National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Xerox ColorQube™ 8700/8900

Report Number: CCEVS-VR-VID10498-2012

Dated: 21 December 2012

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Dr. Patrick Mallett, MITRE Corporation

Paul Bicknell, MITRE Corporation

Common Criteria Testing Laboratory

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Evaluators

Cheryl Dugan

Annette Nadeau

Huan Zhou

Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Xerox ColorQube™ 8700/8900, the target of evaluation (TOE), performed by Computer Sciences Corporation. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on the 21h of December 2012. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Computer Sciences Corporation on behalf of Xerox. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.3, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 3, dated July 2009.

The Xerox ColorQube™ 8700/8900 is a multi-function device (MFD) that copies, prints, scans and faxes. The MFD contains an internal hard disk drive. Standard security functions include SSL, IPSec, a host-based firewall, and an internal audit log. Users may be authenticated to the network or locally at the device. The evaluated configuration includes the Image Overwrite Security package. The Image Overwrite Security package causes any temporary image files to be erased from the internal hard disk drive when those files are no longer needed or on demand at the discretion of the system administrator.

1.1.Interpretations

There are no applicable Common Criteria interpretations.

2. IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NIAP’s Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Xerox ColorQube™ 8700/8900
Protection Profile	U.S. Government Protection Profile for Hardcopy Devices Version (IEEE Std. 2600.2-2009 Protection Profile, v1.0, 26 February 2010
Security Target	Xerox ColorQube™ 8700/8900 Security Target, Version 1.0, Revision 1.8, 25th December 2012
Dates of evaluation	November 2011 to December 2012
Evaluation Technical Report	Xerox Xerox ColorQube™ 8700/8900 Evaluation Technical Report, Computer Sciences Corporation, v1.0, 5th November 2012
Conformance Result	EAL 2 augmented with ALC_FLR.3
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 3, July 2009
Common Evaluation Methodology (CEM) version	CEM version 3.1R3, July 2009
Sponsor	Xerox Corporation
Developer	Xerox Corporation
Evaluators	Cheryl Dugan, Annette Nadeau, Huan Zhou
Validation Team	Patrick Mallett, Paul Bicknell

3. SECURITY POLICY

The TOE enforces the following security policies:

- **Information Flow Security.** The TOE prevents unauthorized data flow between the fax line interface and the network interface.
- **User Data Protection – SSL.** The TOE implements the Secure Sockets Layer (SSL) protocol to protect communication via the Web Graphical User Interface (GUI) and to protect workflow scanning communications to an SSL enabled repository.
- **User Data Protection – IPSec.** The TOE implements Internet Protocol Security (IPSec) to protect print client communications.
- **IP Filtering.** The TOE provides the ability for the system administrator to configure IPv4 filtering rules.
- **Network Management Security.** The TOE implements Simple Network Management Protocol v3 (SNMP) for management communications via the SNMP interface.
- **Privileged User Access Control.** The TOE restricts management of security functions to the authorized system administrator.
- **User Access Control.** The TOE enables system administrators to restrict access to the print, copy, scan and fax functions to authorized users.

A complete list of the security functions of the TOE is provided at section **Error! Reference source not found.**.

4. SECURITY PROBLEM DEFINITION

4.1. Assumptions

The ST identified the following security assumptions:

- 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.
- 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.

4.2. Threats

The ST identified the following threats addressed by the TOE:

- User Document Data may be disclosed to unauthorized persons
- User Document Data may be altered by unauthorized persons
- User Function Data may be altered by unauthorized persons

4.3. Organizational Security Policies

The ST identified the following OSPs addressed by the TOE:

- To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner
- To detect corruption of the executable code in the TOE Security Functions (TSF), procedures will exist to self-verify executable code in the TSF
- To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel
- To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment

4.4.Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.2).
- This evaluation only covers the specific platforms and software version identified in this document, and not any earlier or later versions released or in process.

The following features are not included in the evaluated configuration:

- IPX. Network communication protocol.
- AppleTalk. Network communication protocol.
- Internet Fax. Allows the user to scan documents at the control panel, send them to destination email addresses, or receive and print emails with attachments.
- Network Domain Security (NDS). Network authentication protocol.
- Server Message Block (SMB). Network authentication protocol.
- Network Accounting. Allows users to manage printer usage with detailed cost analysis capabilities.
- Network Authorization. When configured, the printer references an authorization server for authorization information, such as role, for the authenticated user.
- Reprint Saved Jobs. The Reprint Saved Jobs feature allows you to save your print job on the printer so that you can print it at any time.
- Smart eSolutions. Suite of features that provide free services to enable administration of metered billing and supplies replenishment plans for printers on a network.
- Xerox Extensible Interface Platform (EIP). Allows independent software vendors and partners to develop personalized and customized document management solutions. These solutions can be integrated and accessed directly from the printer control panel.

Please see http://www.xerox.com/information-security/product/enus.html for more specific information about maintaining the security of this TOE.

