SecureDoc Disk Encryption V.2.0

Security Target
Common Criteria EAL 1

Version 1.4 15 July 1999

Contents

1. Introduction 3
1.1. Identification 3
1.2. Overview of Document 3
1.3. Conformance Claim 3
2. TOE Description 3
3. Security Environment 6
3.1. Assumptions 6
3.2. Threats 7
4. Security Objectives 8
4.1. TOE Security Objectives 8
4.2. Environmental Security Objectives 8
4.2.1. IT Environmental Security Objectives 8
4.2.2 Non-IT Environmental Security Objectives 8
5. IT Security Requirements 10
5.1 Security Functional Requirements 10
5.2 Security Assurance Requirements 13
6. TOE Summary Specification 13
6.1. Statement of TOE Security Functions 13
6.2. Statement of Assurance Measures 14
7. Rationale 14
7.1. Security Objectives Rationale and Traceability 14
7.1.1. Security Objectives Rationale for Assumptions 15
7.1.2. Security Objectives Rationale for Threats 16
7.1.3. Environmental Security Objectives Rationale for Threats 17
7.2. Security Requirements Rationale 18
7.2.1. Security Functional Requirements (SFRs) Rationale 18
7.2.2. Functional Claims Rationale 19
7.3. TOE Summary Specification Rationale 20
7.3.1. IT Security Functions Rationale (SFRs) 20
7.3.2. Assurance Measures Rationale 23

Security Target: SecureDoc Disk Encryption Version 2.0

1. Introduction

1.1. Identification

Title: SecureDoc™ Disk Encryption software product, version 2.0

Registration: <to be filled in by registry>

Keywords: Access control, Disk Encryption, Information Protection

1.2. Overview of Document

The WinMagic SecureDoc™ Disk Encryption software product, version 2.0 is a disk encryption product for use in a Windows NT environment running on a PC or workstation platform. The SecureDoc™ product performs disk encryption using either DES, Triple DES (DES3), or CAST-128 encryption algorithms on hard disks or logical segments of disks. The Common Criteria Evaluation Assurance Level 1 evaluation documented herein describes assumptions, threats, security objectives that pertain to the product in its normal use and presents findings that establish its functional security properties at that level.

1.3. Conformance Claim

This Security Target (ST) document conforms to the requirements of the Common Criteria (CC) for Information Technology Security Evaluation (Version 15408 FDIS) ISO/IEC SC27 N2161, 15 November 1998, for an Evaluation Assurance Level (EAL) 1 evaluation. The WinMagic SecureDoc™ Disk Encryption software product, version 2.0 release (hereafter referred to as SecureDoc™) is the target of evaluation (TOE) for this Part 3 conformant CC EAL 1 evaluation.

2. TOE Description

Protection of information assets from unauthorized access or disclosure is a major concern of organizations and forms a prominent component of the security policy of most IT systems. One of the most effective solutions to the problem of implementing an effective protection system is the use of appropriate cryptographic algorithms.

Symmetric cryptographic algorithms are characterized by the use a single cryptographic key to encrypt (i.e., protect from access) an information asset and to decrypt (i.e., render accessible) the asset. The secrecy of this key is essential to the protective properties of the system. Most cryptographic algorithms are effective by virtue of the work effort they impose on a threat agent to recover or reconstruct the cryptographic key or the plaintext through various cryptanalysis attacks.

While standard symmetric algorithms such as DES, DES3 and CAST-128 have been made available through publication and implementation (subject to some distribution restrictions), an effective cryptographic protection system requires more than the efficient implementation of cryptographic algorithms. The CAST algorithm is not available for complete encryption of a hard drive. The management and protection of keys is of central importance to the effectiveness of these systems. If keys are lost, disclosed or in use for an unacceptable period of time, security risk can increase to an unacceptable level. The inherent problems of depending on human memory for retention of keys also renders imperative the requirement for an effective automated key management system to assist administration and user functions in a cryptographic access system.

Cryptographic access of information assets in the context of an operating system's file system can be implemented at the file, directory or disk level. While the file or directory level can be useful for certain low risk situations, or for systems that form a part of a communications system, they do not adequately address the problems imposed by contemporary personal computer and workstation operating systems and their applications.

The unpredictable presence and behaviour of temporary backup files, as well as caches and buffers that may reside on or be swapped to a hard drive entails the significant risk that sensitive information may be replicated in a plaintext repository that is unknown to the originator or legitimate owner of the principal file asset. The strategy of encrypting only at a file or directory level does not address this risk. Through the strategy of disk (logical segments or physical) encrypting, however, it is possible to mitigate this risk effectively.

