National Information Assurance Partnership

COMMON CRITERIA EVALUATION AND VALIDATION SCHEME

VALIDATION REPORT

SHARP CORPORATION
DATA SECURITY KIT (DSK) FOR THE SHARP CORPORATION IMAGER FAMILY, (AR-287, AR-337, AR-407, AND AR-507)

Report Number: CCEVS-VR-01-0001-201

Dated: APRIL 18, 2001

VERSION: 1.0

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
INFORMATION TECHNOLOGY LABORATORY
100 BUREAU DRIVE
GAITHERSBURG, MD 20899**

**NATIONAL SECURITY AGENCY
INFORMATION ASSURANCE DIRECTORATE
9800 SAVAGE ROAD STE 6740
FORT GEORGE G. MEADE, MD 20755-6740**

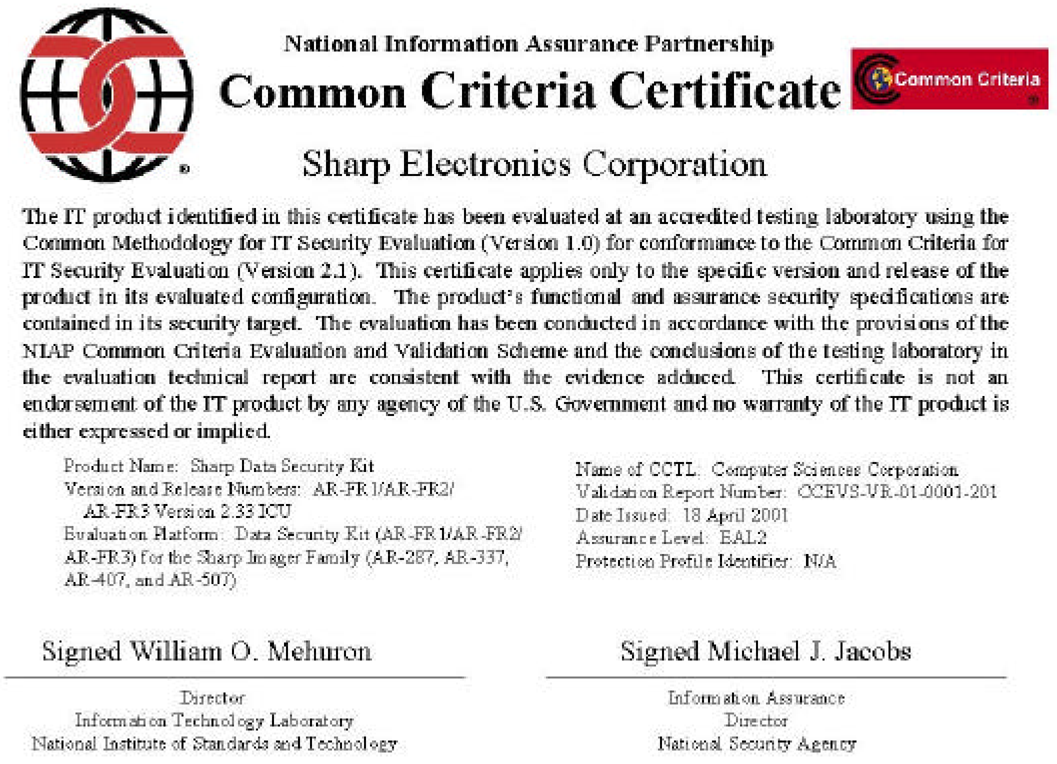
ACKNOWLEDGEMENTS

Validation Team

Mario Tinto
Michael Allen
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Computer Science Corporation
Annapolis Junction, Maryland



National Information Assurance Partnership

Common Criteria Certificate

Common Criteria

Sharp Electronics Corporation

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Sharp Data Security Kit
Version and Release Numbers: AR-FR1/AR-FR2/
AR-FR3 Version 2.33 ICU
Evaluation Platform: Data Security Kit (AR-FR1/AR-FR2/
AR-FR3) for the Sharp Imager Family (AR-287, AR-337,
AR-407, and AR-507)

Name of CCTL: Computer Sciences Corporation
Validation Report Number: CCEVS-VR-01-0001-201
Date Issued: 18 April 2001
Assurance Level: EAL2
Protection Profile Identifier: N/A

Signed William O. Mehuron
Director
Information Technology Laboratory
National Institute of Standards and Technology

Signed Michael J. Jacobs
Information Assurance
Director
National Security Agency

EXECUTIVE SUMMARY

This report provides a description of, and the evaluation results for the hard disk drive (HDD)-erase feature of the Data Security Kit (DSK) for the Sharp Corporation Imager Family (AR-287, AR-337, AR-407, and AR-507). This product provides commercial grade protection against the threat of residual data remaining stored on the hard drive of the digital copier after copy, print, or scan jobs are completed. It addresses this threat by overwriting data files once with random patterns after the copy/print/scan job is completed. Additionally, the "key operator" (i.e., a user with administrative privileges) can choose to manually overwrite the entire HDD. This typically would be done after a power interruption, in order to guarantee that no residual sensitive data remained on the HDD. The manual overwrite could also be performed in cases when the HDD needs to be removed. Doing so would render any recovery of residual data both costly and time-consuming, requiring specialized equipment.

The evaluation was performed by Computer Sciences Corporation (CSC), and was completed during April 2001. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by CSC and submitted to the validators. Key sections of this report are extracted in their entirety from the original CCTL ETR and are so indicated. The evaluation performed by CSC was conformant with the EAL2 level, defined in Version 2.1 of the Common Criteria and Version 1.0 of the CEM, and demonstrates that the product satisfies the functional requirements defined in the Security Target for this product. This validation report presents all evaluation results, their justifications, and any findings derived from the work performed during the evaluation.

The validation team assigned to the evaluation monitored the activities of the CSC evaluation team, participated in team meetings, provided guidance on technical issues as well as evaluation processes, reviewed selected evaluation evidence, and reviewed selected individual work units as well as the various versions of the ETR. The validation team concludes that the CCTL findings are accurate, and their conclusions justified. Accordingly, the family of Data Security Kits (i.e., AR-FR1, AR-FR2, AR-FR3 for the Sharp Imager Family AR-287, AR-337, AR-407, and AR-507), as defined in the Security Target (Version 1.1) are awarded certification at the EAL2 level of assurance.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Identification

1 Table 1~~Table 1~~ provides information needed to identify and control this Validation Report, the Security Target (ST) and the Target of Evaluation (TOE). It also identifies the major participants in the evaluation.

Table 1~~1~~: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
CCTL	Computer Sciences Corporation (CSC)
Validation Report	Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Validation Report, version 1.0. CCEVS-VR-0001; VID-201
Security Target	Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Security Target, version 1.1.
Protection Profile	Not Applicable
Target of Evaluation	Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507)
Assurance Level	EAL2
Developer	Sharp Corporation
Sponsor	Sharp Corporation Sharp Document and Network Solutions Group Sharp Plaza, Mahwah, NJ 07430-2135
Evaluators	Computer Sciences Corporation Ms. Vanessa Schroader Ms. Letty Ruff Ms. Traci Harrell Mr. Halvar Forsberg Mr. Rey Robles Government Participants None
Validators	Mr. Mario Tinto (Aerospace Corporation) Mr. Mike Allen (Aerospace Corporation)

1.2 Background

2 The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories, called Common Criteria Testing Laboratories (CCTL), using the Common

Methodology for Information Technology Security Evaluation (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

3 The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

1.3 References

4 The following documents are referenced throughout this report.

5 [CC_PART1] *Common Criteria for Information Technology Security Evaluation* – Part 1: Introduction and general model, dated August 1999, Version 2.1.

