MFP Data Security Kit
(AR-FR4, AR-FR5 or AR-FR6)

Security Target

Version 1.0

PREPARED BY:

COMPUTER SCIENCES CORPORATION
132 NATIONAL BUSINESS PARKWAY
ANNAPOLIS JUNCTION, MD 20701

PREPARED FOR
SHARP CORPORATION
SHARP DOCUMENT AND NETWORK SOLUTIONS GROUP
SHARP PLAZA, MAHWAH, NJ 07430-2135

Date	Version	Changes Made
March 15, 2002	0.01	Original Draft
April 1, 2002	0.02	Changes made based on Sharp comments to original draft.
May 2, 2002	0.03	Changes made to address EDR001
June 19, 2002	0.04	Changes made to address Evaluator comments
July 12, 2002	0.05	Changes made to address EDR_004
July 18, 2002	0.06	Changes made to address EDR_005
July 19, 2002	0.07	Changes made to address EDR_005
July 19, 2002	0.071	Changes made to add application note.
Sept. 11, 2002	0.072	Changes made to address version of DSK.
Sept. 16, 2002	0.073	Changes made to address Sharp's Comments
Sept. 24, 2002	0.074	Minor changes to make TSS easier to follow.
Sept. 26, 2002	0.075	Changes made to address EDR_014
Nov. 3, 2002	0.076	Changes made to address validator comments.
Nov. 4, 2002	1.0 D	Changed to version 1.0 Draft.
Dec. 3, 2002	1.0	Removed Draft. Removed old appendix, replaced with evaluated appendix.

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An 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 stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

2 The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets Evaluation Assurance Level (EAL)2.

ST Title:	Sharp Corporation Multifunction Device with Data Security Kit (AR-FR4, AR-FR5, or AR-FR6)
ST Version:	0.07
Publication Date:	September 26, 2002
Authors:	Computer Sciences Corporation, Common Criteria Testing Laboratory
TOE Identification:	Multi-Function Device with Data Security Kit (AR-FR4, AR-FR5 or AR_FR6)
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (also known as ISO 15408)
ST Evaluator:	Computer Sciences Corporation (CSC)
Keywords:	Sharp, Sharp Corporation, Sharp Imager Family, copy services, print services, scan services, object reuse, residual information protection.

1.2 References

4 The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

1.3 Conventions, Terminology, and Acronyms

5 This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.3.1 Conventions

6 This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here.

7 The CC allows several operations to be performed on security functional components; *assignment, refinement*, *selection,* and *iteration* as defined in paragraph 2.1.4 of Part 2 of the CC are:

a) The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

b) The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

c) The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

d) *Iterated* functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

e) Plain *italicized text* is used to emphasize text.

1.3.2 Terminology

8 In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions:

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human user Any person who interacts with the TOE.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authentication data Information used to verify the claimed identity of a user.

Object An entity within the TOE Security Function (TSF[1]) Scope of Control (TSC[2]) that contains or receives information and upon which subjects perform operations.

Subject An entity within the TSC that causes operations to be performed.

Authorized User A user who may, in accordance with the TOE Security Policy (TSP[3]), perform an operation.

Security Functional Components Express security requirements intended to counter threats in the assumed operating environment of the TOE.

9 The following terminology is specific to this ST.

Unauthorized User An entity that interacts with the TOE Security Function (TSF) in a benign or malicious manner.

Latent Image Data Residual information remaining on a mass storage device when a copy/print/scan/FAX job is completed, cancelled, or interrupted.

Key Operator An authorized user who manages the Sharp Corporation Data Security Kit (AR-FR4, AR-FR5, or AR-FR6) for the Sharp Imager Family (Digital Imaging Copiers*).

As defined in the CC, Part 1, version 2.1:

[1] 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.

[2] TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

[3] TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Imager Data Information on a mass storage device created by the copy/print/scan/FAX process.

DSK Refers to the Data Security Kit for Sharp Imager Family AR-FR4, AR-FR5, or AR-FR6, exclusively.