SecureDoc™ Disk Encryption software performs disk encryption for personal computer and workstation platforms that run Microsoft Windows 95, 98, or NT version 4.0 operating systems. SecureDoc™ will run on any platform that successfully supports the operating system. Any disk drive or partition can be protected by this product. The operating system is considered to be part of the environment, not part of the TOE.

The SecureDoc™ product performs disk encryption and decryption dynamically at the device driver level. The product does not operate at higher level file system units, such as files. Upon installation, the product can be configured to encrypt all information stored on a physical disk drive or disk partition using a specified encryption algorithm and key. The key is stored in a key database that can be accessed only by entering the correct password, at login, that corresponds to it.

All low level write operations to a logical disk that has been protected by the SecureDoc™ product are encrypted using the user's key. All low level read operations similarly involve decryption using the user's key. This is done transparently by the installed device driver component of the product. Disk drives and partitions not selected by the user for protection are written and read as plaintext in the normal manner. Once the initial configuration is chosen regarding disk drives and choice of algorithm, the operation is transparent and requires no additional user intervention.

The SecureDoc™ product is installed through the standard installation wizard supplied on the installation CD or online executable. Different versions of SecureDoc™ product are not necessarily compatible. This necessitates the decryption of all data protected by a previous version of the SecureDoc™ product before installing a current version.

Some manual configuration and administration is essential to ensure that the normal operation of SecureDoc™ is sufficient to protect against leakage of sensitive information assets. To fully ensure that all repositories of sensitive data are protected, the following additional sources of unprotected data must be manually configured:

- TEMP and TMP directories;
- Auto Recovery files;
- Automatic backup files in MS Word;
- Print spool files;
- Print files (*.prn);
- Notebook PC's Suspend Mode; and
- Notebook PC's Hibernation Mode.

The above data objects must be configured to reside on the disk/partition under protection by the SecureDoc™ product. If they are sited on another unprotected drive, or elsewhere in a network, the encryption services of SecureDoc™ are unable to protect them from unauthorized access. Further consultation with specific application user manuals may be necessary to extend this list for a specific environment.

The system administrator is advised that only compression software recommended by WinMagic should be used to ensure that SecureDoc™ can protect the compressed files residing on encrypted disks.

As with any software product, it is advisable to have a state of the art virus-checking program to ensure viruses are not introduced. Only software approved by the system administrator should be installed on the platform that SecureDoc™ is protecting to prevent the importation of Trojan horses or other destructive software. This is especially true if SecureDoc is used in an enterprise-wide system with Internet access.

3. Security Environment

SecureDoc™ Disk Encryption software performs disk encryption for personal computer and workstation platforms that run the MicroSoft Windows NT operating system. The file system is characterized by hierarchical directory structures (or folders) and individual files that may be logically placed in those folders. Logical Disks are either segments of one or more hard disks on the base platform or diskettes mounted in a floppy drive.

The product is installed and operated through the use of a specialized device driver that replaces the standard disk read and write processes in the OS. This allows encrypted read and write operations to be performed at a low level to those disk sectors selected for encrypted I/O and plaintext operations to be performed for all other disk sectors. The low level boot log-in process is also modified to achieve integration with the OS password authentication process.

3.1. Assumptions

The list of assumptions regarding the security aspects of the environment in which the TOE is intended to be used is as follows:

A.NO_EMSEC	The sensitivity of information assets under protection by the TOE in its environment do not exceed that for which electromagnetic emissions countermeasures are mandatory or recommended by the environment system's responsible authority.
A.NO_EVIL	The selection of personnel for administrative roles with respect to the TOE's deployment and use in the organization must include a proper background check of the individual or be justified by mitigating circumstances that provide the organization with the assurance that administrators will demonstrate competence in their duties and not deliberately misuse or subvert the TOE for non-secure, fraudulent or other improper purposes.
A.NO_OBSERV	The physical environment allows users to enter passwords without being directly observable by other users or potential threat agents.
A.SENS_INFO	The sensitivity of information assets under protection by the TOE in its environment do not exceed that for which the symmetric encryption algorithms supported by the TOE (i.e., DES, DES3 and CAST-128) are recommended by the environment system's responsible authority.
A.VIDEO_CAPT	The environment does not have visible or concealed video capture devices such as closed circuit TV or video camera equipment that could be used to capture a user's key strokes at a distance.

