SecureD® Version 1.6

Security Target

Prepared for:

High Density Devices AS
Postboks 1428
N-4505 Mandal, Norway

Prepared by:

Sun Microsystems
Minnesota Research and Development Center
6705 Wedgwood Court North
Maple Grove, MN 55311
USA

Version Date:December 22, 2005
Date Printed: October 20, 2006

Document Number SecureD v1.6 Security Target - 000506ST – 01.60

Document Revision History

Revision	Date	Author	Notes
01.00	February 15, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Initial, released version.
01.10	September 19, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Edited in response to CC ETR
01.20	October 17, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Edited in response to CC ETR
01.30	November 22, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Edited in response to CC ETR
01.40	December 12, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Edited in response to Validator’s comments
01.50	December 15, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Edited in response to CC ETR
01.60	December 22, 2005	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)	Edited in response to Validator’s comments

U.S. GOVERNMENT LIMITED RIGHTS LEGEND

Contract No. TS-0311-7808
Contractor Name High Density Devices AS
Contractor Address P.O. Box 1428, N-4505 MANDAL, NORWAY

The Government’s rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(3) of the Rights in Technical Data - Non-commercial Items clause contained in the above identified contract. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such data must promptly notify the above named Contractor.

Contents

List of Figures

List of Tables

1 Security Target Introduction

A Security Target (ST) contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet the stated requirements. The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation.

The structure and contents of this ST comply with the requirements specified in [CC_PART1], Annex A, [CC_PART2], and [CC_PART3], Chapter 5.

1.1 ST and TOE identification

This section provides ST and TOE identification information.

ST Title	SecureD Version 1.6 Security Target
ST Author(s)	Alan Dowd (Sun Microsystems); Tormod Fjellgård (HDD)
ST Revision Number	SecureD v1.6 Security Target - 000506ST - 01.60
ST Date	December 22, 2005
TOE Identification	SecureD Version 1.6
CC Identification	Common Criteria for Information Technology Evaluation, Version 2.2, January 2004
Assurance Level	EAL4, augmented with AVA_VLA.3
ST Evaluation	Science Applications International Corporation
Keywords	Cryptography, data storage, AES 256, Hardware-based Encryption, Key Zeroization, IDE/ATA Data Bus Encryption

1.2 Security Target overview

This Security Target describes the SecureD® data storage encryption device (SecureD), a hardware encryption device that can be installed in the data path between an IDE controller and IDE devices in a general computing environment. SecureD applies Advanced Encryption Standard (AES) encryption to protect data at rest from intentional or inadvertent disclosure.

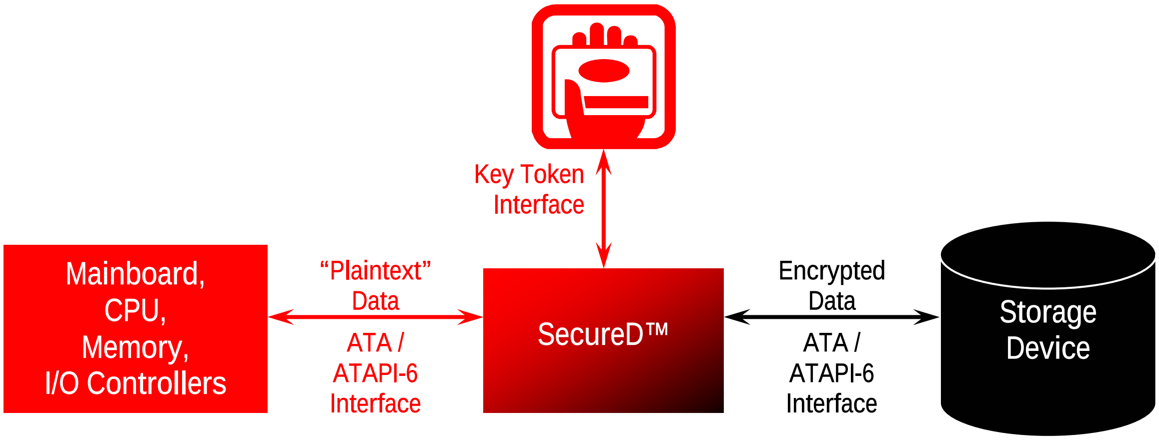

Figure 1. The SecureD data storage solution

This Security Target (ST) contains ten sections, as follows:

Section 1 contains document management and overview information for the ST.

Section 2 provides a general description of the **SecureD**® data storage encryption device.

Section 3 provides the statement of the TOE security environment, which defines the security problem the TOE is intended to meet. It is a discussion of the expected environment for SecureD, in particular the assumptions that must be true about aspects such as physical, personnel, and connectivity conditions. This section then defines the set of threats that either environmental controls or the technical countermeasures implemented in the hardware and software of SecureD address.

Section 4 provides the statement of security objectives, defining what is expected of the TOE and its environment, in order to address the security problem defined in Section 3.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by SecureD to achieve the relevant security objectives defined in Section 4.

Section 6 provides the TOE summary specification, which defines how the TOE meets the IT security requirements defined in Section 5.

Section 7 is a placeholder, since this ST makes no claims of conformance with any existing Protection Profile.

Section 8 provides the ST Rationale, which explicitly demonstrates that the IT security objectives satisfy the threats. The section then explains how the set of requirements are complete relative to the objectives; that one or more relevant component requirements address each security objective. Finally, it demonstrates that:

- the security problem defined in Section 3 will be suitably addressed if the TOE and its environment meet the stated security objectives in Section 4;
- the TOE and IT environment security objectives will be achieved if the TOE and IT environment satisfy the IT security requirements in Section 5;

- the TOE security requirements will be met if the TOE correctly implements the security functions and assurance measures defined in Section 6.

Section 9 provides background material for further investigation by interested users of this ST and the Target of Evaluation it describes.

Section 10 provides a list of abbreviations and a glossary of terms used throughout this document.

1.3 Common Criteria conformance claims

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
  - Part 3 Conformant
  - EAL 4
  - Augmented with AVA_VLA.3

2 TOE Description

2.1 Product type

The SecureD® data storage encryption device (SecureD) is a hardware encryption device, which is fully compatible with the Advanced Technology Attachment (ATA) / ATA Packet Interface (ATAPI)-6 (Integrated Drive Electronics (IDE)) interface, that resides in the data path between an IDE controller and one or two IDE devices(including ATAPI CD_ROM devices) in a general computing environment. Because SecureD resides “on the wire” between the IDE controller and the storage media, it operates both physically and logically at a level below visibility to operating systems and application programs.

SecureD applies Advanced Encryption Standard (AES) encryption at the sector level to protect data at rest from intentional or inadvertent disclosure. It loads its cryptographic keys from an external Key Token – typically a smart card – through an encrypted external interface, logically and physically separate from the data path. SecureD supports multiple key lengths (128, 192, and 256 bits) and up to 32 different keys per Key Token. Each key can be allocated any non-overlapping sector range on the storage medium. If the operating system or an application requests a storage address that the IDE controller maps to an unallocated sector, SecureD returns an I/O error to provide information hiding about the inaccessible sectors. SecureD incorporates hardware functions for zeroizing the data encryption keys.

The evaluated configuration of SecureD consists of a Field Programmable Gate Array (FPGA) chip, an FPGA configuration device (a Xilinx Programmable Read-Only Memory (PROM) (Xilinx part no. XCF32) designed to match the FPGA), and a flash memory chip, all of which are mounted to a small, underlying printed circuit board (PCB); the entire PCB and the components mounted to it are encapsulated in a hard, opaque, tamper-evident coating, leaving only the interface pins accessible.

The Target of Evaluation (TOE) for this ST is an operational storage encryption device (SecureD), consisting of an integrated circuit, including the mechanisms that allow communication with the outside world. The TOE consists of sufficient hardware elements to be capable of establishing an ATA / ATAPI-6 data channel between a typical small computer IDE controller and one or two IDE devices and trusted communications with a trusted source for cryptographic keying information. The TOE, as defined here, provides the following IT features in order to support the intended functionality:

- information processing and storage capability to allow execution of loaded commands
- security-related functions to maintain the confidentiality and integrity of specified user and security function data
- cryptographic functions to support the establishment and control of trusted communications with a trusted source for cryptographic keying information
- cryptographic functions to support encryption and decryption of data passing between the IDE controller and the protected IDE device

This ST does not apply to the cryptographic key source, nor to any device with which the TOE interfaces.

2.2 Evaluation application context

2.2.1 Physical scope and boundary

HDD SecureD is a hardware-based data encryption device designed for encryption of user data stored in a computer storage device. It has been certified as a validated FIPS 140-2 multi-chip, embedded, hardware Cryptographic Module at Security Level 3 (Certificate # 592; http://csrc.nist.gov/cryptval/140-1/1401val2005.html). HDD SecureD is logically and physically separate from the computer processor unit, and is placed directly in the data path between processor unit and storage device. Figure 2 provides an abstract, conceptual view of the TOE, its interfaces, and its place in a host system.

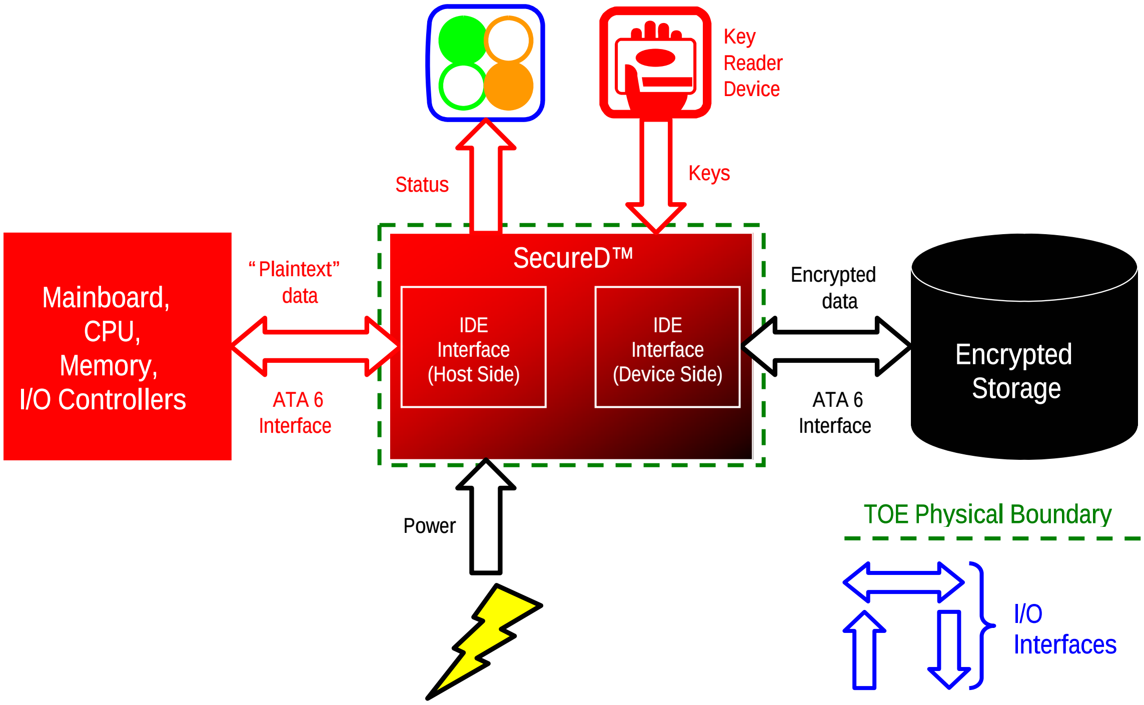

Figure 2. SecureD physical boundary – conceptual

SecureD functionality is implemented in a FPGA form. The SecureD TOE consists of the FPGA, an FPGA configuration device, and a flash memory chip, all of which are mounted to a small, underlying printed circuit board (PCB). The entire PCB and the components mounted to it are encapsulated in a hard, opaque, tamper-evident coating, leaving only the interface pins accessible.

The HDD SecureD TOE is physically embodied as a multi-chip embedded cryptographic module, as defined in Section 4.5 of FIPS PUB 140-2. The physical boundary for the SecureD TOE coincides with hard, opaque, tamper evident block of epoxy and includes all the elements on the PCB board located within this block of epoxy. Figure 3 and Figure 4 show the SecureD TOE as fabricated.

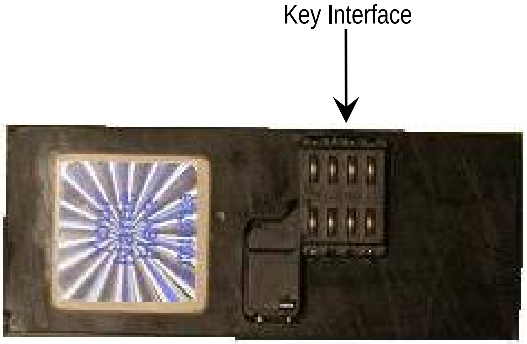

Figure 3. SecureD TOE (front)
– Epoxy Coated with Tamper-Evident Seal

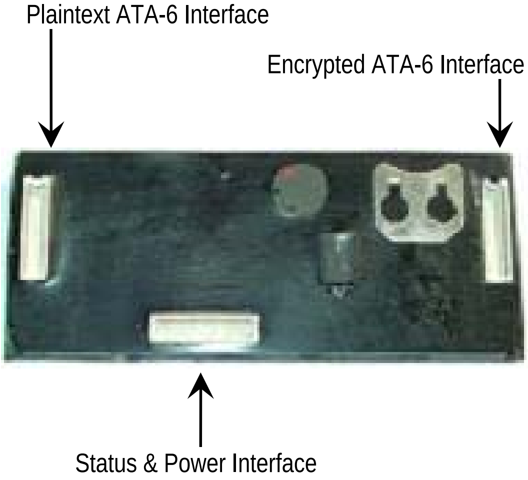

Figure 4. SecureD TOE (back)
– Epoxy Coated

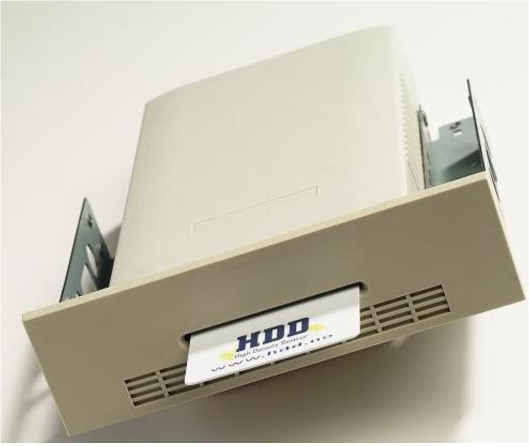

Figure 5. SecureD mounted in desktop adapter – key and status interfaces

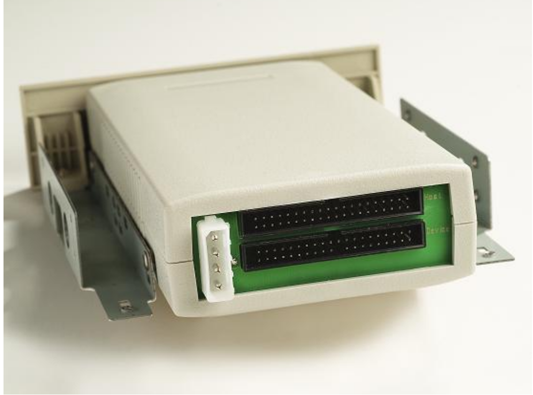

Figure 6. SecureD mounted in desktop adapter – data and power interfaces

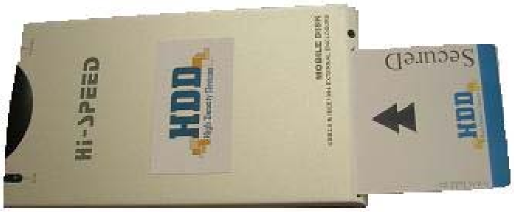

Figure 7. SecureD mounted in an external, USB drive carrier

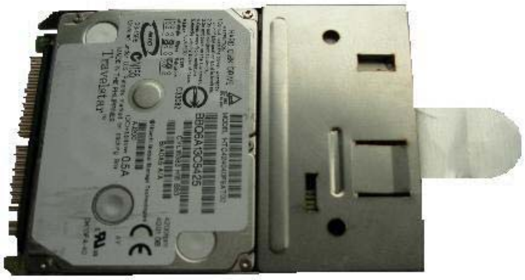

Figure 8. SecureD mounted directly to a hard drive

A family of SecureD products incorporate the SecureD TOE. The SecureD TOE may be mounted in a suitable carrier, such as a 5-1/4" drive bay adapter, to make it easier to use. Such an adapter is a passive, mechanical extension of the device and the interface pins. It does not affect the physical boundary of the TOE and does not provide any security functionality. Other such fielded implementations are possible, without affecting the evaluated configuration. Figure 5 through Figure 8 show examples of the SecureD TOE in place in SecureD products.

