

NOT PROTECTIVELY MARKED

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG



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
ECLYPT *freedom* HMG v3.1

Issue 1

30 July 2009

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

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 13

8. THE KEY MATERIAL APPLICATION PROCESS 13

9. SPECIAL CRYPTOGRAPHIC REQUIREMENTS 14

10. LOSS OR COMPROMISE 14

11. DOS AND DON'TS 15

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 – ECLYPT FREEDOM HMG System Components 20

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

FOREWORD

(1) These Product Description and Application (PDA) Notes have been submitted by Stonewood Group to support the secure use of ECLYPT Freedom 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	ECLYPT FREEDOM HMG Crypto Officer Guide document no: CI 0016 ECLYPT FREEDOM HMG Getting Started document no: CI 0017 ECLYPT FREEDOM HMG User Guide document no: CI 0018	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 ECLYPT FREEDOM Baseline, ECLYPT FREEDOM Baseline Plus and ECLYPT FREEDOM Enhanced, hereafter referred to as ECLYPT FREEDOM HMG, and provides a reference for:

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

1.2 ECLYPT FREEDOM 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 FREEDOM HMG



View of ECLYPT FREEDOM HMG Drive showing USB Connection to PC.

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

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

1.3.2 ECLYPT FREEDOM 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 ECLYPT FREEDOM 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 FREEDOM HMG

3. DATA SHEETS

3.1 Summary of Functionality:

Table 2 - Summary of Functionality	
Maximum PM of Data	ECLYPT FREEDOM Enhanced: TOP SECRET ECLYPT FREEDOM Baseline Plus: CONFIDENTIAL ECLYPT FREEDOM 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 Markings and Handling Descriptors
Key Material CD-ROM	TOP SECRET/SECRET/CONFIDENTIAL CRYPTO RESTRICTED ACCSEC
User Token Data CD_ROM (ECLYPT FREEDOM 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
	ECLYPT FREEDOM Baseline and Baseline Plus: 0934513AEF ECLYPT FREEDOM Enhanced: 0934514AEF

3.2 Protective Markings

Table 3 - Protective Markings	
The PM of the ECLYPT FREEDOM HMG depends on the level of data that are stored on the device (including Key load).	
ECLYPT FREEDOM Enhanced	
Highest PM of Data when Authenticated	PM of ECLYPT FREEDOM Enhanced when NOT Authenticated
TOP SECRET	CONFIDENTIAL
SECRET	RESTRICTED
CONFIDENTIAL	NPM
RESTRICTED	NPM

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

ECLYPT FREEDOM Baseline Plus	
Highest PM of Data when Authenticated	PM of ECLYPT FREEDOM Baseline Plus when NOT Authenticated
CONFIDENTIAL	RESTRICTED
RESTRICTED	NPM
ECLYPT FREEDOM Baseline	
Highest PM of Data when Authenticated	PM of ECLYPT FREEDOM Baseline when NOT Authenticated
RESTRICTED	NPM

3.3 Technical Specifications

Table 4 - Technical Specifications		
Operating Systems Supported (See Paragraph 4)	Encryption	Operating System independent
	Management	When used with the CLI, Operating System independent. When used with the EMA, Windows XP Service Pack 2 and above.
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		USB 2.0 / USB 1.1
Communications Protocols Supported		USB 2.0 / USB 1.1
Dimensions		129 x 79 x 15mm
Electrical Safety		CE, UL
EMC		CE, FCC Class B
Environmental	Temperature	5°C to 40°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 USB connector

4. PRODUCT DESCRIPTION

4.1 Overview.

4.1.1 ECLYPT FREEDOM products are external hardware-based full disk encryptors securing data at rest up to and including TOP SECRET stored on integral magnetic or solid state (flash) media. The stored data can be handled at a lower PM when power is removed and prior to successful authentication. ECLYPT FREEDOM HMG connects to a Personal Computer via a USB port and utilises encryption and authentication to restrict access to the contents of its hard disk. ECLYPT FREEDOM has evolved from the FlagStone product range.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

4.1.2 This document applies to 3 ECLYPT FREEDOM HMG products:

- a. ECLYPT FREEDOM Enhanced, version 3.1
- b. ECLYPT FREEDOM Baseline Plus, version 3.1
- c. ECLYPT FREEDOM Baseline, version 3.1

Each of these ECLYPT FREEDOM portable drives is available with either magnetic or solid state (flash) storage.

