



Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

| | |
|---------------------|---|
| Application date/ID | September 15, 2005 (ITC-5059) |
| Certification No. | C0045 |
| Sponsor | TOSHIBA TEC CORPORATION |
| Name of TOE | System Software for e-STUDIO352/452 |
| Version of TOE | V1.0 |
| PP Conformance | None |
| Conformed Claim | EAL3 |
| TOE Developer | TOSHIBA TEC CORPORATION |
| Evaluation Facility | Electronic Commerce Security Technology Laboratory Inc. Evaluation Center |

This is to report that the evaluation result for the above TOE is certified as follows.

March 24, 2006

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-Technology Promotion Agency, Japan

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the “General Requirements for IT Security Evaluation Facility”.

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations (as of 01 December 2003)

Evaluation Result: Pass

“System Software for e-STUDIO352/452 V1.0” has been evaluated in accordance with the provision of the “IT Security Certification Procedure” by Information-Technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:

This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

| | |
|--|----|
| 1. Executive Summary | 1 |
| 1.1 Introduction | 1 |
| 1.2 Evaluated Product | 1 |
| 1.2.1 Name of Product | 1 |
| 1.2.2 Product Overview | 1 |
| 1.2.3 Scope of TOE and Overview of Operation..... | 1 |
| 1.2.4 TOE Functionality..... | 2 |
| 1.3 Conduct of Evaluation..... | 5 |
| 1.4 Certificate of Evaluation..... | 5 |
| 1.5 Overview of Report | 6 |
| 1.5.1 PP Conformance..... | 6 |
| 1.5.2 EAL | 6 |
| 1.5.3 SOF | 6 |
| 1.5.4 Security Functions..... | 6 |
| 1.5.5 Threat..... | 7 |
| 1.5.6 Organisational Security Policy | 7 |
| 1.5.7 Configuration Requirements | 7 |
| 1.5.8 Assumptions for Operational Environment | 7 |
| 1.5.9 Documents Attached to Product | 7 |
| 2. Conduct and Results of Evaluation by Evaluation Facility..... | 8 |
| 2.1 Evaluation Methods | 8 |
| 2.2 Overview of Evaluation Conducted | 8 |
| 2.3 Product Testing | 8 |
| 2.3.1 Developer Testing..... | 9 |
| 2.3.2 Evaluator Testing..... | 10 |
| 2.4 Evaluation Result | 10 |
| 3. Conduct of Certification | 11 |
| 4. Conclusion..... | 12 |
| 4.1 Certification Result..... | 12 |
| 4.2 Recommendations..... | 12 |
| 5. Glossary | 13 |
| 6. Bibliography | 15 |

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “System Software for e-STUDIO352/452 V1.0” (hereinafter referred to as “the TOE”) conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, TOSHIBA TEC CORPORATION.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product: System Software for e-STUDIO352/452
Version: V1.0
Developer: TOSHIBA TEC CORPORATION

1.2.2 Product Overview

This product is the system software of the digital multi function device “e-STUDIO352/452” (hereafter referred to collectively as the “MFP”) manufactured by TOSHIBA TEC CORPORATION.

The system software provides general functions as a MFP as well as the function of data overwrite and permanently erase on the user document data deleted from the e-STUDIO352/452 HDD.

The function of data overwrite and permanently erase includes the function to collectively and completely delete all user document data from the HDD before the HDD is disposed or replaced. This function also prevents unauthorized restore of data.

1.2.3 Scope of TOE and Overview of Operation

The TOE is the control software of MFP. Figure 1-2 depicts the relation to each part of MFP. As shown in Figure 1-1 below, MFP is used as a terminal to send/receive data to/from facsimiles, a terminal to send Email to Email servers, and a remote printer for

remote PCs in network environments as well as they are installed in general offices as a standalone copier.

