Xerox® VersaLink® C7000 Color Printer & VersaLink® C7020/25/30 Multifunction Color Printer

Information Assurance Disclosure and

Statement of Volatility

Version 2.0

Document Version: 2.0 (January 2017).

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Contents

1. Introduction

1.1 Purpose

The purpose of this document is to disclose information for the Xerox ® C7000/20/25/30 product (hereinafter called as “the product” or “the system”) with respect to device security. Device Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a network environment, and how the product may be accessed both locally and remotely. The purpose of this document is to inform Xerox customers of the design, functions, and features of the product with respect to Information Assurance. This document does not provide tutorial level information about security, connectivity, or the product’s features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

1.2 Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

1.3 Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox has been advised of the possibility of such damages.

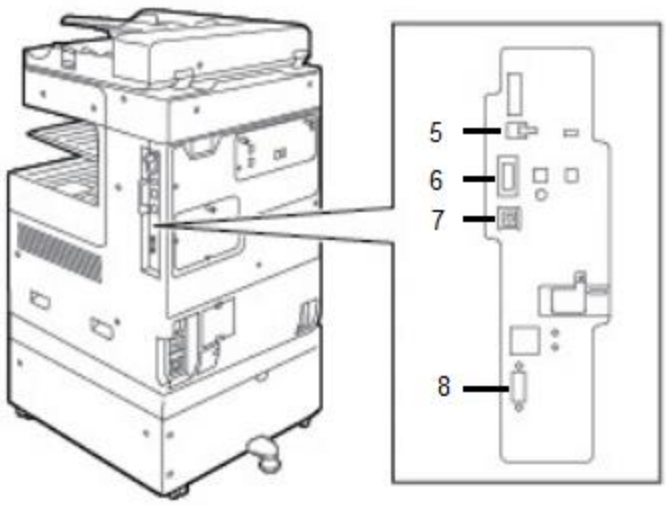
2. Device Description

2.1 Major Components

The product provides the copy and network printer functions and features, and consists of a controller module and marking engine.

Configuration	Marking Engine	Controller
MFP	Included	Included
SFP	Included	Included

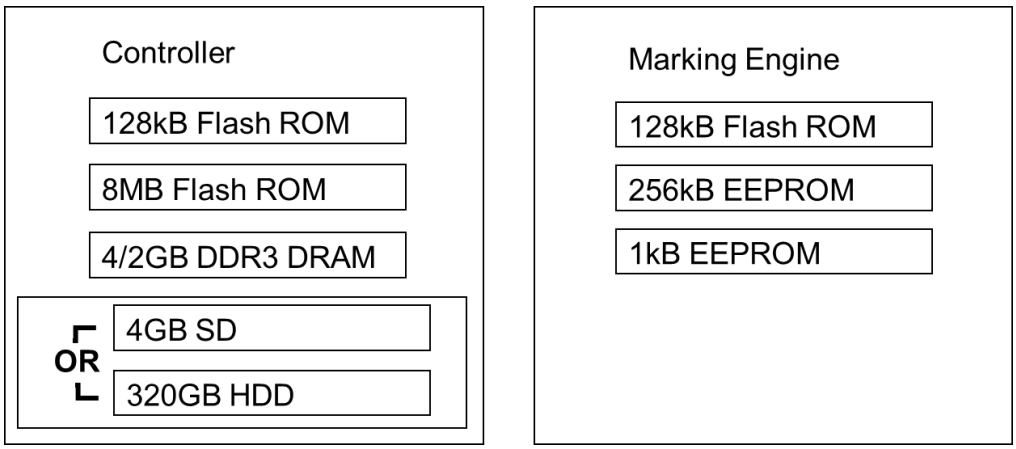
Table 1 Major Elements of the product.



1. Document Feeder.
2. Touch screen user interface.
3. Document output tray.
4. Paper feed tray.
5. USB3.0 (A).
6. Optional Wi-Fi dongle connection.
7. RJ45 Ethernet connection.
8. Service serial debug.

2.2 Volatile and Nonvolatile Memory

This section describes details of the memory devices that are contained within the product. The memory devices are shown below:



This 4GB or 320GB disk reserves approximately 600MB for the device firmware.