4.1.3 ECLYPT FREEDOM HMG is a sector level hardware-based disk encryptor allowing pre-boot and post 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 ECLYPT FREEDOM 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 types:

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

4.1.4.5 Provides a Windows based management and authentication console, the ECLYPT Management Application (EMA) that is entirely compatible with all ECLYPT HMG devices including ECLYPT FREEDOM.

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

4.1.4.7 Is sealed in a tamper-evident enclosure, where encrypted Key Material and account status values are persistently stored.

4.1.5 ECLYPT FREEDOM System Components. See Table 6 at Appendix 4.

4.2 Installation Host.

4.2.1 ECLYPT FREEDOM portable drives will run on any x386 or greater host and are independent of operating system when used with the pre-boot management console (CLI).

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 FREEDOM HMG

4.3 Encryption/Decryption Process.

4.3.1 The process is hardware based on-the-fly encryption transparent to the end user. Every sector stored on the integral Hard Disk Drive (HDD) 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. ECLYPT FREEDOM Enhanced utilises two factor authentication consisting of a username, password and a token. The password is nine characters long and in CLEARVIEW format. ECLYPT FREEDOM Baseline and ECLYPT FREEDOM Baseline Plus utilise single factor authentication mechanisms, requiring entry of a username and password. Initially ECLYPT FREEDOM Baseline generates a 14 character password, whilst ECLYPT FREEDOM Baseline Plus generates a 15 character password.

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

4.4.3 There are 2 authentication platforms:

4.4.3.1 Pre-boot with the CLI allowing ECLYPT FREEDOM to contain a bootable operating system (OS). This platform is OS independent and is suitable for non Windows OS machines without EMA software installed.

4.4.3.2 Windows authentication allows the ECLYPT FREEDOM to act as a hot swappable external USB drive from XP SP2 including: Windows RC 7, Vista, Windows Server 2003 and newer versions.

4.5 Tamper Events and Alarms.

4.5.1 There are no electronic tamper events or alarms on ECLYPT FREEDOM HMG. However the product is supplied with tamper evident labels which must be applied across the plastic end-caps of the ECLYPT FREEDOM case 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 ECLYPT FREEDOM 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

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

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.

5.3 Deployment.

5.3.1 Deployment of ECLYPT FREEDOM 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 ECLYPT FREEDOM 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 ECLYPT FREEDOM, the COMSEC Custodian must inspect the unit to ensure that it has not been modified or tampered with.

5.3.2.3 The ECLYPT FREEDOM 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 Key Material is loaded.

5.3.2.4 ECLYPT FREEDOM must be attached only to computers accredited to the same PM as the data stored on the ECLYPT FREEDOM. (Products such as ECLYPT HMG internal drives can be used to reduce the PM of the host PC when powered down.)

5.3.2.5 The BIOS is to be configured to disable Standby and Suspend modes. Hibernation cannot be used whilst ECLYPT FREEDOM HMG is authenticated.

5.3.2.6 Refer to the ECLYPT FREEDOM HMG Crypto Officer Guide to complete software installation and configuration of the ECLYPT FREEDOM HMG.

5.3.2.7 Follow user guidance for the installed Operating System, disabling Operating System Standby and Suspend modes. If hibernation occurs whilst the Freedom is connected, any open files may be lost.

5.3.2.1 ECLYPT FREEDOM must be connected directly to the host personal computer and not through a USB hub. The number of ECLYPT FREEDOM drives that can be connected to a PC is limited by USB ports and drive letters.

5.3.2.2 Where the ECLYPT FREEDOM is used on a machine with an internal ECLYPT drive, the host ECLYPT must be configured and operational before attempting to

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

load Key Material into the ECLYPT FREEDOM HMG. When using ECLYPT FREEDOM HMG with an ECLYPT HMG equipped machine, Security Procedures must be provided that cover both Ecllypt drives.

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 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 ECLYPT FREEDOM Enhanced units additionally require the programming of User i-Button or KeyStone Tokens. User Token data are ordered from the UKKPA, are supplied with other Key Material and are transferred onto User Tokens using the ECLYPT Token Programmer.

