# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

## Sharp Corporation
## Multifunction Device
## with Data Security Kit
## (AR-FR4 V.M.10, AR-FR5 V.E.10, AR-FR6 V.J.10)

**Report Number: CCEVS-VR-02-0028**

**Dated: 2 December 2002**

**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**

Aerospace Corporation

Columbia, Maryland

**Common Criteria Testing Laboratory**

Computer Sciences Corporation

Annapolis Junction, Maryland

## Table of Contents

# 1 EXECUTIVE SUMMARY

The TOE is a Sharp Corporation printer/copier/scanner/FAX, referred to as a multifunction device (MFD), that is configured with a firmware upgrade that protects document image data that is temporarily stored in the MFD memory or the hard drive.[1] Basically, the product provides a data clear capability for stored image data. During normal operation, the MFD spools temporary document image data to a mass storage device. In the case of printer, copier, and scanner operation this is either a RAM disk or, optionally, a hard drive. For FAX operation, such data is stored in FLASH memory. The data clear function overwrites the image data once the job is completed; the administrator can set the data clear function to perform up to seven overwrites of the spooled image data.

The product also includes a data encryption function that encrypts temporary image data to protect it while in spool memory.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the findings of the evaluation team are accurate, and the conclusions justified. This validation report 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.

[1] The details of the various configuration options and the specific firmware upgrades are discussed in the Security Target.

# 2 IDENTIFICATION

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 (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if applicable);
- The organizations and individuals participating in the evaluation.

| Item | Identifier |
|---|---|
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Target of Evaluation | Sharp Multifunction Device with Data Security Kit (AR-FR4, AR-FR5, or AR-FR6) |
| Protection Profile | None |
| Security Target | *Sharp MFP Data Security Kit (AR-FR4, AR-FR5, or AR-FR6) Security Target;* Version 1.0, dated 3 December 2002 |
| Evaluation Technical Report | Evaluation Technical Report, Sharp Corporation, Sharp Multifunction Device with Data Security Kit (AR-FR4, AR-FR5, or AR-FR6); Version 1.0, 8 November, 2002 |
| Conformance Result | Part 2 conformant, Part 3 conformant, EAL2 |
| Sponsor | Sharp Corporation |
| Developer | Sharp Corporation |
| Evaluators | Computer Sciences Corporation |
| Validators | The Aerospace Corporation |

**Table 1: Evaluation Identifiers**

# 3 SECURITY POLICY

The Sharp MFD with the appropriate Data Security Kit (DSK) does not implement a security policy in the traditional sense of enforcing a set of access control rules. It does, however, protect image data from unauthorized access, and implements a data clear function that makes image data from one job unavailable to subsequent jobs by overwriting the temporary storage between jobs. Temporary image data on FLASH ROM (FAX data) is overwritten with zeroes, and data on RAM disk or the hard drive (print, scan, and copy data) is overwritten with randomly-generated data. In effect, the product implements mechanisms that satisfy the security functional requirement (SFR) for *Subset residual information protection* (i.e., FDP_RIP.1) defined in the CC.

The DSK encrypts spooled temporary image data using the Advanced Encryption Standard (AES). Two 128-bit keys are generated when the MFD is powered on; one key is used for encrypting data stored on RAM or the hard drive, and the other key is used for encrypting data stored on FLASH ROM. This protects the image data while it is in temporary storage.

## 3.1 Role Differentiation Policy

The product supports two roles: the user role and an administrative role (i.e., the *Key Operator*). A "user" is anyone with physical access to the MFD; there is no authentication required of users, and there are no constraints on the ability of users to access the functions of the device. That is, the services provided by the MFD (i.e., print, scan, copy, or FAX) are universally available.

Key Operators are identified by a PIN introduced through the control panel. Authorized key operators may exercise the various options presented by the DSK (e.g., data clear on power-on, number of overwrites).

## 3.2 Security Management

The key operator is authorized by entering a 5-digit PIN through the MFD's control panel. Once authorized, the key operator may choose among several options and set the associated parameters. Specifically, the key operator may choose among the following:

- Clear data at the completion of each job. When this function is chosen the key operator can also choose the number of times the clear function is performed (up to seven times);
- Clear data manually, i.e., when activated by the key operator;
- Clear temporary storage when the MFD is powered up. For this function also, the number of overwrites may be selected.

# 4 ASSUMPTIONS

## 4.1 Usage Assumptions

Administrators are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

For networked or distributed operations, it is assumed that all elements of the network operate under the same security rules and constraints and are subsumed under a single management domain.