The rest of the 4GB or 320GB disk contains executables, fonts, and settings files. During normal operation, job files do not remain stored on this partition. One exception is “Print From” “Saved Jobs” feature. Customer jobs saved on the machine’s hard disk using this feature must be manually deleted by the customer. If On Demand Overwrite and full is selected all saved jobs will be erased.

The device stores images in a proprietary encoded format in non-contiguous blocks. Customer image data is only stored to the partition if EPC memory is full. User data and image data may be completely erased with a full Overwrite using a three-pass algorithm which conforms to U.S. Department of NIST Special Publication 800-88 Rev1, and the entire partition is erased and checked.

2.2.1 Marking Engine

The marking engine has its own control processor running VxWorks 6.8.2. The marking engine is only accessible to the Controller via inter-chip communication with no other access.

MARKING ENGINE MEMORY – NON-VOLATILE

Size	Type	Use	User Data	How to Clear	Volatile
128kB	Flash ROM	Marking Alignment	No	N/A	No
256kB	EEPROM	Marking Engine OS	No	N/A	No
1kB	EEPROM	Marking Alignment	No	N/A	No

2.2.2 Controller

The controller has its own control processor running Wind River Linux 6.0.

CONTROLLER MEMORY – VOLATILE

Size	Type	Use	User Data	How to Clear	Volatile
2/4GB	DDR3 DRAM	Controller Memory	Yes	Power Cycle	Yes

CONTROLLER MEMORY – NONVOLATILE

Size	Type	Use	User Data	How to Clear	Volatile
128kB	Flash ROM	Controller Boot	No	N/A	No
8MB	Flash ROM	Controller OS	No	N/A	No
4GB	SD	Temporary Memory	Yes	N/A	No

320GB	HDD	Temporary Memory	Yes	Image Overwrite	No

2.3 Updating Device Firmware

The programs stored in the Flash ROM listed below can be updated from external sources.

- Controller
- Marking Engine

This updating function can be disabled by a system administrator from the local UI or remotely. However, the only operation that can be disabled remotely is remote downloading. The file contains an electronic signature (using public key cryptosystem) which can be used to detect whether the file has been tampered with, to identify whether the firmware file is legitimate.

2.3.1 Local Firmware Update

Xerox service technicians can update device firmware using a USB port and specially configured USB thumb drive. This ability can be restricted by enabling the Customer Service Engineer Restriction feature which will require entry of a unique, customer set password prior to the update.

2.3.2 Network Firmware Update

Device system administrators can update device firmware using the Embedded Web Server.

2.3.3 Remote Services Firmware Update

Xerox Remote Services can update device firmware securely over the internet using HTTPS. This feature can be disabled, scheduled and does include optional email alerts for system administrators. This feature is configured through the Embedded Web Server.

2.3.4 Update File Security

Update files can only be installed with administrative or service permissions. Update files are encrypted and signed by Xerox. Update files that fail validation of signature and content are not installed on the device. When an update is not successful the firmware in use before the update is restored to service.

2.4 Backup & Restore

Certain system settings can be captured in a ‘clone’ file that may be applied to other systems that are the same model. Clone files are encoded but not encrypted and have the potential to contain sensitive information depending on which device feature setting is selected. Access to both create and apply a clone file can be restricted using role based access controls. Clone files can only be created and applied through the Embedded Web Server.

2.5 CSE Access Restriction

Enabling this feature through the embedded web server allows the customer to enter an additional password independent of the Admin account password that must be entered to allow service of the device. This password is not accessible to Xerox support and cannot be reset by Xerox service personnel.

2.6 Feeders and Finishers

The optional feeders and finishers available to this system do not include management or storage of any user data.

3. System Access

3.1 Physical Access

There are a variety of methods to physically access the product.

3.1.1 User Interface

From the UI, a user can:

- Access to setup menus of Common, Copy, Print, Mail, Network, Fax, Mailbox, etc.
- Change the device configuration settings.

3.1.2 10/100/1000 MB Ethernet RJ-45 Network Connector

This is the standard network connector, and allows access to the connectivity stacks and open ports described in the next section. This connector conforms to IEEE Ethernet 802.3 standards.

