flash))Drive		Stonewood	✓	✓	✓
i-Button User Token Interface Cable USB and Serial connectors available		Stonewood			✓
i-Button User Token		Stonewood			✓
KeyStone User Token		Stonewood			✓
Holographic Serialised Tamper Evident Labels		Stonewood			✓
Eclipt Tamper Label		Stonewood	✓	✓	
Each Crypto Custodian Requires:					
Key Management Kit with Token Programmer CD, Keymat Token and Keymat Token Interface Cable	Eclipt CRYPTO Custodian Kit	Stonewood	✓	✓	✓
Key Material CD-ROM		UKKPA	✓	✓	✓
User Token Data CD_ROM		UKKPA			✓
Installation CD and User Guide		Stonewood	✓	✓	✓