COMMON CRITERIA CERTIFICATION REPORT

ColorQube® 9301/9302/9303 ConnectKey 1.5 Technology with FIPS 140-2 Compliance over SNMPv3

25 July 2016

v1.0

383-4-372

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at 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 Common Criteria Scheme – 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 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 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.

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

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

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 Communications Security Establishment.

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 17025:2005, 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 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 posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

ColorQube® 9301/9302/9303 ConnectKey 1.5 Technology with FIPS 140-2 Compliance over SNMPv3 (hereafter referred to as the Target of Evaluation, or TOE), from Xerox Corporation, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a multi-function device that copies and prints with scan and fax capabilities. The Xerox embedded fax component provides local analog fax capability over public switched telephone network connections and also enables LanFax, a feature that allows a document to be faxed from a workstation without printing it. Xerox's workflow scanning component allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository or kept in a private (scan) mailbox or placed on a personal USB storage device.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 25 July 2016 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.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) 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

TOE Name and Version	ColorQube® 9301/9302/9303 ConnectKey 1.5 Technology with FIPS 140-2 Compliance over SNMPv3
Developer	Xerox Corporation
Conformance Claim	(EAL) 2 + ALC_FLR.3

1.1 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.

1.2 TOE DESCRIPTION

The TOE is a multi-function device that copies and prints with scan and fax capabilities. The Xerox embedded fax component provides local analog fax capability over public switched telephone network connections and also enables LanFax, a feature that allows a document to be faxed from a workstation without printing it. Xerox's workflow scanning component allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository or kept in a private (scan) mailbox or placed on a personal USB storage device.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

