National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Xerox® AltaLink™ B8045/B8055/B8065/B8075/ B8090

Report Number: CCEVS-VR-VID10789-2017

Dated: November 20, 2017

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

Jerome Myers

Marybeth Panock

The Aerospace Corporation

Evaluation Team

Brian Pleffner

Cheryl Dugan

Michael Esposito

DXC Technology

Table of Contents

List of Tables

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® AltaLink™ B8045/B8055/B8065/B8075/ B8090, the Target of Evaluation (TOE), performed by DXC Technology Security Testing and Certification Laboratory (STCL). 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 DXC Technology (DXC) of Annapolis Junction, MD in accordance with the United States evaluation scheme and completed in November 2017. The information in this report is largely derived from the ST, and the evaluation sensitive documents: the Evaluation Technical Report (ETR) and the functional testing report, which are summarized in the Assurance Activity Report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, dated September 2012.

The Xerox® AltaLink™ B8045/B8055/B8065/B8075/ B8090, is a multi-function device that copies and prints with scan and fax capabilities.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Xerox® AltaLink™ B8045/B8055/B8065/B8075/ B8090 System Software version: 100.008.057.09602 with network controller patch 1190013v3
Sponsor and Developer	Xerox Corporation 800 Phillips Road Rochester, NY 14580
CCTL	DXC Technology 10830 Guilford Road, Suite 308 Annapolis Junction, Maryland 20701
Completion Date	November 20, 2017

Item	Identifier
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015.
Disclaimer	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.
Evaluation Personnel	Brian Pleffner Cheryl Dugan Michael Esposito DXC Technology
Validation Personnel	Jerome Myers Marybeth Panock The Aerospace Corporation

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Product Compliant List (PCL).

Table 2 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

Table 2: Evaluation Identifiers

Item	Identifier
ST Title and Version	Xerox® AltaLink™ B8045/B8055/B8065/B8075/ B8090 Security Target version 1.0
Publication Date	November 20, 2017
Vendor	Xerox Corporation
ST Author	CSC Corporation; Eric Jacksch
Target of Evaluation Reference	Xerox® AltaLink™ B8045/B8055/B8065/B8075/ B8090
TOE Software Version	100.008.057.09602 with network controller patch 1190013v3
Keyword	Multi-function Device

3. Security Policy

The core functionality of the Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090 is the ability to define and enforce security policies to protect the data transmitted, stored, and processed on the multifunction device.

This section summaries the security functionality of the TOE:

- Identification and Authentication
- Security Audit
- Access Control
- Security Management
- Trusted Operations
- Encryption
- Trusted Communication
- PSTN Fax-Network Separation
- Data Clearing and Purging

3.1. Identification and Authentication

In the evaluated configuration, the TOE requires users and system administrators to authenticate before granting access to user (copy, print, fax, etc.) or system administration functions via the Web User Interface (Web UI) or the Local User Interface (LUI). The user or system administrator must enter a username and password at either the Web UI or the LUI. The password is obscured as it is being entered. The TOE provides role based access control as configured by the system administrator.

The TOE also supports smart card, Kerberos and Lightweight Directory Access Protocol (LDAP) for network authentication.

3.2. Security Audit

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to identified users. The audit logs, which are stored locally in a 15000-entry circular log, are available to TOE administrators and can be exported in comma separated format for viewing and analysis.

3.3. Access Control

The TOE enforces a system administrator defined role based access control policy. Only authenticated users assigned to roles with the necessary privileges are allowed to perform copy, print, scan or fax on the TOE via the Web UI or the LUI.

Unauthenticated users can submit print or LanFax jobs to the TOE via printing protocols. Release of unauthenticated print jobs to the hardcopy output handler is dependent on the system administrator defined policy.

The TOE allows filtering rules to be specified for IPv4 network connections based on IP address and port number.