3.1.3 Optional Wireless Network Connector

The optional wireless network connector supports the following encryption options:

Encryption	Authentication Options
No Encryption	
WEP	
WPA2 Personal	
WPA2 Enterprise	PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/CHAP EAP-TTLS/MS-CHAPv2
Mixed Mode Personal (AES/TKIP)	
Mixed Mode Enterprise (AES/TKIP)	PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/CHAP EAP-TTLS/MS-CHAPv2

3.1.4 USB Port

USB3.0 (TYPE B) PORT

The USB3.0 port is the USB target connector used for maintenance and printing. To print, a file can be printed via direct connection. Received data is processed by the image processing software installed in the product. This port is located on the back of the system.

OPTIONAL USB3.0 (TYPE A) PORT(S)

The USB3.0 port on the front of the system is used for walk up printing operations. This port requires a FAT-32 formatted USB device. Some system configurations may not include this USB port. This port can be used by service technicians to update system firmware. This port can also be used as a target location for Scan to USB on systems equipped with a scanner.

USB ports on this device can be disabled completely by a system administrator.

Features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls.

3.1.5 Maintenance (Debug Serial)

This port is used for maintenance and connects to a Xerox unique tool. This port is covered and not available to customers. This port can be disabled by a system administrator enabling the Service Technician Restricted Operation. The port enables access to system diagnostic routines and configuration data. The port does not grant access to customer data outside of system configuration.

3.1.6 RJ-11 Analog Fax and Telephone

The fax connection supports the Fax Modem T.30 protocol only and will not accept data or voice communication attempts. An external (EXT) is available to connect an external handset. In this configuration the FAX card acts as a passive relay.

3.1.7 Foreign Device Interface

This port is used to connect optional equipment to control access to the machine. A typical application is a coin-operated device where a user must deposit money to enable the machine to print. The information available via the Foreign Device Interface is limited to optically-isolated pulses that can be used to count impressions marked on hardcopy sheets.

3.2 Logical Access

3.2.1 Network Protocols

Protocol specifications are implemented based on standard specifications such as RFC issued by IETF.

Protocols
DHCP
DHCPv6
DNS
HTTP

HTTPS
IPP
ISAKMP
Kerberos
LDAP
LDAPS
LPR
mDNS
Netbios
SLP
SMB
SMTP
SMTPS
SNMP
SOAP
SSDP
WSD Print
WSD Scan
WS-Discovery

3.2.2 Near Field Communications

The system supports an installable RFID reader for authentication and convenience in certain configurations. This RFID reader is connected to the system via USB on the front of the device. This communication cannot write or change any settings on the system. The data exchanged is not encrypted and may include information including system network status, IP address and device location. NFC functionality can be disabled using the embedded web server of the device. NFC functionality requires a software plugin that can be obtained from Xerox sales and support. NFC functionality is supported via optional touch screen user interface or optional dedicated NFC USB dongle.

Information shared over NFC is:

- IPv4 Address
- IPv6 Address
- MAC Address
- UUID (a unique identifier on the NFC client)
- Fully qualified domain name

3.2.3 Wi-Fi Direct

The system supports an Wi-Fi Alliance certified implementation of Wi-Fi direct to enable walk up and direct connections to the device. Wi-Fi Direct uses WPA2 encryption with a minimum passphrase of eight characters required. Wi-Fi Direct does offer DHCP addresses in the 192.168.0.0 subnet when placed in 'Group Owner' mode.

3.2.4 Network Ports

A number of TCP/IP and UDP/IP ports exist. The following table summarizes all ports that can be opened:

Port#	Type	Service Name
25	TCP	SMTP
53	TCP/UDP	DNS (Client)
68	UDP	BOOTP/DHCP (Client)
80	TCP	HTTP (Web User Interface)
80	TCP	HTTP (UPnP Discovery)
80	TCP	HTTP (WSD)
80	TCP	HTTP (WebDAV)
80	TCP	HTTP (IPP)
88	UDP	Kerberos (Client)
110	TCP	POP3 (Client)
123	UDP	SNTP (Client)
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
162	UDP	SNMP (Trap)
389	TCP	LDAP (Client)
427	TCP/UDP	SLP
443	TCP	HTTPS (Web User Interface)
443	TCP	HTTPS (IPP)
443	TCP	HTTPS (WebDAV)

443	TCP	HTTPS (Authentication Agent)
445	TCP	Direct Hosting
465	TCP	SMTPS (Client)
500	UDP	ISAKMP
515	TCP	LPR
547	UDP	DHCPv6 (Client)
631	TCP	IPP
636	TCP	LDAPS (Client)
995	TCP	POPS (Client)
1900	UDP	SSDP
3702	TCP	WSD (Discovery)
5353	UDP	mDNS
9100	TCP	Raw IP
15000	TCP	Loopback port for SMTP

(Client): The port number is not for the port on the controller side, but for the port of the connecting destination. Unless the port number for the controller side is specified, the port number for the controller side is unknown. Also, the port is not open on the controller all of the time but will open only at time of accessing the remote server.