3.2. Threats

The list of threats that target the assets that the TOE is protecting is as follows:

T.ACCESS	An authorized user of the TOE may access information or resources without having the permission from the person who owns, or is responsible, for the information or resource.
T.DATA_DEST	Execution of a disk format in MS-DOS mode while the logged-in computer is unattended, thereby converting the disk back to an unencrypted resource.
T.EAVESDRP	In the temporary absence of the authorized user during a login session, an unauthorized insider or unescorted visitor may access protected information.
T.KEY_LOSS	A non-hostile user may inadvertently forget the password to the key database created to encrypt information assets, denying access to data from authorized users in the organization.
T.MOVE_FILES	If the computer is unattended, a threat agent could move backup and temporary directories/files to unprotected drives in the immediate environment or network.
T.NEGLECT	An unauthorized agent may attack the integrity of the key database or other security-critical asset without detection by the administrator or system authority
T.OS_FAULT	An unrelated user process may cause an operating system protection fault while disk encryption is taking place and halt the encryption process before completion, resulting in incomplete or corrupted output.
T.PHYSICAL	Security-critical parts of the TOE may be subject to an inadvertent or careless physical attack by privileged users that may compromise security, e.g., loss / destruction of key database.
T.POWER	A power loss results in failure and possible corruption of the encryption process.
T.PRIVILEGE	Compromise of IT assets may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other privileged users.
T.PWD_SHARE	If user passwords are shared, contrary to the organizational policy, an unauthorized agent could access confidential assets
T.TF_LOCN	An unauthorized agent may gain access to sensitive information in a temporary file not protected by the TOE.

4. Security Objectives

4.1. TOE Security Objectives

The Security Objectives of the TOE comprise the following:

SO.ACCESS_CTL	The TOE must prevent access to data that has been written to a drive or partition protected by it to all subjects unable to initiate a session with the password associated with the drive on which the data resides.
SO.CRYPT_STD	The TOE must provide a choice of cryptographic algorithms and strengths based on key sizes with which to protect all protected data.
SO.KEY_BKUP	The security officer must retain a key database maintaining copies of all keys used by users having access to system protected drives.
SO.RESTORE	The TOE should detect and restore interrupted encryption processes at the next power resumption.
SO.SEC_STATE	In the event of an error occurring, the TOE should preserve a secure state.
SO.USER_I&A	Users of the TOE should be reliably identified and authenticated before being permitted access to the TOE and the cryptography-related IT assets therein.

4.2. Environmental Security Objectives

4.2.1. IT Environmental Security Objectives

There are no IT security objectives for the environment.

4.2.2 Non-IT Environmental Security Objectives

The non-IT Environmental Security Objectives comprise the following:

SO.INSPECT	The TOE and its key database should be regularly inspected for signs of errors or attacks
SO.KDB_PROT	Procedural and physical measures should be taken to prevent unauthorized individuals from gaining access to the TOE key database
SO.NO_EMSEC	The sensitivity of information assets under protection by the TOE in its environment do not exceed that for which electromagnetic emissions countermeasures are mandatory or recommended by the environment system's responsible authority.

SO.NO_EVIL	The system administration roles must be staffed by adequately trained, responsible and honest individuals who are not motivated to disable, degrade or subvert the operation of the TOE in the environment for personal gain or other purposes that contradict the security policies of the organization.
SO.NO_OBSERV	The physical environment allows users to enter passwords without being directly observable by other users or potential threat agents.
SO.PHYS_ACC	The PC or workstation hosting protected drives/partitions must be located in a lockable cabinet or room, or be logged-out or powered down when unattended.
SO.PWD_SHARE	The sharing of passwords among users should be forbidden or, if required to enforce role or group access, strictly confined to the users who hold the specified organizational role or are members of the specified group authorized to access the information assets protected by the shared password.
SO.SEC_AWARE	Users should be properly trained in Organizational security policy and have awareness of security procedures
SO.SENS_INFO	The sensitivity of information assets under protection by the TOE in its environment do not exceed that for which the symmetric encryption algorithms supported by the TOE (i.e., DES, DES3 and CAST-128) are recommended by the environment system's responsible authority.
SO.SYS_BKUP	The system must have regular backups that include protected drives.
SO.TF_LOCN	All temporary files that may contain sensitive information, and are either generated or used by their applications, must be located on encrypted drives in accordance with the recommendations of the TOE User Guide.
SO.UNATTEND	Users must be trained on correct procedures to follow when their PCs and workstations are unattended, and password-enabled screen savers and similar protective software should be used if their use is warranted
SO.VIDEO_CAPT	The environment does not have concealed or visible video capture devices such as closed circuit TV equipment or video camera equipment that could be used to capture a user's key strokes at a distance. The use of video recording equipment within line of sight of the PC or workstation hosting protected drives/partitions must be sanctioned by the security officer and all video information resulting from its operation protected from unauthorized access.