6 [CC_PART2] *Common Criteria for Information Technology Security Evaluation* – Part 2: Security functional requirements, dated August 1999, Version 2.1.

7 [CC_PART2A] *Common Criteria for Information Technology Security Evaluation* – Part 2: Annexes, dated August 1999, Version 2.1.

8 [CC_PART3] *Common Criteria for Information Technology Security Evaluation* – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

9 [CEM_PART1] *Common Methodology for Information Technology Security Evaluation* – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

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

1.4 Document Organization

11 This report is organized according to the guidance provided for Validation Reports provided in Scheme Publication #3, Version 0.5. The report is divided into the following chapters:

12 Chapter 1, Introduction, describes the background of the Scheme, identifies Validation Report (VR), ST, and TOE control identifiers, and identifies the developer, sponsor, evaluators, and validators of the evaluation;

13 Chapter 2, Architectural Description of the TOE, provides a high-level description of the TOE and its major components;

14 Chapter 3, Results of the Evaluation, provides a verdict and supporting rationale for each assurance component completed for the evaluation;

15 Chapter 4, Conclusions and Recommendations;

16 Chapter 5, List of Evaluation Deliverables;

17 Chapter 6, List of Acronyms and Glossary of Terms; and

18 Chapter 7, Problem Reports, lists the Evaluation Discovery Reports (EDRs) and Observation Reports (ORs) that were raised during the evaluation and their status.

2 ARCHITECTURAL DESCRIPTION OF THE TOE

19 This section describes the high-level design of the Sharp Data Security Kit (DSK) and identifies its interfaces. The information presented is not intended to describe the complete design, but rather to provide sufficient information to enable the reader to understand the Data Security Kit design and provide evidence that the system (Target of Evaluation, TOE) satisfies its functional requirements, as described in the DSK_ST.

20 The DSK, AR-FR1, AR-FR2, and AR-FR3, are factory- or field-installed ROM upgrades for the Sharp AR-287/337/407/507 family of digital image processing copiers. The AR-FR1 operates on the AR-287 and AR-337 models; the AR-FR2 operates on the AR-407 model, and the AR-FR3 operates on the AR-507 model. Each DSK performs identically in terms of the overwrite function. However, because each copier model has unique engine timing, there is a separate DSK, each distinguished by individual part numbers, for each copier in the Imager Family.

21 The DSK product adds the Hard Disk Drive (HDD)-erase functionality which provides the capability to perform overwrites of the portions of the HDD relevant to the copy, print, or scan job being performed (automatic overwrite), or to overwrite the entire HDD (manual overwrite).

22 The authentication and security administration functions occur outside the TOE, and are provided by the IT environment.

23 The DSK is an optional firmware enhancement to the digital image processor copiers in the form of ROMs. The design of the copiers provides physical separation from the IT environment. The Sharp AR-287/337/407/507 digital image processing copiers buffer document data on a HDD. With automatic HDD-erase enabled, after the completion of any multi-functional printer operation, random numbers are written over the hard disk areas used to temporarily store document data. During that time, usually a second or less, a message is displayed on the operator panel that the HDD data is being cleared and no other operations are available. The Key Operator is provided the capability to enable or disable the automatic HDD-erase function.

24 The DSK also allows the Key Operator to overwrite the entire HDD. For example, on occasions when it is necessary to remove a HDD, the Key Operator can manually invoke the DSK HDD-erase function before removing the drive to mitigate the risk that residual document data might fall into the wrong hands. This function would also be used in the case of loss of power. When power is dropped from the copier, any data that had been written to the HDD remains. After a successful power up, the Key Operator must manually invoke the HDD-erase function to ensure that all residual data is overwritten.

The authentication and security management functions are provided by the Operation Panel Interface (OPE) in the IT environment. Figure 1 depicts the HDD-erase security function concept.

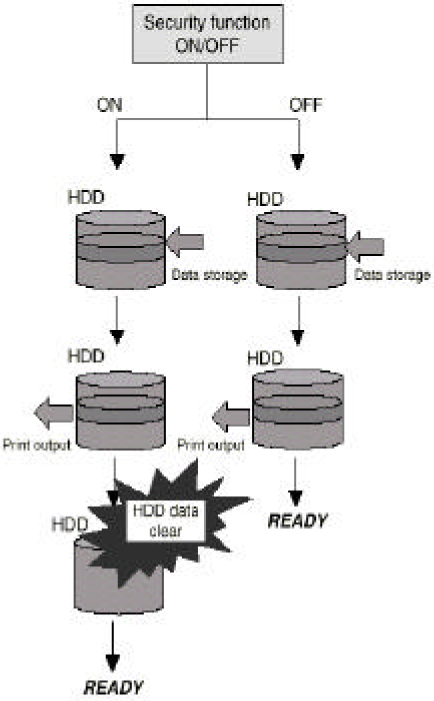


Figure 1~~1~~. DSK HDD-Erase Security Function

~~1.1~~2.1 Evaluation Methods, Techniques, and Standards[1]

25 The *evaluator action elements* documented in [CC_PART3] for EAL2 assurance components were the basis of the approach for evaluating the TOE. In addition, [CEM_PART2] Chapter 6 was used to define the specific evaluator actions for conducting the evaluation.

26 To manage the evaluation effort and to document progress and findings, the evaluation team developed evaluation work package reports for each assurance family as listed in Table 2. A work package captures every *evaluator action element* for the assurance family and corresponding [CEM_PART2] work units and allows the evaluator to document how each action element was addressed during the evaluation. Within each work package, the evaluators identified all the evidence used to support their findings, documented their analysis, and assigned a verdict for each assurance component and evaluator action element based on the results of completing all work units.

Table 2~~2~~: Evaluation Work Packages

Work Package	Assurance Component
Security Target	ASE

[1] This section and the remainder of Chapter 2 were extracted from the CSC ETR in their entirety

Work Package	Assurance Component
Configuration Management	ACM_CAP.2
Delivery and Operation	ADO_DEL.1
	ADO_IGS.1
Development	ADV_FSP.1
	ADV_HLD.1
	ADV_RCR.1
Guidance Documents	AGD_ADM.1
	AGD_USR.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessments	AVA_SOF.1
	AVA_VLA.1

27 Team assignments were given per work package in which primary and secondary evaluators were assigned to complete each work package. The evaluation team conducted weekly status meetings with attendance open to both the Validator and the Developer. The Validator was given copies of all work packages and evaluation evidence upon request.

28 For the ATE_IND.1.2E evaluator action element, the evaluation team wrote a test plan and conducted functional testing in accordance with the plan. For the AVA_VLA.1.2E evaluator action element, the evaluation team did an analysis for possible obvious vulnerabilities. The team concluded the Data Security Kit did not have any obvious vulnerabilities.

29 Prior to testing, the hard drive was initialized with known data. The hard disk was removed and, using a test PC, scanned to ensure that the known data was correct. The hard disk was reinstalled and a copy, print, or scan function was performed with hard disk erase function invoked, either manually and as an automatic option. The hard disk was removed and again checked on the test PC. In each test case, for print, scan, or copy, both in manual and automatic mode, the hard disk had been successfully overwritten with random 1s and 0s (i.e., random data).