3.4. Security Management

A Local User, via the local user interface, or a Remote User, via the browser-based interface, with administrative privileges can configure the security settings of the TOE. The TOE has the capability to assign Users to roles that distinguish Users who can perform administrative functions from Users who can perform User functions via a role based access control policy. The TOE also has the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the TOE and in transit to or from the browser-based interface.

3.5. Trusted Operation

The TOE includes a software image verification feature and Embedded Device Security which employs McAfee software to detect and prevent unauthorized execution and modification of TOE software.

3.6. Encryption

The TOE utilizes digital signature generation and verification (RSA), data encryption (AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA-1) in support of disk encryption, SSH, TLS, TLS/HTTPS, TLS/SMTP and IPsec. The TOE also provides random bit generation in support of cryptographic operations.

The TOE stores temporary image data created during a copy, print, scan and fax job on the single shared hard disk drive (HDD) that is field replaceable. This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDD used for spooling temporary files are encrypted. The hard drive encryption key is derived from a BIOS saved passphrase and is the same value after each power-up (see KMD for details).

3.7. Trusted Communication

The TOE provides support for a number of secure communication protocols:

- Transport Layer Security (TLS) support is available for protecting communication over the Web User Interface (Web UI) and SMTP email communications.
- Secure Shell (SSH) File Transfer Protocol (SFTP) and TLS are available for protecting document transfers to a remote file depository.

- Internet Protocol Security (IPsec) support is available for protecting communication over IPv4 networks.
- TLS support is available for protecting communication with a remote authentication server.

3.8. PSTN Fax-Network Separation

The TOE provides separation between the fax processing board and the network interface and therefore prevents an interconnection between the PSTN and the internal network. This separation is realized in software, as by design, these interfaces may only communicate via an intermediary.

3.9. Data Clearing and Purging

The image overwrite feature overwrites temporary image files created during a copy, print, scan or fax job when those files are no longer needed. Overwrite is also invoked at the instruction of a job owner or administrator and at start-up. The purge feature allows an authorized administrator to permanently delete all customer-supplied data on the TOE. This addresses residual data concerns when the TOE is decommissioned from service or redeployed to a different environment.

4. Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Hardcopy Devices, Version 1.0 10 September 2015 (HCDPP)

That information has not been reproduced here and the HCDPP should be consulted if there is interest in that material.

5. Scope of the Evaluation

The scope of this evaluation was limited to the functionality and assurances covered in the HCDPP as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 (the assurance activities specified in the Hard Copy Device Protection Profile and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the HCDPP and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, the following functionality present in the PAM product was not covered by the evaluation:
    - Workflow Scanning using SFTP (only HTTPS permitted);
    - Xerox Secure Access and Convenience Authentication are not permitted in the evaluation configuration; and,
    - SNMPv3 for device management.

7. Architectural Information

7.1. Physical Scope and Boundary

The TOE is an MFD (Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090) that consists of a printer, copier, scanner, fax and associated administrator and user guidance. The TOE comprises all software and firmware within the MFD enclosure.

Users can determine version numbers and whether the Xerox Embedded Fax Accessory, Xerox Workflow Scan Accessory and Image Overwrite Security Package are installed by reviewing the TOE configuration report.

7.2. Required Non-TOE Hardware, Software, and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a multi-function hard copy device. Additional features require non-TOE support as follows:

- Network security and fax flow features are only useful in environments where the TOE is connected to a network or PSTN.
- Network identification is only available when LDAP or Kerberos remote authentication services are present in the environment.
- Smart card authentication requires Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smart cards and readers or equivalent. In support of smart card authentication, a Windows Domain Controller must also be present in the environment.
- The TOE may be configured to reference an NTP server for time.

8. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Xerox® AltaLink® B80XX Series Multifunction Printer User Guide, Version 1.0*
- *Xerox® AltaLink®Series Multifunction Printer System Administrator Guide, Version 1.0*
- *Secure Installation and Operation of Your AltaLink® B8045 / B8055 / B8065 /B8075 / B8090 Multifunction Printer and AltaLink C8030 / C8035 / C8045 / C8055 / C8070 Color Multifunction Printer Version 1.3*

All documentation delivered with the product is relevant to and within the scope of the TOE.