5. IT Security Requirements

5.1 Security Functional Requirements

This section contains the security functional requirements for the TOE. The following CC Part 2 Components are referenced, with definitions reproduced verbatim or completed where required. Completed definition text (i.e., added text not defined by the CC) is indicated below by *italics*.

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7.1 The TSF shall provide only *asterisks to be displayed* to the user while the authentication is in progress.

FDP_ACC.1.1 The TSF shall enforce the *discretionary access control through cryptographic separation of data* on *file objects that are written to a protected disk drive or partition.*

FDP_ACF.1.1 The TSF shall enforce the *discretionary access control* to objects based on *their storage location (i.e. disk drive or partition) and the encryption algorithm and key assigned to that storage location.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled objects is allowed:

(1) A subject acquires read access to the plaintext content of a protected file object if the subject is authorised, i.e., has been successfully identified and authenticated at login

(2) A subject may create or modify the plaintext content of a protected file object if the subject is authorised, i.e., has been successfully identified and authenticated at login

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

(1) an administrator may access protected file objects through the use of a controlled emergency key.

FDP_ACF.1.4 There are *no additional rules* upon which the TSF explicitly denies access of subjects to objects.

FCS_COP.1.1 The TSF shall perform *encryption* and *decryption* in accordance with a specified cryptographic algorithm *(multiple algorithms and modes of operation described below)* and cryptographic key sizes *(multiple key sizes described below)* that meet the following: *(multiple standards described below)*

Algorithm (Mode)	***Key Size***	***Standards***
DES (CBC)	*56*	*FIPS 46-2, FIPS 81, ANSI 3.106, ISO 8372, ISO/IEC 10116 standards*
Triple DES (CBC)	*168*	*ANSI X9.52, ANSI 3.106, ISO 8372, ISO/IEC 10116*
*CAST (CBC) **	*128*	*RFC 2144, ANSI 3.106, ISO 8372, ISO/IEC 10116*

FRU_FLT.1.1 The TSF shall ensure the operation of *encryption of a disk or partition* when the following failures occur: *power failure or physical anomaly inflicting temporary failure of disk operations while encryption is occurring.*

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *power failure or physical anomaly inflicting temporary failure of disk operations while encryption is occurring.*

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For *disruption of power during a disk encryption operation*, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a *proprietary* cryptographic key generation algorithm and specified cryptographic key sizes, *DES (CBC mode) 56 bit key*, *Triple DES 168 bit key* and *CAST 128 bit key*, that meets *no standard*.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method, *zeroization*, that meets *no standard.*

Among the above IT Security Requirements, some have dependencies that are either included in the above list or are omitted for reasons that are provided below:

IT Security Requirement	Dependencies	Remarks
FIA_UID.2	None	
FIA_UAU.2	FIA_UID.1	Hierarchical component FIA_UID.2 is included.
FIA_UAU.7	FIA_UAU.1	Hierarchical component FIA_UAU.2 is included.
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1	Included
	FMT_MSA.3	Not Included Static attribute initialization for restrictive, permissive or other values of security attributes is not specified. The TOE is software with the installer given the Administrator role by default. No default password is thus needed. The TOE generates keys.
FCS_COP.1	FCS_CKM.1	Included
	FCS_CKM.4	Included
	FMT_MSA.2	Not Included The Administrator can determine a minimum password length and the User's Guide gives an explanation of secure passwords and their use.
FRU_FLT.1	FPT_FLS.1	Included
FPT_FLS.1	ADV_SPM.1	Not Included The Secure State is defined in the *Informal Security Policy Model for WinMagic SecureDoc 2.0 Disk Encryption Recovery Processes, Version 1.1*.
FPT_RCV.2	FPT_TST.1	Not Included No self-tests or authorized user tests for data integrity are present. The maintenance mode for this software module only allows for re-booting or re-installation of the module. The errors that would cause the disruption of the encryption algorithm would be generated by the platform and not the TOE.
	AGD_ADM.1	Included
	ADV_SPM.1	Not Included The Secure State for the TOE is defined in the *Informal Security Policy Model for WinMagic SecureDoc 2.0 Disk Encryption Recovery Processes, Version 1.1*.
FCS_CKM.1	FCS_COP.1	Included
	FCS_CKM.4	Included
	FMT_MSA.2	Not Included
FCS_CKM.4	FCS_CKM.1	Included
	FMT_MSA.2	Not Included

5.2 Security Assurance Requirements

ACM_CAP.1	Version numbers
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_IND.1	Independent testing - conformance

6. TOE Summary Specification

6.1. Statement of TOE Security Functions

The TOE IT Security Functions and their specifications are listed as follows.