2.2.2 Logical scope and boundary

SecureD is a hardware encryption device and, as such, its core security function is to provide encryption for data passing through it. The SecureD device has two ATA interfaces for user data, conventionally labeled "ATA IN" (host side) and "ATA OUT" (storage device side). SecureD encrypts data passing from ATA IN to ATA OUT and decrypts data passing from ATA OUT to ATA IN. SecureD performs this encryption using the Advanced Encryption Standard (AES), with selectable key lengths of 128, 192, and 256 bits. The AES implementation has been validated against the *Advanced Encryption Standard Algorithm Validation Suite* (Certificate # 174; http://csrc.nist.gov/cryptval/aes/aesval.html). SecureD will not allow unencrypted data to be written to a device. However, should unencrypted data for any reason already be present on a disk, SecureD may allow this data to be read (depending on key parameters). The clear read capability is intended for the case where a hard drive and a CD-ROM player are connected to the same SecureD device. This will allow the user to read a clear CD-ROM. (FCS_COP.1 [1]; FDP_IFC.1.1 [1]; FDP_IFF.1 [1]; FPT_RVM.1)

An authorized operator must prepare the cryptographic keying material using tools external to the SecureD TOE. An authorized operator must also use a Key Management System (policies, procedures, hardware, and software) capable of creating cryptographic Key Tokens compatible with SecureD. (FCS_CKM.1) The SecureD TOE does implement functions to zeroize the data encryption keys it contains when operational. (FCS_CKM.4)

The cryptographic keying material enters SecureD through a self-contained Key Interface. SecureD uses Triple Data Encryption Algorithm (TDEA) encryption to validate the role of the user and to protect communications with the Key Token through the Key Interface. The TDEA implementation has been validated against *NIST Special Publication 800-20* (Certificate # 324; http://csrc.nist.gov/cryptval/des/tripledesval.html). (FCS_COP.1 [2]; FDP_IFC.1.1[2]; FDP_IFF.1[2])

SecureD can recognize up to thirty-two AES keys per Key Token. Each AES key can process a selectable storage address range on the encrypted media (ranges are contiguous and non-overlapping, but not necessarily adjacent nor inclusive of all storage device capacity), with a selectable direction (R, W, R/W). Unmapped storage address ranges are invisible to the operating system and applications of the host system; attempts to access those ranges return an error. The AES keys can be stored on SecureD and the Key Token as a split key pair to enhance security of the derived operational data encryption key. (FCS_COP.1 [1]; FCS_COP.1 [2])

Only an authorized operator, acting in the Crypto Officer role and only after the role has been validated, can change the TDEA communications keys and the resident parts of the AES split keys. Only an authorized operator, acting in the User role and only after the role has been validated, can provide the portion of the split key that is resident on the Key Token. (FIA_UID.1; FMT_MSA.1; FMT_MSA.2; FMT_MSA.3; FMT_SMF.1; FMT_SMR.1)

The encryption engine within SecureD exists in a domain that is logically and physically separate from the direct data paths. Keying material and the executing encryption algorithms are never exposed to the I/O devices external to the TOE. This is accomplished by implementing the encryption engine as a separate hardware-only module within SecureD with well defined internal interfaces for the user data as well as the for the keying material. The interface for the keying material is one-way only (no exit). The mechanisms of the internal I/O subsystem ensure that data cannot pass between the two ATA interfaces without passing through the encryption system. The data path is implemented in hardware only. (FPT_RVM.1; FPT_SEP.1)

3 TOE Security Environment

This statement of the TOE security environment defines the security problem the TOE and its environment address. It describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be deployed.

To this end, the statement of TOE security environment identifies the intended method of use of the TOE and the list of assumptions made on the operational environment (including physical and procedural measures), defines the threats that the TOE is designed to counter, and describes the organizational security policies with which the TOE is designed to comply.

The SecureD TOE operates in an environment where it provides encryption for data passing between an IDE controller and one or two IDE devices. Its presence is transparent to both the IDE controller and the IDE devices, thus it is both platform and operating system independent, if the platform and the IDE device both conform to the ATA / ATAPI-6 standards. The Key Token reader connects directly to SecureD, so there are no OS or platform dependencies here, either.

For the purposes of this Security Target, the assumptions, threats, and organizational security policies will be derived from a conceptual operating scenario, as follows. SecureD is installed in a typical workstation computer, protecting the data a rest on the hard drive. The protected system is in a controlled environment where the threat of a hostile overrun is not immediate, but where the ability to render protected data inaccessible is desired (e.g., a military forward deployment). The protected workstation is assigned to an identified user; this user has a Key Token that allows him access to that specific workstation

Application Note: Throughout this discussion of the security environment, this ST uses several terms to describe human interaction with the TOE. These terms are defined as follows:

authorities responsible for operational use	Humans at policy-making or leadership levels, not necessarily involved in direct, physical interaction with the SecureD TOE
authorized administrators	Humans with direct interaction with the SecureD TOE who administer SecureD and its security
authorized users	Humans with direct interaction with the SecureD TOE who use systems protected by SecureD

authorized operator;
authorized human operator;
human operator;
	Collective phrase that incorporates of “authorized administrators” and “authorized users”

those responsible for operational use	Collective phrase that incorporates all of “authorities responsible for operational use,” “authorized administrators,” and “authorized users”
Crypto Officer	A label for a conceptual role within the execution environment of the SecureD TOE; does not necessarily reflect any organizational position or job description of an associated human operator of the TOE
User	A label for a conceptual role within the execution environment of the SecureD TOE; does not necessarily reflect any organizational position or job description of an associated human operator of the TOE
Operator	A collective label for both the Crypto Officer and User roles within the execution environment of the SecureD TOE, when the distinction between those terms is not applicable or not necessary
Key Management System	KMS; the aggregate of policies, procedures, hardware, and software necessary for and capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD

3.1 Assumptions

This part of the security problem definition constrains the scope of the security problem by identifying what aspects of the TOE security environment are assumed to be axiomatic. It identifies the minimum physical and procedural measures required to maintain the security of SecureD.

3.1.1 Assumptions about physical aspects

Table 1. Assumptions about physical aspects

Assumption Identifier	Assumption Description
APh.FIPS_Certification	FIPS certification The SecureD TOE will be certified according to FIPS PUB 140-2 at Security Level 2 or higher.
APh.Crypto_Key_Management	Cryptographic Key Management The IT Environment contains a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD. This KMS will include the necessary policies and procedures for the proper creation, management, distribution, and destruction of cryptographic Key Tokens compatible with SecureD.
APh.Threat_Agent_Moderate	Moderate Attack Potential Systems containing SecureD are subject to deliberate attack by threat agents proficient-to-expert in the security behavior of the system, possessing specialized equipment, but possessing only public information concerning SecureD.

3.1.2 Assumptions about personnel aspects

Table 2. Assumptions about personnel aspects

Assumption Identifier	Assumption Description
APe.Administrator	Designated Administrators Authorities responsible for operational use of SecureD assign one or more individuals (System Administrators) to administer SecureD and its security. These authorized administrators are properly trained and are not careless, willfully negligent, nor hostile.
APe.Administrator_Docs	Documentation for Administrators System Administrators follow the policies and procedures defined in the SecureD documentation for secure installation, administration, and use of SecureD.
APe.Crypto_Token_Management	Cryptographic Token Management Those responsible for operational use of the SecureD TOE make use of a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) to enable operation of the SecureD TOE. System administrators follow the policies and procedures necessary for the proper creation, management, distribution, and destruction of cryptographic Key Tokens.
APe.Protect_From_Mods	SecureD Protection From Modification Those responsible for operational use of the SecureD TOE will physically protect SecureD from unauthorized modification.
APe.User	Authorized Users Authorities responsible for operational use of SecureD identify one or more individuals (Users) to use systems protected by SecureD. These authorized users are properly trained and are not careless, willfully negligent, nor hostile.

3.1.3 Assumptions about connectivity aspects

Table 3. Assumptions about connectivity aspects

Assumption Identifier	Assumption Description
ACo.No_Bypass	Controlled Media Connection Information cannot flow between the IDE controller of a protected system and the protected media except through SecureD.

3.2 Threats

This section of the ST continues the definition of the security problem by identifying and explaining known and presumed threats to the assets against which protection will be required, either by the SecureD TOE or by its operating environment. The identified threats will be explained in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. The threat agents are characterized by addressing expertise, resources, and motivation and the attacks are characterized by attack methods, any vulnerabilities exploited, and opportunity. Note that not all possible threats that might be encountered in the environment will be listed, only those which are relevant for secure operation of the SecureD TOE.

Table 4 identifies the threat agents, the actors in the attacks against the TOE and the assets it protects.

Table 4. Threat agent identification

Threat Agent	Threat Agent Characterization
Nonhuman Agents	Physical environment: Natural events; Man-made infrastructure events
	System hardware, firmware, and software
	Malware – worms, viruses, Trojans (in the host system) … not necessarily directed
Authorized Human Agents	Authorized, unprivileged user; untrained, benign, or malicious
	Authorized, privileged user (administrator); untrained, benign, or malicious
Unauthorized Human Agents	Cracker, hacker, or computer joy rider – novice to highly skilled; limited resources; weak motivation (Hypothetical threat agent; not present in the postulated operating environment.)
	Criminal; corporate raider – moderate to highly skilled; moderate means; financial motives (Hypothetical threat agent; not present in the postulated operating environment.)
	Foreign intelligence agent; military adversary – specialized training; potentially sophisticated tools and techniques; national interests
	Terrorist – novice to highly skilled; unpredictable resources; strong, but focused motivation (Hypothetical threat agent; not present in the postulated operating environment.)

Based on the conceptual operating scenario, the assumptions about personnel aspects, and the threat agent characterizations, the ST authors have identified the attack potential of the major threat agents (foreign intelligence agent; military adversary) as **Moderate.** These threat agents are proficient-to-expert in the security behavior of the system and possess (or can acquire without undue effort) specialized equipment, but possess only public information concerning SecureD.

Table 5 identifies the assets that require protection and describes the character of the protection the TOE provides to those assets.

Table 5. Asset identification

Asset Category	Protection Characterization
The TOE	SecureD needs to protect the algorithms and static cryptographic keying material instantiated in the gates and masks of the SecureD chip from modification or disclosure and ensure that they are accessible when needed, by those who need them
Cryptographic keying material	SecureD needs to manage and protect the dynamic cryptographic keying material from modification or disclosure during operational use. 1) Communication keys – the TDEA keys used for secure communication over the key interface. 2) Media keys – the AES keys used for encrypting the stored data on the media.
Protected media	SecureD protects the information contents of the protected media indirectly. SecureD encrypts the data stream to protect data at rest on the protected media. The choice of encryption algorithm, AES, determines the degree of protection SecureD provides. During operational use, threats to SecureD are also threats to the availability of the information contents of the protected media.

Table 6 refines the Protection Characterization of Table 5 by specifying whether the TOE is protecting the confidentiality, integrity, or availability (CIA) of the asset, or some combination of those properties. The three properties can never be completely separated; the definitions and solutions overlap among the three.

Table 6. CIA allocation

Asset Category	Asset	Security Properties		
		Confidentiality	Integrity	Availability
The TOE	algorithms	—	X	X
	static cryptographic keying material	X	X	X
Cryptographic keying material	communication keys	X	X	—
	media keys	X	X	—
Protected media	information contents	X (at rest)	—	X (during operation)

Table 7 presents some hypothetical attacks, based on the identified threat agents, the identified assets, and the postulated operating environment. Not all identified threat agents necessarily attack all identified assets. For example, a power failure does not threaten the confidentiality of the information content (at rest) on the protected media; therefore, there is no attack.

Table 7. Hypothetical Attacks

Threat Agent	Attack Exemplar	Asset
Nonhuman agents: physical environment	An event external to the host platform occurs that causes significant power fluctuations and subsequent system failure; this threatens the integrity of the TOE itself and the static keying material it contains.	The TOE
Nonhuman agents: host platform	The operating system software, embedded firmware, or component hardware of the host platform fails. This threatens the integrity of the TOE, the integrity and confidentiality of the static keying material it contains, and the confidentiality of the dynamic keying material it contains.	The TOE; Cryptographic keying material
Nonhuman agents: non-directed malware	Generic, malicious software (i.e., a virus, worm, or Trojan horse), not specifically directed at SecureD, begins execution on the host platform; it executes a variety of I/O commands, some of which are intentionally malformed, to retrieve available data from I/O controllers on the platform.	The TOE; Cryptographic keying material
Authorized human agents: authorized, unprivileged user; untrained, benign, or malicious	An authorized, unprivileged user of a system containing SecureD attempts to use an incorrect Key Token, threatening the availability of the information content of the protected media.	Protected media
Authorized human agents: authorized, privileged user (administrator); untrained, benign, or malicious	An authorized, privileged human user of a system containing SecureD uses administrative privileges to change the user split data keys on SecureD, threatening the availability of the information content of the protected media.	Protected media

Unauthorized human agents: foreign intelligence agent; military adversary	A host system, containing SecureD, is captured during a military operation; the confidentiality of the information content of the protected media is threatened.
	A foreign intelligence agent gains unobserved access to a system containing SecureD; the integrity of the TOE and its contents is threatened.
		The TOE;
		Cryptographic keying material;
		Protected media

Table 8. Postulated threat matrix

	Threat Agent		Confidentiality	Integrity	Availability
The TOE	Nonhuman agents	Physical Environment	TO. Physical_ Environment	TO. Physical_ Environment	TO. Physical_ Environment
		Host Platform	TO. Host_ Platform	TO. Host_ Platform	TO. Host_ Platform
		Non-directed malware	TO. Malware	TO. Malware	TO. Malware
	Authorized human agents	Authorized, unprivileged user	TO. Authorized_ Human	TO. Authorized_ Human	TO. Authorized_ Human
		Authorized, privileged user	TO. Authorized_ Human	TO. Authorized_ Human	TO. Authorized_ Human
	Unauthorized human agents	Foreign intelligence agent; military adversary	T. System_ Access	T. System_ Access	T. System_ Access
Cryptographic keying material	Nonhuman agents	Physical Environment	— N/A —	— N/A —	— N/A —
		Host Platform	— N/A —	— N/A —	— N/A —
		Non-directed malware	TO. Malware	TO. Malware	TO. Malware
	Authorized human agents	Authorized, unprivileged user	TO. Authorized_ Human	TO. Authorized_ Human	TO. Authorized_ Human
		Authorized, privileged user	TO. Authorized_ Human	TO. Authorized_ Human	TO. Authorized_ Human
	Unauthorized human agents	Foreign intelligence agent; military adversary	T. System_ Access	T. System_ Access	T. System_ Access
Protected media	Nonhuman agents	Physical Environment	— N/A —	— N/A —	— N/A —
		Host Platform	— N/A —	— N/A —	— N/A —
		Non-directed malware	— N/A —	— N/A —	— N/A —
	Authorized human agents	Authorized, unprivileged user	T. Cryptanalysis TO. Authorized_ Human	TO. Authorized_ Human	— N/A —
		Authorized, privileged user	T. Cryptanalysis TO. Authorized_ Human	TO. Authorized_ Human	— N/A —
	Unauthorized human agents	Foreign intelligence agent; military adversary	T. Cryptanalysis T. System_ Access	T. System_ Access	— N/A —

3.2.1 Threats to be countered by the TOE

The SecureD TOE needs to counter the following threats.

Table 9. Threats to be countered by the TOE

Threat Identifier	Threat Description
T.Cryptanalysis	Cryptanalysis for theft of information A human threat agent performs cryptanalysis on encrypted data at rest in order to recover information content.
T.System_Access	Unauthorized System Access An unauthorized human threat agent gains access to a system incorporating SecureD due to missing, weak, or incorrectly implemented access control allowing potential violations of integrity, confidentiality, or availability.

3.2.2 Threats to be countered in the TOE operational environment

The environment in which SecureD operates needs to counter the following threats to the SecureD TOE.

Table 10. Threats to be countered in the operational environment

Threat Identifier	Threat Description
TO.Authorized_Human	Authorized Human Access An authorized administrator or user; untrained, benign, or malicious, has access to SecureD allowing potential violations of integrity, confidentiality, or availability.
TO.Host_Platform	Host Platform Problems System hardware, firmware, and software fails allowing potential violations of integrity, confidentiality, or availability.
TO.Malware	Malware Malware – worms, viruses, Trojans; not necessarily directed – exists in the host system, allowing potential violations of integrity, confidentiality, or availability.
TO.Physical_Environment	Physical Environment Events Natural and man-made infrastructure events, outside the direct control of those responsible for operational use of SecureD, occur, allowing potential violations of integrity, confidentiality, or availability.
TO.Unauthorized_Human	Unauthorized Human Access An unauthorized human threat agent gains undetected access to a system incorporating SecureD due to missing, weak, or incorrectly implemented access control allowing potential violations of integrity, confidentiality, or availability.

3.3 Organizational security policies

This part of the security problem definition refines the security problem by identifying organizational policy constraints relating to the protection of the assets identified in section 3.2.1. The organization controlling the operational environment of the TOE establishes the organizational security policy, the rules, practices, and guidelines under which the TOE operates. The SecureD TOE and the operational environment of the TOE comply with the following organizational security policies.

Table 11. Organizational security policies

Policy Identifier	Policy Description
P.FIPS_Algorithms	Use of FIPS-approved algorithms The SecureD TOE shall use only FIPS-approved algorithms for its encryption techniques.
P.Guidance_Docs	Installation and usage guidance The SecureD TOE shall include guidance for its secure installation, administration, and use.
P.Physical_Control	Physical protection Those responsible for operational use of the SecureD TOE shall protect it physically from unauthorized use, modification, or destruction.