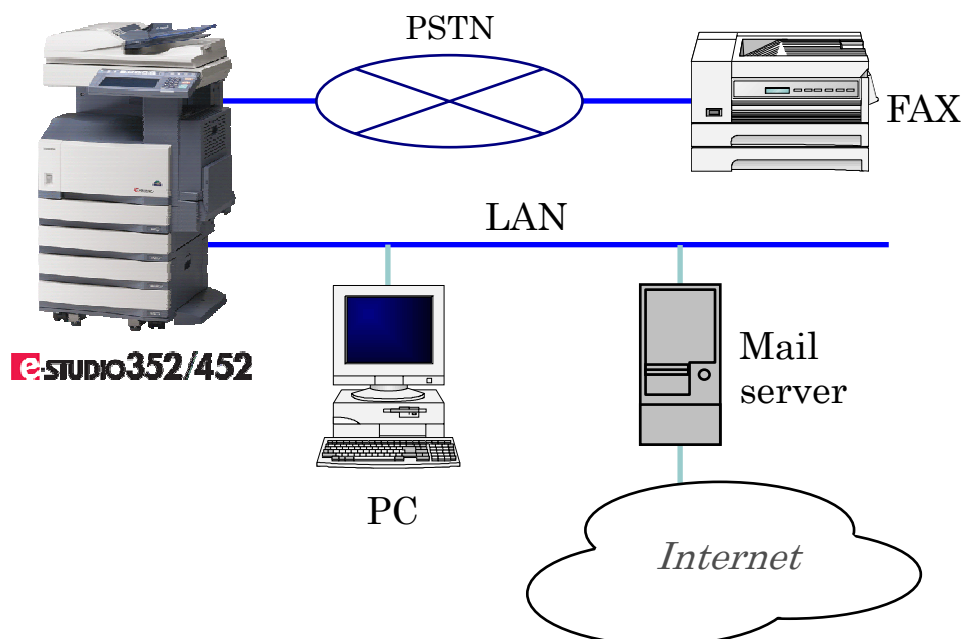


Figure 1-1 Typical operating environment of the TOE

The MFP is a digital copier which inputs, processes, and outputs user documents. Its output processes are copy, print, scan, and fax reception and fax transmission. After each process completes, user document data is deleted by the file delete function provided by the operation system, except for the cases when the MFP user stores his/her user document data stored in temporarily area(*) in the HDD.

User document data stored in temporarily area in the HDD are managed by each MFP user based on importance and confidentiality of the user document data and deleted using the operation system's file delete function as necessary.

Actually, the operation system's file delete function only clears a pointer managed by the operation system which points to the file. This means, an entity of the user document data still exists in the HDD, while the user believes the user document data no longer exists there.

The TOE provides a function to permanently erase user document data deleted by the operation system's file delete function and a function to collectively and permanently erase residual user document data in the HDD before the HDD is disposed of or replaced.

*Caution) In this report, "e-Filing Box" and a shared folder are called temporarily area in the HDD.

1.2.4 TOE Functionality

The TOE has normal mode where MFP users operate these models in ordinary cases, and self-diagnostic mode where service engineers perform maintenance services.

1.2.4.1 Normal Mode

Figure 1-2 shows the configuration of the MFP in normal mode.

