Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-08-31 (ITC-7169)
Certification No.	C0145
Sponsor	RICOH COMPANY, LTD.

Name of TOE	(for Japan)
	    imagio Security Card Type 7 Software
	(Overseas)
	    DataOverwriteSecurity Unit Type H Software

Version of TOE	1.01x
PP Conformance	None
Conformed Claim	EAL3
Developer	RICOH COMPANY, LTD.
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.
2008-02-28

Hideji Suzuki, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"imagio Security Card Type 7 Software (for Japan), DataOverwriteSecurity Unit Type H Software (Overseas) Version 1.01x" 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.

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "imagio Security Card Type 7 Software (for Japan), DataOverwriteSecurity Unit Type H Software (Overseas) Version 1.01x" (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, RICOH COMPANY, LTD.

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: (for Japan) imagio Security Card Type 7 Software
(Overseas) DataOverwriteSecurity Unit Type H Software
Version: 1.01x
Developer: RICOH COMPANY, LTD.

1.2.2 Product Overview

This TOE is the data overwrite module software (hereinafter: DOMS) mounted in MFP produced by Ricoh Co., Ltd., and is provided as a stored data on SD memory card.
This TOE is an option kit, which is available for safer use of MFP, and its function is to overwrite designated areas of the HDD by the MFP for erasure.

1.2.3 Scope of TOE and Overview of Operation

1.2.3.1 TOE Scope
This TOE is the software that is stored on SD memory card, and the SD memory card is attached to the controller board. Figure1-1 shows the TOE and the structure of the MFP, which is operational environment of the TOE.
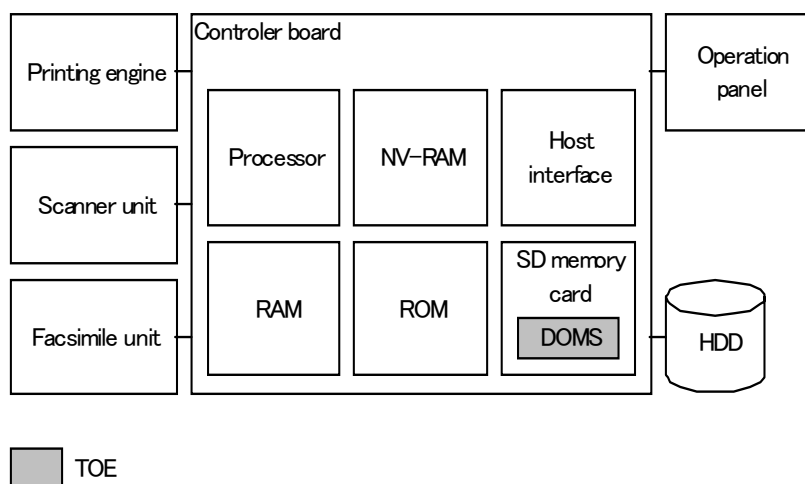
Figure1-1: Hardware Structure of the MFP

The explanations of each element in Figure1-1 are as follows;

- The printing engine prints out data from copy and printer functions and also received data through the facsimile unit in parallel controlling paper feed and paper eject.

- The scanner unit gets in image data from paper documents. It is used for copy, scanner and facsimile sending functions to get in image data.

- The facsimile unit operates sending data and receiving of facsimile data.

- The operation panel displays information to general users and administrator and also receives input command/data entered by general users and administrator. General users and administrator can make use functions of the MFP with operating the operation panel.

- Image data is stored on the HDD. During copying, printing, scanning and facsimile sending/receiving, the MFP temporarily stores image data for working on the HDD. And accumulating image data with instruction of general users is also stored on the HDD.

- The controller board controls whole of the MFP. The controller board is equipped with a processor and RAM to execute software in the MFP, ROM on which software such as operating system (OS) and various application modules are installed, NV-RAM on which setting information for MFP is stored, and Host interface connected to user PC and servers. And also SD memory card, in which software of additional function is stored, can be attached to the controller board. TOE is stored on SD memory card, and SD memory card is mounted in the controller board.