4 Security Objectives

4.1 Security objectives for the TOE

Table 12. Security objectives for the TOE

Objective Identifier	Objective Description
O.Crypto_Data_Separation	Separation of cryptographic data SecureD will provide complete separation between plaintext and encrypted data and between data and keys.
O.Crypto_Officer_Role	Crypto Officer role function SecureD will enable the *Crypto Officer* role to manage cryptographic assets and attributes.
O.Encryption	Encryption SecureD will use encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key.
O.Guidance_Docs	Guidance documentation To minimize operator errors, the SecureD TOE will include guidance for the secure installation, administration, and use of SecureD.
O.Integ_Sys_Data_Ext	Integrity of system data transferred externally SecureD will ensure the integrity of the encryption keys exchanged externally with the Key Token by using a protocol for data transfer that will permit error detection. This includes detecting errors in data received and encoding outgoing data to make it possible for the receiver to detect errors.
O.Maintain_Security_Domain:	Maintain security domain SecureD will protect its own data and resources and will maintain a security domain for TOE Security Function (TSF) execution to protect the TSFs from interference and tampering.
O.Physec_Tamper_Resistance	Tamper Resistance SecureD will be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum and that provides an indication of tampering if physical access to the TOE interior is attempted.
O.Restrict_Unauth_Actions	Restrict actions before authentication SecureD will restrict the actions an operator may perform before it authenticates the role of the operator.
O.Security_Data_Mgmt	Manage security-critical data SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.
O.Security_Roles:	Security roles SecureD will be able to distinguish the security-relevant roles *Crypto Officer* and *User.*
O.User_Role	User role function SecureD will enable the *User* role to activate the SecureD encryption functions.

4.2 Security objectives for the TOE operational environment

Table 13. Security objectives for the TOE operational environment

Objective Identifier	Objective Description
OE.Administrator	Designated Administrators Authorities responsible for operational use of SecureD assign one or more individuals (System Administrators) to administer SecureD and its security. These authorized administrators are properly trained and are not careless, willfully negligent, nor hostile.
OE.Crypto_Key_Mgmt	Cryptographic Key Management The IT Environment will provide a Key Management System (policies, procedures, hardware, and software) capable of creating cryptographic Key Tokens compatible with SecureD. This KMS will include the necessary policies and procedures for the proper creation, management, distribution, and destruction of cryptographic Key Tokens compatible with SecureD.
OE.FIPS_Certification	FIPS certification The SecureD TOE will be certified according to FIPS PUB 140-2 at Security Level 2 or higher.
OE.Guidance_Docs_Use	Guidance documentation usage To minimize operator errors, those responsible for operational use of SecureD will follow the guidance for the secure installation, administration, and use of the SecureD TOE.
OE.User	Authorized Users Authorities responsible for operational use of SecureD identify one or more individuals (Users) to use systems protected by SecureD. These authorized users are properly trained and are not careless, willfully negligent, nor hostile.

5 IT Security Requirements

This part of the ST defines the security requirements that the TOE and its IT environment must meet in order to achieve the corresponding security objectives defined in Section 4.

Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) comprise the security requirements for the TOE. The CC requires that the ST authors construct these, where possible, using security functional and assurance components defined, respectively, in [CC_PART2] and [CC_PART3]. This ST draws its requirements exclusively from [CC_PART2] and [CC_PART3]. The ST authors did not exercise their option to draw up new SFRs or SARs. This part of the ST also states the strength of TOE security function claims (SOF).

5.1 TOE security requirements

5.1.1 TOE security functional requirements

This section identifies the security functional requirements (SFRs) required of the TOE to meet its security objectives. The components taken from [CC_PART2] to specify the SFRs are listed in Table 14 together with an indication of whether the components are *iterated* (indicated by "(*N)" where N identifies the number of iterations) or *refined*.

Table 14. SecureD SFR components

Class	Family	Component
FCS – Cryptographic support	FCS_CKM	FCS_CKM.4 – Cryptographic key destruction
	FCS_COP	FCS_COP.1 [1] – Cryptographic operation (AES)
		FCS_COP.1 [2] – Cryptographic operation (TDEA)
FDP – User data protection	FDP_IFC	FDP_IFC.1 [1] – Subset information flow control (User Data Cryptography SFP)
		FDP_IFC.1 [2] – Subset information flow control (Key Token Communications SFP)
	FDP_IFF	FDP_IFF.1 [1] – Simple security attributes (User Data Cryptography SFP)
		FDP_IFF.1 [2] – Simple security attributes (Key Token Communications SFP)
FIA – Identification and authentication	FIA_UID	FIA_UID.1 – Timing of identification
FMT – Security management	FMT_MSA	FMT_MSA.1 [1] – Management of security attributes User Data Cryptography SFP)
		FMT_MSA.1 [2] – Management of security attributes (Key Token Communications SFP)
	FMT_MSA	FMT_MSA.2 – Secure security attributes
	FMT_MSA	FMT_MSA.3 [1] – Static attribute initialization (User Data Cryptography SFP)
		FMT_MSA.3 [2] – Static attribute initialization (Key Token Communications SFP)
	FMT_SMR	FMT_SMF.1 – Specification of Management Functions
	FMT_SMR	FMT_SMR.1 – Security roles
FPT – Protection of the TSF	FPT_RVM	FPT_RVM.1 – Non-bypassability of the TSP
	FPT_SEP	FPT_SEP.1 – TSF domain separation
FTP – Trusted path/channels	FTP_ITC	FTP_ITC.1 – Inter-TSF trusted channel

In the following SFRs, assignment and selection operations completed by the ST author are indicated using the same notation as used in [CC_PART2]. *Italicized text* indicates completed assignment and selection operations. **Emboldened text** indicates refinements of components.

Per *Request for Interpretation (RI) # 139 – American English Is an Acceptable Refinement*, this ST will consistently change the spelling of elements of CC requirements to use U.S. English spelling conventions. As permitted in RI # 139, the identification of this editorial refinement for the purposes of achieving a consistent spelling style is being performed only once (at the start of the enumeration of the requirements), so as not to clutter the requirements presentation.

5.1.1.1 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following:

- *Security Requirements for Cryptographic Modules [FIPS_140-2].*

5.1.1.2 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 [1] The TSF shall perform *user data encryption and user data decryption* in accordance with a specified cryptographic algorithm *AES in CBC mode* and cryptographic key sizes *of 128, 192, and 256 bits* that meet the following:

- *Advanced Encryption Standard (AES) [AES] and*
- *Recommendation for Block Cipher Modes of Operation [AES-MODES].*

FCS_COP.1.1[2] The TSF shall perform *Key Token communications encryption and Key Token communications decryption* in accordance with a specified cryptographic algorithm *TDEA Cipher Block Chaining with Three-key Triple DES (TCBC (KO 1))* and cryptographic key sizes *of 168 bits* that meet the following:

- *Data Encryption Standard (DES) [TDEA] and*
- *Triple Data Encryption Algorithm Modes of Operation [TDEA-MODES].*

5.1.1.3 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1[1] The TSF shall enforce the *User Data Cryptography SFP* on

a) Subjects: the two ATA interfaces
b) Information: ATA data
c) Operations: Information flow with encryption/decryption between the two ATA interfaces

Application Note: With respect to the User Data Cryptography SFP, the SecureD device has two ATA interfaces for user data, conventionally labeled “ATA IN” (host side) and “ATA OUT” (storage device side); either can be a source or a destination for an information flow.

Application Note: With respect to the User Data Cryptography SFP, a flow is equivalent to a read from a source ATA interface and an associated write to a destination ATA interface.

FDP_IFC.1.1[2] The TSF shall enforce the *Key Token Communications SFP* on

a) Subjects: the Key Interface
b) Information: key data
c) Operations: Information flow with encryption from the Key Interface to the TSF

Application Note: With respect to the Key Token Communications SFP, the SecureD device has a single interface for obtaining information from the Key Token, conventionally labeled the “Key Interface”. Information only flows into the TSF from the Key Interface, although protocol control signals can flow from the TSF to the Key Token through the Key Interface.

5.1.1.4 Simple security attributes (FDP_IFF.1)

5.1.1.4.1 FDP_IFF.1[1] User Data Cryptography SFP

FDP_IFF.1.1[1] The TSF shall enforce the *User Data Cryptography SFP* based on the following types of subject and information security attributes:

- *Subject Security Attributes:*
  ATA interface designation; and
- *Information Security Attributes:*
  Storage device address range,
  Media user key;
  Media resident key;
  Read/write flag;
  No other security attributes.

FDP_IFF.1.2[1] The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) *For information flows from ATA IN to ATA OUT, the TOE will permit information to flow only if:*
There is a Media Device Key associated with the storage device address range; and
The Read/Write flag associated with the storage device address range permits information to be written.

b) *For information flows from ATA OUT to ATA IN, the TOE will permit information to flow only if:*
There is a Media Device Key associated with the storage device address range; and
The Read/Write flag associated with the storage device address range permits information to be read.

FDP_IFF.1.3[1] The TSF shall enforce no[1] *additional information flow control SFP rules*.

FDP_IFF.1.4[1] The TSF shall provide the following

a) *For information flows from ATA IN to ATA OUT, the TOE will provide the capability to encrypt data using the Media Device Key and the storage address range associated with the information flow:*

b) *For information flows from ATA OUT to ATA IN, the TOE will provide the capability to decrypt data using the Media Device Key and the storage address range associated with the information flow:*

FDP_IFF.1.5[1] The TSF shall explicitly authorize an information flow based on the following rules: *None.*

FDP_IFF.1.6[1] The TSF shall explicitly deny an information flow based on the following rules: *None.*

5.1.1.4.2 FDP_IFF.1[2] Key Token Communications SFP

FDP_IFF.1.1[2] The TSF shall enforce the *Key Token Communications SFP* based on the following types of subject and information security attributes:

- *Subject Security Attributes:*
  Crypto Officer Key
  User Key; and

[1] Application Note: The ST author has refined the SFR by replacing “the” with “no” to improve readability.

- *Information Security Attributes:*
  Communications Key Set,
  Media user key;
  Media resident key;
  Read/write flag;
  No other security attributes.

FDP_IFF.1.2[2] The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) *For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as a Crypto Officer, the TOE will permit information to flow only if:*
   The Operator authenticates itself as a Crypto Officer associated with that instance of the TOE.

b) *For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as a User, the TOE will permit information to flow only if:*
   The Operator authenticates itself as a User associated with that instance of the TOE.

FDP_IFF.1.3[2] The TSF shall enforce no[2] *additional information flow control SFP rules*.

FDP_IFF.1.4[2] The TSF shall provide the following

a) *For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as an authenticated Crypto Officer, the TOE will provide the capability to encrypt and decrypt Key Token Communications using the Communications Key Set and the capability to modify the Communications Key Set and the Media Resident Keys:*

b) *For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as an authenticated User, the TOE will provide the capability to encrypt and decrypt Key Token Communications using the Communications Key Set and the capability to import User key data:*

FDP_IFF.1.5[2] The TSF shall explicitly authorize an information flow based on the following rules: *None.*

FDP_IFF.1.6[2] The TSF shall explicitly deny an information flow based on the following rules: *None.*

5.1.1.5 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow *Reset, Self Test, Show Status, and Zeroization* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: With respect to *Timing of identification*, the following list describes the unauthenticated services that the SecureD TOE supports.

Reset: This service erases all plaintext Critical Security Parameters (CSPs) that are stored in the SecureD TOE volatile memory.

Self Test: This service executes the cryptographic algorithm test for the two security functions (TDEA and AES), using a known answer and firmware integrity tests using a 16-bit EDC.

Show Status: This service provides the current status of the TOE.

Zeroization: This service erases all plaintext Critical Security Parameters (CSPs) that are stored in the SecureD TOE (volatile and non-volatile) memory.

[2] Application Note: The ST author has refined the SFR by replacing “the” with “no” to improve readability.

5.1.1.6 Management of security attributes (FMT_MSA.1)

5.1.1.6.1 FMT_MSA.1 [1] User Data Cryptography SFP

FMT_MSA.1.1 [1] The TSF shall enforce the *User Data Cryptography SFP* to restrict the ability to *modify* the security attributes *Storage device address range* and *Media user key* to *the User role*.

5.1.1.6.2 FMT_MSA.1 [2] Key Token Communications SFP

FMT_MSA.1.1 [2] The TSF shall enforce the *Key Token Communications SFP* to restrict the ability to *modify* the security attributes *Communications Key Set and Media Resident Keys* to *the Crypto Officer role*.

5.1.1.7 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.1.8 Static attribute initialization (FMT_MSA.3)

5.1.1.8.1 FMT_MSA.3 [1] User Data Cryptography SFP

FMT_MSA.3.1 [1] The TSF shall enforce the *User Data Cryptography SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 [1] The TSF shall allow the *User role* to specify alternative initial values to override the default values when an object or information is created.

5.1.1.8.2 FMT_MSA.3 [2] Key Token Communications SFP

FMT_MSA.3.1 [2] The TSF shall enforce the *Key Token Communications SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 [2] The TSF shall allow the *Crypto Officer role* to specify alternative initial values to override the default values when an object or information is created.

5.1.1.9 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *Set Crypto Officer Key, Set Device Keys, Set User Key, and Set Media Resident Keys*.

5.1.1.10 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles *Crypto Officer and User*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.1.11 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.1.12 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.1.13 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- *Crypto Officer Authentication*
- *Set Crypto Officer Key*
- *Set Device Keys*
- *Set Media Resident Keys*
- *Set Media User Keys*
- *Set User Key*
- *User Authentication*

Application Note: With respect to the inter-TSF trusted channel, the *remote trusted IT product* is the Key Management System (policies, procedures, hardware, and software), which communicates with the TOE through the Key Interface.

5.1.2 Explicitly stated IT security requirements

This ST draws its requirements exclusively from [CC_PART2] and [CC_PART3]. The ST authors did not exercise their option to draw up new SFRs or SARs; therefore, this ST contains no explicitly stated IT security requirements.

5.1.3 Strength of function claims

This Security Target does not claim an explicit strength of function for any security functional requirement it contains. SecureD does include probabilistic or permutational mechanisms in the form of the cryptographic operations SFRs (FCS_COP.1.1 [1] and FCS_COP.1.1 [2]). These are the only SFRs that are probabilistic or permutational in nature. Evaluation of SOF claims for cryptography is out of scope of the CC, therefore this Security Target can make no explicit claims regarding the SOF of the cryptographic SFRs.

5.1.4 TOE security assurance requirements

The security assurance requirements (SARs) for this ST include the EAL4 SARs in Part 3 of the CC, augmented by AVA_VLA.3. The following table lists these SARs and this ST incorporates them verbatim from Part 3 of the CC by reference.

Table 15. SecureD EAL4 SAR components, augmented with AVA_VLA.3

Assurance class	Assurance components
Class ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Class ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.3 Moderately resistant

5.2 Security Requirements for the IT Environment

The SecureD TOE has dependencies on the IT environment. Table 16 identifies the SFRs that the IT environment must satisfy. The asserted requirements for the IT environment are refined from those specified in [CC_PART2].

In the following SFRs, the ST author indicated completed assignment and selection operations by using the same notation as used in [CC_PART2]. *Italicized text* indicates assignment and selection operations. **Emboldened text** indicates refinements of components. As recommended in [CC_PART1] A.2.6, the requirements stated here were all refined to replace "TSF" with "IT Environment" so that there is no misunderstanding as to the active agent in the requirement.

Per *Request for Interpretation (RI) # 139 – American English Is an Acceptable Refinement*, this ST will consistently change the spelling of elements of CC requirements to use U.S. English spelling conventions. As permitted in RI # 139, the identification of this editorial refinement for the purposes of achieving a consistent spelling style is being performed only once (at the start of the enumeration of the requirements), so as not to clutter the requirements presentation.

Table 16. Security functional requirements for the IT environment

Class	Family	Component	Iterated	Refined
FCS – Cryptographic support	FCS_CKM	FCS_CKM.1 – Cryptographic key generation	2	X

5.2.1 Cryptographic support (FCS)

5.2.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 [1] The **IT Environment**[3] shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *none* and specified cryptographic key sizes *of 128, 192, and 256 bits* that meet the following: *none*.

FCS_CKM.1.1 [2] The **IT Environment**[4] shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *none* and specified cryptographic key sizes *of 168 bits* that meet the following: *none*.

Application Note: With respect to cryptographic key generation, HDD supplies a software utility with its products that incorporate the TOE, which produces Key Tokens compatible with SecureD. Authorities responsible for operational use of SecureD can use this utility as a part of a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials compatible with SecureD. This Key Management System is the remote trusted IT product that communicates with the TOE through the Key Interface.

[3] Application Note: The ST author has refined the SFR by replacing "TSF" with "IT Environment" so that there is no misunderstanding as to the active agent in the requirement.

[4] Application Note: The ST author has refined the SFR by replacing "TSF" with "IT Environment" so that there is no misunderstanding as to the active agent in the requirement.

6 TOE Summary Specification

This TOE Summary Specification defines the instantiation of the security requirements for the TOE. It presents a high-level definition of the security functions and assurance measures, and traces them to the TOE Functional and Assurance security requirements.

6.1 TOE security functions

The Security Functions described in this TOE Summary Specification implement the TOE Security Functional Requirements (SFRs) defined in Section 5.1.1.

Figure 9 and Table 17 identify the various cryptographic keys that the discussion of the TOE security functions will address.