30 Throughout the evaluation, the evaluation team generated Observation Reports (ORs) to request clarification on Common Criteria requirements. ORs were submitted to the Validator for posting and resolution. Evaluation Discovery Reports (EDRs) were generated for the following reasons:

- To identify a potential vulnerability or deficiency found in the TOE;
- To identify deficiencies found in evaluation evidence; and
- To request additional information from the vendor.

31 EDRs were submitted to the vendor and not formally distributed to the NIAP Validation Body, although the Validator did receive a copy of all EDRs. Chapter 7, Problem Reports, contains a listing of all ORs and EDRs that were generated during the evaluation.

2.2 Evaluation Configuration

32 The evaluated TOE configuration consisted of an AR-507 with an AR-FR3 DSK. The DSK consists of a set of three replacement ROMs, one each for the Process Control Unit (PCU), Image control Unit (ICU) and Operation Panel Interface (OPE) circuit boards. The evaluated version of the PCU ROM is 2.30; the evaluated version of the ICU ROM is 2.33, and the evaluated version

of the OPE ROM is 2.33. The DSK ROM on the ICU, the ICU circuit board, and the HDD comprise the TOE physical boundary. The other two DSK ROMs and their associated circuit boards and interfaces to the TOE provide the IT environment.

2.3 Evaluation Tools

33 PTS DiskEditor, version 1.04, was used to verify the TOE hard disk erase functionality.

3 RESULTS OF THE EVALUATION[2]

34 This Chapter presents the findings and results of the evaluation by identifying the verdict with supporting rationale for each assurance component that constitutes an activity for the ST Evaluation and EAL2 Evaluation. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. Three mutually exclusive verdict states can be rendered:

- *Pass*, if the evaluator successfully completes a [CC_PART3] evaluator action element. The conditions for successfully completing an evaluator action element are defined by the constituent work units of the related [CEM_PART2] action.

- *Inconclusive*, if the evaluator has not completed one or more work units of the [CEM_PART2] action related to the [CC_PART3] evaluator action element.

- *Fail*, if the evaluator unsuccessfully completes a [CC_PART3] evaluator action element.

35 Section 5 provides the overall verdict of the evaluation team's findings as defined in [CC_PART1] Chapter 5, and determined by the verdict assignments presented in this Chapter.

36 Table 3 provides a listing of the activities, associated assurance components, and evaluator action elements for a ST Evaluation and an EAL2 Evaluation. Details of evaluator actions for each evaluator action element are documented in the work package reports.

Table 3~~3~~: Evaluation Activities, Assurance Components, and Action Elements

Activity	Assurance Component	Evaluator Action Elements
ST Evaluation	ASE_DES.1	ASE_DES.1.1E, ASE_DSE1.2E, ASE_DES1.3E
	ASE_ENV.1	ASE_ENV.1.1.E, ASE_ENV.1.2E
	ASE_INT.1	ASE_INT.1.1E, ASE_INT.1.2E, ASE_INT.1.3E
	ASE_OBJ.1	ASE_OBJ.1.1E, ASE_OBJ.1.2E
	ASE_PPC.1	No claimed Protection Profile compliance.
	ASE_REQ.1	ASE_REQ.1.1E, ASE_REQ.1.2E
	ASE_SRE.1	There are no explicitly stated requirements.
	ASE_TSS.1	ASE_TSS.1.1E, ASE_TSS.1.2E
Configuration Management	ACM_CAP.2	ACM_CAP.2.1E
Delivery and operation	ADO_DEL.1	ADO_DEL.1.1E, Implied Action based on ADO_DEL.1.2D
	ADO_IGS.1	ADO_IGS.1.1E, ADO_IGS.1.2E
Development	ADV_FSP.1	ADV_FSP.1.1.E, ADV_FSP.1.2E
	ADV_HLD.1	ADV_HLD.1.1E, ADV_HLD.1.2E
	ADV_RCR.1	ADV_RCR.1.1E
Guidance documents	AGD_ADM.1	AGD_ADM.1.1E
	AGD_USR.1	AGD_USR.1.1E

[2] Chapter 3 is extracted from the CSC ETR in its entirety, with the exception of slight editorial changes.

Activity	Assurance Component	Evaluator Action Elements
Tests	ATE_COV.1	ATE_COV.1.1E
	ATE_FUN.1	ATE_FUN.1.1E
	ATE_IND.2	ATE_IND.2.1E, ATE_IND.2.2E, ATE_IND.2.3E
Vulnerability assessment	AVA_SOF.1	AVA_SOF.1.1E, AVA_SOF.1.2E
	AVA_VLA.1	AVA_VLA.1.1E, AVA_VLA.1.2E

3.1 Security Target Evaluation Results

37 The objective of this evaluation is to determine if the Data Security Kit (AR-FR1/ARFR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Security Target, version 1.1, is complete, consistent, technically sound, and to determine if the ST provides a suitable baseline for evaluation of the TOE.

3.1.1 ASE_DES.1 – TOE Description

38 The evaluator examined the TOE description section of the Sharp Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Security Target, and determined that the section describes the Sharp Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), the TOE. The TOE description defines the boundaries of the TOE in both a physical and logical way. It was clear to the evaluator after reading the TOE description that the product is a firmware enhancement to the digital image processor copiers in the form of ROMs. With automatic Hard Disk Drive (HDD) erase enabled, after the completion of any multi-functional copy/print/scan operation, random data is written over the hard disk areas used to temporarily store the document data.

39 The TOE description was examined for any contradictory statements that might appear within this section of the ST. No statements were found while examining the TOE description that contradicted each other. The TOE description was examined for consistency with other sections of the ST. This consistency examination was performed in conjunction with the other ASE work units. The description given of the functionality and assurance measures of the TOE are consistent throughout the entire ST. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

40 The 11/21/00 version of the Common Criteria Interpretations was also reviewed for this work unit.

41 ***ASE_DES.1 Verdict:***

42 The evaluation team concluded that the TOE has met the assurance requirements of ASE_DES.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.1.2 ASE_ENV.1 – Security environment

43 The TOE security environment section of the [DSK_ST] and the 11/21/00 version of the Common Criteria Interpretations were used to satisfy this assurance component. The evaluator examined the Security Environment and determined that it identified the assumptions, organizational security policies, and threats for the TOE and its environment. Because the

[DSK_ST] contains no organizational security policies, the evaluator examined the identified assumptions and threats.

44 In reviewing the individual assumptions and threats, the evaluator also determined that the assumptions and threats were coherent, understandable to the evaluator, and to the audience for the [DSK_ST]. An overall consistency verdict was reached after all the assumptions and threats had been reviewed. Part of the consistency examination was to ensure that no assumptions were in conflict with the threats and that the threats, as specified, were plausible based on the threat agents described, the attack and the asset that could be under attack. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

45 ***ASE_ENV.1 Verdict:***

46 The evaluation team concluded that the TOE has met the assurance requirements of ASE_ENV.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.1.3 ASE_INT.1 – ST Introduction

47 The evaluator checked and examined the security target introduction section of the [DSK_ST] and the 11/21/00 version of the Common Criteria Interpretations to satisfy the evaluator elements of this assurance component. The ST introduction of the [DSK_ST] clearly identifies the [DSK_ST] with a name and a version. Along with the [DSK_ST] identification, it also gives a unique label with a version number for the TOE under evaluation. The CC version used to develop the ST is clearly identified in the [DSK_ST].