1.2.3.2 Overview of Operation
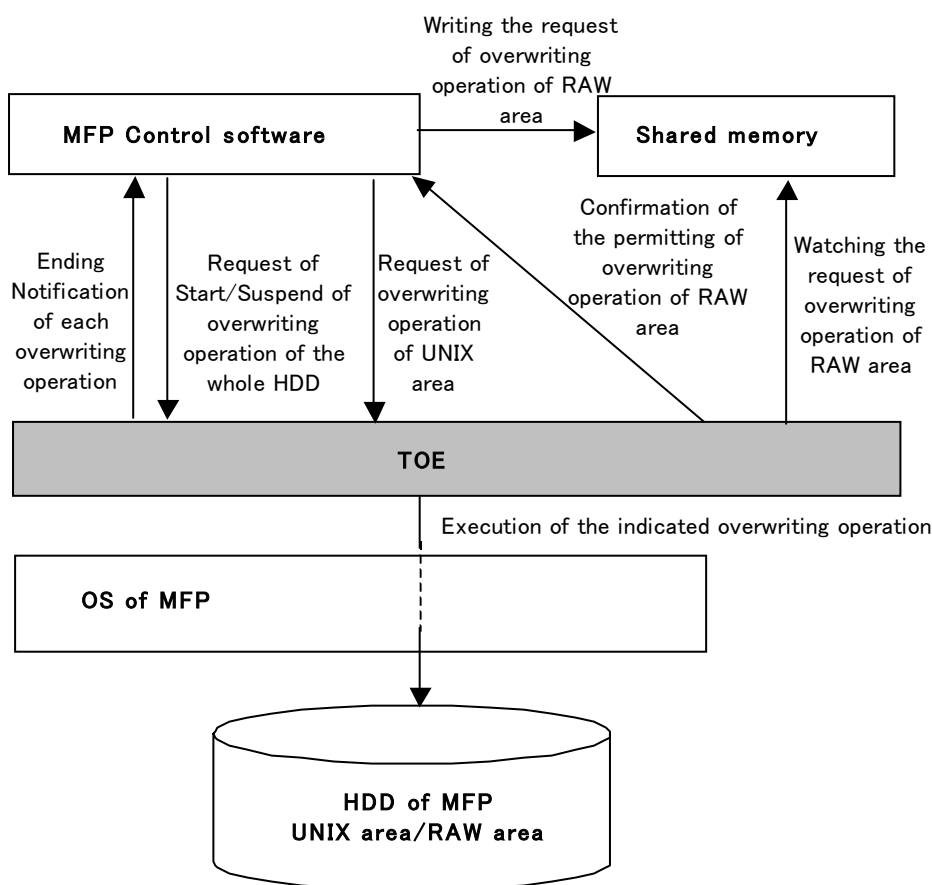
Figure1-2: Operational overview of the TOE

Figure1-2 shows operating overview of the TOE.

Both Control software of the MFP and the OS of the MFP are software existed in ROM on Controller board shown in Figure1-1. The HDD of the MFP, as the HDD shown in Figure1-1, is divided into UNIX area and RAW area. The shared memory is an area defined in RAM on Controller board shown in Figure1-1.

Based on instructions from control software of the MFP, the TOE overwrites specified area on the HDD of the MFP with a specified method.

The TOE has three overwriting functions as follows.

- Function overview of Overwriting RAW area
  The instruction of Overwriting RAW area to the TOE is executed by exchanging information of specified overwriting area and the response to confirmation of permission for Overwriting RAW area from the TOE through the shared memory. At the same time specified overwriting method for erasure is also informed.
  The TOE monitors whether an instruction of Overwriting RAW area exists in the shared memory. When the TOE finds an Overwriting instruction, the TOE requests a permission to overwrite RAW area to the control software of the MFP. After receiving permission from the control software, the TOE executes to overwrite specified RAW area through the use of the OS.
  After completion of overwriting, the TOE informs notice of termination to the control software of the MFP.