5. ARCHITECTURAL INFORMATION

5.1.Logical Scope and Boundary

The TOE logical scope and boundary consists of the security functions provided/controlled by the TOE as follows:

- **Image Overwrite.** The TOE implements an image overwrite security function to overwrite all temporary files created during processing of jobs.
- **Information Flow Security.** The TOE prevents unintentional transmission of data between its interfaces and the network and/or PSTN to which the TOE is connected.
- **Authentication.** The TOE can be configured to authenticate users against an internal database via username and password.
- **Network Identification.** The TOE can be configured to authenticate users against an external database via username and password or smartcard and Personal Identification Number (PIN).
- **Security Audit.** The TOE generates audit logs that track events/actions (e.g., copy/print/scan/fax job completion) to identified users.
- **Network Security.** The TOE supports the following secure communication protocols: TLS for Web UI; SFTP and TLS for document transfers to the remote file depository; IPsec for communication over IPv4 and IPv6; and Kerberos and TLS for remote authentication.
- **Cryptographic Operations.** The TOE utilizes digital signature generation and verification (RSA), data encryption (TDES, AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA-1) in support of disk encryption, SFTP, TLS and IPsec. The algorithms deployed meet the following standard: TDES – FIPS 46-3 (CAVP Certificate No. 826 and CAVP Certificate No. 1174); AES - FIPS 197 (CAVP Certificate No. 1131 and CAVP Certificate No. 1821); SHA-1, SHA-256 – FIPS 180-3 (CAVP Certificate No. 1599), HMAC - FIPS 198 (CAVP Certificate No. 644 and CAVP Certificate No. 1076); RSA - FIPS186-3 (CAVP Certificate No. 914).
- **User Data Protection – Disk Encryption.** The TOE implements AES data encryption to protect all areas of the hard drive where user jobs are temporarily stored for processing. The algorithm deployed meets the following standard: AES-FIPS-197 (CAVP Certificate No. 1131).
- **User Data Protection – IP Filtering.** The TOE provides the ability for the system administrator to configure IPv4 filtering rules.
- **Security Management.** The security functions of the TOE are managed by the system administrator from both the LUI and WebUI. User’s access to the TOE functions, Job or Image Data stored inside the TOE is

restricted, in accordance with the applicable TOE Security Policies. The TOE is capable of verifying the integrity of the TSF at the request of the administrator.

The difference between the various models of the TOE is their supported paper sizes and finishing options.

5.2.Physical Scope and Boundary

The Xerox ColorQube™ 8700/8900 is a multi-function device (MFD). The physical boundary of the TOE consists of the MFD and optional fax accessory, and accompanying user and administrator guidance listed in section 6.

In the evaluated configuration, the TOE is connected to the Public Switched Telephone Network (PSTN) and the Local Area Network (LAN) as described in the user guidance delivered with the TOE.

The following figure depicts the TOE.

Figure 1: Xerox ColorQube™ 8700/8900

The various software and firmware that comprise the TOE are listed in Table 2. A system administrator can ensure that they have a TOE by printing a configuration sheet and comparing the version numbers reported on the sheet to the table below.

Table 2: Evaluated version

Software/Firmware Item	Identifier
System Software	071.160.222.23700
Network Controller Software	071.162.23700
User Interface Software	071.162.23720
Marking Engine Software (Options)	003.003.026
Copy Controller Software	071.162.23720

Software/Firmware Item	**Identifier**
Document Feeder Software (DADH)	010.060.000
Finisher Software	003.008.044
Fax Software	003.010.011
Copy Controller OS	071.162.23720
Network Controller OS	071.162.23720
Scanner Software	030.185.000

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the ColorQube™ 8700/8900. Note that not all evidence is available to customers. The following documentation is available to the customer:

- ColorQube™ 8700/8900 Color Multifunction Printer System Administrator Guide v1.0
- ColorQube™ 8700/8900 Color Multifunction Printer User Guide v1.0
- Secure Installation and Operation of Your Xerox ColorQube™ 8700/8900 v1.1

The remaining evaluation evidence is described in the Evaluation Technical Report developed by Computer Sciences Corporation.

7. IT PRODUCT TESTING

This section describes the testing efforts of the developer and the evaluation team.

7.1.Developer testing

Test procedures were written by the developer and designed to be conducted using manual interaction with the TOE interfaces. The developer tested all of the interfaces to the TOE and in doing so tested all TSFs.

The developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The evaluation team analyzed the developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the developer's actual test results matched the developer's expected test results.

The evaluators assessed that the test environment used by the developers was appropriate and mirrored the test configuration during independent testing.

7.2.Evaluation team independent testing

The evaluation team conducted independent testing at the CCTL facility. The TOE was delivered in accordance with the documented delivery procedures. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the developer's test plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated a sample of the developer's test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the developer test coverage and the ST.

The evaluators examined the design evidence and selected an appropriate test platform.

Each TOE Security Function was exercised and the evaluation team verified that each test passed.

7.3.Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, the evaluation team conducted penetration testing to determine if the identified potential vulnerabilities was indeed exploitable.

The evaluation team concluded that the TOE does not contain exploitable vulnerabilities in the intended environment and for the postulated attackers.

8. EVALUATED CONFIGURATION

The following features are enabled in the evaluated configuration:

- IIO and ODIO (the Image Overwrite Security Package)
- HTTPS (TLS\SSL)
- User Authorization

The Xerox ColorQube™ 8700/8900 must be configured in accordance with the guidance documents listed at section 6. In particular, Secure Installation and Operation of Your Xerox ColorQube™ 8700/8900 v1.1 provides Common Criteria specific advice.

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R3.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.3. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on December 5, 2012. A final Validation Oversight Review (VOR) was held on December 11, 2012 and final changes to the VR were completed on December 21, 2012.

10. VALIDATOR COMMENTS/RECOMMENDATIONS

The validation team's observations support the evaluation team's conclusion that the Xerox ColorQube™ 8700/8900 meets the claims stated in the Security Target.

11. ANNEXES

None

12. SECURITY TARGET

Xerox ColorQube™ 8700/8900 Security Target, Version 1.0, Revision 1.8, 17 December 2012

13. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. BIBLIOGRAPHY

1.) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-001.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

4.) Common Evaluation Methodology for Information Technology Security Evaluation, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

5.) Xerox ColorQube™ 8700/8900 Security Target, Version 1.0, Revision 1.8, 17 December 2012

6.) Computer Sciences Corporation (CSC) Evaluation Technical Report for Xerox ColorQube™ 8700/8900, Version 1.0, 5th November 2012.