48 The evaluator determined that the [DSK_ST] introduction contained a narrative description of the [DSK_ST]. The [DSK_ST] clearly states what is in the [DSK_ST] in a manner and level that clearly defines the Data Security Kit product, as an HDD-erase function that, when enabled, writes random data over the sections of the HDD where data was stored prior to final output.

49 The [DSK_ST] introduction clearly states the conformance claims of the [DSK_ST]. It mentions the relevant Part 2 and 3 conformance claims to the CC.

50 The evaluator determined that the [DSK_ST] introduction is coherent by reading the section and being able to understand what was being described in the section. Further, it was determined that the section was consistent because the statements of functionality and use of terms in this section did not conflict with each other.

51 It was determined that the [DSK_ST] introduction is consistent with the other sections of the [DSK_ST]. The determination of consistency with the other sections of the [DSK_ST] was reached while working on the other evaluator actions in other ASE components. The evaluator examined for consistency in the [DSK_ST] by reviewing all the other sections of the [DSK_ST]. The evaluator looked for any conflict between the description of functionality through out the different sections of the [DSK_ST]. This included looking at the functional requirements and the security functions described in the TOE summary specification. The words of the assumptions, threats, and objectives were compared with each other and the functional requirements to determine that they did not conflict with each other. The conventions and terminology were used consistently throughout the [DSK_ST]. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

52 ***ASE_INT.1 Verdict:***

53 The evaluation team concluded that the TOE has met the assurance requirements of ASE_INT.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.1.4 ASE_OBJ.1 – Security objectives

54 The evaluator checked and examined the security objectives, including the security objectives rationale, of the [DSK_ST] and the 11/21/00 version of the Common Criteria Interpretations to satisfy the evaluator elements of this assurance component. The [DSK_ST] security objective section separates security objectives into those for the TOE and those for the environment.

55 The evaluator examined the mappings supplied by the developer in the [DSK_ST] to see that all security objectives for the TOE were traced to the identified threats to be countered by the TOE. The evaluator developed a table that contained the threats and objectives for the TOE. This table was used to determine that all threats for the TOE were being mapped to the objectives of the TOE and that all the objectives of the TOE were being used and mapped to the threats of the TOE. The evaluator's table was a check on the developer's generated table to determine that it was accurate with respect to the objectives and threats being listed and described elsewhere in the [DSK_ST]. A table was also used to verify that the objectives for the environment were traced to the assumptions. The evaluator read each security objective in the [DSK_ST] to make a determination that each objective was clearly stated and understandable.

56 As part of determining the tracings discussed above, the evaluator also examined the rationale that was being given by the developer as to why a particular mapping was suitable to cover an identified threat and/or assumption. The rationale given by the developer explained how the objectives are suitable to cover the threats and/or assumptions stated in the [DSK_ST]. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

57 ***ASE_OBJ.1 Verdict:***

58 The evaluation team concluded that the TOE has met the assurance requirements of ASE_OBJ.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.1.5 ASE_PPC.1 – PP claims

59 No compliance with Protection Profiles was claimed in this ST, thus all work units in this section are not applicable.

60 ***ASE_PPC.1 Verdict:***

61 The evaluation team concluded that because the TOE has no claims of compliance to a Protection Profile, this requirement is not applicable.

3.1.6 ASE_REQ.1 – IT security requirements

The evaluator checked and examined the [DSK_ST] and the 11/21/00 version of the Common Criteria Interpretations to accomplish the evaluator activities for ASE_REQ. Part of the examination was to see if the IT Security Requirements were transcribed from the CC correctly. The IT security requirements in the [DSK_ST] were compared to Part 2 and Part 3 of the CC. If the IT security requirement was not exactly transcribed from the CC then the operations performed on the IT security requirements in the [DSK_ST] were examined. The examination of the operation was used to determine if the operation fit within the bounds for that specific IT security requirement as stated in the CC. Part of the comparison involved making sure that those operations that were performed in the [DSK_ST] were properly identified.

62 The IT security requirement section of the [DSK_ST] was checked for a statement of Strength of Function (SOF) and checked that the appropriate requirements contained a SOF statement. The SOF rationale was examined to determine if it was appropriate for the TOE and the environment of the TOE.

63 The dependency analysis and rationale was confirmed through independent analysis by the evaluator. The rationale for the assurance and functional requirements was examined. The examination of this rationale determined that the security requirements met the objectives specified in the [DSK_ST]. The evaluator examined the IT security requirements rationale for a demonstration of how the security requirements are a mutually supportive and consistently whole.

64 ***ASE_REQ.1 Verdict:***

65 The evaluation team concluded that the TOE has met the assurance requirements of ASE_REQ.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.1.7 ASE_SRE.1 – Explicitly stated IT security requirements

66 There are no explicitly stated IT security requirements.

67 ***ASE_SRE.1 Verdict:***

68 The evaluation team concluded that since there are no explicitly stated requirements for the TOE all work units in this section are not applicable.

3.1.8 ASE_TSS.1 – TOE summary specification

69 The evaluator checked and examined the TOE summary specification, including the TOE summary specification rationale, of the [DSK_ST] and the 11/21/00 version of the Common Criteria Interpretations to accomplish the evaluator activities for ASE_TSS. The evaluator examined the TOE summary specification for the functional and assurance requirements.

70 The evaluator examined each security function to determine that it was at a level of detail that summarized the security functionality and determined if the security function could satisfy the security functional requirement that it was mapped to. The evaluator also checked that each security functional requirement had at least one security function being mapped to it. The evaluator checked for all TOE security functions that were realized by a probabilistic or permutation mechanism. The evaluator found no TOE security functions realized by a probabilistic or permutation mechanism.

71 The mapping of assurance measures to assurance requirements was examined. The evaluator examined each mapping to ensure that each assurance requirement had a measure mapped to it and the measure was appropriate to satisfy a particular assurance requirement. The evaluator determined that the TOE summary specification, including the TOE summary specification rationale, was complete, coherent, and internally consistent because neither contained conflicting information. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

72 **ASE_TSS.1 Verdict:**

73 The evaluation team concluded that the TOE has met the assurance requirements of ASE_TSS.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.2 Configuration Management (CM) Results

74 The objectives this activity are to determine whether the developer has clearly identified the TOE and its associated configuration items. A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

3.2.1 ACM_CAP.2 – CM capabilities

75 The evaluator checked and examined DSK_ISO9K_SP_E and DSK_ST. The evaluator read the DSK_ST to understand the definition of the TOE and the Interface Control Unit (ICU). The DSK is a factory- or field-installed ROM upgrade for the Sharp AR-287/337/407/507 family of digital image processing copiers.

76 Sharp is a certified ISO 9000 vendor. The DSK_ISO9K_SP_E represents the CM processes that are documented in the Quality Manual required for ISO 9000 certification, and describes how Sharp identifies and tracks configuration items. In addition, the Sharp CM system requires quality inspections and tests throughout production to verify specification compliance. This CM system includes the elements of the TOE, with modifications to the TOE clearly tracked and identified.

