Certification Report

Xerox WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 ConnectKey 1.5 Technology

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-295-CR
Version: 1.0
Date: 10 December 2014
Pagination: i to iii, 1 to 9

DISCLAIMER

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 Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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 CCS, 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 the Communications Security Establishment, 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 Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) 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 CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CSC Security Testing/Certification Laboratories.

By awarding a Common Criteria certificate, the CCS 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.

This certification report is associated with the certificate of product evaluation dated 10 December 2014, and the security target identified in Section 4 of this report.

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

This certification report makes reference to the following trademarks or registered trademarks:

- Xerox is a registered trademark of Xerox Corporation.

TABLE OF CONTENTS

Executive Summary

Xerox WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 ConnectKey 1.5 Technology (hereafter referred to as Xerox MFD), from Xerox Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that Xerox MFD meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Xerox MFD is a Multi-Function Device (MFD) that consists of a printer, copier, scanner and fax. Xerox MFD provides the following security features: Image Overwrite, Hard Disk Encryption, Audit, Network Filtering, Secure Communication, Authentication and Access Control, Network Authentication, and Self Test and Integrity Verification.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 10 November 2014 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Xerox MFD, 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.

Communications Security Establishment, as the CCS Certification Body, declares that the Xerox MFD evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is Xerox WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 ConnectKey 1.5 Technology (hereafter referred to as Xerox MFD), from Xerox Corporation.

2 TOE Description

Xerox MFD is a Multi-Function Device (MFD) that consists of a printer, copier, scanner and fax. Xerox MFD provides the following security features: Image Overwrite, Hard Disk Encryption, Audit, Network Filtering, Secure Communication, Authentication and Access Control, Network Authentication, and Self Test and Integrity Verification.

3 Security Policy

Xerox MFD implements a role-based access control policy to control administrative access to the system. In addition, Xerox MFD implements policies pertaining to the following security functional classes:

Audit;

Cryptographic Support;

User Data Protection;

Identification and Authentication;

Security Management; and

Protection of the TSF.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
Mocana v5.1f	*1276*
OpenSSL v1.2.3	*1051*

4 Security Target

The ST associated with this Certification Report is identified below:

Xerox Multi-Function Device Security Target WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 ConnectKey 1.5 Technology v1.4, December 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Xerox MFD is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
    - ALC_FLR.3 – Systematic flaw remediation.

b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:*
    - FPT_FDI_EXP - Restricted forwarding of data to external interfaces.

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Xerox MFD 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
- Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
- Administrators do not use their privileged access rights for malicious purposes.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

7 Evaluated Configuration

The evaluated configuration for Xerox MFD comprises one of the following Multi-Function devices:

- WorkCentre 5845;
- WorkCentre 5855;
- WorkCentre 5865;
- WorkCentre 5875;
- WorkCentre 5890;

- WorkCentre 7220;
- WorkCentre 7225;
- WorkCentre 7830;
- WorkCentre 7835;
- WorkCentre 7845;
- WorkCentre 7855;
- ColorQube 8700 Xerox ConnectKey Controller;
- ColorQube 8900 Xerox ConnectKey Controller;
- ColorQube 9301 Xerox ConnectKey Controller;
- ColorQube 9302 Xerox ConnectKey Controller; and
- ColorQube 9303 Xerox ConnectKey Controller.

The publication entitled Secure Installation and Operation of Your Xerox Xerox WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 ConnectKey 1.5 Technology *describes the procedures necessary to install and operate Xerox MFD in its evaluated configuration.*

8 Documentation

The Xerox Corporation documents provided to the consumer are as follows:

Title	Version	Date
Xerox WorkCentre 5845/5855/5865/5875/5890 System Administrator Guide	1.0	February 2013
Xerox WorkCentre 7220/7225 System Administrator Guide	1.2	November 2013
Xerox WorkCentre 7800 Series System Administrator Guide	1.2	November 2013
Xerox ColorQube 8700/8900 ConnectKey Controller System Administrator Guide	1.0	April 2013
Xerox ColorQube 9301/9302/9303 System Administrator Guide	1.0	February 2013
Xerox WorkCentre 5845/5855/5865/5875/5890 User Guide	1.0	January 2013
Xerox WorkCentre 7220/7225 User Guide	1.1	April 2013
Xerox WorkCentre 7800 Series User Guide	1.1	February 2013
Xerox ColorQube 8700/8900 ConnectKey Controller User Guide	1.0	April 2013
Xerox ColorQube 9301/9302/9303 ConnectKey Controller User Guide	1.0	February 2013

Title	Version	Date
Secure Installation and Operation of Your Xerox WorkCentre™ 5845/5855/5865/5875/5890 WorkCentre™ 7220/7225 WorkCentre™ 7830/7835/7845/7855 ColorQube™ 8700/8900 Xerox ConnectKey Controller ColorQube™9301/9302/9303 Xerox ConnectKey Controller Version 1.5	1.2	October 2014

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Xerox MFD, including the following areas:

Development: The evaluators analyzed the Xerox MFD functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Xerox MFD security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Xerox MFD 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.

Life-cycle support: An analysis of the Xerox MFD configuration management system and associated documentation was performed. The evaluators found that the Xerox MFD 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 Xerox MFD during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Xerox MFD. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

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

10.1 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 ETR[1].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 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. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Create users and verify Login:

    a. Create normal user account:

    b. Create System Administrator:

    c. User Login:

    d. System Administrator Login:

The objectives of these test goals are to exercise the ability of an administrator to create accounts and then to test the Login abilities of the accounts;

c. Software Self-Test: The objective of this test goal is to initiate software verification self-test and confirm that audit log is generated;

d. Secure Print Access: The objective of this test goal is to demonstrate that only the user that submitted the secure print job will be able to access the data;

e. IPSec:

    a. IPSec Lan Fax:

    b. IPSec Workflow Scanning

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The objectives of these test goals are to verify confidentiality through encryption over IPSec;

f. RBAC (Role-based access control):
    a. Administration:
    b. Fax:
    c. Print:
    d. Scan:
    e. Job Deletion:

The objectives of these test goals are to exercise different access control rules;

g. Audit download and verify: The objective of this test goal is to download a selection of audit events and verify that they contain proper data; and

h. Verify Immediate Image Overwrite: The objective of this test goal is to verify if submitted job has been properly overwritten.

10.3 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.

b. Session Hijack (Cookie): The objective of this test goal is to demonstrate that the TOE is not vulnerable to Session ID attacks;

c. SQL Injection: The objective of this test goal is to demonstrate that TOE is not vulnerable to SQL injection at the login page;

d. Login with unexpected input: The objective of this test goal is to demonstrate the TOE rejects invalid data in login fields; and

e. Malicious PostScript print job: The objective of this test goal is to attempt to access a directory listing using PostScript print jobs.

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

10.4 Conduct of Testing

Xerox MFD was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place onsite at the developers location. The CCS Certification Body did not witness any of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

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

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

The end user is recommended to reference the Secure Installation and Operation of Your WorkCentre™ 5845/5855/5865/5875/5890WorkCentre™ 7220/7225 WorkCentre™ 7830/7835/7845/7855 ColorQube™ 8700/8900 Xerox ConnectKey 1.5 Controller ColorQube™9301/9302/9303 Xerox ConnectKey Controller for proper installation of the TOE.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MFD	Multi Function Device
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Xerox Multi-Function Device Security Target WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 ConnectKey 1.5 Technology v1.4, December 2014

e. ETR WorkCentre 5845, 5855, 5865, 5875, 5890, 7220, 7225, 7830, 7835, 7845, 7855 & ColorQube 8700, 8900, 9301, 9302, 9303 Xerox ConnectKey 1.5 Technology, v1.0, 10 November 2014.