ITSF_UID1 User ID is required by TOE at Login prior to any other actions involving encryption/decryption access of protected data.

ITSF_UA1 TOE requires user ID to be authenticated prior to any other actions involving encryption/decryption access of protected data.

ITSF_UA2 TOE provides only asterisks (*) display as user inputs characters of authentication string

ITSF_AC1 TOE controls access by an identified and authenticated user to those objects which are files on a disk drive or sector that has been encrypted by the TOE. All read and write operations to the encrypted disk or sector are mediated by the TOE.

ITSF_AC2 TOE enforces the policy of access to a specific drive or sector based on the identification and authentication of the user subject.

ITSF_AC3 At installation, the Administrator is prompted to make an emergency key database to access all disks/partitions and this must be updated with each new key generation and deletion.

ITSF_AC4 TOE enforces all low-level read and write operations to incorporate decryption, respectively encryption, operations that utilize the secret key and user-selected algorithm associated with the currently identified and authenticated user subject.

ITSF_COP	TOE performs all cryptographic operations of encryption and decryption with one of the following user-chosen cryptographic algorithms and key sizes: (1) DES (56 bit key size); (2) Triple DES (168 bit key size); and (3) CAST (128-bit key size). The CAST algorithm is not available for complete encryption of a hard drive.
ITSF_FT1	TOE shall recover from an interrupted disk encryption operation (i.e., where only partial encryption of the disk has been achieved) where the interruption is due to loss of power, physical anomaly or attack, contention from another process in the OS environment or system fault requiring reboot.
ITSF_CKM1	The TOE will generate keys using a non-standard key generation method.
ITSF_CKM4	The TOE will delete keys by zeroization.

6.2. Statement of Assurance Measures

The assurance measures that are required for an EAL1 CC evaluation are described in the table below.

Assurance Requirements	Assurance Measures
AM_ACM_CAP	The TOE is identified by a version number. The version number is displayed by the executable, is on the CD-ROM, and is in the user's manual.
AM_ADO_IGS	Automated installation, generation, and start-up procedures are provided by WinMagic's SecureDoc 2.0 installation Wizard.
AM_ADV_FSP	An informal functional specification, *Informal Functional Specification (ADV_FSP.1)*, is supplied for the TOE.
AM_ADV_RCR	An informal correspondence demonstration, *Informal Correspondence Demonstration (ADV_RCR.1)*, is supplied for the TOE.
AM_AGD_ADM	An Administrator guide, *SecureDoc Ver. 2.0 For Windows 95/98/NT User's Guide*, is provided.
AM_AGD_USR	A user guidance document, *SecureDoc Ver. 2.0 For Windows 95/98/NT User's Guide*, is provided.
AM_ATE_IND	Independent testing of TOE and conformance of DES, 3DES and CAST algorithms will be done.

7. Rationale

7.1. Security Objectives Rationale and Traceability

The purpose of this section is to show that the security objectives of the TOE are appropriate to the security problem defined in the security environment section (see section 1.3). This is accomplished through a set of tables that cross-reference threats, security policies and assumptions against the security objectives that address them. Each

threat, policy or assumption is addressed by one or more security objective. Each security objective of the TOE (described in section 1.4) addresses at least one threat, policy or assumption. An informal argument is provided to show, for each threat, policy or assumption, why the identified security objective provides an effective countermeasure that prevents an attack or mitigates risk to acceptable levels.

7.1.1. Security Objectives Rationale for Assumptions

Assumption	Security Objective	Rationale
A.NO_EMSEC	SO.NO_EMSEC	The TOE is only applied to information assets whose sensitivity is appropriate for protection by the symmetric algorithms supported by the TOE independently of any assumptions on emissions security. It outside the scope of control of the TOE to assess the sensitivity of information assets being protected and risk of Emissions Security (EMSEC) attack on the user's login password. It is the decision of the responsible security authority for the system as to whether additional EMSEC protection must be used in conjunction with the TOE or in place of it.
A.NO_EVIL	SO.NO_EVIL	The TOE must be administered by trusted individuals who demonstrate knowledge of and adherence to the organizational security policy and procedures.
A.NO_OBSERV	SO.NO_OBSERV	The TOE must be operable in an immediate environment of relative privacy with respect to other users, so that direct observation of user login passwords is not possible. Unless this objective is met, no access control properties of the TOE can be verified in the target environment.

Assumption	Security Objective	Rationale
A.SENS_INFO	SO.SENS_INFO	The TOE is only applied to information assets whose sensitivity is appropriate for protection by the symmetric algorithms supported by the TOE. It outside the scope of control of the TOE to assess the sensitivity of information assets being protected and the decision of whether to employ the TOE to protect a given information asset rests with the responsible security authority for the system and/or the user.
A.VIDEO_CAPT	SO.VIDEO_CAPT	It is essential that no means of recording the user's login keystrokes be accessible to potential threat agents through video recording equipment whose outputs may be unprotected. Unless this objective is met, no access control properties of the TOE can be verified in the target environment.