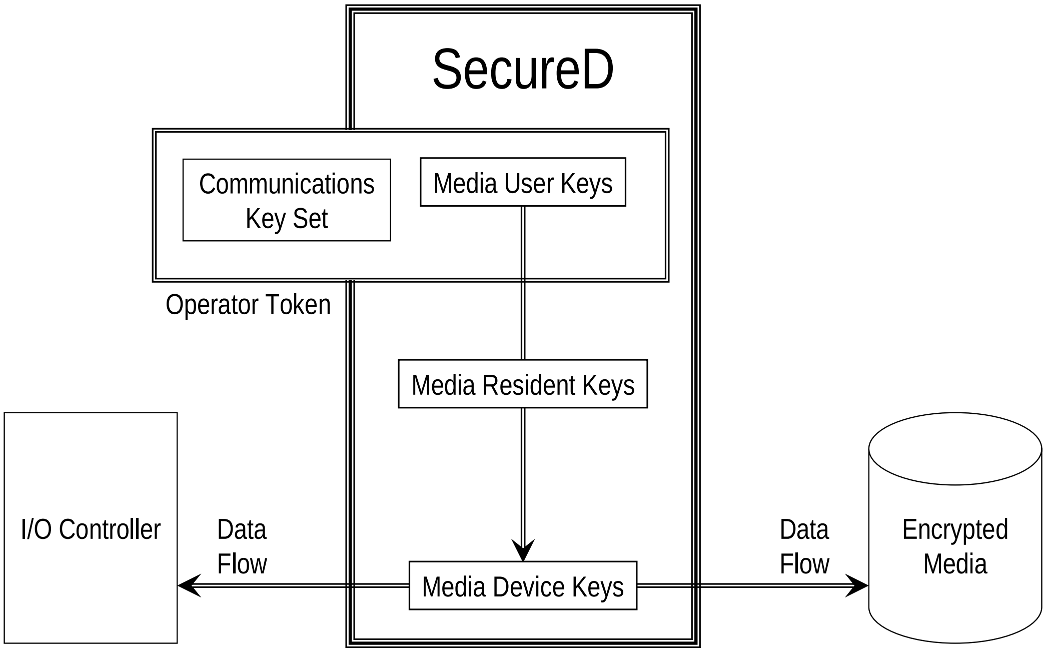

Figure 9. Encryption key labeling conventions

Table 17. Encryption key identification

Key Set Identification	Key Label	Key Description
Communications Key Set	Crypto Officer Key	TDEA 168-bit key for encrypting communications between an operator token and SecureD; used to authenticate Operator in Crypto Officer role
	User Key	TDEA 168-bit key for encrypting communications between an operator token and SecureD; used to authenticate Operator in User role
	Device Key 1	TDEA 168-bit key for encrypting Media User Key
	Device Key 2	TDEA 168-bit key for encrypting Media User Key
Media Encryption Key Set	Media User Key	User component of AES media keys (Media Device Key)
	Media Resident Key	SecureD component of AES media keys (Media Device Key)
	Media Device Key	AES 128-, 192-, or 256-bit key for encrypting and decrypting data to and from the protected storage media

6.1.1 Cryptographic support function

The SecureD TOE implements two types of cryptographic operations. One is the AES encryption and decryption of user data. The other is the TDEA encryption and decryption of the AES keys and other parameters governing the operation of the TOE. Key management in the general sense is outside the scope of the SecureD TOE, and is an assumption of the TOE operational environment (APh.Crypto_Key_Management); however, the SecureD TOE does implement key zeroize functions.

A dedicated module within the SecureD TOE handles communication through the Key Interface. At power up, or when a new Key Token is introduced, this module downloads the AES keys from the Key Token, decrypts and verifies the integrity of the keys, merges the resident and user parts of the keys, and stores them in the correct locations in the Encryption System.

- Crypto Officer message encryption and decryption: The Crypto Officer role has the privilege to write the Communications Key Set and the AES Media Resident Keys. These keys enter SecureD through the key interface with 168-bit TDEA Cipher Block Chaining with Three-key Triple DES (TCBC (KO 1)) encryption and are decrypted by the TOE. SecureD encrypts Crypto Officer role messages from SecureD to the Key Token with the same encryption mechanism before passing them over the key interface to the Key Token. (FCS_COP.1[2])
- User message encryption and decryption: The User role provides the AES Media User Keys. As with Crypto Officer messages, these keys enter SecureD through the key interface with 168-bit TDEA Cipher Block Chaining with Three-key Triple DES (TCBC (KO 1)) encryption and are decrypted by the TOE. The TOE encrypts User role messages from the TOE to the Key Token with the same encryption mechanism before passing them over the key interface to the Key Token. (FCS_COP.1[2])

A separate Encryption System is responsible for the AES encryption/decryption of the user data, as well as selection of the right key for the encryption/decryption based on sector address information from the IDE Module. The Encryption System performs AES encryption and decryption in CBC mode using keys of length 128, 192, and 256 bits. The actual key used for media encryption, the Media Device Key, is created dynamically in SecureD volatile memory by performing combinatorial function on the Media Resident Key, loaded from the Crypto Officer token and stored in SecureD non-volatile memory, and the Media User Key, supplied from the User token.

- User Data encryption and decryption: SecureD encrypts data written to the storage medium and decrypts data read from the storage medium. The Media Resident Keys are stored in an array in the SecureD. The Media User Keys are presented from the Key Token to the SecureD. The Key Token also identifies the element from the Media Resident Key array to be used to complement each Media User Key and the storage range to be associated with the resulting

Media Device Key. The TOE uses the sector number of each block to select the Media Device Key for the process. The smallest block that can be processed is one sector (512 bytes). (FCS_COP.1[1])

The SecureD TOE implements the following cryptographic key management function:

- Zeroize: At power on, or when a Key Token is inserted, the Media User Keys are loaded and merged with the Media Resident Keys to form the Media Device Keys. The Media Device Keys are the keys used for encryption/decryption of user data; disclosure of these keys will give an attacker immediate access to the protected user data. Therefore, as required by FIPS 140-2, the TOE contains two separate hardware zeroization modules, controlled by two separate input pins, to provide for zeroization of key data. Zeroization consists of writing zeroes over critical registers and memory locations.

  One function will zeroize all the current Media Device Keys in volatile memory. This function is invoked whenever a Key Token is inserted, after the timeout period when a key token is removed, and on power-off.

  The other function will zeroize the Communications Key Set and the Media Resident Keys, both of which reside in non-volatile memory; the SecureD will revert to the factory default keys, and the Crypto Officer will have to re-initialize the unit before it can be used again. This function is invoked by triggering the zeroize pins on the utility interface.

  SecureD incorporates hardware functions for zeroizing the data encryption keys. Whenever a Key Token is removed from the SecureD device, the keys in volatile memory are zeroized after a selectable interval (0 to 65534 minutes, or the value 65535, which is interpreted as indefinitely). This permits operation in situations where access to the hard drive contents must be stopped instantly, where access may be desired for a limited period, or where access may be permitted for an indeterminate period. In all cases, the information in volatile memory, which includes the media encryption keys, is lost on power cycling.(FCS_CKM.4)

6.1.2 User data protection function

The SecureD TOE enforces two Security Functional Policies to protect user data, the *User Data Cryptography SFP* and the *Key Token Communications SFP*.

The *User Data Cryptography SFP* applies to user data that traverses the SecureD TOE between its ATA interfaces. SecureD applies AES encryption to this traffic, based on the information flow, the storage device address range, the Media Device Key and the Read/write flag (presented by the User Key Token), and the Media Resident Key (loaded previously into SecureD from the Crypto Officer Key Token). The Encryption System, which performs the actual encryption on the flow of user data, enforces this SFP. To ensure complete separation of the clear and encrypted data, the host side and the device side of SecureD each has its own hardware IDE/ATA controller. The IDE/ATA controllers are physically isolated from each other by the IDE Module, which provides separate interfaces for the IDE/ATA controllers to the Encryption System. The only physical data path between the host side and the device side of SecureD is through the Encryption System. No user data can flow directly from one ATA controller to the other. (FDP_IFC.1[1]; FDP_IFF.1[1])

The *Key Token Communications SFP* applies to user-provided key data supplied to the TSF through the Key Interface TSFI. SecureD applies TDEA encryption to this traffic, based on Operator role and Crypto Officer Key or User Key. The Key Interface enforces this SFP by requesting key data from the Key Token with an encrypted protocol command. Only a Key Token for an authorized Crypto Officer or User associated with that instance of the SecureD can recognize the command and respond appropriately; any other Key Token will respond with an error. Only after the Key Token has authenticated itself will the Key Interface permit an information flow from the Key Token to the TSF. (FDP_IFC.1[2]; FDP_IFF.1[2])

6.1.3 Identification and authentication function

Identification and authentication, role allocation, and trusted channel communications are tightly integrated in the SecureD TOE. The same module within the TOE that supports the trusted channel functionality also authenticates the Operator identity and validates the role claimed for that identity.

To provide assured identification, SecureD uses TDEA encryption for Operator authentication.

- If a Key Token claiming the Crypto Officer role is presented, SecureD will use the Crypto Officer Key to query the Key Token. A legitimate Crypto Officer Key Token will possess the correct Crypto Officer Key and be able to respond to this message. Any other Key Token will not be able to decipher the Crypto Officer message and will return an error.
- If a Key Token claiming the User role is presented, SecureD will use the User Key to query the Key Token. A legitimate User Key Token will possess the correct User Key and be able to respond to the message. Any other Key Token will not be able to decipher the User message and will return an error.

When the Operator identity is authenticated and the Role validated, the SecureD TOE then permits execution of the TSFs allocated to that role. (FIA_UID.1.2)

Until the SecureD authenticates the Operator and then validates the Role, the TOE will only permit four functions to be executed: *Reset, Self Test, Show Status, and Zeroization.* These functions are independent of role and are even available when no Key Token is present. (FIA_UID.1.1)

- Show Status: The status module within the SecureD TOE runs continuously whenever power is applied to the SecureD TOE. This service indicates to the Operator the state of the device via an output-only interface. In the HDD products incorporating the TOE, this output is connected to a red/green bipolar LED, to provide user-visible status signals.
- Self Test: This service executes the cryptographic algorithm test for the two encryption functions (TDEA and AES), using a known answer, and executes embedded firmware integrity tests, using a 16-bit Error-Detecting Code (EDC). All these services are performed immediately after power is applied. The TDEA test is also performed when a new Key Token is introduced to the TOE. Both the TDEA and AES tests run periodically whenever an authenticated Key Token is present.
- Reset and Zeroization provide the capability to destroy any plaintext cryptographic keying material that may be present in the SecureD TOE.
  - Reset: This service erases all plaintext key data that is stored in the SecureD TOE volatile memory. It executes when the Reset input is activated, on demand whenever a new Key Token is introduced to the SecureD TOE, and whenever a key lifetime expires.
  - Zeroization: This service erases all plaintext key data (the Communications Key Set, the Media Resident Keys, and the contents of relevant registers and buffers) that is stored in the SecureD TOE (volatile and non-volatile) memory. This service is activated through a separate physical interface. If it is activated, the SecureD reverts to the factory default keys, and the Crypto Officer will have to re-initialize the unit before it can be used again.

6.1.4 Security management function

The SecureD TOE maintains two distinct and separate Operator roles: Crypto Officer and User. Each role is allocated a subset of the security functions provided by the TOE; the two subsets are disjoint. (FMT_SMR.1.1) SecureD uses the same mechanisms for role association that it uses for Operator identification and authentication and for establishing an inter-TSF trusted channel, to bind Operators to roles. (FMT_SMR.1.2)

- Crypto Officer

  The Crypto Officer role provides all of the services necessary for the Crypto Officer to manage the keying material stored in the SecureD TOE. (FMT_SMF.1)

Security Function	Key Data	Action
Crypto Officer Authentication	Crypto Officer Key	Read
Set Crypto Officer Key	Crypto Officer Key	Write
Set Device Keys	Device Key 1	Write
	Device Key 2	Write
Set User Key	User Key	Write
Set Media Resident Keys	Media Resident Keys	Write

- User

  The User role provides all of the services necessary for the encryption and decryption of data passing through the SecureD TOE.

Security Function	Key Data	Action
User Authentication	User Key	Read
Erase Media Device Keys	Media Device Keys	Write
Set Media User Keys	Media User Keys	Write
	Media Resident Keys	Read
	Media Device Keys	Write
Encrypt Data	Media Device Keys	Read
Decrypt Data	Media Device Keys	Read

The SecureD TOE applies the *Key Token Communications SFP* to manage security attributes (user-provided key data) retained in the TSF. Specifically, the TSF restricts the ability to modify the security attributes *Communications Key Set* and *Media Resident Keys* to the Crypto Officer role. The Key Interface enforces the SFP based on authentication of the Key Token (6.1.3) presented to the SecureD TOE via a trusted channel (6.1.6) from a key management system (policies, procedures, hardware, and software). The Key Interface interrogates the Key Token for a new Communications Key Set and new Media Resident Keys. The Key Interface then stores (*Set Crypto Officer Key, Set Device Keys, Set User Key*) the new Communications Key Set (if supplied) for subsequent Key Interface communications and provides (*Set Media Resident Keys*) the new Media Resident Keys (if supplied) to the Encryption System for use in subsequent user data encryption. (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1)

6.1.5 Protection of the TSF function

The SecureD TOE is a self-contained module and does not share resources (memory, processors, registers, etc.) with any other components of the system that contains it. The cryptographic modules and the data path for the user data are all implemented in hardware only. Embedded firmware is loaded during manufacture of the device. The integrity of the embedded firmware is protected by a checksum. At power-on, a checksum verification is performed on the embedded firmware, and known-answer tests are performed on the AES and TDEA encryption engines. Periodically during operation, a known answer test is performed on the AES encryption engine using information from the Key Token. Since the keys and the known answers have to be correctly decrypted for the AES test to succeed, this effectively also verifies the TDEA engine. (FPT_SEP.1)

The data path through the TOE is constructed in hardware only. To enforce separation between the security domains of subjects in the TSC, that is, complete separation of the clear and encrypted data, the host side and the device side of SecureD each has its own IDE/ATA controller. The only physical data path between the host side and the device side of SecureD is through the Encryption System. No user data can flow directly from one ATA controller to the other. (FPT_SEP.1.2)

SecureD will not allow clear data to be written to the storage media. An independent hardware module continuously compares the data going into the TOE with the data going out. If more than a fixed number of bytes are equal, an alarm is raised. However, to retain compatibility with the ATA specification, SecureD will allow command parameters to pass through the data channel to the device. The alarm module will independently check the control signals governing the current transfer, and determine if a clear write is consistent with the values in the control registers. If not, the TOE will enter an alarm state and block the data path through a separate hardware function. Reading of clear data is allowed, should unencrypted data for any reason already be present on the disk. The clear read capability is intended for the case where a hard drive and a CD-ROM player are connected to the same SecureD device. This will allow the user to read a clear CD-ROM. (FPT_RVM.1)

6.1.6 Trusted path/channels function

The Key Interface is the entrance point for all the cryptographic keys used for operating SecureD. This interface is both physically and logically distinct from all other interfaces to the SecureD TOE. Its sole purpose is to provide an interface for loading encryption keys and other key data from authorized Operators into the SecureD TOE. At the hardware level, the Key Interface conforms to the *ISO/IEC 7816-1:1998 – Identification cards interface* standard. Keying material is managed externally with a user-provided key management system (policies, procedures, hardware, and software). The Key Token acts on behalf of the “remote trusted IT product” (the Key Management System) to provide the user data (Communications Key Sets and Media Encryption Key Sets) to the TSF.

To provide assured identification of its end points and protection of the channel data from modification or disclosure, SecureD uses TDEA encryption for both Operator authentication (endpoint authentication) and data transfer (protection of channel data).

- If a Key Token claiming the Crypto Officer role is presented, SecureD will use the Crypto Officer Key to query the Key Token for a new key set to be downloaded. A legitimate Crypto Officer Key Token will possess the correct Crypto Officer Key and be able to respond to this message. Any other Key Token will not be able to decipher the Crypto Officer message and will return an error. If authentication fails, the Key Interface will wait a predetermined interval (no less than one second) before attempting reauthentication; this mitigates “wardialling” attacks.

- If a Key Token claiming the User role is presented, SecureD will use the User Key and send a message asking for Media User Keys. A legitimate User Key Token will possess the correct User Key and be able to respond to the message. If authentication fails, the Key Interface will wait a predetermined interval (no less than one second) before attempting reauthentication; this mitigates “wardialling” attacks.

- To protect the key data when in transit, SecureD encrypts all communications over the Key Interface with 168-bit TDEA encryption. Four different keys are used for the key transfer protocol; the Crypto Officer Key, the User Key, and two communications (wrapping) keys.

- The Key Interface uses a checksum to verify the integrity of received keying material, and discards keys that are not properly verified. The Key Interface does NOT return any error messages when it discards unverified keying material.

All of these measures combined provide the security functions necessary to satisfy the SFRs for an Inter-TSF trusted channel, as defined in 5.1.1.13 Inter-TSF trusted channel (FTP_ITC.1).

6.1.7 Strength of function

This Security Target does not claim an explicit strength of function for any security functional requirement it contains.