1.3.3 Acronyms

10 The following acronyms are used in this Security Target:

ACRONYM	DEFINITION
AUT	Authentication
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DSK	Data Security Kit
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FPT	Protection of Security Functions
FSP	Functional Specification
HDD	Hard Disk Drive
HLD	High Level Design
ICU	Image Control Unit
ISO	International Standards Organization
ISO 15408	Common Criteria 2.1 ISO Standard
IT	Information Technology
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MOF	Management of Functions
MTD	Management of TSF Data
NT	New Technology
OSP	Organization Security Policy
PP	Protection Profile
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target

ACRONYM	DEFINITION
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

1.4 TOE Overview

11 The TOE is a multi-function device with print, copy, scan and FAX options (hereafter referred to as a MFD). A Data Security Kit (DSK) is available to upgrade existing printers and copiers to the evaluated configuration. The TOE is available for purchase under a number of different models as shown below.

Table 1: DSK and MFD Models

DSK Model Version	Name	MFD Model
AR-FR4 version M.10	Data security kit for MFDs	*Overseas MFP-model* AR-M350, AR-M450AR-M280N, AR-M350N, AR-M450N, AR-M280U, AR-M350U, AR-M450U, AR-M310U and AR-M310N DM-3551, DM-4551 *Japanese MFP-model* AR-310M, AR-350M, AR-450M, AR-310S, AR-350S, AR-450S, AR-310F, AR-350S, AR-450S, DM-3551, DM-4551
AR-FR5 version E.10	Data security kit for Printers[4]	*Overseas model* AR-P350, AR-P450DM-3500, DM-3501DM-4500, DM-4501
AR-FR6 version J.10	Data security kit for Printers[4]	*Japanese model* AR-350LP, AR-450LP DM-3500, DM-4500

12 A MFD may store temporary document image data in RAM, on a hard disk drive (HDD) or in FLASH memory, depending on the hardware configuration.

13 The TOE provides DATA CLEAR and DATA ENCRYPTION functions to enhance the security of the MFD. The DATA CLEAR function overwrites temporary document image data with random data at the completion of each print, scan or copy job. When clearing temporary document image data from a FAX job, the DATA CLEAR function writes zeros (0) into the FLASH memory, overwriting the document images.

[4] **If a MFD is configured to print only, it is more commonly referred to as a printer.**

14 The TOE also encrypts document images prior to temporarily storing them into RAM, HDD or Flash Memory, providing an additional layer of protection from the unauthorized or accidental disclosure of temporary document images.

15 A summary of the DSK security functions can be found in Section 2, TOE Description. A detailed description of the DSK security functions can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance Claim

16 This ST conforms to Part 2 and Part 3 of the CC, Version 2.1.

2 TOE DESCRIPTION

17 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

18 The TOE is a multi-function device (MFD) configured with the AR-FR4, AR-FR5, or AR-FR6 DSK. These DSKs are factory- or field-installed firmware upgrades for a line of products listed in Table 1 in Section 1.4. These MFDs provide printer and optionally, copy, scan and FAX operations for an office where the security of sensitive information is important. The DSK provides functions for protecting document image data temporarily stored on memory or hard disk inside the MFD.

19 When the MFD is configured as a simple printer, the AR-FR5 or AR-FR6 DSK is installed. The AR-FR5 DSK is installed in printers sold outside Japan. The AF-FR6 is installed in printers sold inside Japan.

20 The AR-FR4 DSK is installed in the MFD when it is configured with an optional scanner. The AR-FR4 also supports the installation of an optional FAX board.

