# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

## Xerox® AltaLink™ EC8036 & EC8056

### Report Number: CCEVS-VR-VID11270-2022

**Dated: June 14, 2022**

**Version: 1.0**

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

**Department of Defense**
**ATTN: NIAP, SUITE: 6982**
**9800 Savage Road**
**Fort Meade, MD 20755-6982**

**ACKNOWLEDGEMENTS**

**Validation Team**

Jerome Myers

Meredith Martinez

Alex Korobchuk

Dale Schroeder

**The Aerospace Corporation**

**Evaluation Team**

Travis Hoffmeister

Thibaut Marconnet

Dylan Paynter

Furukh Siddique

Kevin Steiner

**Lightship Security, USA**

# Table of Contents

# List of Tables



# List of Figures

# 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™ EC8036/EC8056 of Evaluation (TOE), performed by Lightship Security USA Common Criteria Laboratory (CCTL). 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 Lightship Security USA (LS) of Austin, Texas in accordance with the United States evaluation scheme and completed in June 2022. The information in this report is largely derived from the ST, and the evaluation sensitive documents: Evaluation Technical Report (ETR) and the functional testing report, which are summarized in the Assurance Activity Report (AAR). The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated April 2017, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 5, April 2017.

The Xerox® AltaLink™ EC8036 & EC8056 is a multi-function printer device that copies and prints with scan and fax capabilities.

**Table 1: Evaluation Details**

| Item | Identifier |
|---|---|
| Evaluated Product | Xerox® AltaLink™ EC8036 & EC8056<br>System Software version: 103.023.031.35105 |
| Sponsor and Developer | Xerox Corporation<br>800 Phillips Road<br>Rochester, NY 14580 |
| CCTL | Lightship Security USA<br>11044 Research Blvd., Suite A-220<br>Austin, Texas 78759 |
| Completion Date | June 14, 2022 |

| Item | Identifier |
|---|---|
| Interpretations | There are the following Technical Decisions for this evaluation.<br>0562 - Test Activity for Public Key Algorithms<br>0494 – Removal of Mandatory SSH Cipher Suites for HCD<br>0474 – Removal of Mandatory Cipher Suite For FCS_TLS_EXT.1<br>0393 – Require FTP_TRP.1(b) only for printing<br>0299 – Update to FCS_CKM.4 Assurance Activities<br>0261 – Destruction of CSPs in flash<br>0253 – Assurance Activities for Key Transport<br>0219 – NIAP Endorsement of Errata for HCD PP v1.0<br>0176 – FDP_DSK_EXT.1.2 - SED Testing<br>0157 – FCS_IPSEC_EXT.1.1 - Testing SPDs<br>0074 – FCS_CKM.1(a) Requirement in HCD PP v1.0 |
| CEM | Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017 |
| Conformance Result | CC Part 2 extended; CC Part 3 conformant |
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Protection Profile | Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 and Errata for the Hard Copy Device Protection Profile v1.0. |
| 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 | Travis Hoffmeister<br>Thibaut Marconnet<br>Dylan Paynter<br>Furukh Siddique<br>Kevin Steiner<br>Lightship Security USA |
| Validation Personnel | Jerome Myers<br>Meredith Martinez<br>Alex Korobchuk<br>Dale Schroeder<br>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 1 and Table 2 provide 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.
- The Protection Profile configuration to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 2: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| ST Title and Version | Xerox® AltaLink™ EC8036 & EC8056 Security Target, v1.4 |
| Publication Date | June 1, 2022 |
| Vendor | Xerox Corporation |
| ST Author | Xerox Corporation, Erin Huber |
| Target of Evaluation Reference | Xerox® AltaLink™ EC8036 & EC8056 |
| TOE Software Version | 103.023.031.35105 |
| Keyword | Multi-function Device |

# 3. Security Policy

The core functionality of the Xerox® AltaLink™ EC8036 & EC8056 Security Target is the ability to protect the data transmitted to the multifunction device.