6.2 TOE assurance measures

This section specifies the assurance measures applied to the development of SecureD® by High Density Devices AS. It demonstrates that the TOE was methodically designed, tested, and reviewed and thus satisfies the requirements of the EAL4+ SARs described in Section 5.1.4.

HDD applied the following assurance measures to satisfy the Common Criteria EAL4+ assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process assurance

6.2.1.1 Configuration management

Because multiple developers are working on SecureD, HDD controls changes to the TOE implementation representation with the support of automated tools. In particular, these automated tools support the numerous changes that occur during development and ensure that those changes are authorized. HDD applies configuration management measures to ensure that configuration items are uniquely identified, that documented procedures are used to control and track changes that are made to the TOE, and that security flaw reports are not lost or forgotten.

HDD ensures changes to the implementation representation are controlled, that TOE-associated configuration item modifications are properly controlled, and that developers can track security flaws to their resolution. HDD performs configuration management on the CM documentation, the life-cycle documentation, the guidance documentation, the TOE design documentation, the TOE implementation representation, the test plans, test procedures, test analyses, and test results, the vulnerability assessments, and security flaw reports.

These Configuration Management assurance measures are documented in:

- *High Density Devices Configuration Management Policy* – The HDD CM Policy describes the corporate CM System and identifies the roles and responsibilities of the various participants in the CM process.
- *SecureD Configuration Management Plan* – The SecureD CM Plan describes the instantiation of the CM system that supports the SecureD development. It maps the repository structure, describes the automated tools, and explains how the tools are used in the system
- *Configuration Item & Product Labeling* –The Configuration Item & Product Labeling document defines the unique naming conventions for the product and CIs and lists the configuration item categories.
- *Concurrent Versions System Implementation* – Details of using the Concurrent Versions System (CVS) to support SecureD development.
- *Modification Request Registry System* – Details of using the Modification Request Registry System (MRRS) to support SecureD development.
- *SecureD CC v1.6 Configuration Items.xls* – Spreadsheet identifying the CIs comprising the TOE.

The Configuration Management assurance measures satisfy the following assurance requirements:

- ACM_AUT.1 Partial CM automation
- ACM_CAP.4 Generation support and acceptance procedures
- ACM_SCP.2 Problem tracking CM coverage

6.2.1.2 Life-cycle

Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance. HDD manages life-cycle support with a life-cycle model, corporate security practices, and well-defined development tools and techniques.

The HDD Corporate Information Security Policy describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. HDD has also established a model for the development and maintenance of the TOE. The developers' tools and techniques documentation identifies the development tools being used for the TOE, the implementation-dependent options of the development tools, and the meaning of all statements and implementation-dependent options used in the implementation.

These Life-cycle assurance measures are documented in:

- *Corporate Information Security Policy*
- *Product Life-Cycle Policy*
- *Tools & Techniques*

Details of the security measures and version control tools, specific to the SecureD product, are documented in:

- *SecureD Configuration Management Plan*
- *Concurrent Versions System Implementation*
- *Modification Request Registry System*

The Life-cycle assurance measures satisfy the following assurance requirements:

- ALC_DVS.1 Identification of security measures
- ALC_LCD.1 Developer defined life-cycle model
- ALC_TAT.1 Well-defined development tools

6.2.2 Delivery and guidance

HDD maintains a policy for delivery of its products that establishes procedures to ensure that the SecureD is generated correctly and that a recipient receives the SecureD that HDD intended to send, without any modifications. The delivery procedures describe everything that is necessary to maintain security when distributing versions of SecureD to a user's site. The delivery policy describes how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site. The delivery policy also l describes how the various procedures allow detection of attempts to masquerade as HDD, even in cases in which HDD has sent nothing to the user's site.

HDD provides guidance with the SecureD that describes how to determine secure delivery of the SecureD, how to install it, and how to initialize it. The installation procedures, included in the package documentation, describe the steps necessary to install and operate SecureD in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration.

The Delivery and Guidance assurance measures are documented in:

- *Product Delivery Policy*
- *SecureD Production & Distribution*
- *SecureD Evaluated Configuration Guide, v01.30, 10-14-2005*

The Delivery and Guidance assurance measures satisfy the following Assurance requirements:

- ADO_DEL.2 Detection of modification
- ADO_IGS.1 Installation, generation, and start-up procedures
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

6.2.3 Development

HDD prepared an informal functional specification that describes the SecureD TOE and the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions, and error messages. The informal functional specification is an instantiation of the SFRs contained in this ST. It includes an analysis that shows that all the SFRs are addressed.

HDD prepared an informal model of the TOE Security Policy that corresponds to the Functional Specification. The TSP model describes the rules and characteristics of all policies of the TSP that can be modeled and demonstrates that it is consistent and complete with respect to all such policies of the TSP.

HDD prepared an informal high-level design of the SecureD TOE that describes the TSF in terms of subsystems. For each subsystem of the TSF, the high-level design describe its purpose and function, and identified the security functions contained in the subsystem. The high-level design identified all interfaces to the subsystems of the TSF and identified which of the interfaces to the subsystems of the TSF are externally visible. The high-level design described the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions, and error messages, as appropriate.

HDD prepared an informal low-level design of the SecureD TOE that describes the TSF in terms of modules. For each module of the TSF, the low-level design described its purpose, function, interfaces, dependencies, and the implementation of any TSP-enforcing functions. The low-level design defined the interrelationships between the modules in terms of provided security functionality and described the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions, and error messages, as appropriate.

HDD presented the implementation representation in the form of source code, firmware, and hardware drawings to capture the detailed internal workings of the TSF in support of analysis.

HDD prepared an informal correspondence analysis between the various TSF representations (i.e. TOE summary specification, functional specification, high-level design, low-level design, and implementation representation) to demonstrate the correct and complete instantiation of the requirements to the least abstract TSF representation provided.

In summary, the Design Documentation for the SecureD consists of a functional specification, a security policy model, a high-level design, six low-level designs, source code, and correspondence analyses. These documents serve to describe the security functions of the TOE, the architecture of the TOE (in terms of subsystems), its interfaces both external and between subsystems, and correspondence between the available design abstractions (including the ST).

The Development assurance measures are documented in:

- *SecureD Functional Specification*
- *SecureD Informal Security Policy Model*
- *SecureD High-level Design*
- SecureD Low-Level Design Documents
  - *AES Core Design Specification* - This document describes the implementation of the Advanced Encryption Standard (AES) encryption algorithm in SecureD.
  - *Encryption System Design Specification* - This document describes the implementation of the Encryption System in SecureD, which encrypts or decrypts all data received from the bus interface.
  - *IDE Module Design Specification* - This document describes the implementation of the IDE Module in SecureD, which provides the external interface for the user data.
  - *SecureD FW – Design Specification* - This document describes all Firmware in the SecureD TOE, i.e. for all modules.
  - *SecureD and Pata Design Specification* - This document describes the “glue” logic that surrounds the other modules.
  - *uC_System Design Specification* - This document describes the implementation of the uC_System in SecureD, which loads the keys and vectors used in the Encryption System, communicates with external units, and monitors the system.
- *Source Code Subset* – The subset is a sample of the representation of the security functions.
- *Correspondence Analysis*

The Design Documentation security assurance measures satisfy the following security assurance requirements:

- ADV_FSP.2 Fully defined external interfaces
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF

- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ADV_SPM.1 Informal TOE security policy model

6.2.4 Tests

HDD performed functional testing of the SecureD TOE to establish that it exhibits the properties necessary to satisfy the functional requirements of this ST. HDD prepared test plans, test procedure descriptions, and expected test results and recorded actual test results. The test plans identify the security functions to be tested and describe the goals of the tests. The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. The expected test results present the anticipated outputs from a successful execution of the tests. The test plans, test procedures, and expected test results were consolidated into a single volume, the *SecureD CC Test Plan.* The test results from execution of the tests demonstrate that each tested security function behaved as specified.

HDD performed a test coverage analysis to establish that the SecureD TOE was tested against its functional specification in a systematic manner. The analysis of the test coverage demonstrates that a correspondence between the tests identified in the test documentation and the TSF as described in the functional specification exists and is complete.

HDD performed a test depth analysis to establish that the tests identified in the test documentation are sufficient to demonstrate that the SecureD TOE operates in accordance with its high-level design. The subsystems of a TSF provide a high-level description of the internal workings of the TSF. By testing the SecureD TOE at the level of the subsystems, in order to demonstrate the presence of any flaws, HDD provides assurance that the TSF subsystems have been correctly realized.

The Tests assurance measures are documented in:

- *SecureD CC Test Plan*
- *SecureD Test Coverage Analysis*
- *SecureD – Depth of Testing Analysis*

The Tests assurance measures satisfy the following assurance requirements:

- ATE_COV.2 Analysis of coverage
- ATE_DPT.1 Testing: high-level design
- ATE_FUN.1 Functional testing

In addition, HDD supplied a TOE, suitable for testing, to the CCTL to support the following assurance requirement:

- ATE_IND.2 Independent testing - sample

6.2.5 Vulnerability assessment

HDD performed an analysis of the guidance documentation to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, that secure procedures for all modes of operation have been addressed, and that insecure states are easy to detect.

Each probabilistic or permutational mechanism used by the TOE must satisfy the SOF-Basic requirements. SecureD does include the probabilistic or permutational mechanism in the form of the cryptographic operations. However, this is out of scope for a CC evaluation, therefore, HDD did not perform a Strength-of-Function analysis because the strength of function analysis of the cryptographic algorithms is not part of the evaluation.

HDD performed a vulnerability analysis to ascertain the presence of security vulnerabilities, and to confirm that attackers possessing a moderate attack potential cannot exploit them in the intended environment for the TOE.

Results of the Vulnerability Assessment assurance activities are presented in:

- *SecureD Misuse of Guidance Analysis*
- *SecureD Vulnerability Analysis*

The Vulnerability Assessment assurance measures satisfy the following assurance requirements:

- AVA_MSU.2 Validation of analysis
- AVA_VLA.3 Moderately resistant

7 PP Claims

This Security Target makes no claims of conformance with any existing Protection Profile.

8 Rationale

8.1 Security objectives

The security objectives are a concise statement of the intended solution to the security problem. There are two types of security objectives:

a) *Security objectives for the TOE:* these describe the security functionality that the TOE will provide.

b) *Security objectives for the TOE operational environment:* these describe properties of the operational environment of the TOE, necessary in order for the TOE to be able to provide its security functionality.

This ST contains a security objectives rationale that shows which security objectives address which threats, organizational security policies (OSPs), and assumptions and that these security objectives effectively address the threats, OSPs, and assumptions.

Table 18 presents the basic evidence that:

1. The security objectives for the SecureD TOE trace back to aspects of the identified threats SecureD counters or to organizational security policies SecureD meets.
   - Each security objective for SecureD traces back to at least one threat or organizational security policy.
   - This complete traceability implies that the security objectives rationale is complete, the threats and organizational security policy statements are complete, and the security objectives for SecureD have a useful purpose.
2. The security objectives for the environment trace back to aspects of the identified threats SecureD does not completely counter or to organizational security policies or assumptions SecureD does not completely meet.
   - Each security objective for the environment traces back to at least one assumption, threat, or organizational security policy.
   - This complete traceability implies that the security objectives rationale is complete, the threats, assumptions, and organizational security policy statements are complete, and the security objectives for the environment have a useful purpose.

Table 18. Mapping TOE security objectives to the security environment

Objective Identifier	Security Problem Identifier																		
	Assumption Identifier									Threat Identifier							Policy Identifier		
	APh.Crypto_Key_Management	APe.Administrator	APe.Administrator_Docs	APe.Crypto_Token_Management	APh.FIPS_Certification	APe.Protect_From_Mods	APh.Threat_Agent_Moderate	APe.User	ACo.No_Bypass	T.Cryptanalysis	T.System_Access	TO.Authorized_Human	TO.Host_Platform	TO.Malware	TO.Physical_Environment	TO.Unauthorized_Human	P.FIPS_Algorithms	P.Guidance_Docs	P.Physical_Control
Objectives for the TOE																			
O.Crypto_Data_Separation										✓	✓		✓	✓					
O.Crypto_Officer_Role												✓						✓	
O.Encryption										✓							✓		
O.Guidance_Docs											✓	✓						✓	✓
O.Integ_Sys_Data_Ext																			
O.Maintain_Security_Domain:														✓					
O.Physec_Tamper_Resistance											✓	✓				✓			✓
O.Restrict_Unauth_Actions											✓	✓				✓			
O.Security_Data_Mgmt																			
O.Security_Roles:												✓				✓		✓	
O.User_Role												✓						✓	
Objectives for the TOE Operational Environment																			
OE.Administrator		✓																✓	
OE.Crypto_Key_Mgmt	✓		✓				✓												
OE.FIPS_Certification					✓														
OE.Guidance_Docs_Use		✓	✓	✓		✓	✓	✓	✓			✓	✓	✓	✓	✓		✓	✓
OE.User								✓										✓	

8.1.1 Security objectives for the TOE

This portion of the ST will establish that each security objective for the SecureD TOE traces back to aspects of at least one identified threat SecureD counters or to aspects of an organizational security policy SecureD meets.

Table 12 in Section 4.1 presents the security objectives for the SecureD TOE asserted by this ST.

8.1.1.1 Threats

This portion of the ST will establish that for each threat it identifies there is an appropriate justification that one or more security objectives for the SecureD TOE are suitable to counter that threat.

Table 18 presented the complete mapping between all objectives and all threats, policies, and assumptions. Table 19 presents the detailed rationale justifying the coverage of each threat by one or more of the objectives for the TOE.

Table 19. TOE Coverage of Threats

Threat	Coverage Rationale
T.Cryptanalysis	The threat T.Cryptanalysis describes a human threat agent performing cryptanalysis on encrypted data at rest in order to recover information content. The SecureD TOE will be used to protect attractive information assets; this is a direct invitation for a human threat agent to attempt cryptanalysis on the encrypted data at rest in order to recover information content. SecureD addresses this threat directly by satisfying the objective O.Encryption . Further, SecureD supports that objective by protecting the data stream and cipher material from cross-contamination by meeting the objectives O.Crypto_Data_Separation
T.System_Access	The threat T.System_Access describes an unauthorized human threat agent gaining access to a system incorporating SecureD due to missing, weak, or incorrectly implemented access control allowing potential violations of integrity, confidentiality, or availability. The TOE objective O.Guidance_Docs addresses this threat by requiring the TOE to include clear guidance documentation for those responsible for operational use of the SecureD TOE. Two additional objectives for the TOE (O.Restrict_Unauth_Actions and O.Crypto_Data_Separation) describe self-protection for those situations when the guidance documentation objective is not met; they restrict unauthenticated functionality and segregate the classes of data the TOE handles. The final mechanism is physical; the TOE objective O.Physec_Tamper_Resistance dictates that even if a threat agent gains physical access to the module, the attempted compromise will be identifiable.
TO.Authorized_Human	The threat TO.Authorized_Human describes an authorized administrator or user; untrained, benign, or malicious, whose access to SecureD allows potential violations of integrity, confidentiality, or availability. The objectives for the TOE cover this threat through three mechanisms. First, the objective O.Guidance_Docs addresses this threat by requiring the SecureD TOE to include guidance for the secure installation, administration, and use of SecureD, minimizing operator errors. Next, the role objectives O.Security_Roles, O.Crypto_Officer_Role, O.User_Role, and O.Restrict_Unauth_Actions minimize the scope of the threat by restricting unauthenticated actions and by restricting the actions of authenticated operators to only those appropriate to their role. The final mechanism is physical; the TOE objective O.Physec_Tamper_Resistance dictates that even if a threat agent gains physical access to the module, the attempted compromise will be identifiable.
TO.Host_Platform	The threat TO.Host_Platform describes how system hardware, firmware, or software can fail, allowing potential violations of integrity, confidentiality, or availability. The TOE objective O.Crypto_Data_Separation addresses this threat by requiring that the SecureD provide complete separation between plaintext and encrypted data and between data and keys, protecting Critical Security Parameters from disclosure in the event of host system failure.
TO.Malware	The threat TO.Malware describes how malware – worms, viruses, Trojans, not necessarily directed – could exist in the host system, allowing potential violations of integrity, confidentiality, or availability. The TOE objective O.Maintain_Security_Domain addresses this threat by requiring that SecureD protect its own data and resources and maintain a security domain for TOE Security Function (TSF) execution to protect the TSFs from interference and tampering. Further, the TOE objective O.Crypto_Data_Separation addresses this threat by requiring that the SecureD provide complete separation between plaintext and encrypted data and between data and keys, protecting Critical Security Parameters from disclosure in the event of host system compromise.

Threat	Coverage Rationale
TO.Physical_Environment	The threat TO.Physical_Environment describes how natural and man-made infrastructure events, outside the direct control of those responsible for operational use of SecureD, could occur, allowing potential violations of integrity, confidentiality, or availability. These threats are the most remote and least easily addressed by the TOE.~~.~~
TO.Unauthorized_Human	The threat TO.Unauthorized_Human describes how an unauthorized human threat agent could gain <u>undetected</u> access to a system incorporating SecureD due to missing, weak, or incorrectly implemented access control, allowing potential violations of integrity, confidentiality, or availability. The objectives O.Restrict_Unauth_Actions and O.Security_Roles directly address the TO.Unauthorized_Human threat by restricting unauthenticated actions and by restricting the actions of authenticated operators to only those appropriate to their role. Also, as with the authorized human threat agent, the TOE objective O.Physec_Tamper_Resistance dictates that even if a threat agent gains physical access to the module, the attempted compromise will be identifiable.