2.1.1 Physical Scope and Boundary

21 The TOE is a Multi-Function Device that consists of a printer and an optional scanner/FAX card as shown in Figure 1.

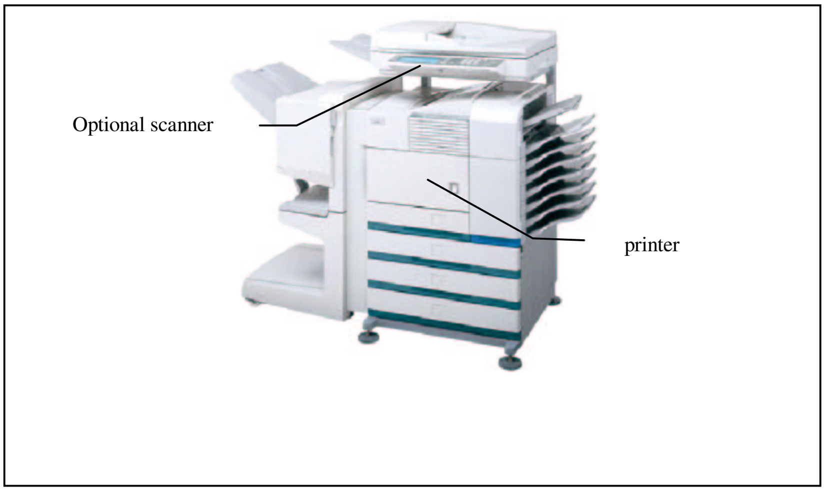

Figure 1: MFD with Optional Scanner Installed

22 The figure does not show optional sorters and paper trays.

2.1.2 Logical Scope and Boundary

23 The TOE logical boundary is the following security functions controlled by the TOE:

- Data Clear (TSF_FDC)
- Data Encryption (TSF_FDE)
- Key Generation (TSF_FKG)
- Key Destruction (TSF_FKD)
- Authentication (TSF_AUT)
- Security Management (TSF_FMT)

24 During normal operation, the MFD spools temporary document image data to a mass storage device. For printer, copier and scanner operation, the mass storage device is a RAM disk or an optional hard disk drive. For FAX operation, temporary document image data is stored in FLASH memory. The Data Clear function (TSF_FDC) clears temporary document image data from these mass storage devices by writing over the image data with a random pattern of data. For temporary document image data stored on FLASH memory, the Data Clear function overwrites a series of zeros (0) rather than random data. The key operator is able to set the number of overwrites from one to seven.

25 The Data Clear function clears data once a job is completed. To protect document image data that may remain on a mass storage device after a job is completed, the Data Encryption

function (TSF_FDE) is used to encrypt temporary document image data. Since the encryption key is stored in RAM, once the MFD is turned off or otherwise loses power, there is no way to recover the key and hence the data, from the mass storage device. Additionally, a job will not be cleared if power is removed from the MFD, however, the Key Operator has the option to configure the TOE to perform the Data Clear function when to TOE is powered on.

26 The Key Generation (TSF_FKG) and Key Destruction (TSF_FKD) functions handle the encryption keys automatically for the MFD. The MFD automatically generates an encryption key on startup (TSF_FKG) and that key is used until the MFD is turned off or otherwise loses power (TSF_FKD).

27 Only users who are assigned as Key Operators and authenticated via a personal identification number (PIN) can access the DSK security settings (TSF_AUT). Any user can utilize the other non-security-related features/functions of the MFD without authentication.

28 Security Management (TSF_FMT) reduces the likelihood of damage resulting from users abusing their authority by taking actions outside their assigned functional responsibilities. A key operator is assigned to administer the MFD. Prior to accessing any key operator functions, the key operator must provide a five (5) digit PIN.

3 TOE SECURITY ENVIRONMENT

3.1 Secure Usage Assumptions

29 This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

30 The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/Key Operator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.1.1 Environment Assumptions

31 The environmental assumptions delineated in Table 2 are required to ensure the security of the TOE:

Table 2: Environmental Assumptions

Assumption	Description
A.INSTALL	The TOE hardware and software have been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.MANAGE	There will be one or more competent Key Operator(s) assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The Key Operator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Key Operator documentation.
A.PROCEDURE	Procedures exist for granting Key Operator(s) access to the TSF.
A.CHANGE_KOC	Key Operator's Code is changed at least every sixty (60) days.

3.2 Threats

32 Table 3 identifies the threats to the TOE. The threats to the TOE are considered to be users with public knowledge of how the TOE operates and possess the skills and resources to remove the HDD or RAM from the MFD and use publicly available software and hardware tools to read the information. However, the threats do not possess access to the resources necessary to exploit the encryption or recovery of latent residual information from a HDD or RAM. The threat has access to the TOE. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 3: Threats to the TOE

Threat	Description
T.RECOVER	A user may attempt to recover temporary document image data from a copy/scan/print/FAX job by removing the mass storage device (MSD) and using commercially available tools to read its contents.

3.3 Organizational Security Policies

33 There are no organizational security policies that are determined to be relevant for the TOE.

4 SECURITY OBJECTIVES

34 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1 Security Objectives for the TOE

35 This section identifies and describes the security objectives of the TOE.

36 The TOE accomplishes the security objectives defined in Table 4.

Table 4: Security Objectives for the TOE

Objectives	Description
O.RESIDUAL	Temporary document image data from a job must not remain on a mass storage device once that job is completed.
O.REMOVE	Temporary document image data must be protected in case the MSD is removed from the TOE.
O.MANAGE	Only Key Operators shall have the capability to exercise security management functions provided by the TSF.