- Function overview of Overwriting UNIX area

The instruction of Overwriting remaining data in UNIX area to the TOE is executed by specifying discarded UNIX file and Overwriting method. When the TOE receives an instruction of Overwriting discarded UNIX file, the TOE executes to overwrite specified file through the use of the OS.
After completion of overwriting, the TOE informs notice of termination to the control software of the MFP.

- Function overview of Overwriting whole of the HDD
When TOE receives an instruction of Overwriting whole of the HDD, the TOE executes to overwrite all areas of the HDD through the use of the OS.
Overwriting method for erasure is specified with the instruction of Overwriting whole of the HDD.
After completion of overwriting, the TOE informs notice of termination to the control software of the MFP.
The TOE can receive a cancellation instruction for overwriting from the MFP during operation of overwriting whole of the HDD, and the operation is suspended when received the cancellation instruction.

1.2.4 TOE Functionality

The TOE provides the functions of overwrite for each area on the HDD. Those areas are as follows.

- Specified area of RAW area

- Specified file of UNIX area

- Whole of the HDD

Overwriting method for erasure can be chosen from following three methods.

- NSA method

  NSA method overwrites target data in following procedure.

  > NSA method

  > Overwrite twice with random numbers,

  > Overwrite once with Null (0).

- DoD method

  DoD method overwrites target data in following procedure.

  > Overwrite once with fixed numbers,

  > Overwrite once with complement of above fixed numbers,

  > Overwrite once with random numbers,

  > Carry out verification finally.

- Random Numbers method

  Random Numbers method overwrites specified number of times (from one to nine times) with random numbers.

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 "Security Target for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H" 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 B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) 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] or [13]) as its rationale. Such evaluation procedure and its result are presented in "imagio Security Card Type 7 Software (for Japan), DataOverwriteSecurity Unit Type H Software (Overseas) Version 1.01x Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation 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 2008-01 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

The minimum strength level claimed for the TOE is SOF-Basic in this ST.
It is assumed that the MFP, which is operation environment of the TOE, is used in general offices. Therefore it is appropriate that minimum strength of function for the TOE is SOF-Basic.

1.5.4 Security Functions

The TOE security functions are the functions of overwrites for each area on HDD. Those areas are as follows.

- The specified area on RAW area

- The specified files on UNIX area

- All area of the HDD

The method of overwrites for erasing can be specified as one of following methods.

- NSA method

  NSA method overwrites data in following procedure.

  > Overwrite twice with random numbers,

  > Overwrite once with Null (0).

- DoD method

  DoD method overwrites data in following procedure.

  > Overwrite once with fixed numbers,

  > Overwrite once with complement of above fixed numbers,

  > Overwrite once with random numbers,

  > Carry out final verification.

- Random Numbers method

  Random Numbers method overwrites specified number of times (from one to nine times) with random numbers.

1.5.5 Threat

There are no threats countered by the TOE.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-1.

Table 1-1 Organisational Security Policy

Identifier	Organisational Security Policy
P.UNREADABLE	The TOE shall prevent from retrieving information on the HDD area specified by the MFP.

1.5.7 Configuration Requirements

Target MFP of the TOE are listed in Table1-2.

Table1-2: Target MFP of the TOE

	Product names in Japan	Product names in other country
Model 1	Ricoh imagio C6000 series Ricoh imagio C7500 series	Ricoh Aficio MP C6000 series Ricoh Aficio MP C7500 series Savin C6055/C7570 series Lanier LD260c/275c series Lanier MP C6000/C7500 series Gestetner MP C6000/C7500 series Infotec MP C6000/C7500 series NRG MP C6000/C7500 series

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.MODE.AUTOMATIC	**It is assumed that the execution of Auto Erase Memory of the TOE is not aborted.** The execution of Auto Erase Memory of the TOE is not aborted by turning off the power of the MFP before the TOE finishes overwriting.
A.MODE.MANUAL	**It is assumed that the execution of Erase All Memory of the TOE is not suspended.** The execution of Erase All Memory of the TOE is not suspended without user's intent by pressing the [Suspend] button or turning off the power of the MFP before the function finishes.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