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

5.3.3.4 A programmed Keymat Token must be handled according to the PM of the Key Material. The ECLYPT 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 ECLYPT FREEDOM 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.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

5.4 Disposal.

5.4.1 Purging of Key Material. The ECLYPT FREEDOM 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.

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. 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 ECLYPT FREEDOM HMG. The ECLYPT 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 ECLYPT FREEDOM HMG units ordered. Each Key Material file contains the data for a single ECLYPT FREEDOM HMG.

6.2.1.3 For ECLYPT FREEDOM Enhanced Only. The User Token data CD-ROM contains the data¹ to be transferred on to the User Token issued to each user of ECLYPT FREEDOM 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 ECLYPT FREEDOM 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 ECLYPT FREEDOM HMG for as long as it takes to transfer the Key Material from the

¹ These data are one part of the authentication data set; they are not a Key.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

CD-ROM on to the Keymat Token and then into the ECLYPT FREEDOM 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 ECLYPT FREEDOM HMG drive to be loaded with Key Material. Key Material is loaded into the ECLYPT FREEDOM 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.

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

6.2.2 ECLYPT Key Management Kit

6.2.2.1 A standalone PC is required for hosting the ECLYPT Key Management Kit application software for programming ECLYPT FREEDOM 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 The ECLYPT Key Management Kit application software can programme all ECLYPT HMG devices including ECLYPT FREEDOM HMG. ECLYPT FREEDOM HMG Key Material can be used with ECLYPT HMG devices of equivalent protective marking.

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

Table 5 - Definitions of Elements of Key Material			
Key Material Purpose	Short Title	Supplied Medium	Remarks
ECLYPT FREEDOM Baseline v3.1	***/7586/XXXX	CD-ROM	RESTRICTED ACCSEC
ECLYPT FREEDOM Baseline Plus v3.1	***/7586/XXXX	CD-ROM	CONFIDENTIAL CRYPTO
ECLYPT FREEDOM Enhanced	***/7586/3/XXXX	CD-ROM	PM of data to be protected plus CRYPTO
ECLYPT FREEDOM Enhanced User Token data	***/7586U/3/XXX X	CD-ROM	NPM ACCSEC

In Table 5:

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

7586 identifies the Key Material for ECLYPT HMG.

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

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

7. THE SALES APPLICATION PROCESS

7.1 Stonewood Group holds sole production and distribution rights for ECLYPT FREEDOM 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 ECLYPT FREEDOM 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, ECLYPT FREEDOM HMG is subject to formal sales approval procedures. It should be noted that CESG Sales Approval covers only ECLYPT FREEDOM Encrypted Portable 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 CESG Cryptography” forms, customised for ECLYPT FREEDOM 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 ECLYPT FREEDOM HMG is produced by CESG using the root 7586 for ECLYPT FREEDOM Baseline and Baseline Plus, 7586/3 for ECLYPT FREEDOM 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

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 FREEDOM HMG

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 ECLYPT FREEDOM 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 ECLYPT FREEDOM HMG, including its host, shall be treated as an Information Security Incident in accordance with JSP 541. All other cases of 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 ECLYPT FREEDOM HMG Device

10.2.1 If evidence of tampering is found on the ECLYPT FREEDOM device, the ECLYPT FREEDOM HMG unit must immediately be handled at the same PM as the data on the drive.

10.2.2 If the ECLYPT FREEDOM HMG or associated User Token is lost, the remaining item 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 ECLYPT FREEDOM 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 are lost, all user accounts across all ECLYPT FREEDOM HMG machines that are using the lost data must be changed to a new User Token. Refer to the ECLYPT FREEDOM 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 ECLYPT FREEDOM Software CD. If the ECLYPT FREEDOM 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 ECLYPT 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.