7.1.2. Security Objectives Rationale for Threats

The TOE addresses the following security threats.

Threat	Security Objective	Rationale
T.ACCESS	SO.ACCESS_CTL SO.CRYPT_STD SO.USER_I&A	The TOE controls access, restricting access to authorized users when installed correctly and administered by a security officer.
T.KEY_LOSS	SO.KEY_BKUP	The TOE provides a master key database to enable the administrator to access encrypted disks if a user's password is forgotten or unknown.
T.OS_FAULT	SO.RESTORE SO.SEC_STATE	The TOE has the capability to restore the interrupted encryption process when a system fault occurs. The TOE maintains a secure state when a system fault occurs.
T.POWER	SO.RESTORE SO.SEC_STATE	The TOE has the capability to restore the interrupted encryption process when a power failure has occurred. The TOE maintains a secure state when a power interruption occurs.

7.1.3. Environmental Security Objectives Rationale for Threats

The traceability of threats to the Environmental Security Objectives is as follows:

Threat	Security Objective	Rationale
T.ACCESS	SO.UNATTEND	The Organization must inform and train users in the proper procedures for unattended sessions in which sensitive information is accessible on their PC / workstations.
T.DATA_DEST	SO.SEC_AWARE, SO.UNATTEND SO.PHYS_ACC	The Organization must train users on correct procedures to follow when their PCs and workstations are unattended, and must provide password-enabled screen savers and similar protective software if warranted
T.EAVESDRP	SO.PHYS_ACC	The Organization must provide adequate protection of the installed TOE PC or workstation to prevent access of a login session while the device is unattended.
T.MOVE_FILES	SO.UNATTEND SO.PHYS_ACC	The Organization must train users on correct procedures to follow when their PCs and workstations are unattended, and must provide password-enabled screen savers and similar protective software if warranted.
T.NEGLECT	SO.INSPECT, SO.KDB_PROT, SO.SEC_AWARE	The Organization must enforce regular inspection of the key databases and must protect such assets from theft or duplication. Users must be aware of consequences of mistreating access control information.
T.PHYSICAL	SO.SYS_BKUP SO.SEC_AWARE	The Organization must enforce effective protection of TOE-critical information such as the key database to prevent loss of security-critical information on a hard drive or diskette.
T.PRIVILEGE	SO.SEC_AWARE SO.NO_EVIL	The Organization must provide administrators with adequate security awareness and training to prevent careless, willfully negligent, or hostile actions on the part of administrators.
T.PWD_SHARE	SO.SEC_AWARE SO.PWD_SHARE	The Organization must train users and provide security awareness that prevents the sharing of passwords among users `unless sanctioned by security policy.
T.TF_LOCN	SO.TF_LOCN	The Organization must make sure that users properly locate application-specific temporary files and swap-areas on the protected disk / partition, if they contain sensitive information.

The security objectives of the environment are considered effective in countering the effect of the threats cited if correctly applied by the organization. Security objectives of the TOE are effective in countering the threats identified in section 3.2 that are not found above. This traceability of threats to TOE-specific security objectives is found in section 7.1.2.

7.2. Security Requirements Rationale

7.2.1. Security Functional Requirements (SFRs) Rationale

The rationale for the SFRs against the security objectives of the TOE is given in the table below. For each security objective of the TOE, a list of assigned SFRs is given, followed by an argument stating how each SFR addresses or satisfies the security objective in question.

Security Objective	SFR	Rationale
SO.ACCESS_CTL	FDP_ACC.1	FDP_ACC.1 provides that access control to protected objects is based on cryptographic separation on file objects that are written to a protected disk drive or partition.
	FDP_ACF.1	FDP_ACF.1.1 provides that the access control to protected objects is based on their location (logical disk drive) attribute. FDP_ACF.1.2 provides that if a subject is correctly identified and authenticated, then read and write access to a controlled object (i.e., a file on a protected drive/partition) is granted through encryption/decryption operations employing a correct cryptographic key.
SO.CRYPT_STD	FCS_COP.1	FCS_COP.1 provides that the TSF performs encryption and decryption operations in accordance with one of the following three algorithms: DES with 56-bit key size; Triple DES with two keys having 56-bit key sizes; and CAST with 128-bit key size, in accordance with the following standards: FIPS 46-2, FIPS 74, FIPS 81, ANSI X3.106, ISO 8372, ISO/IEC 10116, ANSI X9.52, RFC 2144. The Cipher Block Chaining (CBC) mode of operation is employed as defined in the aforesaid standards.
	FCS_CKM.1	FCS_CKM.1 provides key generation for encryption and decryption processes.
	FCS_CKM.4	FCS_CKM.4 provides key deletion for keys used in encryption and decryption processes by zeroization.
SO.KEY_BKUP	FDP_ACF.1	FDP_ACF.1.3 provides the administrator access to all partitions with the use of an emergency key database, which requires no password in the event an employee, leaves without decrypting the disk or a password is forgotten.