3.3 User Authentication

The product provides a number of authentication methods for different types of users.

The definition of each method is as follows.

- **Simple:** Easy login - passwords are not required. Pick User Names from the list.
- **Local:** Basic security - passwords required. Pick User Names from the list or type in User Names.
- **Network:** Basic security with authentication handled by a remote server.
- **Convenience:** Swipe or tap your access card to log in. Requires optional card reader hardware and software plugin. Authentication is handled by a remote server.
- **Smart Card:** Two-factor security - Smart Card plus User Name/Password combination. Requires optional card reader hardware and software plugin. Authentication is handled by a remote server. Supported remote authentication methods include Kerberos, SMB and LDAP.

System administrators can assign permissions to individual users or create roles that users can assume. The authentication model allows for both local and network authentication and authorization. In the local and network cases, authentication and authorization take place as separate processes: a user must be authenticated before being authorized to use the services of the device.

If the device is set for local authentication, user account information will be kept in a local accounts database and the authentication process will take place locally. The system administrator can assign authorization privileges on a per user basis. User access to services will be provided based on the privileges set for each user in the local accounts database.

When the device is set for network authentication, the user's network credentials will be used to authenticate the user at the network domain controller. Users can be authorized on an individual basis to access one or any combination of the available services. Authentication can also be achieved via CAC, SIPR, smart access cards.

User Roles are stored in the local account database and users are either directly assigned to the roles in the database, or the role is associated with an LDAP/SMB group. Once the device determines what group the user is a member of, it determines what roles in the local database are associated with that group and define access based on the roles.

Use of the local accounts database or a network database can be set independently for both authentication and authorization. It is possible to enable network authentication and local authorization, or vice versa.

3.4 User Permissions Role Based Access Control (RBAC)

User Permissions provides permissions based on the authentication of the user through either the Local UI or network authentication. Commonly referred to as Role Based Access Control it assigns each user the permissions to use the device based on a default role, a customized role or a Non-Logged-In User role.

3.5 Device Authentication Method

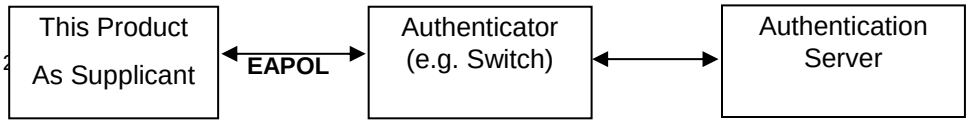
The product provides the device authentication feature that is required for network connection to LAN port or Wireless network where access is controlled.

The following device authentication method is provided:

Device Authentication Method	Operation
802.1x	Wired/Wireless 802.1X authentication is supported. When the product is activated using the User ID and password set for the product, authentication to the switch device starts in order to connect to the LAN port or Wireless network.

3.5.1 802.1x Authentication

In 802.1X authentication, when the product is connected to the LAN port of Authenticator such as the switch as shown below, the Authentication server authenticates the product, and the Authenticator controls access of the LAN port according to the authentication result. The product starts authentication processing at startup when the startup settings for 802.1X authentication are enabled.



Of the authentication methods in 802.1X Authentication, the product supports the following:

802.1x Authentication Method	Operation
MD5	Performs authentication using the ID information in plain text and MD5 hashed password.
MS-CHAPv2	Performs authentication using the ID information in plain text and MD5 hashed password that is encrypted using a key generated from random numbers.
PEAP/MS-CHAPv2	Performs authentication in the encrypted channel established between the product and the Authentication server, using the following information: • ID information in plain text. • Password encrypted in MN-CHAPv2 method.
EAP-TLS	Performs authentication in the encrypted channel established between the product and the authentication server, using the client certificate of the product. ID information and password are not used.

4. Data Flow

4.1 Print Service

4.1.1 Direct Print

Direct print is to print by outputting data to the printer without using the temporary memory

after decomposition of the received PDL.

