



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

# CANADIAN CENTRE FOR **CYBER SECURITY**

## COMMON CRITERIA CERTIFICATION REPORT RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 v.JE-1.00-H

RICOH COMPANY, LTD.

6 January 2020

383-4-486

V1.0

# FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services

Edward Drake Building

[contact@cyber.gc.ca](mailto:contact@cyber.gc.ca) | 1-833-CYBER-88 (1-833-292-3788)



# OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are listed on the Certified Products list (CPL) for the Canadian CC Scheme and posted on the Common Criteria portal (the official website of the International Common Criteria Project).



# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>6</b>
<b>1 Identification of Target of Evaluation .....</b>	<b>7</b>
1.1 Common Criteria Conformance .....	7
1.2 TOE Description.....	7
1.3 TOE Architecture .....	8
<b>2 Security Policy.....</b>	<b>9</b>
2.1 Cryptographic Functionality .....	9
<b>3 Assumptions and Clarification of Scope .....</b>	<b>10</b>
3.1 Usage and Environmental Assumptions.....	10
3.2 Clarification of Scope .....	10
<b>4 Evaluated Configuration.....</b>	<b>11</b>
4.1 Documentation.....	11
<b>5 Evaluation Analysis Activities .....</b>	<b>12</b>
5.1 Development.....	12
5.2 Guidance Documents.....	12
5.3 Life-Cycle Support .....	12
<b>6 Testing Activities .....</b>	<b>13</b>
6.1 Assessment of Developer tests.....	13
6.2 Conduct of Testing .....	13
6.3 Independent Functional Testing .....	13
6.3.1 Functional Test Results.....	13
6.4 Independent Penetration Testing.....	14
6.4.1 Penetration Test results.....	14
<b>7 Results of the Evaluation .....</b>	<b>15</b>
7.1 Recommendations/Comments.....	15
<b>8 Supporting Content.....</b>	<b>16</b>
8.1 List of Abbreviations.....	16
8.2 References.....	16



# LIST OF FIGURES

Figure 1: TOE Architecture ..... 8

# LIST OF TABLES

Table 1: TOE Identification ..... 7

Table 2: Cryptographic Implementation(s)..... 9



## EXECUTIVE SUMMARY

The RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 v.JE-1.00-H (hereafter referred to as the Target of Evaluation, or TOE), from RICOH COMPANY, LTD. , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

Lightship Security is the CCEF that conducted the evaluation. This evaluation was completed on 6 January 2020 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

# 1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

**Table 1: TOE Identification**

<b>TOE Name and Version</b>	RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 v.JE-1.00-H
<b>Developer</b>	RICOH COMPANY, LTD.