# 4. Security Problem Definition

## 4.1. Assumptions

The ST identified the following security assumptions contained in Table 3:

**Table 3: Secure Usage Assumptions**

| ID | Assumptions |
|---|---|
| **A.PHYSICAL** | Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment. |
| **A.NETWORK** | The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface. |
| **A.TRUSTED_ADMIN** | TOE Administrators are trusted to administer the TOE according to site security policies. |
| **A.TRAINED_USERS** | Authorized Users are trained to use the TOE according to site security policies. |

## 4.2. Threats

The ST identified the following threats addressed by the TOE:

**Table 3: Threats Addressed**

| ID | Threats |
|---|---|
| **T.UNAUTHORIZED_ACCESS** | An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces. |
| **T.TSF_COMPROMISE** | An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces. |
| **T.TSF_FAILURE** | A malfunction of the TSF may cause loss of security if the TOE is permitted to operate. |
| **T.UNAUTHORIZED_UPDATE** | An attacker may cause the installation of unauthorized software on the TOE. |
| **T.NET_COMPROMISE** | An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication. |

### 4.3. Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

**Table 4: Organizational Security Policies**

| ID | Organizational Security Policy |
|---|---|
| **P.AUTHORIZATION** | Users must be authorized before performing Document Processing and administrative functions. |
| **P.AUDIT** | Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity. |
| **P.COMMS_PROTECTION** | The TOE must be able to identify itself to other devices on the LAN. |
| **P.STORAGE_ENCRYPTION** | If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices. |
| **P.KEY_MATERIAL** | Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device. |
| **P.FAX_FLOW** | If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN. |
| **P.IMAGE_OVERWRITE** | Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices. |
| **P.PURGE_DATA** | The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices. |

# 5. Architectural Information

## 5.1. TOE Description

The TOE is a hardcopy device that copies and prints with scan and fax capabilities, commonly known as Multi-Function Device (MFD), Multi-Function Printer (MFP) or simply printer. See Section 2 of the ST for more information on the TOE usage, administration, and secure communication.

## 5.2. TOE Evaluated Configuration

The TOE evaluated configuration is the Xerox® AltaLink™ EC8036 & EC8056 multi-function device products running system software version: 103.023.031.35105.

## 5.3. Physical Scope and Boundary

The TOE is an MFD (Xerox® AltaLink™ EC8036 & EC8056) that consists of a printer, copier, scanner, fax and associated administrator and user guidance. The TOE comprises the hardware, all software and firmware within the MFD enclosure.

Xerox® AltaLink™ EC8036 & EC8056 are color MFP or color printers. All models have an Intel Atom E3845 (Bay Trail) processor and run Wind River Linux 6.0. Each model consists of an input document handler and scanner, Xerox embedded Fax accessories, marking engine, controller, Xerox Workflow scanning accessory and user interface. Differences between models is limited to print speed and options such as finishers, paper trays and document handlers. The differences between the models are not security relevant.

## 5.4. 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 that the TOE operates with the following non-TOE components in the environment:

a. IPv4 or IPv6 network environment
b. Publicly Switched Telephone Network (PSTN)
c. LDAP server for authentication services
d. NTP server for time services
e. File server for Workflow Scanning
f. Log server (file server) for remote log storage
g. Printer drivers on supported OS per

   https://www.support.xerox.com/en-us/product/xerox-ec8036-ec8056-multifunction-printer
h. 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.

# 6. Logical Scope of the TOE

The TOE provides the following security features:

**Identification and Authentication**

In the evaluated configuration, the TOE requires users and system administrators to authenticate before granting access to printer or system administration functions via EWS or the Control Panel. The TOE supports username/password and smartcard-based authentication.

**Security Audit**

The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

**Access Control**

The TOE enforces a system administrator defined role-based access control policy.

**Security Management**

System administrators manage the TOE's security configuration via the Control Panel and/or EWS. The TOE allows filtering rules to be specified for IPv4 network connections based on IP address and port number.