<Condition>

This is a mode used at printing a single copy, or at printing multiple sets of copies without collating.

<Operation>

1. Stores the received PDL in the spool area. *
2. Reads out the PDL stored in the spool area.
3. Decomposes the read-out PDL per page, and writes in the page buffer (DRAM).
4. Compresses the image per page, and outputs the compressed image for the page read out from the DRAM to the printer through decompression when compression for one page is completed.
5. Deletes the received PDL data when printing of all data is completed. * *

* In non-spool mode, PDL is not spooled and the ring buffer is overwritten.
* * In spool mode only.

4.1.2 EPC Print

EPC print is to print by outputting data to the printer using the temporary memory after decomposition of the received PDL.

<Operation>

STEP1

1. Stores the received PDL in the spool area. *
2. Reads out the PDL stored in the spool area.
3. Decomposes the read-out PDL per page, and writes in the page buffer (DRAM).
4. Compresses the page buffer per page and transfers to the DRAM.
5. Reads out the compressed data from the DRAM, then transfers and stores it in temporary memory.
6. Deletes the information in the page buffer after page image is transferred to the temporary memory.

   * In non-spool mode, PDL is not spooled and the ring buffer is overwritten.

STEP2

7. Reads out the compressed image from the temporary memory and transfers to the DRAM.
8. Outputs the compressed image read out from the DRAM to the printer through decompression.

9. Deletes the received PDL data when printing of all data is completed.

PASSWORD IN SECURE PRINT

In the case of secure print, the user ID and password is included in the received PDL and stored in the temporary memory with the page image. When printing, the user ID and password input from the control panel are compared with that stored in the temporary memory. Printing is conducted only when the two matches. Deletes the user ID and password recorded in the temporary memory when printing for all data is completed. User can set the product to keep the user ID and password in the temporary memory even after printing is completed.

4.2 Fax Service

Please note that the Fax subsystem does not connect to the network subsystem in any way.

Fax configuration information can be cleared by performing a device reset to factory defaults using the local user interface. Please see the System Admin Guide for the details.

Fax image information can be cleared using Immediate Image Overwrite (IIO) or On Demand Image Overwrite (ODIO) as described in this document.

4.2.1 Storage of Scanned Image

This is to scan image from the scanner, execute image processing as required, and then store in the

HDD.

<Operation>

1. Stores the image data scanned by the scanner in the page memory.
2. Transfers the image data for one page read out from the page memory to the DRAM through compression. Deletes the content of the page memory after transferring of the image data is completed.
3. Stores the compressed data for one page read out from the DRAM to the temporary memory. Deletes the page image in the DRAM and Fax Card after storing the compressed data in the temporary memory.

Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.

4.2.2 Fax Send

In fax send, image data stored in the temporary memory is read out and output to the Fax Card.

<Operation>

1. Reads out the image data from the HDD and transfers to the DRAM
2. Transfers the source information generated in the CPU and the image data read out from the DRAM to the Fax Card.
3. Deletes the page image in the Fax Card every time a page of the document is sent.
4. Conducts the operations (1) to (3) for the number of times that equals to the number of pages scanned.
5. Deletes the document image in the temporary memory when all pages are sent completely.

4.2.3 Fax Receive

In fax receive, image data received by the Fax Card is stored in temporary memory.

<Operation>

1. Reads out the image data from the Fax Card and transfers directly to the DRAM.
2. Transfers the image data read out from the DRAM directly to the HDD.
   Deletes the page image in the DRAM after data is transferred to the HDD.

Conducts the operations (1) to (2) for the number of times that equals to the number of pages received.

4.2.4 Fax Print

In fax print, image data received by the Fax Card is read out from temporary memory. After decompression, image processing and compression of the data is performed, the image data is again stored in temporary memory. Then, the image data stored in temporary memory is output to the printer.

<Operation>

STEP1

1. Reads out the image data from temporary memory and transfers to the DRAM.
2. Decompresses the image data of DRAM and restores it in the DRAM.
3. Converts resolution, merges or divides the page, and/or rotates the image read out from the DRAM as required, then restores the data in the DRAM.
4. Compresses the image data read out from the DRAM and restores in the DRAM.
5. Stores the image data in the temporary memory. Deletes the page image in the DRAM and the image data in the Fax Card.