Documents for Japan;

- imagio Security Card Type 7
  imagio Security Card Type 9
  Operating Instructions
  Version D377-7902

Documents for overseas;

- DataOverwriteSecurity Unit Type H
  DataOverwriteSecurity Unit Type I
  Operating Instructions
  Version D377-7940

- Notes for Users
  Version D377-7250

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM 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.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on 2007-09 and concluded by completion the Evaluation Technical Report dated 2008-01. 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 2007-12 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 2008-01.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

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

   Developer's testing was performed using TOE-installed MFP circumstances as follows.

   - Ricoh imagio MP C6000/ Ricoh Aficio MP C6000 (System version: 1.02)

   And the following devices were used for testing operation and observation of results:

   - Testing PC
     Terminal software connected to MFP through RS232C/Ethernet communication was used.

   - IDE Bus Analyser

IDE-Pocket Ultra DMA/100 supported (TOYO Corporation)

- Others
  Boot server to start up the MFP in boot-mode.
  Mail server for sending messages to check out the mail-sending function.

2) Outlining of Developer Testing

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

a. Test configuration

Some models of MFPs, those are distinguished in ST, were used as the testing environment. As the result of the investigation of the difference among the MFPs distinguished in ST, the evaluator assured that some models of MFPs used as the testing environment cover the difference among the MFPs distinguished in ST well. Therefore, the evaluator assured that developer's testing environment was equal to the TOE configurations distinguished in ST.

b. Testing method

Following methods were employed for stimulation testing of TSFI and observations.

- Checking out the panel operation and its indication.

- Checking out the logging body, which was displayed on PC monitor. The PC was connected to the testing MFP.

- Monitoring data at the interface of HDD, using IDE bus analyser.

c. Scope of Testing Performed

Testing is performed about 51 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

Test configuration performed by the evaluator shall be the same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Evaluator's testing was performed in the same configuration with developer testing.

b. Testing method

Following methods were employed for stimulation testing of TSFI and observations.

- Checking out the panel operation and its indication.

- Checking out the logging body, which was displayed on PC monitor. The PC was connected to the testing MFP.

- Monitoring data at the interface of HDD, using IDE bus analyser.

c. Scope of Testing Performed

Total of 15 items of testing; namely 4 items from testing devised by the evaluator and 11 items from testing from sampling of developer testing was conducted. The criterion for choosing was considered in accordance with CEM 2:ATE_IND.2-4 and 2-9. Those key viewpoints are as follows.

1. If the results of developer tests cause the evaluator to doubt from viewpoints of the coverage of parameters or the use timing of TSF interfaces, then the evaluator has to devise proprietary test items to complement the results.
2. The evaluator has to select a sufficient number of items out of the developer tests in consideration of the coverage of all security functions and interfaces.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM 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. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation 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

Definitions of specific terms used in this report are listed below.

MFP: Multi Function Product
It is the printer that has multiple functions such as copier, printer in a single machine.

NV-RAM: Non-volatile random access memory
Semiconductor memory that can maintain memory content without supply of power.

UNIX area: HDD area, which managed by OS file system.
The data that exists on this area can be accessed by normal file operation.

RAW area: HDD area, which not managed by OS file system
The data that exists on this area is managed by CSM in its way without OS file operation.

SD memory card:
Secure Digital memory card
It is a stamp-size memory device with the function for copyright protection.

6. Bibliography

[1]   Security Target for imagio Security Card Type 7, DataOverwriteSecurity Unit Type H version 1.00 (December 13, 2007) RICOH COMPANY, LTD.

[2]   IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3]   IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4]   Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5]   Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6]   Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7]   Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8]   Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9]   Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10]   Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11]   ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12]   ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13]   ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14]   Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15]   Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16]   ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17]   imagio Security Card Type 7 Software (for Japan), DataOverwriteSecurity Unit Type H Software (Overseas) Version 1.01x Evaluation Technical Report Version 1.0, January 30, 2008, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center