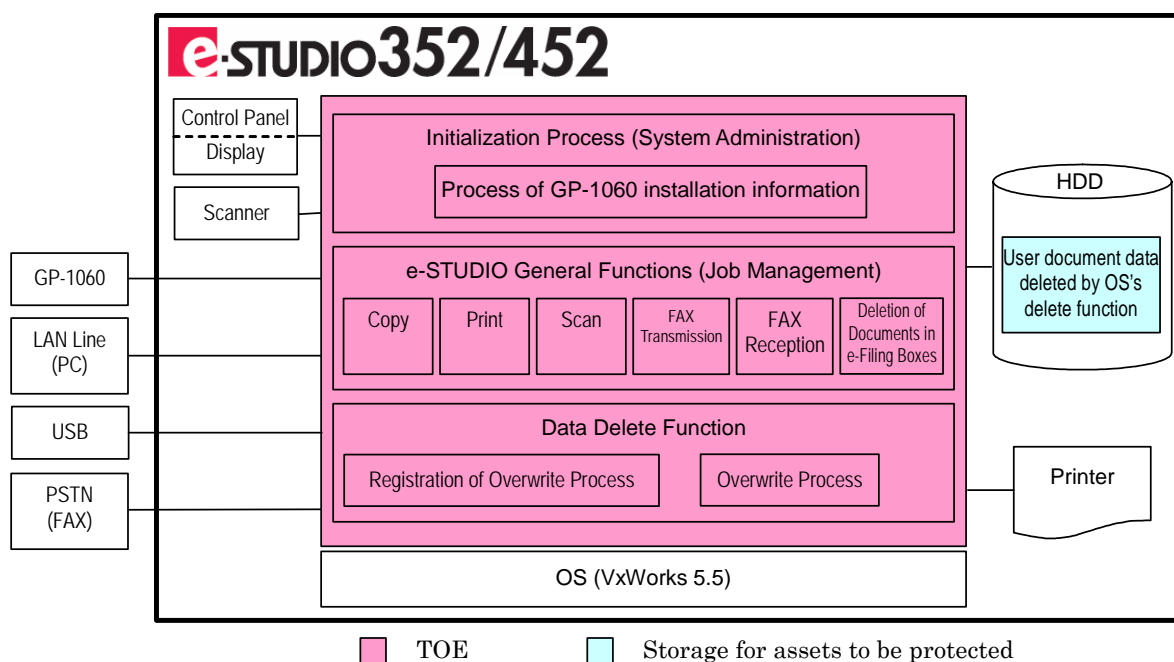


Figure 1-2 Product Configuration in Normal Mode

This section describes the functionality of the TOE.

1) Process of GP-1060 Installation Information

This process checks whether or not the GP-1060 is installed.

In order to make the MFP users aware that the Data Delete Function is available, the TOE name and TOE version are displayed on the LCD display of the control panel.

2) Copy process

This process scans user document data using the scanner and writes the scanned data in the HDD work area.

Then, this process reads the user document data in the work area and performs both or either of the following processes, “Outputs the user document data to the printer” and “Saves the user document data in the HDD temporary area specified by the MFP user”

3) Print process

This process receives user document data from PC or reads a USB, and writes the data in the HDD work area.

Then, this process reads the user document data in the work area and performs both or either of the following processes, “Outputs the user document data to the printer” and “Saves the user document data in the HDD temporary area specified by the MFP user.”

4) Scan process

This process scans user document data using the scanner and performs both or either of the following processes, “Saves the user document data in the HDD temporary area specified by the MFP user” and “Sends Email to a destination specified by the MFP user”.

5) Fax transmission process

This process scans user document data using the scanner and writes the scanned data in the HDD work area.

Then, this process reads the user document data in the work area and sends the data to facsimile(s). The data can also be saved in the HDD temporary area specified by the MFP user

6) Fax reception process

This process receives user document data from a facsimile and writes the data in the HDD work area.

Then, this process reads the user document data in the work area and performs both or either of the following processes, “Outputs the user document data to the printer” and “Saves the user document data in the HDD temporary area specified by the MFP user”.

7) HDD temporary Data delete process

This process deletes user document data saved in the HDD temporary area by operating the control panel or PC.

8) Data Overwrite allocation process (Security Function)

- After each process of the MFP General Functions described above, this process registers it with the trash box where user document data in the work area, deleted by the operation system’s file delete function, is stored
- When user document data is saved in and deleted from an e-Filing Box or a shared folder in the HDD during Process (7) described above, this process registers it with the trash box where user document data in the work area, deleted by the operation system’s file delete function, is stored.

9) Data Overwrite process (Security Function)

This TOE checks if user document data has been registered with the trash box and if any, permanently erases it. While this process is being executed, the message “ERASING DATA” is displayed on the control panel.

The MFP users must make sure that user document data has been permanently erased from the HDD by checking that the “ERASING DATA” message on the LCD display, if displayed on the control panel, has disappeared properly.