Security Objective	SFR	Rationale
SO.RESTORE	FRU_FLT.1	FRU_FLT.1 provides that the TOE can continue correct operation (following a reboot) and an automated recovery in the event of a power failure or system fault while encryption of a disk/partition is in progress.
SO.SEC_STATE	FPT_FLS.1	FPT_FLS.1 provides that an interrupted disk encryption process will result in the TOE returning to a secure state as defined in the partial security policy model.
	FPT_RCV.2	FPT_RCV.2 provides that for at least one type of service discontinuity (e.g., power failure) automated recovery to secure state, without human intervention will be performed by the TOE. For other types of failures/discontinuities, the TOE will require re-booting.
SO.USER_I&A	FIA_UID.2	FIA_UID.2 provides that identification (by selection of user ID from the login form) must be done prior to any other TSF actions, such as encryption / decryption of protected data.
	FIA_UAU.2	FIA_UAU.2 provides that the user cannot perform actions such as encryption / decryption of protected data (other than selection of user ID from the login form) prior to authentication of the user's identity.
	FIA_UAU.7	FIA_UAU.7 provides that the authentication feedback to the user be limited, allowing specifically that the characters of the user authentication string could be represented by asterisks (*).

The coverage of the above table against the SFRs satisfies the following properties:

- for every security objective of the TOE, there is at least one SFR that satisfies it;
- for every SFR, there is at least one security objective of the TOE that it addresses.
- for every security objective of the TOE, an informal argument as to why the identified SFRs are sufficient to meet it is provided.

7.2.2. Functional Claims Rationale

The selected functionality for this ST is consistent with and appropriate for the security objectives for the TOE. There are 4 main categories of security service that the TOE provides:

- User Identification and Authentication must precede all other access to protected information, providing binding between the user and the symmetric key used in read and write access to protected information stores;
- All access to the protected information is through decryption using specified algorithms and key lengths that are of appropriate strength for business, financial and personal private data under a broad class of applications;

- Restoration of a partially encrypted disk that has been created when a disk encryption process is interrupted either through power failure or operating system fault or interruption through contention for resources is automated.

These security services embody the security objectives of the TOE and are consistent with the level of capability and motivation that a threat agent would be expected to possess, given the assumptions regarding data sensitivity of information assets and sophistication of threat agent. Elimination of all potential threat agents clearly requires environmental support, procedural security and training. The latter safeguards are complementary security objectives that the environment is expected to supplement the TOE functional properties with in order to obtain an overall acceptable level of risk. They do not constitute weaknesses or omissions in the TOE, as the majority of the environmental security objectives are beyond the scope of any conceivable software solution. In addition, not all may represent serious risk to the average system in which the TOE is deployed.

7.3. TOE Summary Specification Rationale

7.3.1. IT Security Functions Rationale (SFRs)

The TOE IT Security Functions are listed with cross-references to the SFRs, described in section 5, that are provided by the defined IT Security Function. Specifications of IT Security Functions are provided in section 6.1. A Coverage Mapping is included to describe how the IT Security Function covers the referenced SFRs.

Security Functional Requirement	IT Security Function	IT Security Function to SFR Coverage Mapping
FIA_UID.2	ITSF_UID1	It is required that the timing of identification be such that users must identify themselves before any action, such as read or write to/from the protected disk, be permitted.
FIA_UAU.2	ITSF_UA1	It is required that the user be successfully authenticated before any action, such as read or write to/from the protected disk, be permitted. This is covered in the functionality of the TOE by prompting the user for his/her secret password to authenticate the user and retrieve his/her secret key.
FIA_UAU.7	ITSF_UA2	It is required that only asterisks (*) be presented to the user while authentication is in progress. This is covered in the functionality of the TOE, i.e., while the user is entering his/her password, only a single asterisk appears for each character entered.