8.1.1.2 Organizational Security Policies

This portion of the ST will establish that for each organizational security policy it identifies there is an appropriate justification that one or more security objectives for the SecureD TOE are suitable to cover that organizational security policy.

Table 18 presented the complete mapping between all objectives and all threats, policies, and assumptions. Table 20 presents the detailed rationale justifying the coverage of each organizational security policy by one or more of the objectives for the TOE.

Table 20. TOE Coverage of Organizational Security Policies

Organizational Security Policy	Coverage Rationale
P.FIPS_Algorithms	The organizational security policy P.FIPS_Algorithms requires that the SecureD TOE use only FIPS-approved algorithms for its encryption techniques. The TOE objective O.Encryption addresses this organizational security policy directly by requiring that the SecureD TOE use encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key. The two SFRs for cryptographic operation derived from this objective (FCS_COP.1 [1] [2]) specify FIPS-approved algorithms, thus the objective covers the policy.
P.Guidance_Docs	The organizational security policy P.Guidance_Docs requires that the SecureD TOE include guidance for its secure installation, administration, and use. Administrators require proper documentation concerning the SecureD TOE to install, administer, and use it securely. The TOE objective O.Guidance_Docs addresses this organizational security policy directly by restating the policy as an objective for the TOE. Three additional objectives (O.Security_Roles, O.Crypto_Officer_Role, and O.User_Role) support the O.Guidance_Docs objective by establishing the existence and capabilities of different roles within the SecureD TOE.
P.Physical_Control	The organizational security policy P.Physical_Control requires that those responsible for operational use of the SecureD TOE protect it physically from unauthorized use, modification, or destruction. The TOE cannot protect itself from physical threats originating outside its physical boundary. Responsible persons must provide protection in that domain (i.e., they will install SecureD correctly, protect the installed TOE from physical modification, and monitor the installed TOE regularly for evidence of tampering). The TOE objective O.Guidance_Docs addresses this organizational security policy by requiring that the SecureD TOE include appropriate guidance for the secure installation and use of SecureD. In addition, the SecureD TOE supports the P.Physical_Control OSP through the TOE objective O.Physec_Tamper_Resistance, which provides additional protection, should physical control of SecureD, or the system it is protecting, be compromised.

8.1.2 Security objectives for the TOE operational environment

This portion of the ST will establish that each security objective for the TOE operational environment traces back to at least one assumption, to aspects of an identified threat SecureD does not completely counter, or to aspects of an organizational security policy SecureD does not completely meet.

Table 13 in Section4.2 presents the security objectives for the TOE operational environment asserted by this ST.

8.1.2.1 Threats

This portion of the ST will establish that for each threat it identifies, aspects of which SecureD does not completely counter, there is an appropriate justification that one or more security objectives for the environment are suitable to counter those aspects of that threat.

Table 18 presented the complete mapping between all objectives and all threats, policies, and assumptions. Table 21 presents the detailed rationale justifying the coverage of each threat by one or more of the objectives for the TOE operational environment.

Table 21. Environmental Coverage of Threats

Threat	Coverage Rationale
TO.Authorized_Human	The threat TO.Authorized_Human describes an authorized administrator or user; untrained, benign, or malicious, whose access to SecureD allows potential violations of integrity, confidentiality, or availability. The environmental objective OE.Guidance_Docs_Use addresses this threat by requiring that those responsible for operational use of SecureD follow the guidance for the secure installation, administration, and use of the SecureD TOE.
TO.Host_Platform	The threat TO.Host_Platform describes how system hardware, firmware, or software can fail, allowing potential violations of integrity, confidentiality, or availability. The environmental objective OE.Guidance_Docs_Use addresses this threat by requiring that those responsible for operational use of SecureD follow the guidance for the secure installation, administration, and use of the SecureD TOE, thus minimizing the opportunity for system failure.
TO.Malware	The threat TO.Malware describes how malware – worms, viruses, Trojans, not necessarily directed – could exist in the host system, allowing potential violations of integrity, confidentiality, or availability. The environmental objective OE.Guidance_Docs_Use addresses this threat by requiring that those responsible for operational use of SecureD follow the guidance for the secure installation, administration, and use of the SecureD TOE, thus minimizing the opportunity for system failure.
TO.Physical_Environment	The threat TO.Physical_Environment describes how natural and man-made infrastructure events, outside the direct control of those responsible for operational use of SecureD, could occur, allowing potential violations of integrity, confidentiality, or availability. The environmental objective OE.Guidance_Docs_Use addresses this threat by requiring that those responsible for operational use of SecureD follow the guidance for the secure installation, administration, and use of the SecureD TOE.
TO.Unauthorized_Human	The threat TO.Unauthorized_Human describes how an unauthorized human threat agent could gain undetected access to a system incorporating SecureD due to missing, weak, or incorrectly implemented access control, allowing potential violations of integrity, confidentiality, or availability. The environmental objective OE.Guidance_Docs_Use addresses this threat by requiring that those responsible for operational use of SecureD follow the guidance for the secure installation, administration, and use of the SecureD TOE.

8.1.2.2 Organizational Security Policies

This portion of the ST will establish that for each organizational security policy it identifies that SecureD does not completely meet, there is an appropriate justification that one or more security objectives for the environment are suitable to meet those aspects of that organizational security policy.

Table 18 presented the complete mapping between all objectives and all threats, policies, and assumptions. Table 22 presents the detailed rationale justifying the coverage of each organizational security policy by one or more of the objectives for the TOE operational environment.

Table 22. Environmental Coverage of Organizational Security Policies

Organizational Security Policy	Coverage Rationale
P.FIPS_Algorithms	The organizational security policy P.FIPS_Algorithms requires that the SecureD TOE use only FIPS-approved algorithms for its encryption techniques. The SecureD TOE meets this policy completely; therefore, no objectives for the environment are allocated to it.
P.Guidance_Docs	The organizational security policy P.Guidance_Docs requires that the SecureD TOE include guidance for its secure installation, administration, and use. The environmental objective OE.Guidance_Docs_Use addresses this organizational security policy directly by restating the policy as an objective for the IT operational environment. Two additional objectives (OE.Administrator and OE.User) support the OE.Guidance_Docs_Use objective by establishing the existence of different users in the SecureD operational environment.
P.Physical_Control	The organizational security policy P.Physical_Control requires that those responsible for operational use of the SecureD TOE protect it physically from unauthorized use, modification, or destruction. The environmental objective OE.Guidance_Docs_Use addresses this organizational security policy by requiring that those responsible for operational use of SecureD follow the provided guidance for the secure installation and use of the SecureD TOE; i.e., they will install SecureD correctly, protect the installed TOE from physical modification, and monitor the installed TOE regularly for evidence of tampering.

8.1.2.3 Assumptions

This portion of the ST establishes that for each assumption it asserts, there is an appropriate justification that the security objectives for the environment are suitable to cover that assumption.

Table 18 presented the complete mapping between all objectives and all threats, policies, and assumptions. Table 23 presents the detailed rationale justifying the coverage of each assumption by one or more of the objectives for the TOE operational environment.

Table 23. Environmental Coverage of Assumptions

Assumption	Coverage Rationale
ACo.No_Bypass	The connectivity assumption ACo.No_Bypass asserts that Information cannot flow between the IDE controller of a protected system and the protected media except through SecureD. The environmental objective OE.Guidance_Docs_Use addresses this assumption by requiring that those responsible for operational use of SecureD follow the guidance necessary to install and administer the SecureD TOE correctly; i.e., they will install SecureD so that it is not bypassed, protect the installed TOE from physical modification, and monitor the installed TOE regularly for evidence of tampering.

Assumption	Coverage Rationale
APe.Administrator	The personnel assumption APe.Administrator asserts that the authorities responsible for operational use of SecureD will assign one or more individuals (System Administrators) to administer SecureD and its security. It further asserts that these authorized administrators will be properly trained and that they are not careless, willfully negligent, nor hostile. The environmental objective OE.Administrator addresses this assumption directly by restating the assumption as an objective for the operational environment. The environmental objective OE.Guidance_Docs_Use addresses this assumption by requiring that those responsible for operational use of SecureD will follow the guidance for the secure installation, administration, and use of the SecureD TOE.
APe.Administrator_Docs	The personnel assumption APe.Administrator_Docs asserts that the system administrators follow the policies and procedures defined in the SecureD documentation for secure installation, administration, and use of SecureD. The environmental objective OE.Guidance_Docs_Use addresses this assumption directly by requiring that those responsible for operational use of SecureD will follow the guidance for the secure installation, administration, and use of the SecureD TOE. Further, the environmental objective OE.Crypto_Key_Mgmt addresses this assumption by requiring that the IT Environment contain a Key Management System with appropriate policies and procedures for its correct operation.
APe.Crypto_Token_Management	The personnel assumption APe.Crypto_Token_Management asserts that those responsible for operational use of the SecureD TOE make use of a Key Management System (policies, procedures, hardware, and software) and that system administrators follow the policies and procedures necessary for the proper creation, management, distribution, and destruction of cryptographic Key Tokens. The environmental objective OE.Crypto_Key_Mgmt addresses this assumption by requiring that the IT Environment contain such a Key Management System (policies, procedures, hardware, and software) and that the KMS will include the necessary policies and procedures for the proper creation, management, distribution, and destruction of cryptographic Key Tokens. Further, the environmental objective OE.Guidance_Docs_Use supports this by requiring that those responsible for operational use of SecureD will follow the guidance for the secure installation, administration, and use of the SecureD TOE.
APe.Protect_From_Mods	The physical assumption APe.Protect_From_Mods asserts that those responsible for operational use of the SecureD hardware and embedded software involved in security policy enforcement will physically protect SecureD from unauthorized modification. The environmental objective OE.Guidance_Docs_Use addresses this assumption by requiring that those responsible for operational use of SecureD follow the provided guidance for the secure installation and use of the SecureD TOE; i.e., they will install SecureD correctly, protect the installed TOE from physical modification, and monitor the installed TOE regularly for evidence of tampering.
APe.User	The personnel assumption APe.User asserts that the authorities responsible for operational use of SecureD will identify one or more individuals (Users) to use systems protected by SecureD. It further asserts that these authorized users will be properly trained and that they are not careless, willfully negligent, nor hostile. The environmental objective OE.User addresses this assumption directly by restating the assumption as an objective for the operational environment. Furthermore, the environmental objective OE.Guidance_Docs_Use addresses this assumption by requiring that those responsible for operational use of SecureD will follow the guidance necessary to administrate and use the SecureD TOE properly; i.e., they will identify and train responsible operators.

Assumption	Coverage Rationale
APh.FIPS_Certification	The physical assumption APh.FIPS_Certification asserts that the SecureD TOE will be certified according to FIPS PUB 140-2 at Security Level 2 or higher. The environmental objective OE.FIPS_Certification addresses this assumption directly by restating the assumption as an objective for the IT operational environment.
APh.Crypto_Key_Management	The physical assumption APh.Crypto_Key_Management asserts that the IT Environment contains a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD and that those responsible for the operational use of the SecureD TOE make use of that KMS. The environmental objective OE.Crypto_Key_Mgmt addresses this assumption directly by restating the assumption as an objective for the IT operational environment.
APh.Threat_Agent_Moderate	The personnel assumption APh.Threat_Agent_Moderate asserts that systems containing SecureD are subject to deliberate attack by threat agents who are proficient-to-expert in the security behavior of the system, who possess specialized equipment, but who possess only public information concerning SecureD. The environmental objective OE.Guidance_Docs_Use addresses this assumption by requiring that those responsible for operational use of SecureD will utilize the guidance for the secure installation, administration, and use of SecureD provided with the TOE.

8.2 Security requirements

This section of the ST demonstrates that the TOE security requirements (both the TOE security functional requirements and the TOE security assurance requirements) and the security requirements for the IT environment are complete and consistent, and that they provide an adequate basis for the development of a TOE that will achieve the security objectives presented in section 4.

Table 24 and Table 25 present a mapping of the SFRs and SARs specified in section 5 to the objectives identified in section 4.

Table 24. SFRs Allocated to Objectives

Component	O.Crypto_Data_Separation	O.Crypto_Officer_Role	O.Encryption	O.Integ_Sys_Data_Ext	O.Guidance_Docs	O.Maintain_Security_Domain	O.Physec_Tamper_Resistance	O.Restrict_Unauth_Actions	O.Security_Data_Mgmt	O.Security_Roles	O.User_Role	OE.Crypto_Key_Mgmt
FCS_CKM.1 – Cryptographic key destruction			✓									✓
FCS_CKM.4 – Cryptographic key destruction			✓									
FCS_COP.1 – Cryptographic operation			✓									
FDP_IFC.1 – Subset information flow control									✓			
FDP_IFF.1 – Simple security attributes									✓			
FIA_UID.1 – Timing of identification								✓				
FMT_MSA.1 – Management of security attributes		✓							✓		✓	
FMT_MSA.2 – Secure security attributes									✓			
FMT_MSA.3 – Static attribute initialization									✓			
FMT_SMF.1 – Specification of Management Functions		✓										
FMT_SMR.1 – Security roles		✓								✓	✓	✓
FPT_RVM.1 – Non-bypassability of the TSP						✓						
FPT_SEP.1 – TSF domain separation	✓					✓	✓					
FTP_ITC.1 – Inter-TSF trusted channel				✓								

Table 25. SARs Allocated to Objectives

Component	O.Crypto_Data_Separation	O.Crypto_Officer_Role	O.Encryption	O.Integ_Sys_Data_Ext	O.Guidance_Docs	O.Maintain_Security_Domain:	O.Physec_Tamper_Resistance	O.Restrict_Unauth_Actions	O.Security_Data_Mgmt	O.Security_Roles:	O.User_Role	OE.Crypto_Key_Mgmt
ADO_IGS.1 - Installation, generation, and start-up procedures					✓							
AGD_ADM.1 - Administrator guidance					✓							
AGD_USR.1 - User guidance					✓							
AVA_MSU.2 - Validation of analysis					✓							

8.2.1 TOE security functional requirements

8.2.1.1 Cryptographic key destruction (FCS_CKM.4)

SFRs	FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: • *Security Requirements for Cryptographic Modules [FIPS_140-2]*.
Objectives	O.Encryption SecureD will use encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key.	
Rationale	The cryptographic key destruction SFR supports the second clause of the O.Encryption objective, “or knowledge of the encryption key” by providing a mechanism that denies knowledge of the encryption key to a hypothetical threat agent.	

8.2.1.2 Cryptographic operation (FCS_COP.1)

SFRs	FCS_COP.1.1[1]	The TSF shall perform *user data encryption and user data decryption* in accordance with a specified cryptographic algorithm *AES in CBC mode* and cryptographic key sizes of *128, 192, and 256 bits* that meet the following: • *Advanced Encryption Standard (AES) [AES] and* • *Recommendation for Block Cipher Modes of Operation [AES-MODES]*
	FCS_COP.1.1[2]	The TSF shall perform *Key Token communications encryption and Key Token communications decryption* in accordance with a specified cryptographic algorithm *TDEA Cipher Block Chaining with Three-key Triple DES (TCBC (KO 1))* and cryptographic key sizes of *168 bits* that meet the following: • *Data Encryption Standard (DES) [TDEA], and* • *Triple Data Encryption Algorithm Modes of Operation [TDEA-MODES]*
Objectives	O.Encryption SecureD will use encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key.	
Rationale	The two iterations of the cryptographic operation SFR satisfy the O.Encryption objective by establishing TOE conformance to well-known, strong cryptographic algorithms. SecureD uses the Advanced Encryption Standard (AES) to encrypt and decrypt user data. (FCS_COP.1.1[1]) The SecureD implementation of the AES algorithm has been validated against the *Advanced Encryption Standard Algorithm Validation Suite* (Certificate # 174; http://csrc.nist.gov/cryptval/aes/aesval.html), thus demonstrating that SecureD uses encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key, to protect user data. SecureD uses the Triple Data Encryption Algorithm (TDEA) to protect Key Token communications. (FCS_COP.1.1[2]) The SecureD implementation of TDEA has been validated against *NIST Special Publication 800-20* (Certificate # 324; http://csrc.nist.gov/cryptval/des/tripledesval.html), thus demonstrating that SecureD uses encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key, to protect key communications.	

8.2.1.3 Subset information flow control (FDP_IFC.1)

SFRs	FDP_IFC.1.1[1]	The TSF shall enforce the *User Data Cryptography SFP* on *a) Subjects: the two ATA interfaces* *b) Information: ATA data* c) *Operations: Information flow with encryption/decryption between the two ATA interfaces*
Objectives	O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.	
Rationale	This iteration of the subset information flow control SFR, FDP_IFC.1[1], addresses the O.Security_Data_Mgmt objective by specifying the security critical data and the allowable operations for the user data information flow. With respect to the User Data Cryptography SFP, the SecureD device has two ATA interfaces for user data, conventionally labeled “ATA IN” (host side) and “ATA OUT” (storage device side); either can be a source or a destination for an information flow. With respect to the *User Data Cryptography SFP*, a flow is equivalent to a read from a source ATA interface and an associated write to a destination ATA interface.	