**Trusted Operation**

The TOE preforms a suite of self-tests to verify correct operation during start-up and verifies the authenticity and integrity of firmware updates.

**Cryptographic Operations**

The TOE incorporates two cryptographic modules:

Mocana. Provides cryptographic services for hard disk encryption/decryption and encryption/decryption services for the IPSec protocol and for asymmetric key generation

OpenSSL. Provides cryptographic services for HTTPS/TLS and SSH encryption/decryption services.

**Storage Encryption**

The TOE stores temporary files created during a copy, print, scan and fax job on a single shared hard disk drive (HDD). All partitions of the HDD used for spooling temporary files are encrypted.

**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 Embedded Web Server (EWS) and SMTP

email communications. TLS is also used to protect communication with the remote authentication server (LDAPS)

- Secure Shell (SSH) File Transfer Protocol (SFTP) is available for audit log secure transfers to a remote file repository.
- Internet Protocol Security (IPsec) support is available for protecting communication with print clients and communication with the domain controller when using SmartCard authentication.
- HTTPS support is available for communication between EWS and remote users Workflow Scanning uses HTTPS between the TOE and the Workflow Repository file server.

**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.

**Data Clearing and Purging**

The Image Overwrite Security 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.

# 7. Assumptions & Clarification of Scope

## 7.1. Assumptions

The scope of this evaluation was limited to the functionality and assurances covered in the PP 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.

## 7.2. 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 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.
- Apart from the Admin Guides listed in Section 8, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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 PP and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation. Specifically, the following functions are not covered by the evaluation should not be enabled/used in the product to remain in the evaluated configuration:
    - Reprint from Saved Job
    - SMart eSolutions
    - Custom Services (Extensible Interface Platform or EIP)
    - Network Accounting and Auxiliary Access
    - Internet Fax
    - Embedded Fax mailboxes
    - Wi-Fi Direct Printing
    - Weblet Services
    - InBox Apps
    - Remote Control Panel
    - SFTP when used for scanning
    - SNMPv3
    - Scan to USB
    - Print from USB
    - SMB Filing
    - Convenience Authentication
    - Xerox Workplace Cloud
    - Proximity Card Authentication

# 8. Documentation

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

- *Secure Installation and Operation of your Xerox® EC8036/EC8056 Color Multifunction Printer, v1.3*
- *Xerox® EC8036/EC8056 Color Multifunction Printer System Administrator Guide, v1.0*
- *Xerox® AltaLink® EC8036/EC8056 Series Multifunction Printer Multifunction Printer User Guide, v1.0*
- *Xerox® AltaLink® Series Smart Card Installation and Configuration Guide, v3.0*

All documentation delivered with the product is relevant to and within the scope of the TOE. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

# 9. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Xerox® AltaLink™ EC8036 & EC8056 HCD 1.0 Detailed Test Report, Version 1.1, May 2022 (DTR), as summarized in the evaluation Assurance Activity Report.

## 9.1. Evaluation team independent testing

The evaluation team conducted independent testing at Lightship Security USA lab in Austin, Texas. The evaluation team configured the TOE according to vendor installation instructions and 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 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. Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

## 9.3. Evaluated Configuration

The evaluated configuration includes the Xerox MFP –Xerox AltaLink™ EC8036/EC8056 running system software version: 103.023.031.35105.

The TOE Test Setup is depicted in Figure 1 and the testing environment components are identified in Table 5 and Table 6 below. The Secure Installation and Operation of your Xerox® EC8036/EC8056 Color Multifunction Printer [SIG] was used to setup and configure the evaluated configuration.