9. IT Product Testing

This section describes the testing efforts of the evaluation team. The Assurance Activity Report (AAR): For Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090 Document version: 1.0 November 2017, reference 16 in the Bibliography, summarizes the proprietary detailed test report.

9.1. Evaluation team independent testing

The evaluation team conducted independent testing at the DCX Technology Security Testing and Certification Lab in Annapolis Junction, MD and the Xerox Corporation in Rochester, NY. The evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target. The AAR, in section 7 Test Configuration, provides the test configurations, including the TOE components, the various test environments, and the test tools used.

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 Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

9.2. Evaluated Configuration

The evaluated configuration consists of the Multifunction Function Printers (MFPs), as defined by Table 2: Xerox MFPs, in the Security Target, and the Xerox Embedded Fax Accessory, and Smart Card Authentication. To implement the security features identified the Security Target, the TOE must be configured in accordance with the Secure Installation and Operation guidance document identified in section 7 Documentation (and reference 6 in the Bibliography)

The secure Common Criteria configuration information is contained in references 6 and 7, “Secure Installation and Operation of Your AltaLink™ B8045 / B8055 / B8065 / B8075 / B8090 Multifunction Printer AltaLink™ C8030/C8035/C8045/C8055/C8070 Multifunction Printer, Version 1.3” and “Xerox® AltaLink Series® System Administrator Guide, Version 1.0” respectively.

The evaluated configuration was tested on the Xerox MFP – AltaLink™ B8055. The test configuration, test environments, and test tools are summarized in section 7 of the AAR. The tests for each Security Functional Requirement (SFR) are also summarized in the AAR.

9.3. 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, there were no identifiable vulnerabilities found at the time of certification. The details of the vulnerability analysis are summarized in the Evaluation Technical Report (ETR), reference 17 in the Bibliography. The public databases searched include Security Focus, SEI CERT, and the National Vulnerability Database. Vulnerabilities for the Xerox printers as well as the underlying operating systems were explored.

10. 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 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

DXC Technology has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on November 20, 2017.

11. Validator Comments

The validators have no additional comments.

12. Annexes

None

13. Security Target

Xerox Multi-Function Device Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090 Security Target, Version 1.0

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. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
CSC	DXC Technology
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HCDPP	Hard Copy Device Protection Profile
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. Xerox Multi-Function Device Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090 Security Target, Version 1.0
6. Secure Installation and Operation of Your AltaLink™ B8045 / B8055 / B8065 / B8075 / B8090 Multifunction Printer AltaLink™ C8030/C8035/C8045/C8055/C8070 Multifunction Printer, Version 1.3
7. Xerox® AltaLink Series® System Administrator Guide, Version 1.0
8. Xerox® AltaLink™ B80XX Multifunction Printer User Guide, 1.0
9. Protection Profile for Hardcopy Devices, Version 1.0
10. TD0074: FCS_CKM.1(a) Requirement in HCD PP, Version 1.0
11. TD0176 – FDP_DSK_EXT.1.2 - SED Testing
12. TD0157 – FCS_IPSEC_EXT.1.1 – Testing for SPDs
13. TD0219 – NIAP Endorsement of Errata for HCD PP v1.0
14. Xerox Key Management Description for Xerox Atlantis Multi-Function Device, Version 1.10
15. Xerox B8045 / B8055 / B8065 /B8075 / B8090 Entropy Assessment Report, Version 0.5
16. Assurance Activity Report: For Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090 Document version: 1.0 November 2017
17. Xerox Evaluation Technical Report For Xerox® AltaLink™ B8045 / B8055 / B8065 /B8075 / B8090 Document version: 1.0 November 2017