The MFP users check the message on the LCD display when collecting printout from the MFP and confirm the area was overwritten.

1.2.4.2 Self-diagnostic Mode

Figure 1-3 shows the configuration of the MFP in self-diagnostic mode.

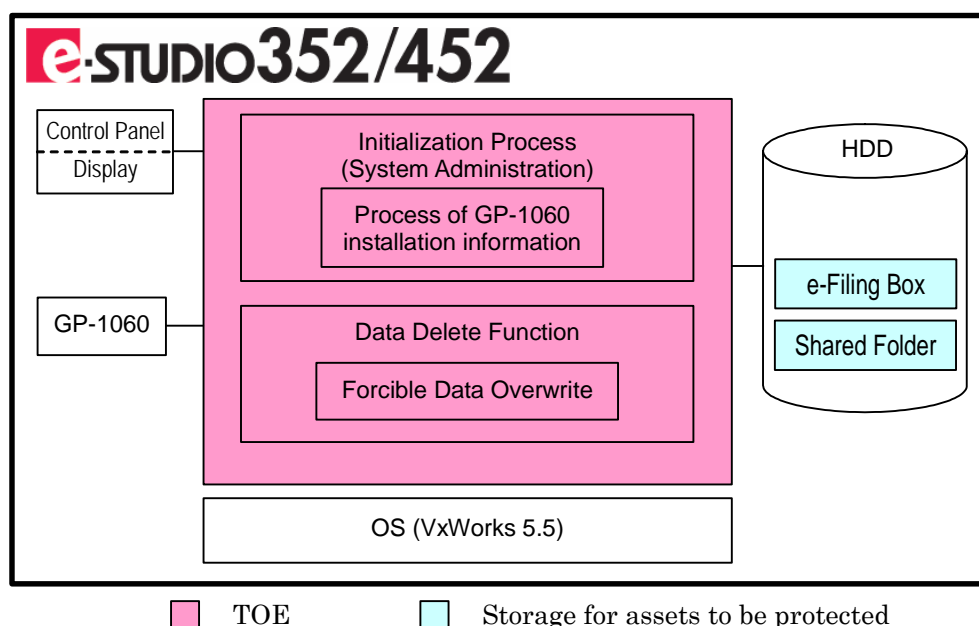


Figure 1-3 Product Configuration in Self-diagnostic Mode

This section describes the functionality of the TOE.

1) Process of GP-1060 Installation Information

This process checks whether or not the GP-1060 is installed.

In order to make the MFP users aware that the Data Delete Function is available, the TOE name and TOE version are displayed on the LCD display of the control panel.

2) Forcible Data Overwrite process (Security Function)

When HDD is disposed or replaced, this process overwrites all HDD areas where user document data are saved in the HDD temporary area.

The service engineer operates forcible Data Overwrite function upon request from the MFP administrator.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as “IT Security Evaluation and Certification Scheme”[2], “IT Security Certification Procedure”[3] and “Evaluation Facility Approval Procedure”[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined “System Software for e-STUDIO352/452 V1.0” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in “System Software for e-STUDIO352/452 V1.0 Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”)[22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations (either of [20] and [21]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated March, 2006 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body

prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.

Although this TOE is utilized by being installed at generic offices and it is assumed that attackers' attack capabilities are low. For this reason, the appropriate minimum SOF is SOF-basic.

1.5.4 Security Functions

Security functions of the TOE are as follow.

SF.TEMPDATA_OVERWRITE

- In normal mode, register an area in which user document data, deleted from the HDD, are stored, in the trash box.
- Completely overwrite the registered areas in which user document data, deleted from the HDD, were stored, in the trash box. The method used here is DoD5220.22-M of the US Department of Defense. (0x00 Fill + 0xFF Fill + random number Fill + validation)

SF.STOREDATA_OVERWRITE

- In self-diagnostic mode, collectively and completely overwrite all areas of the HDD. The method used here is DoD5220.22-M of the US Department of Defense. (0x00 Fill + 0xFF Fill + random number Fill + validation)

1.5.5 Threat

This TOE assumes such threats presented in Table 1-1 and provides functions for countermeasure to them.