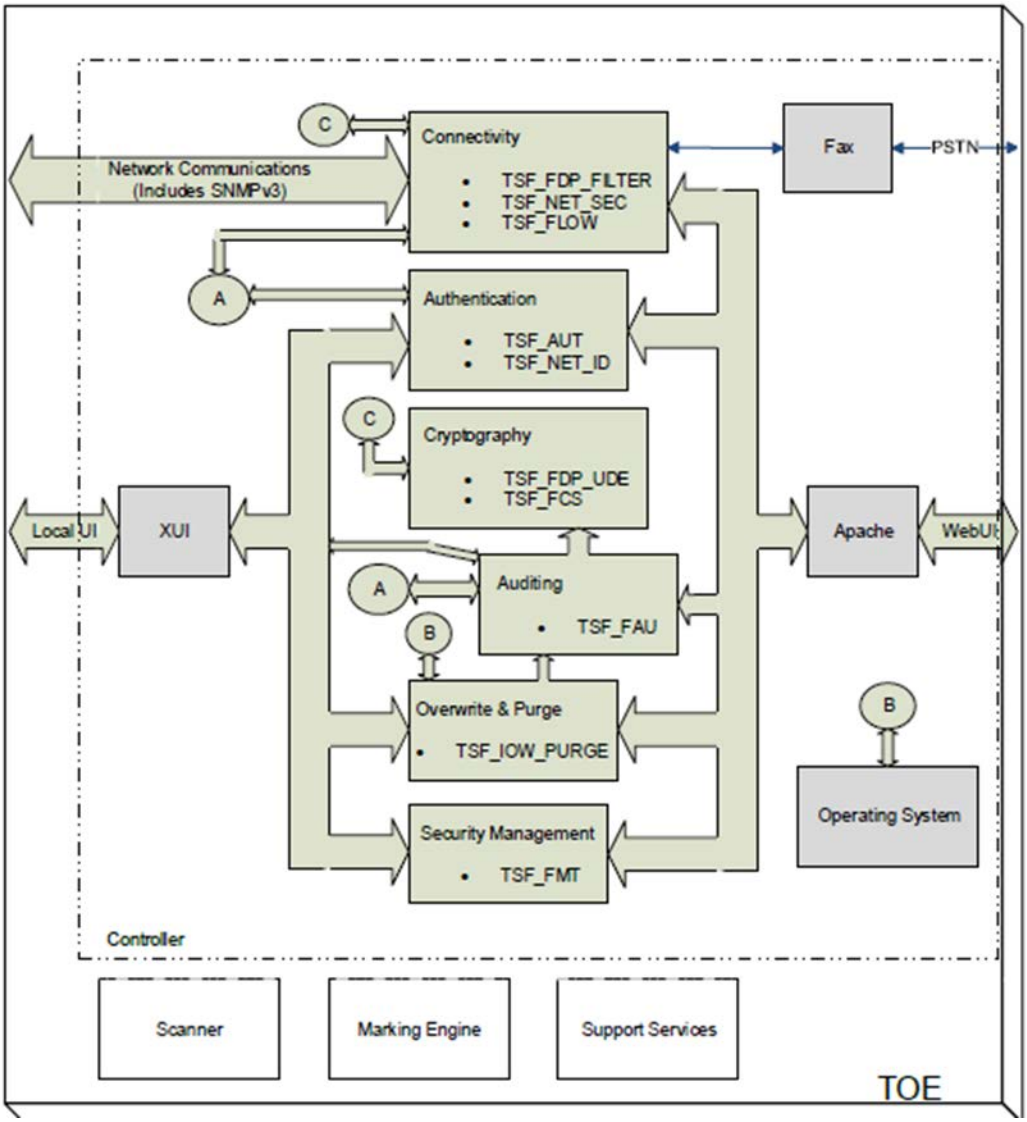

Figure 1 TOE Architecture

A - Connectivity

B - Authentication

C - Cryptography

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; and
- Trusted Path/Channel.

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 Government of Canada approved cryptographic algorithms were evaluated for correct implementation in the TOE:

Table 2 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Triple-DES (3DES)	FIPS 46-3	826 & 1174
Advanced Encryption Standard (AES)	FIPS 197	695 & 1131 & 1821
Rivest Shamir Adleman (RSA)	FIPS 186-4	914
Secure Hash Algorithm (SHS)	FIPS 180-3	1599
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	644 & 1076
Random Number Generator	ANSI X9.31	1018

3 ASSUMPTIONS AND CLARIFICATIONS 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:

- 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; and
- 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.

3.2 CLARIFICATION OF SCOPE

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

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

Model	System Software
ColorQube® 9301/9302/9303	072.180.165.14201 with FIPS SNMPv3 patch 303576v2.dlm

4.1 DOCUMENTATION

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

a. Xerox® ColorQube® 9301 / 9302 / 9303 Xerox ConnectKey Controller System Administrator Guide, version 1.2, November 2013;

b. Xerox® ColorQube® 9301/9302/9303 ConnectKey Controller User Guide, version 1.0, February 2013 ; and

c. Secure Installation and Operation of Your ColorQube® 9301/9302/9303 ConnectKey 1.5 Technology with FIPS 140-2 Compliance over SNMPv3, version 1.1, July 2016.

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 TOE 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 TOE 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.

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.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.

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 ETR.

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.

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. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Local User: The objective of this test case is to demonstrate creation of a normal user account by configuring the security password parameters;

c. Create System Administrator: The objective of this test case is to demonstrate creation of a Privileged user account by configuring the security password parameters;

d. System Administrator and unprivileged user Login: The objective of this test goal is to demonstrate that an administrator as well as an unprivileged user must present a valid username and password to authenticate;

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

f. Confirm Roles Rules: The objective of this test goal is to demonstrate that unprivileged users cannot access administrative functions;

g. Audit Verify: The objective of this test goal is to demonstrate that specific records are written to the audit log;

h. Immediate Image Overwrite: The objective of this test goal is to demonstrate that a submitted job has been properly overwritten;

i. Audit Log Rollover: The objective of this test goal is to demonstrate that the most recent events are retained when the number of log entries exceeds the maximum; and

j. SSL Verification: The objective of this test goal is to demonstrate that only certified versions of SSL can be used to connect to 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;

b. Port Scan: The objective of this test goal is to discover open ports on the TOE for further investigation;

c. Session Management: The objective of this test goal is to attempt to perform a session hijack;

d. Verify Input Validation: The objective of this test goal is to demonstrate that the TOE is not vulnerable to unexpected inputs and SQL injections at the Login Page;

e. Illicit Software Update: The objective of this test goal is to attempt to load a custom software package; and

f. PostScript Hack: The objective of this test goal is to attempt to access the TOE directories by submitting malicious PostScript print jobs.

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 the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

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 CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CPL	Certified Products List
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
USB	Universal Serial Bus
XUI	User Interface Subsystem

Term	Definition

8.2 REFERENCES

Reference
CCS Publication #4, Technical Oversight, Version 1.8, October 2010.
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Xerox Multi-Function Device Security Target, ColorQube® 9301/9302/9303 ConnectKey 1.5 Technology with FIPS 140-2 Compliance over SNMPv3, version 1.2, June 2016
Evaluation Technical Report ColorQube® 9301/9302/9303 ConnectKey 1.5 Technology with FIPS 140-2 Compliance over SNMPv3, version 1.0, July 2016