   Conducts the operations (1) to (5) for the number of times that equals to the number of pages stored.

STEP2

6. Reads out the compressed image from temporary memory and transfers to the DRAM.
7. Outputs the compressed image read out from the DRAM to the printer while performing decompression.
8. Deletes the page image in the DRAM and document image in temporary memory after all the pages are printed.

4.2.5 Direct Fax Service

In direct Fax service, the received PDL is decomposed and the compressed image is stored in temporary memory then parameters concerning send are output to the Fax Card.

<Operation>

STEP1

1. Stores the received PDL in the spool area (DRAM).
2. Reads out the PDL stored in the spool area.
3. Decomposes the read out PDL and writes in the page buffer (DRAM).
4. Compresses the page buffer by each page and transfers to the memory.

5. Reads out the compressed image data from the DRAM, then transfers and stores in temporary memory.
6. Deletes the received PDL information and page buffer information after transferring of the page image to temporary memory is completed.

STEP2

7. Please refer to ‘Fax Send” within this document.

5. Security Aspects of Selected Features

5.1 Data Encryption

By default any data to be written to the Controller **temporary memory (SSD/**eMMC/Hard Drive**)** is encrypted before writing. There is no way to disable this feature.

5.1.1 Algorithm

The algorithm used in the product is the 256-bit block encryption that conforms to the AES (Advanced Encryption Standard). The 256-bit encryption key is automatically created at start up and stored in the DRAM. The key is deleted by a power-off, due to the physical characteristics of the DRAM.

5.1.2 IPsec

IPSEC protocol specifications supported by device:

Item	Description
Supported IP Versions	IPv4 and IPv6 (available in both single and dual stack configurations)
Key exchange authentication method	IKE pre-shared key and IKE digital signature supported.
Transport mode	Only transport mode supported (tunnel mode not supported)
Security protocol	Only ESP supported (AH not supported)
ESP encryption methods	AES/3DES/DES
ESP authentication methods	SHA256/SHA384/SHA512/SHA1/MD5
IPComp	Not supported

5.2 Email Signing and Encryption

This system allows users to sign and encrypt email using S/MIME.

Supported S/MIME protocols are listed in the table below:

Supported Protocol	Description
S/MIME V3.2	Complies with RFC5750, 5751 Signature MIME type=multipart/signed Signature MIME type =application/pkcs7-mime, application/x-pkcs7-mime

S/MIME V3	Complies with RFC2632, 2633, 3369 Signature MIME type=multipart/signed Signature MIME type=application/pkcs7-mime, application/x-pkcs7-mime
S/MIME V2	Complies with RFC2311, 2312, 2315 Signature MIME type=multipart/signed Signature MIME type=application/pkcs7-mime, application/x-pkcs7-mime

Supported S/MIME algorithms are listed in the table below:

Supported Algorithm	Description
Digest method	SHA1 [Default] MD5 SHA256
Content encryption method	3DES; key length: 168 bits [default] RC2; key length: 40/64/128 bits selectable AES; key length: 128,192, 256 bits
Public key encryption method	RSA only; key length: 512 bits or longer 4096 bits or shorter.

5.3 FIPS140-2

FIPS140-2 are series of publications which are U.S. government security standards that specify requirements for cryptography modules.

The following operation modes can be selected:

Operation Mode	Description
FIPS140-2 approved mode	In this mode, the algorithms that are specified in FIPS and are recommended by NIST are used in accordance with the requirements for FIPS140-2.
FIPS140-2 non-approved mode	The algorithms that are specified in FIPS and/or are recommended by NIST, and other algorithms operate in this mode.

Although Kerberos, SMB, SNMPv3, and PDF Direct Print Service use encryption algorithms that are not approved by FIPS140-2, they can operate in FIPS140-2 approved Mode in order to maintain compatibility with conventional products after an exception is approved by a system administrator. They do not use FIPS compliant algorithms when in this configuration.

5.4 Image Overwrite

Image Overwrite provides both Immediate Image Overwrite (IIO) and On-Demand Image Overwrite (ODIO) functions. When IIO is enabled, immediately before a job is considered complete, IIO will overwrite any temporary files that have been created on the Hard Disk. The ODIO feature can be executed at any time. Scheduling of Image Overwrite can be done at the WebUI as well.