## 1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance;

Protection Profile for Hardcopy Devices Version: 1.0, dated 2015-09-11

## 1.2 TOE DESCRIPTION

This TOE is a Digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

### 1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

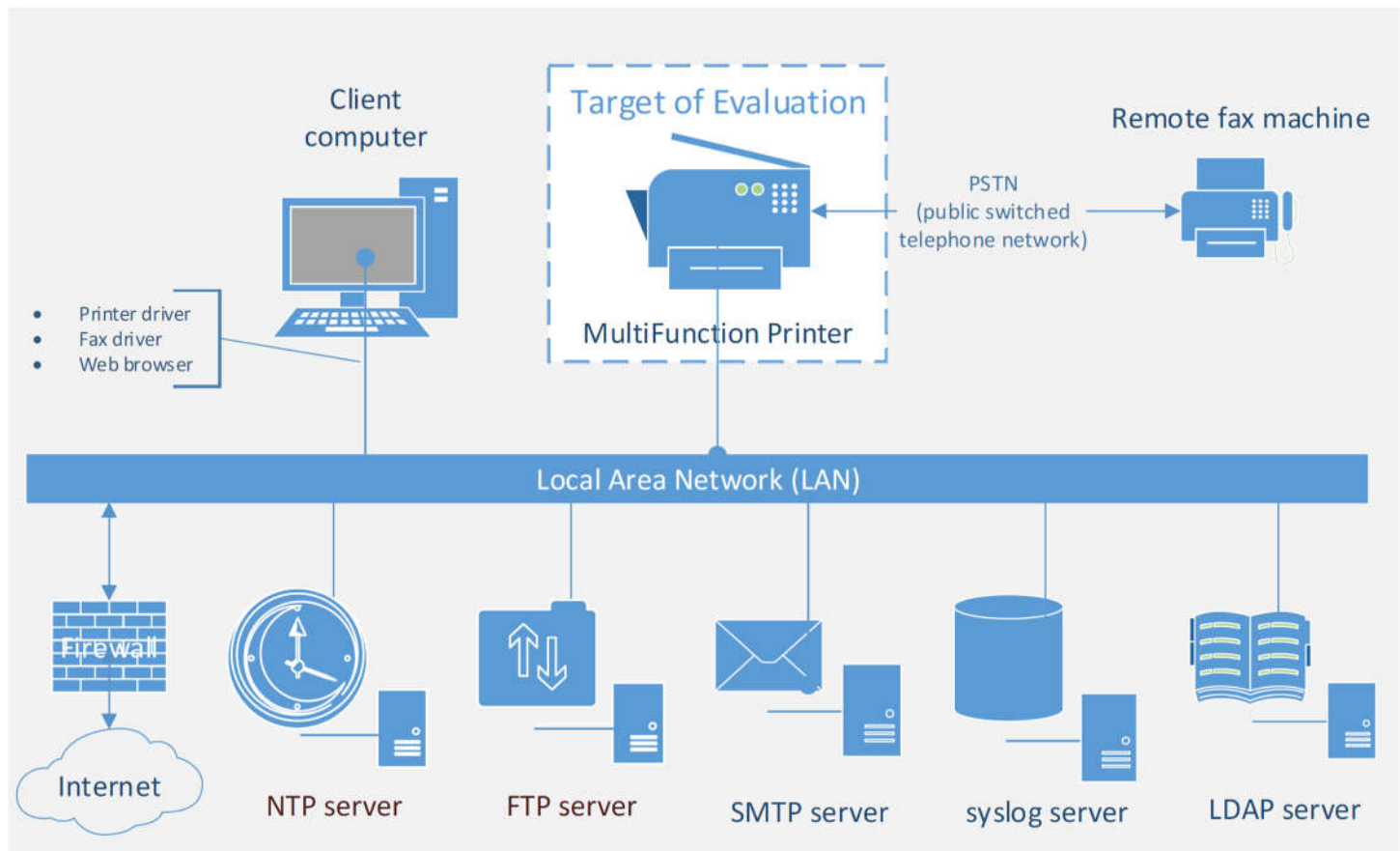


Figure 1: TOE Architecture



## 2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Paths/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

### 2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations have been evaluated by the CAVP/CMVP and are used by the TOE:

**Table 2: Cryptographic Implementation(s)**

Cryptographic Module/Algorithm	Certificate Number
Advanced Encryption Standard Algorithm (AES)	#5364, #3921, #4560, #5315
Keyed-Hash Message Authentication Code (HMAC)	#3552, #3515
Secure Hashing (SHS)	#4306, #4269, #3231, #C629, #C582
Random Number Generator (DRBG)	#2075
Digital Signature Algorithm (DSA)	#1385
Component Testing	#1826
Rivest-Shamir-Adleman Algorithm (RSA)	#2869, #C582
Elliptic Curve Digital Signature Algorithm (ECDSA)	#C629, #C582

## 3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

### 3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
- The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.

### 3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

The following functions supported by the TOE are not included in this evaluation:

- Fax over IP
- Store while copying documents
- Store while sending documents by fax
- Menu Protect
- PDF Group Passwords
- SMTP Authentication
- File Transfer Authentication
- Erase All Memory