4.2 Security Objectives for the Environment

37 The security objectives for the IT Environment are defined in Table 5.

Table 5: Security Objectives for the TOE Environment

Objectives	Description
OE.MANAGE	Have a responsible individual be assigned as the key operator who will see that the TOE is installed, and is operated in accordance with all applicable policies and procedures necessary operate the TOE in a secure manner.

5 IT SECURITY REQUIREMENTS

38 This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

39 The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

40 These requirements are discussed separately within the following subsections.

5.1 TOE Security Functional Requirements

41 The TOE satisfies the SFRs delineated in Table 6. The rest of this section contains a description of each component and any related dependencies.

Table 6: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
Cryptographic Support (TSF_FDE, TSF_FKG, TSF_FDK)	
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
Data Clear (TSF_FDC)	
FDP_RIP.1	Subset Residual Information Protection
Authentication (TSF_AUT)	
FIA_UAU.2	User Authentication before any Action
FIA_UAU.7	Protected Authentication Feedback
Security Management (TSF_FMT)	
FMT_MOF.1 (1)	Management of Security Functions Behavior (1)
FMT_MOF.1 (2)	Management of Security Functions Behavior (2)
FMT_SMR.1	Security Roles

5.1.1 Class FCO: Cryptographic Support

42 Application Note: The AES data encryption key is generated automatically when power to the MFD is turned on. That same key is stored in RAM and is available until the MFD is turned off, or power is otherwise removed. Once the key is lost, there is no way to recover it.

43 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components

FCS_CKM.1.1 TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [none] and specified cryptographic key size [128 bits] that meet the following [AES Standard].

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

44 FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components

FCS_CKM.4.1 TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [none] that meets the following: [none].

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

45 Application Note: The AES data encryption key is stored in volatile RAM. When the MFD is turned off or power is otherwise removed that encryption key is lost.

46 FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components

FCS_COP.1.1 The TSF shall perform [data encryption] in accordance with a specified cryptographic algorithm [Rijdael algorithm] and cryptographic key size [128 bits] that meet the following [AES Standard].

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.2 Class FDP: User Data Protection

47 FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: No other components

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [

FLASH ROM, RAM disk or Hard Disk Drive].

Dependencies: No dependencies

5.1.3 Class FIA: Identification and Authentication

48 FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication

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

Dependencies: FIA_UID.1 Timing of Identification

49 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components

FIA_UAU.7.1 The TSF shall provide only [obscured feedback] to the **Key Operator** while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of Authentication

5.1.4 Class FMT: Security Management

50 FMT_MOF.1 (1) Management of Security Functions Behavior (1)

Hierarchical to: No other components

FMT_MOF.1.1(1) The TSF shall restrict the ability to *disable* and *enable* the functions [Key Operator Functions] to [the Key Operator].

Dependencies: FMT_SMR.1 Security Roles

51 FMT_MOF.1 (2) Management of Security Functions Behavior (2)

Hierarchical to: No other components

FMT_MOF.1.1(2) The TSF shall restrict the ability to *determine the behavior of* the functions [user defined automatic and manual overwrite count]to [the Key Operator].

Dependencies: FMT_SMR.1 Security Roles

52 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [Key Operator].

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

Dependencies: FIA_UID.1 Timing of identification

53 Application Note: The TOE does not support FIA_UID.1 directly. Please see the Security Functional Rational for additional details.

5.2 TOE Security Assurance Requirements

54 Table 7 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2. The SARs are not iterated or refined from Part 3.

Table 7: EAL2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1

5.3 Security Requirements for the IT Environment

55 There are no security functional requirements for the IT Environment.

5.4 Explicitly Stated Requirements for the TOE

56 This ST does not contain explicitly stated requirements for the TOE. All SFRs have been drawn from the CC.

5.5 SFRs With SOF Declarations

57 The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

58 FIA_UAU.2: The authentication mechanism has a PIN space of 10^5.

59 The product also provides two additional authentication mechanisms that are not part of the TSF. These mechanisms are associated with two different administrative interfaces to the TOE. The network interface controller (NIC) provides two interfaces to allow network settings to be viewed and optionally changed. A TELNET interface on port 23/tcp and a web interface on 129/tcp. To change NIC settings, the key operator must use the username **admin** and enter the appropriate password.