Please note that Solid State Drives such as eMMC or SSD do not support Image Overwrite.

5.4.1 Algorithm

The overwrite mechanism for both IIO and ODIO conforms to the NST Special Publication 800-88 Rev1. Once an ODIO has begun, it cannot be cancelled.

5.4.2 Overwrite Timing

ODIO takes a varying amount of time to complete depending on the amount of data that must be overwritten. IIO is performed as a background operation, with no user-perceivable reduction in print performance.

5.5 Xerox Diagnostic Data Collection

Xerox service personnel have access to a restricted web page hosted on the device. This information is only available via the Web User Interface. This web page requires a username and password for access. A diagnostic log file is generated when this page is accessed. The log file contains a limited amount of personally identifiable information from the device (host name, server names). Access to this restricted web page can be limited by setting IP or domain access restrictions on the device.

5.6 Security Audit Log

Events targeted for audit log are recorded to the NVRAM with timestamps. Up to 15,000 events can be stored in the temporary memory. When the number of events exceeds 15,000, audit log events will be deleted in order of timestamp, and then new events will be recorded. Access to audit log is possible only when the system administrator uses the Web User Interface and only after HTTPS communication has been enabled. Access from the control panel is not possible. Audit logs can be downloaded as tab-delimited text files.

5.7 Self-Test

The product can execute a Self-Test feature to verify the integrity of firmware and the validity of system configuration information. If any abnormal condition is found, the product halts and records the information in the audit log.

Self-test examines the both the signature of the firmware and the checksum of the firmware.

If the self-test fails during software update, the device will resume operation using the previous version.

If self-test fails at any time other than software update you must contact Xerox support to recover.

5.8 Remote Services Upload

The product can be configured to report system status to Xerox Corporation if connected to the internet either directly or by proxy. This feature can be disabled completely using the embedded web server. Customers can configure this feature to send email to a system administrator when this data is collected and sent to Xerox. The time for an upload can also be scheduled. Data is transferred over HTTPS using TLS1.1 or higher encryption. Changes and errors with Remote Services Upload are recorded in the system audit log. Proper operation of the Remote Services Upload rely on correct network and email configuration on the system. Data that is shared with Xerox includes device configuration, device usage, supply levels and faults in the system. No private data is transferred. The Audit log is not shared with Xerox.

5.9 IP Address Filtering

When enabled all traffic is prohibited regardless of interface (wired/wireless) unless enabled by IP filter rule. IPv4 and IPv6 are enabled separately. If IP Filter and IPsec are both enabled, IPsec is evaluated first. Up to 25 addresses can be enabled for IPv4 and an additional 25 for IPv6. Addresses include IP and subnet allowing individual system or subnets to be enabled. A system administrator can disable this feature using the embedded web server.

5.10 Domain Name Filtering

The system allows up to fifty domain names to be entered. All fifty will be used to either allow or deny access to the device. A system administrator can disable this feature using the embedded web server.

5.11 TPM Chip

The TPM is compliant with ISO/IEC 11889, the international standard for a secure cryptoprocessor, dedicated to secure cryptographic keys. The TPM is used to securely hold the product storage encryption key.

5.12 Legacy Protocol Restriction

Legacy protocols like TLS1.0, SMB, FTP can be enabled or disabled using the WebUI. Enabling certain features such as the VersaLink Plug-In feature may impact legacy protocol use.

5.13 Device Certificate Requirements

Only RSA keys are supported.

Length of public key of device certificate that can be imported is as follows:

512 / 1024 / 2048 / 4096

Supported signature algorithm is as follows:

SHA1 / SHA224 / 256 / 384 / 512

Maximum length of issuerDN of imported certificate (decoded) is 1023 character(UTF-8).

Certificates with issuerDNs or subjectDNs of lengths exceeding this size cannot be imported.

Bundle Device certificate + private key required format is PKCS#12

CA Certificate required format is PKCS#7 DER (.CER)

Upon private key / device certificate import, if old key and certificate exist and the new key and certificate are valid, and the key/certificate storage is in base storage, the old key and certificate are replaced (overwritten) by the new ones.

If key/certificate storage is on optional storage (SSD/HDD), the old key and certificate are not replaced leaving both certificates on the device until one is manually removed via the embedded web server.

6. Responses to Known Vulnerabilities

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see http://www.xerox.com/security.

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html