Table 1-1 Assumed Threats

| Identifier | Threat |
|--------------------|---|
| T.TEMPDATA_ACCESS | By using off-the-shelf tools and by means of reverse engineering to the areas where residual user document data exists, a malicious e-STUDIO user or non-privileged user may attempt to recover or decode user document data, deleted from the HDD of the e-STUDIO352/452 by the operation system's file delete function. |
| T.STOREDATA_ACCESS | Using off-the-shelf tools, a malicious e-STUDIO user or non-privileged user may attempt to recover or decode the areas in the HDD of the e-STUDIO352/452 where user document data had existed and were deleted when all files were deleted collectively by the operation system's file delete function. |

1.5.6 Organisational Security Policy

There are no organizational security policies required for using the TOE.

1.5.7 Configuration Requirements

This TOE is the System Software installed on the TOSHIBA TEC CORPORATION's digital copier.

This operating environment of the TOE is indicated below.

- Installing on e-STUDIO352 / e-STUDIO452 with GP-1060.

1.5.8 Assumptions for Operational Environment

No assumptions required in environment using this TOE presents.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- Operator's Manual [Common], OMJ05009600 00
- Operator's Manual for Basic Function (North America), OME05009700 00
- Operator's Manual for Basic Function (Europe), OME05009800 00
- Data Overwrite Kit, OMM050034C0 03
- Insertion Sheet[Japanese], OME06005600 00
- Insertion Sheet, OME06005700 00

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM Part 2.

2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on October, 2005 and concluded by completion the Evaluation Technical Report dated March, 2006. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on February, 2006 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on February, 2006.

No concerns were found in evaluation activities for each work unit.

2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the developer is shown in the Table 2-1.

Table 2-1: Developer test configuration

| TOE | Version | | |
|--|--|-------------|-----------------------------|
| TOE V1.0 | Item | Japanese | English |
| | ROM | T364SY0J030 | T364SY0U030, T364SY0E030 |
| | System Software | VT308.100 | VT308.100 |
| | UI data frame | V007.000 0 | V007.000 0 |
| Equipments | Speciation | | |
| Digital Multi Function Peripheral (MFP) | e-STUDIO452 | | |
| Option of MFP | GP-1060 | | |
| PC for the tests | DELL OPTIPLEX GX100 | | |
| Mail server | SuperMicro 5013C-MT Model P4SCT+ | | |
| Circuit board for debug, Serial cable | Circuit board for serial communications connecting with logic circuit board of digital multifunction peripheral: 6LA70328000 PWB-F-SERIAL-IF-360, and DSUB9 pin serial cross cable | | |
| FAX | e-STUDIO350 with SuperG3 FAX | | |
| Telephone exchange emulator | AVM TLE101III | | |

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

Developer testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

1. Confirming that the user document data were registered in each HDD_work and trash box with the same position, capturing HDD dumps of file's position before, processing, after overwrite, and comparing.
2. Capturing HDD dumps of each top / middle / end position before and after overwrite, and comparing.

c. Scope of Testing Performed

Testing is performed about 104 items by the developer.

The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

d. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The evaluator used the same test configuration as the test configuration used by the developer, plus an additional tool for penetration testing against the developer test configuration.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator is shown in the Figure 2-1. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

The same testing approaches as those of the developer testing were used.

c. Scope of Testing Performed

Total of 31 items of testing; namely 6 items from testing devised by the evaluator and 25 items from testing from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

1. Covering all scenarios including the test items of the developer testing.
2. Including one more tests in the test items for each interface at least.