**Figure 1: Test Setup**

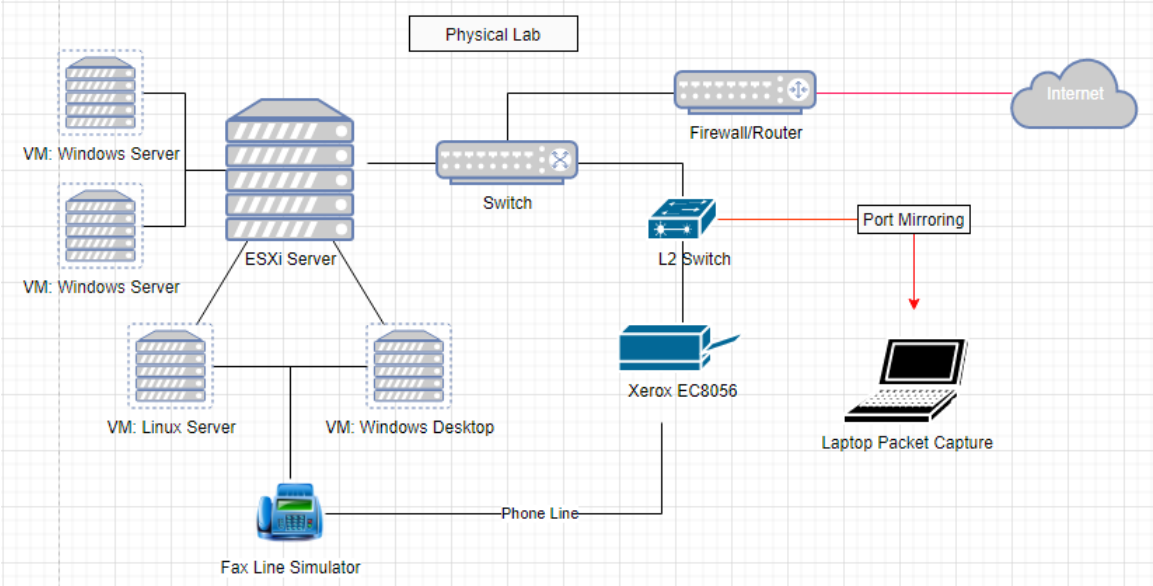


**Table 5: Devices in the Testing Environment**

| Device Name | OS Version | Tools |
|---|---|---|
| Windows Server 1 (VM) | Windows Server 2019 Standard Edition | Active Directory, Scan to Mailbox Server, Print Server, Window DNS Server, Wireshark. |
| Windows Server 2 (VM) | Windows Server 2019 Standard Edition | Active Directory, Scan to Mailbox Server, Print Server, Window DNS Server, Wireshark. |
| Linux Server (VM) | Linux 4.9.0-13-amd64 Debian 4.9.228-1 | NTP, Audit Server, FTP Server, TLS Server, TLS Client, IPsec Endpoint, SSH Client, SSH Server, SMTP, Wireshark. |
| Windows Desktop VM | Windows 10 | TOE Print Drivers, Fax |
| ESXi Server | ESXi-6.7.0 Update 3 (Build 14320388) | N/A |
| Laptop | Windows 10 Pro | Wireshark |
| Fax Line Simulator | Viking Model DLE-300 | N/A |
| Xerox EC8056 | 103.023.031.35105 | N/A |

**Table 6: Tools Used for Testing**

| Tool | Version | Tool Location | Tool Purpose |
|---|---|---|---|
| GreenLight | 3.0.31 | Linux Server (VM) | FCS_TLS_EXT.1 and FCS_SSH_EXT.1 testing |
| IPSec | strongSwan U5.5.1/K4.9.0-13-amd64 | Linux Server (VM) | FCS_IPSEC_EXT.1 testing |
| Ping | N/A | Linux Server (VM) | FCS_IPSEC_EXT.1 testing |
| sshd-ls | OpenSSH_7.1p2-Lightship | Linux Server (VM) | FCS_SSH_EXT.1 testing |
| SNMP | V3 | Linux Server (VM) | FAU_STG.4 testing |
| SMTP | Postfix v3.5.6 | Linux Server (VM) | FCS_TLS_EXT.1 testing |
| SNMP | Net-SNMP | Linux Server (VM) | FAU_STG.4 testing |
| LPR | Part of Windows 10 | Windows Desktop (VM) | FDP_ACF.1 testing |
| Xerox Drivers | Version 7.132.19.0 | Windows Desktop (VM) | FDP_ACF.1 and FTP_TRP.1(b) |
| Wireshark | Version 3.2.6 | Linux Server (VM) | Packet captures throughout testing |
| DNSmasq | Version 2.76 | Linux Server (VM) | DNS services |
| Active Directory | objectVersion 88 | Windows Server (VM) | FTP_ITC.1 testing |
| Cerberus | Version 9.0.5.3 | Windows Server (VM) | FCS_SSH_EXT.1 testing |
| Postfix | Version 3.5.6 | Linux Server (VM) | FAU_STG.4 testing |
| Tera Term | Version 4.105 | Laptop | FDP_DSK_EXT.1 and FDP_FXS_EXT.1 |
| OpenSSL | Version 1.0.2g-LS (tls, ssh) | Linux Server (VM) | FCS_TLS_EXT.1 testing |