77 The TOE (ICU) is stamped with a number identifier that associates it with the Sharp AR-287, AR-337, AR-407, and AR-507 digital image processing copiers that can be configured with the DSK. The vendor provided a Configuration Item (CI) list that references a recent software revision for the DSK. The CI list identifies the Interface Control Unit (the TOE). The evaluator confirmed that the CI list provided by the Sharp Corporation uniquely identified the ICU. The ICU is referenced by version number, and the files on the CI list were identified by file name, file size, date and time of last modification. A second CI list showed changes had been made to six software files on the list and they were also identified by the date, time, and it was noted that modifications were also reflected by a change in file size.

78 ***ACM_CAP.2 Verdict:***

79 The evaluation team concluded that the TOE has met the assurance requirements of ACM_CAP.2. Therefore, a **pass** verdict has been issued for this assurance component.

3.3 Delivery and Operation Results

80 The objectives of this activity is:

- to determine whether the delivery documentation describes all procedures used to maintain integrity when distributing the TOE to the user's site, and

- to determine whether the procedures and steps for the secure installation, generation, and start-up of the TOE have been documented and result in a secure configuration.

3.3.1 ADO_DEL.1 – Delivery Procedures

81 The requirements for delivery call for system control and distribution facilities and procedures that provide assurance that the recipient receives the TOE that the sender intended to send.

82 An Observation Report (DSK_OR_001) was generated for ADO_DEL.1 because the Sharp Corporation (the developer) is in possession of the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) and accompanying Data Security Kits (AR-FR1/AR-FR2/AR-FR3) throughout the delivery and installation process. The Oversight Board concurred with the evaluator that integrity was maintained and the requirement for publicly available TOE delivery procedures was not necessary.

83 ***ADO_DEL.1 Verdict:***

84 The evaluation team concluded that the TOE has met the assurance requirements of ADO_DEL.1. Therefore, a **pass** verdict was issued for this assurance component.

3.3.2 ADO_IGS.1 – Installation, generation, and start-up procedures

85 "To confirm that the start-up procedures result in a secure configuration," the evaluator followed the instructions provided in the manuals to change the Key Operator's Code and to engage the security features. Once the "auto clear at job end" was turned on, it remained on until the Key Operator disengaged it. The "clear all HDD-data" executed the manual erase as designed. All features functioned as advertised.

86 The AR-FR1, AR-FR2, AR-FR3 Installation Manual did not specifically address changing the factory installed Key Operator Code, which was addressed in EDR_001. Sharp Corporation provided Errata Sheets that addressed changing the Key Operator code from the factory default setting. One Errata Sheet states, "… the procedure used to change the Operator Key Code from the default to a new user selected code, must be completed by the Key Operator once the copier has been installed. Under no circumstances should the key operator use the default "Key Operator Code"."

87 A second potential problem was identified in the Key Operator's Guides. The guides address "whether persons other than persons who know the key operator code number will be permitted access via a computer or other equipment, either directly or through a telephone line, to the copier's key operator programs. To require key operator code entry for access to key operator programs, press the check box of 'DISABLING OF PC/MODEM ACCESS' to display a check mark in the check box. … NOTE: The customers must choose the setting of this program by themselves. If this program is not set, external operators can access the key operator programs from a computer or other equipment without key operator code entry. (This program is set in the factory default setting.)" As a result of this finding, EDR_004 was generated to address this issue. In the Errata Sheets prepared by Sharp, in response to EDR_004, it states that the PC Modem Access "is not available on the Sharp Imager copiers marketed in the United States."

88 ***ADO_IGS.1 Verdict***

89 The evaluation team concluded that the TOE has met the assurance requirements of ADO_IGS.1. Therefore, a **pass** verdict was issued for this assurance component.

3.4 Development Results

90 The objective of this activity is:

- to determine whether the developer has provided an adequate description of the security functions of the TOE and whether the security functions provided by the TOE are sufficient to satisfy the functional requirements of the ST;
- to determine whether the high-level design is sufficient to satisfy the functional requirements of the ST, provides a description of the TSF in terms of major structural units with functional coherence, and is a realization of the functional specification; and
- to determine whether the developer has correctly and completely implemented the requirements of the ST and functional specification in the high-level design.

3.4.1 ADV_FSP.1 – Informal functional specification

91 To satisfy this assurance component, the evaluator initially reviewed the CCIMB list of interpretations for those relative to the evaluation for this assurance component. The evaluator found only one interpretation, CCIMB_INTERP-0029 that was relative to this work unit, and used the guidance presented during this effort. The evaluator also relied on the supporting information provided in the [DSK_KOG], and [DSK_SCHEMATICS_A-F] to corroborate and supplement the [DSK_FSP]. The evaluator used the [DSK_ST] and the supporting descriptions of the TOE provided in the aforementioned evidence to determine the TOE boundary. Through examination of these documents the evaluator determined that the external interfaces to the TOE are the Operation Panel Interface (OPE) to Image Control Unit (ICU), and Process Control Unit (PCU) to Image Control Unit (ICU). An interface between the raw copy/scan/print image data and the ICU was also identified. This interface was determined not to be security relevant because it is simply a data stream and not processed by the ICU.

92 The [DSK_FSP] identifies the TOE Security Functional Interfaces (TSFIs) and maps the TSFIs to SFRs as required at the EAL2 level of assurance. The [DSK_FSP] also specifies the TSFI input parameters and behavior of the TSFIs in the management of the functional components of the TOE.

93 The evaluation of the functional specification was linked to the review of the ST. The evaluator used the information provided in the [DSK_ST] to map the security functional requirements to the security functions and the TSFIs, as presented in the [DSK_FSP]. This permitted the evaluator to confirm the TOE security functions satisfy the security functional requirements.

94 Using the above mapping, the evaluator examined the security functions described in the TOE Summary Specification [DSK_ST] to confirm the security functional requirements were completely satisfied, and that the security functionality actually existed in the TOE to support the functional requirement. The evaluator also used the interface “descriptions” in the [DSK_SCHEMATICS_A-F] to assess the appropriateness of the listed external interfaces.

95 Through examination of the correspondence mappings and the description of the security functions it can be seen that the TOE has all the necessary security functionality to satisfy the security functional requirements in the [DSK_ST].

96 ***ADV_FSP.1 Verdict:***

97 The evaluation team concluded that the TOE has met the assurance requirements of ADV_FSP.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.4.2 ADV_HLD.1 – Descriptive high level design

98 The high-level design document provided all the necessary information that was required in these work units. The document clearly provided a description of the TSF in terms of major structures (subsystems). These subsystem are:

a) HDD-erase Subsystem

b) Monitoring Subsystem

c) Data Manipulation Subsystem

d) OPE Subsystem

99 These subsystems are fully described in the [DSK_HLD] document along with the hardware, firmware and software associated in each subsystem. [DSK_HLD] also provides the required description of the interfaces to and from these subsystems. The evaluator has verified that the [DSK_HLD] has identified all the externally visible interfaces to these subsystems.

100 The evaluator also noted that the TOE Security Functional Requirements found in the [DSK_ST] were identified and addressed in the high-level design document. These subsystems were clearly identified as to the security functionality of each subsystem and the interfaces between subsystems.

101 ***ADV_HLD.1 Verdict:***

102 The evaluation team concluded that the TOE has met the assurance requirements of ADV_HLD.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.4.3 ADV_RCR.1 – Informal correspondence demonstration

103 The evaluator has reviewed the key documents in these work units.

a) The ST [DSK_ST]

b) The Functional Specification [DSK_FSP]

c) The High Level Design [DSK_HLD]

d) The correspondence analysis between the TOE summary specification and the functional specification [DSK_RCR]

104 In accordance with the work units’ activities, the evaluator has determined that all security functions identified in the TOE summary specification were represented in the functional specification and that they are represented properly. The evaluator noted that the security functions were addressed properly in the corresponding interfaces.