## 4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The following hardware models;

- RICOH IM C2000, IM C2000A, IM C2000F, and IM C2000G
- RICOH IM C2500, IM C2500A, IM C2500F, and IM C2500G
- RICOH IM C3000, IM C3000A, IM C3000F, and IM C3000G
- RICOH IM C3500, IM C3500A, IM C3500F, and IM C3500G
- RICOH IM C4500, IM C4500A, IM C4500F, and IM C4500G
- RICOH IM C5500, IM C5500A, and IM C5500F
- RICOH IM C6000, IM C6000F, and IM C6000G

Running the JE-1.00-H software upgrade and the Fax Control Unit Type M37 (for Fax functionality)

- With support from the environment for;
  - Syslog Server.

### 4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- a) Notes for Administrators: Using This Machine in a Network Environment Compliant with Protection Profile for Hardcopy Devices PP\_HCD\_V1.0, v1.0.
- b) [https://support.ricoh.com/services/device/ccmanual/IM\\_C2000\\_C2500\\_C3000\\_C3500\\_C4500\\_C5500\\_C6000/en-GB/booklist/int/index\\_book.htm](https://support.ricoh.com/services/device/ccmanual/IM_C2000_C2500_C3000_C3500_C4500_C5500_C6000/en-GB/booklist/int/index_book.htm)
- c) [https://support.ricoh.com/services/device/ccmanual/IM\\_C2000\\_C2500\\_C3000\\_C3500\\_C4500\\_C5500\\_C6000/en-GB/pdf/SafetyInformation.html](https://support.ricoh.com/services/device/ccmanual/IM_C2000_C2500_C3000_C3500_C4500_C5500_C6000/en-GB/pdf/SafetyInformation.html)
- d) [https://support.ricoh.com/services/device/ccmanual/IM\\_C2000\\_C2500\\_C3000\\_C3500\\_C4500\\_C5500\\_C6000/en-GB/pdf/User.html](https://support.ricoh.com/services/device/ccmanual/IM_C2000_C2500_C3000_C3500_C4500_C5500_C6000/en-GB/pdf/User.html)
- e) [https://support.ricoh.com/services/device/ccmanual/IM\\_C2000\\_C2500\\_C3000\\_C3500\\_C4500\\_C5500\\_C6000/SecurityReference/en-GB/booklist/int/index\\_book.htm](https://support.ricoh.com/services/device/ccmanual/IM_C2000_C2500_C3000_C3500_C4500_C5500_C6000/SecurityReference/en-GB/booklist/int/index_book.htm)

## 5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

### 5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

### 5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

### 5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.



## 6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

### 6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

### 6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

### 6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

- a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP; and
- b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementation was present in the TOE.

#### 6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

## 6.4 INDEPENDENT PENETRATION TESTING

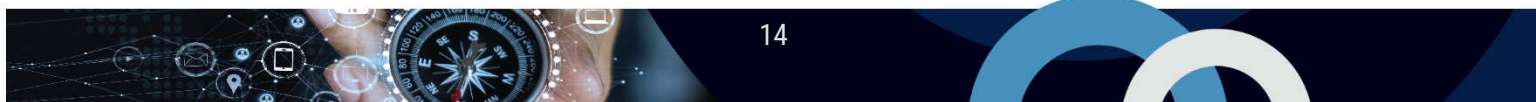
---

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- a) Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and
- b) HTML Injection: The evaluator injected HTML markup into a user field in an attempt to modify the address book page.

### 6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.



## 7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

### 7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.



## 8 SUPPORTING CONTENT

### 8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

### 8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 v.JE-1.00-H v1.0, 19 Dec 2019
Evaluation Technical Report for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 v.JE-1.00-H v1.2, 6 Jan 2020
Assurance Activity Report for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 v.JE-1.00-H v1.1, 6 Jan 2020