60 A separate web interface is provided for configuration of FAX services and various accounting features of the TOE. These interfaces do not affect the TOE security policy or TOE security functions, however, if resources are deleted through this interface, the data clear function is invoked to clear the data associated with the resource. These interfaces do not affect the TSFI. To change settings, the key operator must enter the username **admin** and authenticate to the interface using a password.

6 TOE SUMMARY SPECIFICATION

61 This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

62 This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1. Traceability to SFRs is also provided.

6.1.1 Cryptographic Support (TSF_FDE, TSF_FKG, TSF_FKD)

63 During normal operation, the MFD temporarily stores document image data in a mass storage device. A FLASH ROM is used to store FAX data. Copy, scan and print document image data are stored on either a RAM disk or HDD. The DSK encrypts temporary image data that is spooled to these mass storage devices using the Advanced Encryption Standard or AES. The MFD also handles the generation and destruction of cryptographic keys to support the encryption of temporary document image data. Two 128-bit keys are generated when the power is applied to the MFD. One key is used for the RAM/HDD and the other key is used for FLASH ROM.

64 **Functional Requirements Satisfied:** FCS_CKM.1, FCS_CKM.4, FCS_COP.1

6.1.2 Data Clear (TSF_FDC)

65 The DSK also provides the CLEAR DATA function that clears temporary document image data. The CLEAR DATA function over writes document image data on FLASH ROM with zeros (0). Temporary document image data residing on RAM disk or HDD are over written with a series of random data. The CLEAR DATA function can be invoked automatically after job completion, manually upon request of the key operator, and automatically upon power up if so configured by the key operator. The AUTO CLEAR AT JOB END function can be programmed to repeat the overwrite of memory one to seven times at the end of a print/scan/copy job. Since the overwrite is a time consuming operation, the DSK provides a cancel option that is only accessible to the key operator.

66 The key operator program, POWER UP AUTO CLEAR, is disabled by default. The key operator has the capability to enable this function and can change the number of times the temporary image data is overwritten from one to seven times. Random number patterns, (0s and 1s), are used in the overwrite process.

67 **Functional Requirements Satisfied:** FDP_RIP.1

6.1.3 Authentication (TSF_AUT)

68 The TOE utilizes the operation panel software module security mechanisms to provide authentication functionality through the process of the Key Operator properly entering a 5-digit PIN before access to Key Operator functions is allowed. The Key Operator must change the default PIN after installation is complete. While the Key Operator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered.

69 **Functional Requirements Satisfied:** FMT_SMR.1, FIA_UAU.2, FIA_UAU.7

6.1.4 Security Management (TSF_FMT)

70 The TSF_FMT utilizes the operation panel software module security mechanisms to allow only Key Operators the capability to enable or disable the POWER UP AUTO CLEAR function and to select the number of times an overwrite is performed for the following clear memory DSK functions:

- AUTO CLEAR AT JOB END,
- CLEAR ALL MEMORY, and
- POWER UP AUTO CLEAR.

71 The TOE restricts access to the configuration of DSK functions to the key operator.

72 **Functional Requirements Satisfied:** FMT_SMR.1, FMT_MOF.1 (1), FMT_MOF.1 (2)

6.2 Assurance Measures

73 The TOE satisfies CC EAL2 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by Sharp to satisfy the CC EAL2 assurance requirements.

Assurance Component	How requirement will be met
ACM_CAP.2 Configuration Items	The requirement for configuration items will be met by the submission of ISO 9000 documentation that shows that the vendor has a well-documented procedure for naming and tracking configuration items for each product.
ADO_DEL.1 Delivery Procedures	The requirement for delivery procedures will be met by demonstrating that the TOE is installed by the vendor at the customer's site.
ADO_IGS.1 Installation, Generation and Startup procedures	The requirement for IGS is trivially satisfied because factory certified Sharp technicians deliver the TOE and perform all necessary IGS procedures prior to releasing the TOE to the customer. This procedure meets the intent of the IGS requirement.