Security Functional Requirement	IT Security Function	IT Security Function to SFR Coverage Mapping
FDP_ACC.1	ITSF_AC1	It is required that subset access control be in place for a subset of possible operations, on a subset of objects in the TOE. This is covered in the functionality of the TOE in that all file objects on the protected disk / partition are successfully read from or written to if the user has authenticated himself/herself prior to the specified read/write operations and related transactions in the login session. If the authentication is unsuccessful, the correct key will not be initialized for the session and all specified operations will fail. Files not residing on the protected disk / partition are not covered by this functionality, thus the subset-only access control requirement is appropriate.
FDP_ACF.1	ITSF_AC1 ITSF_AC2	It is required that the access control functions specified in FDP_ACC.1 be further described in terms of the rule: The TSF shall enforce the encryption of objects based on the key associated by authentication to the user currently logged in. The functionality covers this rule through the exclusive use of the key associated with the current user through successful login and authentication for all encryption and decryption operations concerning the protected disk / partition.
	ITSF_AC3	The Administrator can make an emergency key database to access all disks/partitions and be updated with each new key generation and deletion.
FCS_COP.1	ITSF_COP	It is required that the TOE performs cryptographic operations of encryption and decryption in accordance with a specified algorithm, cryptographic key size and standard. The functionality of the TOE includes three algorithms that are defined by standards and employ key lengths appropriate to the algorithms and standards referenced. The TOE performs encryption and decryption operations in accordance with one of the following three algorithms: DES with 56-bit key size, Triple DES (DES3) with a combined key size of 168 bits and CAST with 128-bit key size, in accordance with the following standards: FIPS 46-2, FIPS 74, FIPS 81, ANSI X3.106, ISO 8372, ISO/IEC 10116, ANSI X9.52, RFC 2144.
	ITSF_AC4	All low-level read and write operations incorporate decryption (respectively, encryption) operations that utilize the secret key and user-selected algorithm associated with the currently identified and authenticated user subject. The functionality covers this rule through the exclusive use of the key associated with the current user through successful login and authentication for all encryption and decryption operations concerning the protected disk or partition.

Security Functional Requirement	IT Security Function	IT Security Function to SFR Coverage Mapping
FRU_FLT.1	ITSF_FT1	It is required that the TOE have the capability to recover from an interrupted disk encryption operation (i.e., where only partial encryption of the disk has been achieved) where the interruption is due to loss of power, unrelated process running in the OS or system fault requiring reboot. This functionality covers this requirement through the automated recovery operation of the TOE.
FPT_FLS.1	ITSF_FT1	The TOE preserves a secure state when a power failure or temporary OS fault occurs during disk encryption.
FPT_RCV.2	ITSF_FT1	The TOE provides that, for at least one type of service discontinuity (e.g., power failure) automated recovery to secure state, without human intervention will be performed by the TOE.
FCS_CKM.1	ITSF_CKM1	The TOE generates DES, Triple DES and CAST keys using a non-standard method of key generation.
FCS_CKM.4	ITSF_CKM4	The TOE deletes keys by zeroization.

The combined aggregate of the TOE security functions satisfy the set of identified TOE SFRs as shown above. Given that the cryptographic power of the TOE (in terms of algorithm choice and key size) is sufficient to protect information assets within the requirements of the organization / environment, then it can be concluded that the security functionality of the TOE is effective in applying that cryptographic protection to a restricted user-selected set of information assets. It is clear that the problems of protecting residual objects and temporary application-created objects containing sensitive information is effectively solved through the scoping of the TOE to logical drives and partitions, rather than to individual files. The embedding of cryptographic services in the device driver layer of the environment ensures application transparency. Certain utilities such as compression software must be selectively chosen. These criteria are identified in the user documentation. Provided the configuration and maintenance of the TOE is carried out in a secure way, following vendor recommendations, the TOE security functional claims are valid.

7.3.2. Assurance Measures Rationale

The compliance of the TOE with the required assurance measures is established in the table below.

Assurance Components	Assurance Measures	Compliance
ACM_CAP.1	AM_ACM_CAP	TOE releases are adequately identified with the version number.
ADO_IGS.1	AM_ADO_IGS	Automated installation procedures are adequate to ensure that the user starts the TOE within a secure configuration.
ADV_FSP.1	AM_ADV_FSP	An informal functional specification is supplied for the TOE.
ADV_RCR.1	AM_ADV_RCR	A representational correspondence is supplied to connect the TOE summary specification to the informal functional specification of TSFs provided.
AGD_ADM.1	AM_AGD_ADM	The administrator's guide is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AGD_USR.1	AM_AGD_USR	The User guidance is adequate to provide the user with the required knowledge to correctly perform login procedures and to provide security awareness of the TOE and its policies.
ATE_IND.1	AM_ATE_IND	The functional testing will be performed by an independent third party.