105 The evaluator also identified that for all the security functions there was a correspondence indicator to a TSF subsystem associated to it. The evaluator using the correspondence analysis document verified that it was possible to map each security function identified in the functional specification to a TSF subsystem described in the high-level design.

106 **ADV_RCR.1 Verdict:**

107 The evaluation team concluded that the TOE has met the assurance requirements of ADV_RCR.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.5 Guidance Documents Results

108 The objectives of this activity are:

- to determine whether the administrator guidance to system administrative personnel describes how they administer the TOE in a secure manner, and
- to determine whether the user guidance describes the security functions and interfaces provided by the TSF for non-administrative users and whether this guidance provides instructions and guidelines for the secure use of the TOE.

3.5.1 AGD_ADM.1 – Administrator guidance

109 The Sharp Data Security Kit is an option that can be factory-installed onto specific models of the Sharp imager or can be installed at the customer site by a Sharp factory technician. The administrator (Key Operator) guidance for the Data Security Kit consists of the AR-FR1/AR-FR2/AR-FR3 Data Security Kit Operation Manual (DSK_KOM). The TOE installation manual (DSK_DIM) is boxed with the TOE. However, as the TOE is installed either at the factory or by a Sharp factory technician, the consumer does not use this manual.

110 The individual(s) designated as the Key Operator(s) is/are responsible for performing the security functions associated with the TOE. The DSK_ST and Sharp Data Security Kit Documentation Additions and Corrections (Errata Sheets) state that the Key Operator must change the factory default password upon installation and change the password at lease every 60 days to maintain proper security. The DSK_KOM describes the Key Operator's security-relevant functions specific to the TOE. These are enabling or disabling the automatic hard disk erase option that erases the hard disk after the completion of a copy, print or scan job, or performing the manual erase option after the end of a print, scan or copy function. The DSK_KOM also specifies the conditions under which the automatic hard disk erase function does not complete and the condition under which the Key Operator must perform a manual erase of the hard disk.

111 The evaluator examined the administrator guidance, the DSK_ST, DSK_DOM, the DSK_KOG, the DSK_KOG2, and the Sharp Data Security Kit Documentation Additions and Corrections (Errata Sheets) and determined that administrative security functions and interfaces available to the administrator (Key Operator) are described.

112 The DSK_DOM is the administrator guidance specific to the DSK. The DSK_DOM explains the conditions that result in a job interrupt or when the power is interrupted while data is being cleared. Sharp Corporation provided an errata sheet that warns the user that any data that was on the hard drive prior to the power loss is not erased.

113 ***AGD_ADM.1 Verdict:***

114 The evaluation team concluded that the TOE has met the assurance requirements of AGD_ADM.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.5.2 AGD_USR.1 – User guidance

115 The evaluation team determined that because there is no interface provided to human users, the requirements for user guidance is trivially satisfied.

116 ***AGD_USR.1 Verdict:***

117 The evaluation team determined that because there is no interface provided to human users, the requirements for user guidance are **trivially satisfied**.

3.6 Testing Results

118 The objectives of this activity is:

- to determine whether the test coverage evidence shows correspondence between the tests identified in the test documentation and the functional specification;
- to determine whether the developer's functional testing demonstrates that all security functions perform as specified; and
- to determine whether the TOE behaves as specified and to gain confidence in the developer's test results by independently testing a subset of the TSF and by performing a sample of the developer's tests.

3.6.1 ATE_COV.1 – Evidence of coverage

119 The vendor provided the test procedure and the testing results from tests performed on the Sharp copier models, AR-507, AR-407, AR-337, and AR-287, equipped with the Data Security Kit, AR/FR1, AR/FR2, and AR/FR3. Testing is performed on all releases as part of Sharp Corporation's normal operating procedures. The tests were to assure that the DSK hard disk erase function operated as claimed (automatic and manual HDD-erase for copy, print, scan jobs). At the end of a job, the data on the hard drive was erased by invoking either the manual erase function or by the selection of the automatic erase function prior to the job. The tests performed verified to the evaluator's satisfaction that the hard disk erase function operated as claimed, thereby satisfying the FDP_RIP.1 SFR.

120 ***ATE_COV.1 Verdict:***

121 The evaluation team concluded that the TOE has met the assurance requirements of ATE_COV.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.6.2 ATE_FUN.1 – Functional testing

122 The developer provided functional testing of the TOE security functions. Sharp testing was both thorough and exhaustive. They tested each of the DSK functions (manual and automatic

overwrite) in each of the operating modes (copier, scanner, printer) on each of the copier models. In each case, Sharp verified the DSK overwrote the data on the HDD.

123 The evaluator reviewed these tests and procedures and found them to be engineered properly with the proper use of controlled items (i.e., after each test, Sharp verified that the data on the HDD was overwritten). The tests provided details that were easy to follow, thus making them easy to reproduce. The evidence provided contained all of the key elements required for functional testing:

a) test plan,

b) test procedures,

c) expected test results, and

d) actual test results.

124 Using this evidence, the evaluator was able to piece together the rationale provided in these work units. The verdicts and rationale of these work units clearly verify that the developer has provided, and performed, adequate functional testing on the copier to prove that the security feature of hard disk erase worked as described.

125 ***ATE_FUN.1 Verdict:***

126 The evaluation team concluded that the TOE has met the assurance requirements of ATE_FUN.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.6.3 ATE_IND.2 – Independent testing – sample

127 The objective of ATE_IND.2 is for the evaluator to review and sample test the test results provided by the developer and to introduce some independent tests to verify the developer's security functions. The evaluator examined the developer supplied tests, the 11/21/00 Common Criteria Interpretations, and used the independent testing document [DSK_EAL2_IND] to accomplish the evaluator activities for ATE_IND.2. The developer-supplied test plans provided good coverage of the security functionality of the TOE. The Sharp method of verification was to physically examine the contents of the hard drive for each test case. The evidence for ATE_IND.2 is documented in the Sharp Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Independent Testing Report.

128 The TOE was delivered and installed by trained Sharp Technicians, making it operational and ready for testing. The developer's testing in conjunction with the evaluator's independent test clearly displayed the operations required to setup the TOE as well as its coverage of the key security function, user data protection, as stated in [DSK_ST].

129 The evaluator's tests consisted of a sampling of the developer's supplied test and the test described in the independent testing document [DSK_EAL2_IND]. The evaluator selected the following tests to reproduce test results for the copy mode: [AUTO MODE VERIFICATION], [MANUAL MODE VERIFICATION] and [INTERRUPT]. The DSK performed overwrites identically for each condition, not discriminating between modes, other than to write to different sectors of the hard drive. The sampling performed by the evaluation team is sufficient to verify the Sharp test results and conclusions. The [DSK_EAL2_IND] provides a complete record of all

independent tests including verification of developer's test data. The results of the tests were consistent with the expected test results and verified the requirements as stated by the [DSK_ST].

130 Specific emphasis was placed on the function that enforced the user data protection, FDP_RIP.1. Additionally, the evaluator wanted assurance that all required user data protection actions were successful.

131 The independent testing targeted the user data protection security function. A mapping of independent test sets to security functionality is provided in the table below.