## 4.2 Environmental Assumptions

It is assumed that the hardware has been delivered, installed, and configured in accordance with the manufacturer's established procedures. Additionally, it is presumed that there are procedures in place that require the key operator to change his access code (i.e., the PIN) at least each sixty (60) days.

# 5 ARCHITECTURAL INFORMATION

The Data Security Kits are hardware and firmware upgrades to the standard Multi-Function Devices (i.e., printer/copier/scanner/fax). These are proprietary, and are either installed at the factory or at the user's site by a vendor technician.

For simple printer configurations of the MFD, the AR-FR5 or AR-FR6 is installed; the AR-FR4 DSK is installed for configurations that include the optional scanner and/or FAX capabilities.

# 6 DOCUMENTATION

The following product documentation is provided to consumers:

- Sharp MFP Data Security Kit (AF-AR4, AF-AR5, AF-AR6) Security Target, Version 1.0, dated 2002/12/03;
- Sharp Data Security Kit Operation Manual;
- Operations Manuals.

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence, covering:

- Functional specification;
- High-level design;
- Test plans, test scripts, and test results;
- Installation manuals;

# 7 IT PRODUCT TESTING

## 7.1 Vendor Testing

At EAL2 testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TSF have been tested."[2]

The vendor testing covered 13 of the 53 interfaces identified in the functional specification, and included:

- Data clear function;
- Cryptographic support functions (e.g., key generation,, cryptographic operation);

The authentication capability, administrator management functions, and key destruction were not included in the vendor test suite.[3]

## 7.2 Evaluator Testing

The evaluators had the TOE installed, as required by the published procedures, by a Sharp technician. Installation, generation and startup were witnessed by the evaluation team, and tests were subsequently performed to determine whether the configurations (for each of the Data Security Kits) conformed to the specifications. Versions and model numbers were also verified.

Evaluator testing covered the following areas:

- Verification of encryption of data stored on hard drive;
- Verification of data clear function;
- Administrator capabilities;
- Authentication of administrator and enforcement of administrator role.

[2] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

[3] The evaluation team ascertained that the cryptographic function (AES algorithm) was previously tested by the vendor, using test vectors provided by NIST. The testing of the cryptographic function was documented by the vendor, and reviewed by the evaluators.

# 8 EVALUATED CONFIGURATION

The evaluated configurations encompassed all three of the identified Data Security Kits, as identified in the Security Target. Each of the DSKs is associated with specific models of the MFD, as a function of the particular MFD model and associated capabilities (e.g., print, scan, copy, or fax). There are no configuration options as usually understood. The appropriate DSK is installed, either at the factory or on-site, by a Sharp technician.

# 9 RESULTS OF THE EVALUATION

The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL 2**. The product was evaluated and tested against the claims presented in *Sharp MFP Data Security Kit (AR-FR4, AR-FR5, or AR-FR6) Security Target;* Version 1.0, dated 3 December 2002, as well as the associated interface specification (i.e., FSP).

## 9.1 Evaluator comments

There are no Evaluator Comments.

# 10 SECURITY TARGET

The ST, *Sharp MFP Data Security Kit (AR-FR4, AR-FR5, or AR-FR6) Security Target;* Version 1.0, dated 3 December 2002 is included here by reference.

# 11 GLOSSARY

| | |
|---|---|
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| DSK | Data Security Kit |
| CCTL | Common Evaluation Testing Laboratory |
| CEM | Common Evaluation Methodology |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| MFD | Multi Function Device |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards & Technology |
| NSA | National Security Agency |
| PP | Protection Profile |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| TSFI | TOE Security Function Interface |

# 12 BIBLIOGRAPHY


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

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

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

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

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

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

[7] Sharp MFP Data Security Kit (AF-AR4, AF-AR5, AF-AR6) Security Target, Version 1.0, Rev. 1.46; dated 2002/12/03.

[8] Sharp Multifunction Device with Data Security Kit (AF-AR4, AF-AR5, or AF-AR6), Independent Test Plan and Report; October 30, 2002

[9] Evaluation Technical Report, Sharp Corporation, Sharp MFP Data Security Kit (AF-AR4, AF-AR5, or AF-AR6) Version 1.0; 8 November 2002

[10] Penetration Test Plan and Report, Sharp Multifunction Device with Data Security Kit (AF-AR4, AF-AR5, or AF-AR6); November 6, 2002.