Assurance Component	How requirement will be met
ADV_FSP.1 Informal function specification	The vendor provided an informal function specification.
ADV_HLD.1 Descriptive high-level design	The vendor provided a descriptive high-level design document.
ADV_RCR.1 Informal correspondence demonstration	The informal correspondence demonstration is provided in the design documentation. ST to FSP in the FSP, FSP to HLD in the HLD.
AGD_ADM.1 Administrator Guidance	The vendor submitted a key operator manual and release notes.
AGD_USR.1 User Guidance	The vendor submitted a release note.
ATE_COV.1 Evidence of coverage	The analysis of test coverage was submitted in the evaluation evidence.
ATE_FUN.1 Functional testing	The test evidence was submitted to the CCTL.
ATE_IND.2 Independent testing - sample	The laboratory used development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.
AVA_SOF.1 Strength of Function	The vendor submitted an analysis of the SOF for the PIN.
AVA_VLA.2 Independent vulnerability analysis	The vendor submitted vulnerability analysis was confirmed. The laboratory conducted an independent vulnerability assessment by building on the vendor's. The laboratory conducted penetration testing.

7 PROTECTION PROFILE (PP) CLAIMS

74 The TOE does not claim conformance to a PP.

8 RATIONALE

75 This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

- security objectives to threats encountered
- environmental objectives to assumptions met
- SFRs to objectives met

Assurance Level A justification is provided for selecting an EAL2 level of assurance for this ST.

SOF A rationale is provided for the SOF level chosen for this ST.

Dependencies A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

76 This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

Table 8: Security Objectives Rationale

Objective	Threat Organizational Security Policy Assumption	Rational
O.RESIDUAL	T.RECOVER	O.RESIDUAL helps to counter the threat T.RECOVER my limiting the amount of time that temporary document image data is on the mass storage device. By removing this temporary data, the window of opportunity is reduced to the time necessary to process the job. If the job is HELD, then the data remains as long as necessary but only in encrypted form. The CLEAR MEMORY function overwrites

Objective	Threat Organizational Security Policy Assumption	Rational
		any residual data with random data, leaving the residual data virtually unreadable.
O.REMOVE	T.RECOVER	This security objective counters the threat T.RECOVER because it ensures that the temporary document image data stored on the mass storage device is encrypted. If the mass storage device is removed from the TOE prior to the completion of any jobs, the temporary document image data from those jobs is protected through the Data Encryption function making the recovery of that data impractical.
O.MANAGE	T.RECOVER	The security functions of the TOE are provided automatically once the TOE is installed in the evaluated configuration. The protection against T.RECOVER is provided by the TOE as long as a competent Key Operator maintains the TOE in accordance with the Administrator Guidance.

Table 9: Security Objectives Rationale for the Environment

Objective	Threat Organizational Security Policy Assumption	Rational
OE.MANAGE	A.CHANGE_KOC A.INSTALL A.MANAGE A.NO_EVIL_ADM A.PROCEDURE	OE.MANAGE is met by A.CHANGE_KOC, A.INSTALL, A.MANAGE, A.NO_EVIL_ADM, A.PROCEDURE by providing a trustworthy and responsible, person to oversee the installation, configuration and operation of the TOE.

8.2 Security Requirements Rationale

77 This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

78 These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Rationale For TOE Security Requirements

79 This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following paragraphs provide the security requirement to security objective mapping and a rationale to justify the mapping.

SFR	Rationale
FCS_CKM.1	Ensures that the system generates random encryption keys to support [O.REMOVE]. The strength of AES depends on random keying material.
FCS_CKM.4	Ensures that the encryption keys are destroyed when no longer needed. This requirement directly supports O.REMOVE.
FCS_COP.1	Ensures that temporary document image data written to HDD, RAM disk or FLASH ROM is encrypted. This requirement directly addresses [O.REMOVE].
FIA_UAU.2	Ensures that Key Operators are authenticated before accessing the security functionality of the TOE. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FIA_UAU.7	Ensures that only obscured feedback generated by the authentication process is provided to Key Operators before successful authentication. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FMT_MOF.1 (1)	Ensures that only Key Operators have the capability to enable, disable, or manually invoke the Security Mode SFP. This SFR traces back and aids in meeting the following objective: O.MANAGE.
FMT_MOF.1 (2)	This SFR ensures that only Key Operators have the capability to determine the behavior of the Security Mode SFP. This SFR traces back and aids in meeting the following objective: O.MANAGE.
FMT_SMR.1	Ensures that the TOE maintains the Key Operator role – a trusted individual who can administer the TOE. This SFR traces back and aids in meeting O.MANAGE.
FDP_RIP.1	Ensures that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing[5]. This SFR traces back and meets O.RESIDUAL.