Independent Test Set	Security Function	Security Functional Requirement
TSF_UDP_1	TSF_UDP	FDP_RIP.1
TSF_UDP_2 (Sample Test)	TSF_UDP	FDP_RIP.1
TSF_UDP_3 (Sample Test)	TSF_UDP	FDP_RIP.1

132 In conclusion, the tests provided and the additional test performed by the evaluator adequately covers the developer's corresponding security functions. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

133 ***ATE_IND.2 Verdict:***

134 The evaluation team concluded that the TOE has met the assurance requirements of ATE_IND.2. Therefore, a **pass** verdict has been issued for this assurance component.

3.7 Vulnerability Assessment Results

135 The purpose of the vulnerability assessment activity is to determine the exploitability of flaws or weaknesses in the TOE in the intended environment. This determination is based upon analysis performed by the developer, and is supported by evaluator penetration testing.

3.7.1 AVA_SOF.1 – Strength of TOE security functions

136 The evaluator checked the [DSK_ST] and found that there were no security mechanisms for which there were SOF claims expressed as a SOF metric. The SOF claim for the security of the TOE is expressed solely as a rating, SOF-basic. In the [DSK_SOF] there is an analysis of the SOF for the authentication mechanism allocated to the IT environment as claimed in the [DSK_ST].

137 The functional specification, the high-level design, and the administrative guidance were examined for each product model. It was determined that the only probabilistic or permutational mechanism, claimed to provide security functionality for the TOE, is the authentication mechanism (i.e., personal identification number) associated with the Key Operator authentication. This authentication mechanism has a PIN space of 10^5. However, it must be noted that this mechanism is outside of the TOE boundary.

138 The evaluator reviewed the analysis presented by the developer regarding the number of random authentication number entries. To evaluate this claim, the evaluator used the test platform to experiment/test the number of entries per minute possible. This test was performed in the CCTL lab, without the "pressure of being discovered." Over a 5-minute period the evaluator was able to average twelve (12) random authentication code attempts per minute. This rate was based on using memory recall to prevent duplicate number entry, as well as, focusing on entering only

digits versus mixed control panel elements. Through this analysis, the evaluator was able to verify the claim of SOF-basic.

139 The only other means of attacking the TOE is through disassembling the copier. The evaluator agrees with the developer's assertion that in the operational environment proposed for the TOE/product, the elapsed time to identify and exploit an attack on the TOE was not practical. The evaluator performed an informal test of this assertion through observing the amount of time where both printers and copiers were idle in the CSC office spaces. This observation showed that on average, there was about 10 min. of idle time where the product was unattended. Additionally, the evaluator considered the issue that to realize the threat of obtaining a latent image, the attacker would have to have prior knowledge of when a targeted document would be processed by the product. Based on the analysis performed, it was determined that a direct attack on the TOE would result in a claim of SOF-high, making this form of attack impractical.

140 Also, it must be noted that the administrative/operator guidance discuss that the hard disk drive is overwritten with random numbers generated by the TOE. However, since there are no claims, security or otherwise, made in the ST with respect to the data used to over-write the hard disk drive, the evaluator considered this probabilistic mechanism irrelevant to this evaluation.

141 Therefore, based on the total analysis of SOF, the only practical means of attacking the TOE is through the authentication mechanism, providing the overall claim of SOF-basic.

142 ***AVA_SOF.1 Verdict:***

143 The evaluation team concluded that the TOE has met the assurance requirements of AVA_SOF.1. Therefore, a **pass** verdict has been issued for this assurance component.

3.7.2 AVA_VLA.1 – Vulnerability analysis

144 The evaluator reviewed the Sharp Security Target, Functional Specification, High Level Design, Administrative Guidance, Strength of Function Analysis, and the Vulnerability Analysis for this work package. Based on the Vulnerability Analysis, the developer's search for obvious vulnerabilities included threat agents, residual data on the HDD, tampering with the copier, environmental threats, and vendor documentation. The developer also checked public domain sources for possible identified vulnerabilities and attacks.

145 The vulnerabilities that were determined to exist for the TOE were residual data left on the HDD and tampering with the DSK. The residual data left on the HDD is mitigated through the use of the HDD erase functions. "The administrative documentation identifies and describes the conditions under which the HDD auto-erase function can not be performed until a copier problem is cleared and the job completes (i.e., paper tray empty, paper jam, toner empty, and interrupt copy), and conditions under which a HDD erase can not be performed (i.e., during warm-ups or service call)." The fact that the documentation calls attention to the times when the erase function cannot be performed makes the Key Operator aware and thus enables him to take proper action and mitigate the threat.

146 The tamper threat is mitigated by the fact that the TOE is internal to the copier and therefore physically inaccessible without disassembling the copier. Even though data can be printed from the network, there is no direct path between the TOE and the network. Since there is no direct access to the TOE, it is safe from tampering.

147 The efforts of the team to develop penetration tests resulted in the conclusion that obvious penetration attempts are unlikely. A number of attempts to get the copier to respond to incorrect Key Operator Codes or conflicting/multiple sets of directions provided no response from the copier.

148 As indicated in the DSK_HLD and DSK_FSP, direct access to the TOE is not possible without disassembling the copier, thus penetration is not possible via the product control, i.e., user interface panel. Penetration is also not possible via the network because the network does not have a direct path to the TOE. Whether copies are made from the platen or via the network the TOE does not process the data. It simply receives a data stream. Therefore, there is not a penetration test that can be devised to directly penetrate the TOE.

149 ***AVA_VLA.1 Verdict:***

150 The evaluation team concluded that the TOE has met the assurance requirements of AVA_VLA.1. Therefore, a **pass** verdict has been issued for this assurance component.

4 CONCLUSIONS AND RECOMMENDATIONS[3]

151 This evaluation applied to Data Security Kit, AR-FR3; however, the findings also apply to DSK AR-FR1 and AR-FR2 because they all function identically. Each DSK has a unique part number (AR-FR1, AR-FR2, or AR-FR3) to correlate to a specific copier model in the Imager Family because each copier model has unique engine timing.

152 The Sharp Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Security Target, version 1.1 was assessed for this evaluation. The assurance component verdicts presented in Chapter 5 of this report received final evaluation verdicts of **Pass**. Therefore, the evaluation team assigns an overall **Pass** verdict for satisfying the evaluator action elements defined for EAL 2. As defined by [CC_PART1] Chapter 5, the TOE was found to be Part 2 conformant and Part 3 conformant. The evaluation team recommends that an EAL 2 certificate rating be issued for the TOE.

[3] Chapter 4 is extracted from the CSC ETR in its entirety.

5 VALIDATOR COMMENTS

This product has been evaluated as “commercial grade” equipment to protect against “scavenging” of data from temporary storage media (i.e., a hard disk drive or HDD). It does this by overwriting the appropriate section of the imager’s HDD once with random data after each job is completed. It also provides an administrator (called the key operator) a function to overwrite the whole HDD once with a random pattern. This equipment has not been evaluated against requirements that warrant its use to counter threats in high risk environments where there is the possibility of use of specialized data recovery equipment.