| | | | |
|---|---|---|---|
| OpenSSH | Version 7.1p2-Lightship | Linux Server (VM) | FCS_SSH_EXT.1 testing |
| Syslog-ng | Version 3.28.1 | Linux Server (VM) | Remote audit services |

# 10. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the TOE to be Part 2 extended, and to meet the SARs contained in the PP.

## 10.1. Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Xerox® AltaLink™ EC8036 & EC8056 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 10.2. Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the PP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 10.3. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE.

Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 10.4. Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 10.5. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the PP and recorded the results in a Test Report, summarized in the Assurance Activities Report (AAR).

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 10.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The evaluation team performed a search of publicly available information to identify potential vulnerabilities in the TOE using guidelines from Labgram #116/Valgram #135.

The public sources searched included:

- Xerox Security Information, Bulletins and Advisory Responses: https://security.business.xerox.com/
- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html
- Wind River CVE Database: https://support2.windriver.com/index.php?page=cve

The evaluator used the following search terms:

- Xerox AltaLink
- Xerox
- Printer
- Multi-Function Printer
- IPsec
- TLSv1.2
- OpenSSL 1.0.2r
- SSH
- SFTP
- Libssh2 v1.7.0
- Wind River Linux
- Mocana

The vulnerability search was performed on 4/6/2022 with a follow-up search completed on 5/23/2022. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 10.7. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

# 11. Validator Comments

All validator comments addressed in the Section 7 Assumptions and Clarification of Scope.

# 12. Annexes

*None*

# 13. Security Target

Xerox® AltaLink™ EC8036 & EC8056 Security Target, Version 1.4, June 2022.

# 14. 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.

# 15. Acronym List

| | |
|---|---|
| AAR | Assurance Activities Report |
| 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 |
| LS | Lightship Security USA CCTL |
| DHCP | Dynamic Host Configuration Protocol |
| DTR | Detailed Test Report |
| ETR | Evaluation Technical Report |
| HCD | Hardcopy Device |
| 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 |
| PP | Protection Profile |
| ST | Security Target |
| TOE | Target of Evaluation |

| | |
|---|---|
| VR | Validation Report |

# 16. Bibliography

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
5. Protection Profile for Hardcopy Devices, Version 1.0
6. Protection Profile for Hardcopy Devices, Version 1.0, Errata #1
7. Xerox® AltaLink™ EC8036 & EC8056 Security Target, v1.4, June 2022
8. Secure Installation and Operation of your Xerox® EC8036/EC8056 Color Multifunction Printer v1.3, June 2022
9. Xerox® EC8036/EC8056 Color Multifunction Printer System Administrator Guide v1.0, July 2021
10. Xerox® EC8036/EC8056 Color Multifunction Printer User Guide v1.0, July 2021
11. Xerox® AltaLink® Series Smart Card Installation and Configuration Guide, v3.0, December 2020
12. Xerox AltaLink Printers Key Management Description, version 1.5, December 2021
13. Xerox® AltaLink™ EC8036 and EC 8056 EAR, v1.1 March 2022