National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Xerox ColorQube™ 9201/9202/9203

Report Number: CCEVS-VR-VID 10371

Dated: December 20, 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 STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell

Franklin Haskell

Common Criteria Testing Laboratory

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Evaluators

John Daniels
Cheryl Dugan
Annette Nadeau
Lachlan Turner

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™ 9201/9202/9203, 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 5th of November, 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 2, dated September 2007 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 2, dated September 2007.

The Xerox ColorQube™ 9201/9202/9203 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, SNMPv3, 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, a consumer option. 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 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™ 9201/9202/9203
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™ 9201/9202/9203 Security Target, Version 1.0, Revision 1.11, 19th December 2012
Dates of evaluation	June 2009 to November 2012
Evaluation Technical Report	Xerox ColorQube™ 9201/9202/9203 Evaluation Technical Report, Computer Sciences Corporation, v1.0, 5 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 2, September 2007
Common Evaluation Methodology (CEM) version	CEM version 3.1R2, September 2007
Sponsor	Xerox Corporation
Developer	Xerox Corporation
Evaluators	John Daniels, Cheryl Dugan, Annette Nadeau, Lachlan Turner
Validation Team	Paul Bicknell, Franklin Haskell

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 5.1.

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 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.

In the evaluated configuration, the following options should be disabled:

- Network Accounting
- Copy/Print, Store and Reprint
- SMart eSolutions
- Xerox Extensible Interface Platform (EIP)
- USB direct printing

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 unauthorized data flow between the fax line interface and the network interface.
- **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.
- **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.
- **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.
- **User Data Protection – 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.
- **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.
- **Cryptographic Operations.** The TOE utilizes data encryption (AES, RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted

products. The algorithms deployed have the associated Cryptographic Algorithm Validation Program (CAVP) certificates: 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 - 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).

The difference between the TOE models is their printing speed. The following figure depicts the TOE's architectural subsystems and its environment.

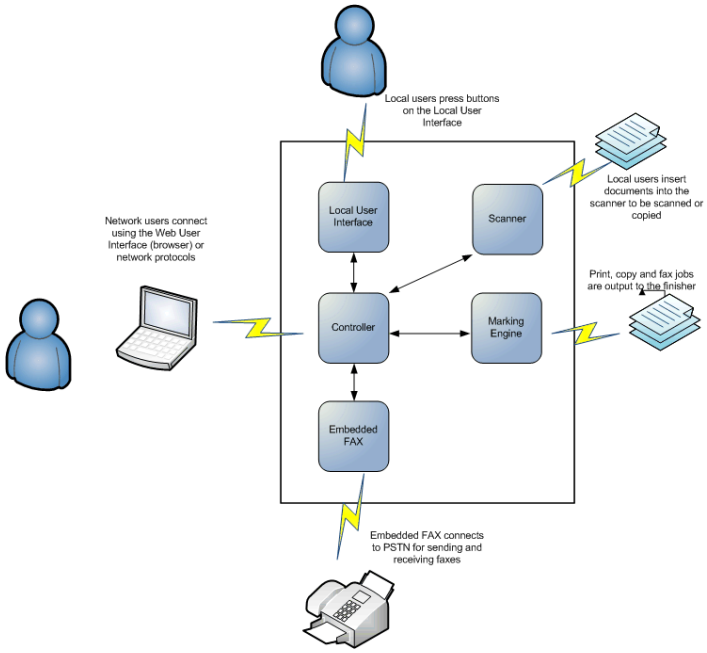

Figure 1: Depiction of TOE and Subsystems

5.2. Physical Scope and Boundary

The Xerox ColorQube™ 9201/9202/9203 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 2: Xerox ColorQube™ 9201/9202/9203

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	ColorQube 9201/9202/9203
System Software	**061.080.221.36200**
Network Controller Software	**061.081.36140**
User Interface Software	**061.051.34940**
Marking Engine Software	**008.036.006**
Copy Controller Software	**061.051.35740**
Document Feeder Software (Options)	
DADH 75	**016.027.000**
DADH 100	**025.020.000**
DADH 100 Quiet Mode	**020.012.000**
Finisher Software (Options)	
LCSS	**002.000.045**
High Volume Feeder (HVF)	**002.003.097**

HVF with BookletMaker	**010.020.000**
Fax Software	**003.010.004**
Scanner Software	**010.159.000**

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 Xerox ColorQube™ 9201/9202/9203. Note that not all evidence is available to customers. The following documentation is available to the customer:

- ColorQube™ 9201/9202/9203 System Administrator Guide v1.0
- ColorQube™ 9201/9202/9203 Interactive User Guide
- Secure Installation and Operation of Your ColorQube™ 9201/9202/9203 v1.3

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

In its evaluated configuration, IIO and ODIO (the Image Overwrite Security Package) are installed and enabled on the TOE; SSL is enabled on the TOE; and User Authorization is enabled on the TOE. The FAX (Xerox Embedded Fax accessory) option, if purchased by the consumer, is installed and enabled on the TOE. The LanFax option is included in the evaluated configuration of the TOE. USB Direct Printing is not included in the evaluated configuration of the TOE.

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

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 3.1R2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R2.

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 November 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

No product features (or lack thereof), configuration considerations, or environmental assumptions need to be noted for the customer, except for the following.

An observation decision generated by a similar product produced by the same vendor was determined to be applicable to this product. The problem is that it is possible, though not very likely, that the audit trail can be filled in a matter of hours. The applicable resolution is:

Because this model is no longer produced but still being used, Xerox must amend their user guidance to provide information about the possible security vulnerability, including guidance about monitoring the audit logs to safeguard the entries.

Customers of this product should verify that their administrative procedures include periodic checks of the audit log.

11. ANNEXES

None

12. SECURITY TARGET

Xerox ColorQube™ 9201/9202/9203 Security Target, Version 1.0, Revision 1.11, 19th 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 September 2006, Version 3.1, Revision 1, CCMB-2006-09-001.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2007, Version 3.1, Revision 2, CCMB-2007-09-002.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2007, Version 3.1, Revision 2, CCMB-2007-09-003.

4.) Common Evaluation Methodology for Information Technology Security Evaluation, dated September 2007, Version 3.1, Revision 2, CCMB-2007-09-004.

5.) Xerox ColorQube™ 9201/9202/9203 Security Target, Version 1.0, Revision 1.11, 19th December 2012

6.) Computer Sciences Corporation (CSC) Evaluation Technical Report for Xerox ColorQube™ 9201/9202/9203, Version 1.0, 5 November 2012.