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

11. DOS AND DON'TS

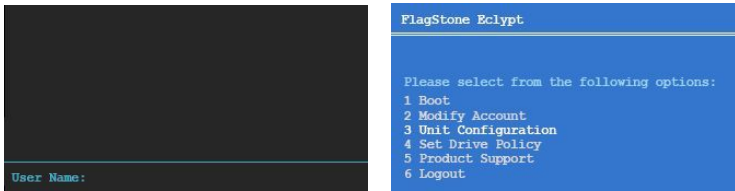
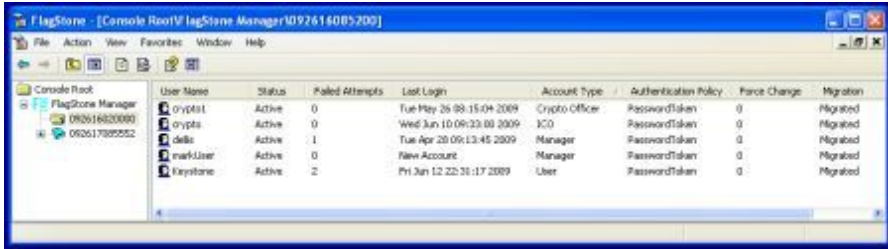
Table 6 - Dos and Don'ts	
DO	DO NOT
Ensure all users of ECLYPT FREEDOM HMG are trained in its use.	Attach the ECLYPT FREEDOM to a host computer accredited to a different PM.
Safely Remove the ECLYPT FREEDOM using normal Windows procedures before disconnecting the device.	Leave a secure environment with the ECLYPT FREEDOM still connected.
Carry User Tokens separately from the ECLYPT FREEDOM.	
Ensure that power saving modes such as Standby, Sleep and Suspend are disabled.	
Safely Remove the ECLYPT FREEDOM device before activating Hibernation.	
Remember that passwords are PM the same as the information on the host.	

Appendices:

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

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

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 –provides a pre-boot ECLYPT 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
ECLYPT FREEDOM	The generic name for ECLYPT FREEDOM Baseline, ECLYPT FREEDOM Baseline Plus and ECLYPT FREEDOM Enhanced.
ECLYPT HMG	The generic name for all ECLYPT internal and ECLYPT FREEDOM portable drives including: ECLYPT Baseline, ECLYPT Baseline Plus, ECLYPT Enhanced, ECLYPT FREEDOM Baseline, ECLYPT FREEDOM Baseline Plus and ECLYPT FREEDOM Enhanced.
EMA	ECLYPT Management Application - A Windows based management and authentication console. 
EMC	Electromagnetic Compatibility

NOT PROTECTIVELY MARKED

PRODUCT DESCRIPTION AND APPLICATION (PDA) NOTES FOR
STONEWOOD GROUP ECLYPT FREEDOM HMG

GCAT	Government Catalogue
Hibernate	Hibernate copies the RAM to the ECLYPT's encrypted internal drive (into a file such as C:\hiberfil.sys) and then shuts down the host PC removing power from the ECLYPT 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
OGD	Other Government Department
OS	Operating System – ECLYPT FREEDOM is OS independent when CLI authenticated.
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 ECLYPT FREEDOM drive but does not destroy it. The data on the ECLYPT FREEDOM can be recovered by loading the same key that was originally used to encrypt the data onto the ECLYPT FREEDOM drive.
Purge Disposal	Electronically destroys the ECLYPT FREEDOM Electronics. This is irreversible.
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 FREEDOM HMG

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 Proc10b
Building 009, Basil Hill Site, Corsham, Wiltshire, SN13 9NR

Tel: 01225 815877
Fax: 01225 815814
Internal Email: DESDCA-Proc10b
Internet Email: DESDCA-Proc10b@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 Service (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 FREEDOM HMG

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 FREEDOM HMG

Appendix 4 – ECLYPT FREEDOM HMG System Components

Table 7 – ECLYPT FREEDOM System Components Component		Supplied By	Required for ECLYPT FREEDOM		
			Baseline	Baseline Plus	Enhanced
Each ECLYPT FREEDOM HMG Comprises					
ECLYPT FREEDOM Encrypted Portable (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			✓
ECLYPT Tamper Label		Stonewood	✓	✓	
Each Crypto Custodian Requires:					
Key Management Kit with Token Programmer CD, Keymat Token and Keymat Token Interface Cable	ECLYPT CRYPTO Custodian Kit	Stonewood	✓	✓	✓
Key Material CD-ROM		UKKPA	✓	✓	✓
User Token Data CD_ROM		UKKPA			✓
Installation CD and User Guide		Stonewood	✓	✓	✓