SFRs	FDP_IFC.1.1[2] The TSF shall enforce the Key Token Communications SFP on *a) Subjects: the Key Interface* *b) Information: key data* c) *Operations: Information flow with encryption from the Key Interface to the TSF*
Objectives	O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.
Rationale	This iteration of the subset information flow control SFR, FDP_IFC.1[2], addresses the O.Security_Data_Mgmt objective by specifying the security critical data and the allowable operations for the key token communications information flow. With respect to the Key Token Communications SFP, the SecureD device has a single interface for obtaining information from the Key Token, conventionally labeled the “Key Interface”. Information only flows into the TSF from the Key Interface, although protocol control signals can flow from the TSF to the Key Token through the Key Interface.

8.2.1.4 Simple security attributes (FDP_IFF.1)

SFRs

FDP_IFF.1.1[1] The TSF shall enforce the *User Data Cryptography SFP* based on the following types of subject and information security attributes:

a) Subject Security Attributes:
   - ATA interface designation; and

b) Information Security Attributes:
   - Storage device address range,
   - Media user key;
   - Media resident key;
   - Read/write flag;
   - No other security attributes.

FDP_IFF.1.2[1] The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) For information flows from ATA IN to ATA OUT, the TOE will permit information to flow only if:
   - There is a Media Device Key associated with the storage device address range; and
   - The Read/Write flag associated with the storage device address range permits information to be written.

b) For information flows from ATA OUT to ATA IN, the TOE will permit information to flow only if:
   - There is a Media Device Key associated with the storage device address range; and
   - The Read/Write flag associated with the storage device address range permits information to be read.

FDP_IFF.1.3[1] The TSF shall enforce no additional information flow control SFP rules.

FDP_IFF.1.4[1] The TSF shall provide the following

a) For information flows from ATA IN to ATA OUT, the TOE will provide the capability to encrypt data using the Media Device Key, and the storage address range associate with the information flow:

b) For information flows from ATA OUT to ATA IN, the TOE will provide the capability to decrypt data using the Media Device Key, and the storage address range associate with the information flow:

FDP_IFF.1.5[1] The TSF shall explicitly authorize an information flow based on the following rules: None.

FDP_IFF.1.6[1] The TSF shall explicitly deny an information flow based on the following rules: None.

Objectives

O.Security_Data_Mgmt

SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.

Rationale

This iteration of the simple security attributes SFR, FDP_IFF.1[1], addresses the O.Security_Data_Mgmt objective by specifying in detail the rules for permitting information flow using the *User Data Cryptography SFP* .

SFRs	FDP_IFF.1.1[2]	The TSF shall enforce the *Key Token Communications SFP* based on the following types of subject and information security attributes: a) Subject Security Attributes: • Crypto Officer Key • User Key; and b) Information Security Attributes: • Communications Key Set, • Media user key; • Media resident key; • Read/write flag; • No other security attributes.
	FDP_IFF.1.2[2]	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: a) For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as a Crypto Officer, the TOE will permit information to flow only if: • The Operator authenticates itself as a Crypto Officer associated with that instance of the TOE. b) For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as a User, the TOE will permit information to flow only if: • The Operator authenticates itself as a User associated with that instance of the TOE.
	FDP_IFF.1.3[2]	The TSF shall enforce no additional information flow control SFP rules.
	FDP_IFF.1.4[2]	The TSF shall provide the following a) For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as an authenticated Crypto Officer, the TOE will provide the capability to encrypt and decrypt Key Token Communications using the Communications Key Set and the capability to modify the Communications Key Set and the Media Resident Keys: b) For information flows from the Key Interface to the TSF, if the Key Token identifies the Operator as an authenticated User, the TOE will provide the capability to encrypt and decrypt Key Token Communications using the Communications Key Set and the capability to import User key data:
	FDP_IFF.1.5[2]	The TSF shall explicitly authorize an information flow based on the following rules: None.
	FDP_IFF.1.6[2]	The TSF shall explicitly deny an information flow based on the following rules: None.
Objectives	O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.	
Rationale	This iteration of the simple security attributes SFR, FDP_IFF.1[2], addresses the O.Security_Data_Mgmt objective by specifying in detail the rules for permitting information flow using the *Key Token Communications SFP.*	

8.2.1.5 Timing of identification (FIA_UID.1)

SFRs	FIA_UID.1.1 The TSF shall allow *Reset, Self Test, Show Status, and Zeroization* on behalf of the user to be performed before the user is identified. FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Objectives	O.Restrict_Unauth_Actions SecureD will restrict the actions an operator may perform before it authenticates the role of the operator.
Rationale	These SFRs satisfy the O.Restrict_Unauth_Actions objective directly by explicitly identifying all the actions that may be performed before an operator is authenticated and by requiring an operator to be authenticated to perform any other TSF-mediated actions.

8.2.1.6 Management of security attributes (FMT_MSA.1)

SFRs	FMT_MSA.1.1 [1] The TSF shall enforce the *User Data Cryptography SFP* to restrict the ability to *modify* the security attributes *Storage device address range* and *Media user key* to *the User role*.
Objectives	O.User_Role SecureD will enable the *User* role to activate the SecureD encryption functions. O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.
Rationale	This iteration of the management of security attributes SFR, FMT_MSA.1.1 [1], addresses the general objective O.Security_Data_Mgmt and the specific objective O.User_Role by explicitly identifying the cryptographic attributes that the User role can manipulate and the information flow policy that constrains that manipulation.

SFRs	FMT_MSA.1.1 [2] The TSF shall enforce the *Key Token Communications SFP* to restrict the ability to modify the security attributes *Communications Key Set* and *Media Resident Keys* to the *Crypto Officer role*.
Objectives	O.Crypto_Officer_Role SecureD will enable the *Crypto Officer* role to manage cryptographic assets and attributes. O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.
Rationale	This iteration of the management of security attributes SFR, FMT_MSA.1.1 [2], addresses the general objective O.Security_Data_Mgmt and the specific objective O.Crypto_Officer_Role by explicitly identifying the cryptographic attributes that the Crypto Officer role can manage and the information flow policy that constrains that management.

8.2.1.7 Secure security attributes (FMT_MSA.2)

SFRs	FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.
Objectives	O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.
Rationale	By establishing a requirement that the TSF only accept secure values, this SFR explicitly supports the initialization and limits clauses of the O.Security_Data_Mgmt objective.

8.2.1.8 Static attribute initialization (FMT_MSA.3)

SFRs	FMT_MSA.3.1 [1]	The TSF shall enforce the *User Data Cryptography SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.
	FMT_MSA.3.2 [1]	The TSF shall allow the *User role* to specify alternative initial values to override the default values when an object or information is created.
Objectives	O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.	
Rationale	By establishing a requirement that the TSF enforce restrictive default values and by permitting the User to override those values, this SFR explicitly supports the initialization and limits clauses of the O.Security_Data_Mgmt objective.	

SFRs	FMT_MSA.3.1 [2]	The TSF shall enforce the *Key Token Communications SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.
	FMT_MSA.3.2 [2]	The TSF shall allow the *Crypto Officer role* to specify alternative initial values to override the default values when an object or information is created.
Objectives	O.Security_Data_Mgmt SecureD will manage the initialization of, limits on, and allowable operations on security-critical data.	
Rationale	By establishing a requirement that the TSF enforce restrictive default values and by permitting the Crypto Officer to override those values, this SFR explicitly supports the initialization and limits clauses of the O.Security_Data_Mgmt objective.	

8.2.1.9 Specification of Management Functions (FMT_SMF.1)

SFRs	FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *Set Crypto Officer Key, Set Device Keys, Set User Key, and Set Media Resident Keys*.
Objectives	O.Crypto_Officer_Role SecureD will enable the *Crypto Officer* role to manage cryptographic assets and attributes.	
Rationale	The specification of management functions SFR, FMT_SMF.1, supports the O.Crypto_Officer_Role objective by enumerating the exact list of security management functions available to the Crypto Officer.	

8.2.1.10 Security roles (FMT_SMR.1)

SFRs	FMT_SMR.1.1	The TSF shall maintain the roles Crypto Officer and User.
	FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Objectives	O.Crypto_Officer_Role SecureD will enable the Crypto Officer role to manage cryptographic assets and attributes.	
	O.Security_Roles SecureD will be able to distinguish the security-relevant roles *Crypto Officer* and *User.*	
	O.User_Role SecureD will enable the *User* role to activate the SecureD encryption functions.	
Rationale	These SFRs directly satisfy the objectives by establishing the two security roles, Crypto Officer and User.	

8.2.1.11 Non-bypassability of the TSP (FPT_RVM.1)

SFRs	FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Objectives	O.Maintain_Security_Domain SecureD will protect its own data and resources and will maintain a security domain for TOE Security Function (TSF) execution to protect the TSFs from interference and tampering.	
Rationale	This SFR supports satisfaction of O.Maintain_Security_Domain objective directly by ensuring that the TOE security policies cannot be bypassed.	

8.2.1.12 TSF domain separation (FPT_SEP.1)

SFRs	FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
	FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Objectives	O.Crypto_Data_Separation SecureD will provide complete separation between plaintext and encrypted data and between data and keys.	
	O.Maintain_Security_Domain SecureD will protect its own data and resources and will maintain a security domain for TOE Security Function (TSF) execution to protect the TSFs from interference and tampering.	
	O.Physec_Tamper_Resistance SecureD will be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum and that provides an indication of tampering if physical access to the TOE interior is attempted.	
Rationale	This SFR satisfies the O.Maintain_Security_Domain objective directly by explicitly defining TSF domain separation within SecureD. This SFR satisfies the O.Crypto_Data_Separation objective by treating keys, plaintext data, and encrypted data as separate domains. The FPT_SEP.1.1 SFR addresses the O.Physec_Tamper_Resistance objective by establishing a requirement for protection from interference and tampering. For a hardware TOE, this protection includes application of methods that protect the TOE embodiment in the gates and masks of the hardware chips.	

8.2.1.13 Inter-TSF trusted channel (FTP_ITC.1)

SFRs	FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. FTP_ITC.1.2 The TSF shall permit the TSF to initiate communication via the trusted channel. FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for a) Crypto Officer Authentication b) Set Crypto Officer Key c) Set Device Keys d) Set Media Resident Keys e) Set Media User Keys f) Set User Key g) User Authentication
Objectives	O.Integ_Sys_Data_Ext SecureD will ensure the integrity of the encryption keys exchanged externally with the Key Token by using a protocol for data transfer that will permit error detection. This includes detecting errors in data received and encoding outgoing data to make it possible for the receiver to detect errors.
Rationale	These SFRs satisfy the O.Integ_Sys_Data_Ext objective directly by explicitly identifying a trusted channel for communications with the Key Management System, the remote trusted IT product.

8.2.1.14 Satisfaction of O.Guidance_Docs

SARs	ADO_IGS.1 Installation, generation, and start-up procedures ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
	AGD_ADM.1 Administrator guidance AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.
	AGD_USR.1 User guidance AGD_USR.1.1D The developer shall provide user guidance.
	AVA_MSU.2 Validation of analysis AVA_MSU.2.1D The developer shall provide guidance documentation. AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.
Objectives	O.Guidance_Docs To minimize operator errors, the SecureD TOE will include guidance for the secure installation, administration, and use of SecureD.
Rationale	These four SARs satisfy the O.Guidance_Docs objective by explicitly requiring that the TOE incorporate guidance for the secure installation, administration, and use of SecureD, by requiring that the guidance documentation be complete, clear, consistent and reasonable, and by requiring that the guidance documentation be analyzed to provide additional assurance that misleading, unreasonable and conflicting guidance is absent from the guidance documentation

8.2.2 Explicitly stated IT security requirements

This ST draws its requirements exclusively from [CC_PART2] and [CC_PART3]. The ST writers did not exercise their option to draw up new SFRs or SARs; therefore, it is not necessary to provide a rationale for explicitly stated IT security requirements.

8.2.3 Strength of function claims

This Security Target does not claim an explicit strength of function for any security functional requirement it contains; therefore, it contains no explicit rationale for Strength of Function.

8.2.4 TOE security assurance requirements

8.2.4.1 Justification for selection of EAL4

This ST contains the assurance requirements from the CC EAL4 assurance package, based on good rigorous commercial development practices. The ST authors developed this ST for a generalized environment with a medium level of risk to the protected assets.

The TOE will be used to protect attractive information assets and it is assumed that possible attackers will have a medium-to-high level of expertise, resources and motivation—an attack potential of Moderate. The ST authors derived the Security Objectives for the TOE to resist attackers with these characteristics; CC EAL4 is generally sufficient to provide the assurance for that environment. Furthermore, the ST authors chose EAL4 because the developers and users require a moderate to high level of independently assured security in conventional commodity.

8.2.4.2 Justification for augmentation with AVA_VLA.3

Based on the conceptual operating scenario and the threat agent characterizations, the ST authors have identified the attack potential of the threat agents (foreign intelligence agent; military adversary) as Moderate. These threat agents are proficient-to-expert in the security behavior of the system and possess (or can acquire without undue effort) specialized equipment, but possess only public information concerning SecureD. Time is not a consideration.

Under these circumstances, the threats to and consequences of data disclosure and loss of data integrity are significant. As a result, the TOE must be shown to be resistant to penetration attacks. EAL 4 requires vulnerability assessment through imposition of AVA_VLA.2. This requires a review of only the identified vulnerabilities. Component AVA_VLA.3 requires, in addition, that a systematic search for vulnerabilities be documented and presented. This provides a significant increase in the consideration of vulnerabilities over that provided by the AVA_VLA.2 component of the unaugmented EAL4.

8.2.5 Security requirements for the IT environment

This ST contains one iterated security functional requirement for the IT environment, *FCS_CKM.1 Cryptographic key generation*.

Assumptions	Cryptographic Key Management The IT Environment contains a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD. Those responsible for operational use of the SecureD TOE make use of this KMS to enable operation of the SecureD TOE.
Objectives	OE.Crypto_Key_Mgmt The IT Environment will provide a Key Management System (policies, procedures, hardware, and software) capable of creating cryptographic Key Tokens compatible with SecureD. The functional capabilities of the KMS will be sufficient to satisfy the Common Criteria SFR for Cryptographic Key Generation (FCS_CKM.1). O.Encryption SecureD will use encryption techniques to produce cipher text that cannot be decrypted without knowledge of the encryption key.
SFRs	FCS_CKM.1.1 [1] The IT Environment shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *none* and specified cryptographic key sizes *of 128, 192, and 256 bits* that meet the following: *none*.
	FCS_CKM.1.1 [2] The IT Environment shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *none* and specified cryptographic key sizes *of 168 bits* that meet the following: *none*.
Rationale	The physical assumption APh.Crypto_Key_Management asserts that the IT Environment contains a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD. The environmental objective OE.Crypto_Key_Mgmt addresses this assumption directly by restating the assumption as an objective for the IT operational environment. Finally, the two iterations of the cryptographic key generation SFR allocated to the IT environment satisfy the OE.Crypto_Key_Mgmt objective by directly instantiating cryptographic key generation. They also support satisfaction of the O.Encryption objective by providing the necessary keying material for the well-known, strong cryptographic algorithms implemented by the TOE.

This ST contains no security assurance requirements for the IT environment; therefore, no trace-back of security assurance requirements for the IT environment to security objectives for the environment is required.

8.2.6 Non-satisfaction of dependencies

8.2.6.1 Cryptographic Operation SFRs

The fundamental security functional requirement for SecureD is to perform cryptographic operations (FCS_COP). A number of additional SFRs derive from this basic requirement, based on the predecessor dependencies specified in [CC_PART2]. The ST authors took FCS_COP.1 from [CC_PART2] and tailored it suitably. They then traversed the dependencies called out in [CC_PART2], generated a dependency table, and selected and tailored the additional SFRs needed to support FCS_COP.1. The ST authors allocated the tailored SFRs to the TOE or the IT Environment as appropriate. This selection and allocation process guarantees that all dependencies specified in [CC_PART2] are satisfied. Table 26, at the end of this section, presents the SFRs selected for the TOE, their allocation to the TOE or the IT Environment, and their dependency relationships.

FCS_COP.1 Cryptographic operation

Dependencies:	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
Application Note:	SecureD does not contain a mechanism to create crypto keys; therefore, the FCS_CKM.1 dependency must be satisfied in the IT environment.

FCS_CKM.1 Cryptographic key generation
Application Note: SecureD does not contain a mechanism to create crypto keys; it cannot satisfy FCS_CKM.1, therefore the ST cannot include FCS_CKM.1 among the SFRs satisfied by the TOE. However, it can and does include it among the SFRs satisfied by the IT environment. Because this SFR is allocated to the IT environment, its dependencies are not applicable to the TOE.

FCS_CKM.4 Cryptographic key destruction
Dependencies: FCS_CKM.1 Cryptographic key generation
FMT_MSA.2 Secure security attributes

Application Note: SecureD does contain a mechanism to destroy crypto keys; it can satisfy FCS_CKM.4 and the ST includes FCS_CKM.4 among the SFRs. However, SecureD does not contain a mechanism to create crypto keys; therefore, the FCS_CKM.1 dependency must be satisfied in the IT environment.