The penetration testing comprised 4 tests to confirm that there were no obvious vulnerabilities that the developer was not considering existed.

d. Result

The evaluator successfully completed all the tests and observed the behavior of the TOE security functions. The evaluator confirmed that the actual test results match the expected test results, and that there are no obvious exploitable vulnerabilities in the TOE.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
2. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
3. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

No concerns were found in certification process.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

| | |
|------|---|
| CC: | Common Criteria for Information Technology Security Evaluation |
| CEM: | Common Methodology for Information Technology Security Evaluation |
| EAL: | Evaluation Assurance Level |
| PP: | Protection Profile |
| SOF: | Strength of Function |
| ST: | Security Target |
| TOE: | Target of Evaluation |
| TSF: | TOE Security Functions |

The glossaries used in this report are listed below.

| | |
|-----------------------------------|--|
| MFP (Multi Function Peripherals): | Digital copier: A single multi-functional peripheral device which integrates several functions such as copy, print, and fax. |
| e-STUDIO: | MFPs where the TOE is installed, i.e., e-STUDIO352/452 (e-STUDIO352, and e-STUDIO452). |
| HDD: | Hard Disk Drive |
| User document data: | e-STUDIO user's document data digitized by utilizing the e-STUDIO General Functions. Note that data received by the e-STUDIO using its fax function is not user document data of the e-STUDIO users but the data of a person who has sent it. |
| e-Filing Box, Shared folder: | A temporary area where the e-STUDIO users stores and refers their user document data. The e-STUDIO users delete user document data stored by themselves. Such user document data is automatically deleted from an area after a specified effective period expires and this data is no longer recognized as assets to be protected. |
| GP-1060: | A product installed in the e-STUDIO352/452 to enable the Data Overwrite Function, a security function of the System Software |
| Users: | Users who utilize the e-STUDIO General Functions |

Administrators:

Administrators make each setting of the e-STUDIO General Functions (including copy, network, and fax settings) and ask service engineers to execute the forcible Data Overwrite function to the HDD.

Service Engineers:

Service engineers perform service maintenance operations such as installation of the e-STUDIO (including installation of the GP-1060).

6. Bibliography

- [1] System Software for e-STUDIO352/452 Security Target Ver 1.3 (March 7, 2006)
TOSHIBA TEC CORPORATION
- [2] IT Security Evaluation and Certification Scheme, July 2005,
Information-Technology Promotion Agency, Japan EC-01
- [3] IT Security Certification Procedure, July 2005, Information-Technology
Promotion Agency, Japan EC-03
- [4] Evaluation Facility Approval Procedure, July 2005, Information-Technology
Promotion Agency, Japan EC-05
- [5] Common Criteria for Information Technology Security Evaluation Part 1:
Introduction and general model Version 2.1 August 1999 CCIMB-00-031
- [6] Common Criteria for Information Technology Security Evaluation Part 2:
Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- [7] Common Criteria for Information Technology Security Evaluation Part 3:
Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- [8] Common Criteria for Information Technology Security Evaluation Part 1:
Introduction and general model Version 2.1 August 1999 CCIMB-99-031
(Translation Version 1.2 January 2001)
- [9] Common Criteria for Information Technology Security Evaluation Part 2:
Security functional requirements Version 2.1 August 1999 CCIMB-99-032
(Translation Version 1.2 January 2001)
- [10] Common Criteria for Information Technology Security Evaluation Part 3:
Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
(Translation Version 1.2 January 2001)
- [11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques -
Evaluation criteria for IT security - Part 1: Introduction and general model JIS
- [12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques -
Evaluation criteria for IT security - Part 2: Security functional requirements
- [13] ISO/IEC 15408-3:1999 - Information technology - Security techniques -
Evaluation criteria for IT security - Part 3: Security assurance requirements
- [14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security -
Part 1: General Rules and general model
- [15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security -
Part 2: Security functional requirements
- [16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security -
Part 3: Security assurance requirements

- [17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999
- [18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999 (Translation Version 1.0 February 2001)
- [19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation
- [20] CCIMB Interpretations (as of 01 December 2003)
- [21] CCIMB Interpretations (as of 01 December 2003) (Translation Version 1.0 August 2004)
- [22] System Software for e-STUDIO352/452 V1.0 Evaluation Technical Report Version 2.0, March 9, 2006, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center