[5] **The TOE has the ability to hold fax/print/scan/copy jobs for later use. Users may associate a PIN number with these held jobs to limit access to them. The temporary document image data for a held job remains on the mass storage device until the held job is removed via the web interface or the operator panel.**

Table 10: TOE SFR Mapping to Objectives

	O.RESIDUAL	O. REMOVE	O.MANAGE
FDP_RIP.1 Subset Residual Information Protection	X		
FIA_UAU.2 User Authentication before any Action			X
FIA_UAU.7 Protected Authentication Feedback			X
FMT_MOF.1 (1) Management of Security Functions Behavior (1)			X
FMT_MOF.1 (2) Management of Security Functions Behavior (2)			X
FDP_SMR.1 Security Roles			X
FCS_CKM.1 Cryptographic Key Generation		X	
FCS_CKM.4 Cryptographic Key Destruction		X	
FCS_COP.1 Cryptographic Operation		X	

8.3 Rationale For Assurance Level

80 This ST has been developed for Sharp digital image processing copiers incorporating a DSK. The TOE environment will be exposed to a low level of risk because the TOE sites in office space where it is under almost constant supervision. Agents cannot physically access the HDD, RAM disk or FLASH ROM without disassembling the TOE. Agents have no means of infiltrating the TOE with code to effect a change. As such, the Evaluation Assurance Level 2 is appropriate.

8.4 Rationale For TOE Summary Specification

81 This section demonstrates that the TSFs and Assurance Measures meet the SFRs.

82 The specified TSFs work together to satisfy the TOE SFRs. Table 11 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 11: Mapping of SFRs to Security Functions

SFR	Name	TSF	Name
FCS_CKM.1	Cryptographic Key Generation	TSF_FDE	Data Encryption
FCS_CKM.4	Cryptographic Key Destruction	TSF_FDE	Data Encryption
FCS_COP.1	Cryptographic Operation	TSF_FDE	Data Encryption

SFR	Name	TSF	Name
FDP_RIP.1	Subset Residual Information Protection	TSF_FDC	Data Clear
FIA_UAU.2	User Authentication before any Action	TSF_AUT	Authentication
FIA_UAU.7	Protected Authentication Feedback	TSF_AUT	Authentication
FMT_MOF.1 (1)	Management of Security Functions Behavior (1)	TSF_FMT	Security Management
FMT_MOF.1 (2)	Management of Security Functions Behavior (2)	TSF_FMT	Security Management
FMT_SMR.1	Security Roles	TSF_FMT	Security Management

8.4.1 TOE Assurance Requirements

83 Section 6.2 of this document identifies the Assurance Measures implemented by Sharp to satisfy the assurance requirements of EAL2 as delineated in the table in Annex B of the CC, Part 3. Table 12 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

Table 12: Assurance Measure Compliance Matrix

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ACM_CAP.2	X					
ADO_DEL.1		X				
ADO_IGS.1		X				
ADV_FSP.1			X			
ADV_HLD.1			X			
ADV_RCR.1			X			
AGD_ADM.1				X		
AGD_USR.1				X		
ATE_COV.1					X	
ATE_FUN.1					X	
ATE_IND.2					X	
AVA_SOF.1						X
AVA_VLA.1						X

8.4.2 TOE SOF Claims

84 The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2.1 and 8.2.2 demonstrate that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because the TOE protects against an unskilled attacker with no special tools from accessing the TOE. The claim of SOF-basic ensures that the mechanism is resistant to a low attack potential because the residual information cannot be accessed by subjects without sophisticated data recovery tools. RAM overwrite mitigates the threat of residual data recovery from RAM.

8.5 Rationale For SFR and SAR Dependencies

85 Table 13 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

86 All of the dependencies have been satisfied with the exception of FIA_UID.1 and FMT_MSA.2.1. FIA_UID.1 allows the user to perform certain tasks prior to being identified. The TOE has no auditing capability nor is there any gradation of privilege that would correspond to a user's identity. In other words, all users have full and equal access to the product (except for the management functions of the Key Operator). For these reasons, the TOE does not implement a user identification function and thus there is no need for the protections offered by FIA_UID.