FMT_MSA.1 Management of security attributes
Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.2 Secure security attributes
Dependencies: ADV_SPM.1 Informal TOE security policy model
FDP_IFC.1 Subset information flow control
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

Application Note: This requirement is obligatory to partially satisfy the dependencies of both FCS_COP.1 and FCS_CKM.4, therefore the ST must include it among the SFRs SecureD satisfies

FMT_MSA.3 Static attribute initialization
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Dependencies: No Dependencies

FMT_SMR.1 Security roles
Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification
Dependencies: No Dependencies

8.2.6.2 Additional SFRs

These additional SFRs represent protection capabilities, independent of the cryptographic operations, which exist in SecureD and were evaluated as part of its FIPS certification. Because they are free-standing requirements with no dependency relationships, they were not presented in the dependency graph; however, they are represented in Table 26 at the end of this section.

FPT_RVM.1 Non-bypassability of the TSP
Dependencies: No Dependencies

FPT_SEP.1 TSF domain separation
Dependencies: No Dependencies

FTP_ITC.1 Inter-TSF trusted channel
Dependencies: No Dependencies

Table 26. SecureD TOE SFR dependencies

SFR ⇩ Depends on ⇨	Allocated to	FCS_COP.1 **	FCS_CKM.1	FCS_CKM.4	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_SMR.1	FMT_SMF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FPT_RVM.1 **	FPT_SEP.1 **	FTP_TRP.1 **
FCS_COP.1	TOE		⇗	⇗											
FCS_CKM.1*	IT Environment														
FCS_CKM.4	TOE														
FMT_MSA.1	TOE								⇗						
FMT_MSA.2	TOE				⇗			⇗							
FMT_MSA.3	TOE														
FMT_SMR.1	TOE											⇗			
FMT_SMF.1 *	TOE														
FDP_IFC.1	TOE										⇗				
FDP_IFF.1	TOE						⇗			⇗					
FIA_UID.1 *	TOE														
FPT_RVM.1 *	TOE														
FPT_SEP.1 *	TOE														
FTP_ITC.1 *	TOE														

* No dependencies
** No dependents

8.2.7 Internal consistency and mutual support

The ST includes no instance of a requirement that contradicts another requirement in the ST. In instances where different requirements apply to the same events or types of data, the requirements and the operations performed within the requirements do not contradict each other, but provide supporting functionality ensuring that the TOE is internally consistent.

The combination of several different supporting security functions, and the handling of dependencies as presented in Section 8.2.6, ensures that together the selected requirements form a mutually supportive whole.

The following items also support this claim:

- mapping and suitability of the requirements to security objectives (as justified in Table 27); and
- inclusion of architectural requirements FPT_RVM.1 and FPT_SEP to protect the TSF.

8.3 Summary specification

8.3.1 Security functional requirements

Table 27 provides a mapping of TOE security functions to those security functional components that HDD implemented to meet the requirements specified in Section 5.1, *TOE security requirements*. The security functions described in the TOE summary specification and indicated in Table 27 are all necessary for the required security functionality in the TSF. The collection of security functions work together to provide all of the security requirements. Table 27, in conjunction with Section 6.1, provides evidence that the TOE Security Functional Requirements are suitable to meet the TOE security requirements.

Table 27. Security Functions mapped to TOE SFRs

Security Function	Security Functional Component
Cryptographic support	FCS_CKM.4 – Cryptographic key destruction
	FCS_COP.1 – Cryptographic operation
User data protection	FDP_IFC.1 – Subset information flow control
	FDP_IFF.1 – Simple security attributes
Identification and authentication	FIA_UID.1 – Timing of identification
Security management	FMT_MSA.1 – Management of security attributes
	FMT_MSA.2 – Secure security attributes
	FMT_MSA.3 – Static attribute initialization
	FMT_SMF.1 – Specification of management functions
	FMT_SMR.1 – Security roles
Protection of the TSF	FPT_RVM.1 – Non-bypassability of the TSP
	FPT_SEP.1 – TSF domain separation
Trusted path/channels	FTP_ITC.1 – Inter-TSF trusted channel

8.3.2 Strength of function claims

This Security Target does not claim an explicit strength of function for any security functional requirement it contains; therefore, it contains no explicit rationale for Strength of Function.

8.3.3 Security assurance requirements

Table 28 provides a mapping of TOE security assurance functions to those security assurance measures that HDD implemented to ensure that the TOE meets the requirements specified by CC EAL4, augmented with AVA_VLA.3. This table, in conjunction with Section 6.2, provides evidence that the security assurance measures are suitable to meet the TOE security assurance requirements and that, in fact, HDD did execute these measures.

Table 28. TOE SARs mapped to Security Assurance Functions

SARs	Process Assurance	Delivery and guidance	Design Documents	Test	Vulnerability Assessment
ACM_AUT.1 Partial CM automation	X				
ACM_CAP.4 Generation support and acceptance procedures	X				
ACM_SCP.2 Problem tracking CM coverage	X				
ADO_DEL.2 Detection of modification		X			
ADO_IGS.1 Installation, generation, and start-up procedures		X			
ADV_FSP.2 Fully defined external interfaces			X		
ADV_HLD.2 Security enforcing high-level design			X		
ADV_IMP.1 Subset of the implementation of the TSF			X		
ADV_LLD.1 Descriptive low-level design			X		
ADV_RCR.1 Informal correspondence demonstration			X		
ADV_SPM.1 Informal TOE security policy model			X		
AGD_ADM.1 Administrator guidance		X			
AGD_USR.1 User guidance		X			
ALC_DVS.1 Identification of security measures	X				
ALC_LCD.1 Developer defined life-cycle model	X				
ALC_TAT.1 Well-defined development tools	X				
ATE_COV.2 Analysis of coverage				X	
ATE_DPT.1 Testing: high-level design				X	
ATE_FUN.1 Functional testing				X	
ATE_IND.2 Independent testing – sample				X	
AVA_MSU.2 Validation of analysis					X
AVA_SOF.1 Strength of TOE security function evaluation					X
AVA_VLA.3 Moderately resistant					X

8.4 Protection Profile claims

This Security Target makes no claims of conformance with any existing Protection Profile; therefore, it is not necessary to provide a rationale for Protection Profile claims.

9 References

This ST refers to the following documents and incorporates them by reference:

[AES] Advanced Encryption Standard (AES), FIPS Publication 197. National Institute of Standards and Technology, November 2001, <http://cs-www.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf>, viewed 08 September 2003.

[AES-MODES] Recommendation for Block Cipher Modes of Operation - Methods and Techniques, Special Publication 800-38A, 2001 Edition. National Institute of Standards and Technology, December 2001, <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>, viewed 11 September 2003.

[ANSI_ATA] Information Technology – AT Attachment with Packet Interface – 6 ATA/ATAPI-6, ANSI INCITS 361-2002 .

[ANSI_ATAPI] Information Technology – Multimedia Commands – 4 (MMC-4), ANSI INCITS XXX T10/1545-D (Draft)

[ATA-ATAPI] Landis, Hale. “ATA-ATAPI.COM”. <http://www.ata-atapi.com>, viewed 2 May 2005.

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-001, <http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part1.pdf>, viewed 01 September 2004.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, January 2004, Version 2.2, CCIMB-2004-01-002, <http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part2.pdf>, viewed 01 September 2004.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, January 2004, version 2.2, Revision 256, CCIMB-2004-01-003, <http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part3.pdf>, viewed 01 September 2004.

[CMITSE] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-004, <http://niap.nist.gov/cc-scheme/cc_docs/cem_v12.pdf>, viewed 01 September 2004.

[FIPS_140-2] Security Requirements for Cryptographic Modules, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001, <http://cs-www.ncsl.nist.gov/publications/fips/fips140-2/fips1402.pdf>, viewed 08 September 2003.

[INFORMIT] “InformIT.com” <http://www.informit.com/index.asp> June 21, 2005. “Information Security Must Balance Business Objectives” <http://www.informit.com/articles/article.asp?p=26952&redir=1> June 21, 2005.

[INFOSEC_GLOSS] “The Information Security Glossary.” <http://www.yourwindow.to/information-security/index.htm> June 21, 2005. “Information Security Glossary – Confidentiality, Integrity and Availability.” <http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailabili.htm> June 21, 2005.

[MS_DICT] Microsoft Press Computer Dictionary, 5th ed. Redmond, WA: Microsoft Press, 2002.

[TDEA] Data Encryption Standard (DES), FIPS Publication 46-3. National Institute of Standards and Technology, October 1999, <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>, viewed 29 November 2004.

[TDEA-MODES] Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52-1998.

[UMIAMI_ETHICS] “Privacy / Data Protection Project.” <http://privacy.med.miami.edu/index.htm> June 21, 2005. “confidentiality, integrity, availability (CIA).” <http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm> June 21, 2005.

10 Terms

This section contains some of the terms that are used in a specialized way throughout the CC or this ST. The majority of terms in the CC and this ST are used either according to their accepted dictionary definitions or according to commonly accepted definitions that may be found in ISO security glossaries or other well-known collections of security terms.

Term	Explanation
Advanced Encryption Standard	See AES
AES	"Acronym for Advanced Encryption Standard. A cryptographic algorithm specified by the National Institute of Standards and Technology (NIST) to protect sensitive information. AES is specified in three key sizes: 128, 192, and 256 bits. AES replaces the 56-bit key Data Encryption Standard (DES), which was adopted in 1976." [MS_DICT]
AES 256	AES using a 256-bit key size
Approved	FIPS-Approved and/or NIST-recommended [FIPS_140-2]
Approved mode of operation	A mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode) [FIPS_140-2]
Approved security function	Within FIPS 140-2, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Approved standard, b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or c) specified in the list of Approved security functions. [FIPS_140-2]
Asset	Entities that those responsible for the TOE value. The entity itself, and the property of that entity that give the entity value, describe the asset(s).
Assurance	Grounds for confidence that an entity meets its security objectives
ATA	"Acronym for Advanced Technology Attachment. ANSI group X3T10's official name for the disk drive interface standard for integrating drive controllers directly on disk drives. The original ATA standard is commonly known as Integrated Drive Electronics (IDE)." [MS_DICT]
ATAPI	"…ATAPI […] stands for ATA Packet Interface. ATA/ATAPI is the most popular device interface today. Of the approximately 140 million hard disk drives made in the last year, 90+ percent are ATA. […] [T]he vast majority of CD-ROM drives are ATAPI devices. Most PCMCIA and CFA mass storage devices are also ATA or ATAPI devices." [ATA-ATAPI] "The interface used by the IBM PC AT system for accessing CD-ROM devices." [MS_DICT]
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package

Term	Explanation
Availability	“Assurance that the systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them.” [INFOSEC_GLOSS] “Availability refers, unsurprisingly, to the availability of information resources. … Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate).” [UMIAMI_ETHICS] “The third objective of security is availability: ensuring that data stored in the computer can be accessed by the people who should access it. … Availability means ensuring that the data can be accessed by all authorized people.” [INFORMIT]
BLACK	Designation for information system equipment or facilities that handle (and for data that contains) only cyphertext (or, depending on the context, only unclassified information), and for such data itself This term derives from U.S. Government COMSEC terminology
CIA	Acronym for Confidentiality, Integrity, and Availability. These three objectives are the "motherhood and apple pie" of information security. Securing information is equivalent to ensuring that computers keep your secrets, hold valid information, and are ready to work when you are. Confidentiality, Integrity and Availability are typically ranked as high, medium, and low to help measure each of these criteria. These classifications represent the key security requirements of any system and are extremely important for risk analysis. The three objectives can never be completely separated; the definitions and solutions overlap among the three.
Class	A grouping of families that share a common focus
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package
Confidentiality	“Assurance that information is shared only among authorised persons or organisations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. … The classification of the information should determine its confidentiality and hence the appropriate safeguards.” [INFOSEC_GLOSS] “Confidentiality refers to limiting information access and disclosure to the set of authorized users, and preventing access by or disclosure to unauthorized ones.” [UMIAMI_ETHICS] “The first objective of security is confidentiality: keeping information away from people who should not have it. Accomplishing this objective requires that we know what data we are protecting and who should have access to it. It requires that we provide protection mechanisms for the data while it is stored in the computer and while it is being transferred over networks between computers. … Confidentiality mechanisms keep information from being read by unauthorized people.” [INFORMIT]
Crypto Officer	One of two authorized Roles that an Operator of the SecureD may assume. See also Operator and User.
Cryptographic module	The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary [FIPS_140-2]
Cryptography	“The use of codes to convert data so that only a specific recipient will be able to read it using a key. The persistent problem of cryptography is that the key must be transmitted to the intended recipient and may be intercepted. Public key cryptography is a recent significant advance. “ [MS_DICT]

Term	Explanation
Data storage	“data n. Plural of the Latin datum, meaning an item of information. In practice, data is often used for the singular as well as the plural form of the noun.“ [MS_DICT] “storage n. In computing, any device in or on which information can be kept. Microcomputers have two main types of storage: random access memory (RAM) and disk drives and other external storage media. Other types of storage include read-only memory (ROM) and buffers. “ [MS_DICT]
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives
Development environment:	The environment(s) in which the TOE is being designed, developed, produced, and delivered. Note that this environment is conceptually distinct from the operational environment, though if the TOE is being developed in the same environment as that in which it is being used, they may be the same.
EDC	Error-Detecting Code “error-detection coding n. A method of encoding data so that errors that occur during storage or transmission can be detected. Most error-detection codes are characterized by the maximum number of errors they can detect. See also checksum. Compare error-correction coding.” [MS_DICT]
EIDE	“Acronym for Enhanced Integrated Drive Electronics. An extension of the IDE standard, EIDE is a hardware interface standard for disk drive designs that house control circuits in the drives themselves. It allows for standardized interfaces to the system bus while providing for advanced features, such as burst data transfer and direct data access. EIDE accommodates drives as large as 8.4 gigabytes (IDE supports up to 528 megabytes). It supports the ATA-2 interface, which permits transfer rates up to 13.3 megabytes per second (IDE permits up to 3.3 megabytes per second), and the ATAPI interface, which connects drives for CD-ROMs, optical discs and tapes, and multiple channels.” [MS_DICT]
Element	An indivisible security requirement
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor
FIPS	Federal Information Processing Standard
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts

Term	Explanation
FPGA	“Acronym for Field Programmable Gate Array. A type of programmable logic chip that can be configured for a wide range of specialized applications after manufacture and delivery. FPGAs can be reprogrammed to incorporate innovations and upgrades. Because of their flexibility and adaptability, FPGAs are used in devices from microwave ovens to supercomputers.” [MS_DICT]
Hardware-based Encryption	“Hardware designed to handle the cryptographic functions necessary for data security.” [MS_DICT]
IDE	“Acronym for Integrated Device Electronics. A type of disk-drive interface in which the controller electronics reside on the drive itself, eliminating the need for a separate adapter card. The IDE interface is compatible with the controller used by IBM in the PC/AT computer but offers advantages such as look-ahead caching.” [MS_DICT]
IDE/ATA Data Bus Encryption	The process of applying cryptographic operations to data passing through an IDE/ATA data bus, at bus speeds.
Informal	Expressed in natural language
Integrity	“Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon.” [INFOSEC_GLOSS] “Integrity refers to the trustworthiness of information resources. It includes the concept of "data integrity" -- namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes "origin" or "source integrity" -- that is, that the data actually came from the person or entity you think it did, rather than an imposter. … On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.” [UMIAMI_ETHICS] “The second objective of security is integrity: assuring that the information stored in the computer is never contaminated or changed in a way that is not appropriate. Both confidentiality and availability contribute to integrity. … Integrity mechanisms assure that information stored in the computer is never contaminated or changed in a way that is not appropriate.” [INFORMIT]
Iteration	The use of a component more than once with varying operations
Key Management System (KMS)	The aggregate of policies, procedures, hardware, and software necessary for and capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD
Key Zeroization	The process of erasing active keys in a cryptographic module
Operational environment:	The environment(s) in which the TOE is used
Operator	This is the collective term for users of the SecureD, for use before SecureD has authenticated the authorized role or for use in situations where the role distinction is irrelevant. See also Crypto Officer and User.
Organizational security policy (OSP)	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Term	Explanation
Package	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
Product	A package of IT software, firmware, and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
PROM	"Acronym for Programmable Read-Only Memory. A type of read-only memory (ROM) that allows data to be written into the device with hardware called a PROM programmer. After a PROM has been programmed, it is dedicated to that data, and it cannot be reprogrammed." [MS_DICT]
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
RED	Designation for information system equipment or facilities that handle (and for data that contains) only plaintext (or, depending on the context, classified information), and for such data itself This term derives from U.S. Government COMSEC terminology.
RED/BLACK separation	An architectural concept for cryptographic systems that strictly separates the parts of a system that handle plaintext (i.e., RED information) from the parts that handle cyphertext (i.e., BLACK information) This term derives from U.S. Government COMSEC terminology.
Refinement	The addition of details to a component
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Selection	The specification of one or more items from a list in a component
Semiformal	Expressed in a restricted syntax language with defined semantics
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.
System	A specific IT installation, with a particular purpose and operational environment
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation

Term	Explanation
Threat	Threats consist of a threat agent, an asset, and a possible adverse action of that threat agent on that asset.
Threat Agent	Threat agents consist of entities, such as hackers, users, viruses, worms, and TOE development personnel, which can adversely act on assets. Threat agents may be further classified by aspects such as expertise, resources, opportunity, and motivation
TOE resource	Anything useable or consumable in the TOE
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	One of two authorized Roles that an Operator of the SecureD may assume. See also Crypto Officer and User.