6 LIST OF EVALUATION DELIVERABLES[4]

153 Table 4 provides a listing of evidence supplied to the CCTL as evaluation deliverables.

Table 44: Evaluation Deliverables

Identifier	Date of Receipt	Issuing Body	Title
[DSK_DSMS]	08/17/00	Sharp Corporation	Data Security Mode Specification for Cougar 2000
[DSK_HIS]	08/17/00	Sharp Corporation	Sharp Digital Copying Machine HDD Security Instructions (Spreadsheet)
[DSK_SM]	08/17/00	Sharp Corporation	Sharp Service Manual Digital Copier, Code 00ZAR507//PIE for Models AR-287;337;407;and 507
[DSK_PARTS1]	08/17/00	Sharp Corporation	Sharp Parts Guide, Code 00ZAR507//PIE for Models AF-287;337;407; and 507.
[DSK_PARTS2]	08/17/00	Sharp Corporation	Sharp Parts Guide, Code 00ZAR507//PIE for Models AF-280/285/335;AR-281/286/336; and AR-250/405/505.
[DSK_MOM]	8/17/00	Sharp Corporation	Sharp Model AR287, AR-337, AR-407 Digital Copying Machine Operation Manual
[DSK_KOG2]	10/30/00	Sharp Corporation	Sharp Model AR287, AR-337, AR-407 Digital Copying Machine Key Operator's Guide
[DSK_SCHMATICS_A]	08/17/00	Sharp Corporation	Sharp Circuit Diagram Code 00AR507//C1E, Digital Copier, Models AR-287;AR-337;AR-407;AR-507
[DSK_SCHMATICS_B]	08/17/00	Sharp Corporation	File CD01.PDF: Circuit Diagrams
[DSK_SCHMATICS_C]	08/17/00	Sharp Corporation	File CD02.PDF: Circuit Diagrams
[DSK_SCHMATICS_D]	08/17/00	Sharp Corporation	File CD03.PDF: Circuit Diagrams
[DSK_SCHMATICS_E]	08/17/00	Sharp Corporation	File CD04.PDF: Circuit Diagrams
[DSK_SCHMATICS_F]	08/17/00	Sharp Corporation	File Ar505cle Sharp Circuit Diagram Code 00ZAR505//C1E, Digital Copier, Models AF-501;AR505.
[DSK_SFC]	08/28/00	Sharp Corporation	C2000 Security Function Check
[DSK_ISO9K_SP_E]	08/28/00	Sharp Corporation	ISO-9001 Quality Manual, Eighth Edition, May 9, 1997, English Translation

[4] This section extracted from the CSC ETR in its entirety

Identifier	Date of Receipt	Issuing Body	Title
[DSK_ISO9K_SP_J]	08/28/00	Sharp Corporation	ISO-9001 Quality Manual, Eighth Edition, May 9, 1997 – Japanese
[DSK_ISO9_CERT]	08/28/00	Sharp Corporation	Certification of Registration, Certificate, JMI-0015, revision May 14, 1999 for Quality Management System compliant with ISO-9001:1994.
[DSK_ITD]	09/12/00	Sharp Corporation	Sharp Imager Documentation, Confidential Imager Technical Documentation for CSC Project
[DSK_DIM]	10/30/00	Sharp Corporation	AR-FR1/AR-FR2/AR-FR3 Installation Manual
[DSK_DOM]	10/20/00	Sharp Corporation	AR-FR1/AR-FR2/AR-FR3 Data Security Kit Operations Manual
[DSK_INSTL]	10/30/00	Sharp Corporation	Installation Guide, AVA-1505AE/AI External and Internal ISA to-SCSI-2 Host Adapters
[DSK_KOG]	10/30/00	Sharp Corporation	Model AR-507 Digital Copying Machine Key Operator’s Guide
[DSK_MOM2]	10/30/00	Sharp Corporation	Sharp Model AR507 Digital Copying Machine Operation Manual
[DSK_ONTRK]	10/30/00	Sharp Corporation	Ontrack Test Results of HDD Erase Function
[DSK_TST_EA1] [DSK_TST_EA2]	03/02/01	Sharp Corporation	Sharp Developer Test Report - Email Answers Sharp Developer Test Report (revised) – Email Answers
[DSK_SUB_D]	03/02/01	Sharp Corporation	Sharp Data Security Kit Subsystem Diagram
[DSK_SEC_MOD]	03/02/01	Sharp Corporation	Cougar Comparison of Setting Security Mode
[DSK_DAT_HIST]	03/02/01	Sharp Corporation	AR-FR3 ICU Program File Data History (Configuration Item List)
[DSK_Errata Sheet2]	03/02/01	Sharp Corporation	Sharp Data Security Kit Documentation Additions and Corrections (Errata Sheet) for the Data Security Kit Operation Manual and Sharp Imager Digital Copying Machine Key Operator’s Guide (revised information)
[DSK_Errata Sheet1]	02/21/01	Sharp Corporation	Sharp Data Security Kit Documentation Additions and Corrections (Errata Sheet) for the Circuit Diagram CODE 00ZAR507//C1E – PDFAr507c1e and Sharp Imager Digital Copying Machine Key Operator’s Guide
[DSK_ISO9_INFO]	03/02/01	CSC Consulting	ISO9001 Description Information

Identifier	Date of Receipt	Issuing Body	Title
[DSK_FSP]	02/27/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Functional Specification, version 0.6
[DSK_HLD]	03/01/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) High Level Design, version 0.3
[DSK_RCR]	02/20/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Correspondence Evidence, version 0.2
[DSK_ST]	03/06/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Security Target, version 1.1
[DSK_TST_COV]	02/28/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Test Coverage Analysis, version 1.0
[DSK_AVA]	03/05/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Vulnerability Assessment, version 0.3
[DSK_SOF]	03/02/01	CSC Consulting	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Strength of Function, version 0.2

7 LIST OF ACRONYMNS AND GLOSSARY OF TERMS[5]

154 The following acronyms are used throughout this document.

CC	Common Criteria
CCEL	Common Criteria Evaluation Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CSC	Computer Sciences Corporation
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
ETR	Evaluation Technical Report
MRA	Mutual Recognition Arrangement
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
OR	Observation Report
PP	Protection Profile
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

[5] This section also reproduced from the CSC ETR in its entirety.

8 PROBLEM REPORTS[6]

8.1 Evaluation Discovery Reports

155 This section contains all EDRs raised as a result of work performed during the evaluation. Table 5 provides the EDRs unique identifier, the work package in which the problem was discovered, a brief summary of the problem, and the status.

Table 5~~5~~: List of Evaluation Discovery Reports

Identifier	Work Package	Title	Status
EDR-01	ADO_IGS	Key Operator Code Change	Closed
EDR-02	Security Target	Security Target Evaluation Discoveries	Closed
EDR-03	ADV_FSP	DSK - Additional External Interfaces	Closed
EDR-05	Development	Correspondence Evaluation Discoveries	Closed
EDR-06	Security Target	Security Target Evaluation Discoveries	Closed

8.2 Observation Reports

156 This section of contains all ORs raised as a result of work performed during the evaluation. Table 6 provides the ORs unique identifier with corresponding Scheme identifier in parenthesis, as appropriate, a brief summary of the problem, and an indication of the problem's current status. The OR that remains open is not expected to impact the final verdict or results of this evaluation.

Table 6~~6~~: List of Observation Reports

Identifier	Work Package	Title	Status
DSK_OR_001	ADO_DEL.1	TOE delivered and installed by Sharp Technicians	Closed
DSK_OR_002	AGD_USR.1	User Guidance for the Sharp Data Security Kit	Closed
DSK_OR_003	ACM_CAP.2	ACM_CAP.2 – CM under ISO9000	Open

[6] This section extracted from the CSC ETR in its entirety.