87 FMT_MSA.2 requires that only secure values be used for security attributes. Since all users have full and equal access to the product (except for the management functions of the Key Operator) all users have equal access authorizations. There is no need to implement security attributes with subjects. Therefore, FMT_MSA.2 is trivially satisfied.

Table 13: SFR Dependencies Status

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FCS_CKM.1	Cryptographic Key Generation	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	No. With explanation
FCS_CKM.4	Cryptographic Key Destruction	FCS_CKM.2 or FCS_CKM.1, FCS_CKM.4 FMT_MSA.2	No. With explanation

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FCS_COP.1	Cryptographic Operation	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4	Yes
FDP_RIP.1	Residual Information Protection	None	
FIA_UAU.2	User Authentication before any Action	FIA_UID.1	No. With explanation
FIA_UAU.7	Protected Authentication Feedback	FIA_UAU.1	Yes
FMT_MOF.1 (1)	Management of Security Functions Behavior (1)	FMT_SMR.1	Yes
FMT_MOF.1 (2)	Management of Security Functions Behavior (2)	FMT_SMR.1	Yes
FMT_SMR.1	Security Roles	FIA_UID.1	No. With explanation

88 SAR dependencies identified in the CC have been met by this ST as shown in Table 14.

Table 14: EAL2 SAR Dependencies Satisfied

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration items	None	NA
ADO_DEL.1	Delivery procedures	None	NA
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	YES
ADV_FSP.1	Informal functional specification	ADV_RCR.1	YES
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1	YES
ADV_RCR.1	Informal correspondence demonstration	None	YES
AGD_ADM.1	Administrator guidance	ADV_FSP.1	YES
AGD_USR.1	User guidance	ADV_FSP.1	YES
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1	YES
ATE_FUN.1	Functional testing	None	NA

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	YES
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	YES
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1	YES

8.6 Rationale for Explicitly Stated Requirements

89 This ST does not contain explicitly stated requirements.

8.7 Internal Consistency and Mutually Supportive Rationale

90 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b) The security functions of the TOE satisfy the SFRs as shown in Table 11. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 13 and Table 14 and described in Section 8.6.

c) The SARs are appropriate for the assurance level of EAL2 and are satisfied by the TOE as shown in Table 12. EAL2 was chosen to provide a basic level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d) The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.

APPENDIX A:

ADDITIONAL UNEVALUATED OPTIONS

ADDITIONAL UNEVALUATED OPTIONS

The following is a list of additional options or products that could be used with the Sharp DSK to provide additional complementary security solutions. As of the writing of this ST, the items listed below have not been evaluated. These options/products were not installed on the evaluated copier.

• **AR-NC5J:** This is the standard Ethernet interface card hardware which is installed on all of the models addressed by the ST. A security update is available for the cards firmware which provides:

- IP address filtering which can restrict access to an administrator controlled list of IP addresses.
- Mac address filtering filtering which can restrict access to an administrator controlled list of Mac addresses.

In addition the following protocols are disabled:

TELNET
RARP

• **Mail Server and NT Server Authentication:** This enhancement to the evaluated products scanning application firmware adds desktop-like log-on with user name and password to control access to copier scanning and provide a network based audit trail.

• **Secure Print Release:** This NT/W2000 server-based application complements the Data Security Kit by holding documents to be printed on the evaluated MFP in the network's secured NT/W2000 print queue until the user arrives at the copier/printer and provides identification in the form of an ID card and PIN. This minimizes the risk that unauthorized personnel would see a print job before it is recovered from the printer. Immediately after the job prints, the Data Security Kit clears the print job data from the copier's memory.

• **Secure Print Release Station:** This computer-based application provides security control over the release of print jobs making it possible to manually deny printing of a particular job or delete it.

• **Enterprise Accounting Server:** This NT/W2000 server application bundle can track all print and copy activity by user, by workgroup, or by device providing complete records on usage patterns. It provides a network-based audit trail of print and copy activity and can control access to print and copy services.

The product, as evaluated, did not include any of the above-mentioned options/products. No claims are made in this ST regarding Data Security Kit functionality not included in this ST.

Use of the server based applications above do not modify the evaluated configuration. The network interface card hardware with the security updates described above is identical to that in the evaluated configuration. It is emphasized that *operating the TOE outside its evaluated configuration negates the security claims made in this ST*.