Xerox® Phaser 6510 Color Printer &
Xerox® WorkCentre 6515 Color Multifunction Printer

Information Assurance Disclosure and Statement of Volatility
Version 1.0

Table of Contents

February 2017

Section 1 Introduction

1.1   Purpose

The purpose of this document is to disclose information for the Xerox® *6510/6515* 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.

Section 2 Device Description

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

The following table lists the major elements of the product.

Configuration	Marking Engine	Controller
MFP	X	X
SFP	X	X

Table 1: Product Configuration Elements

X: Included
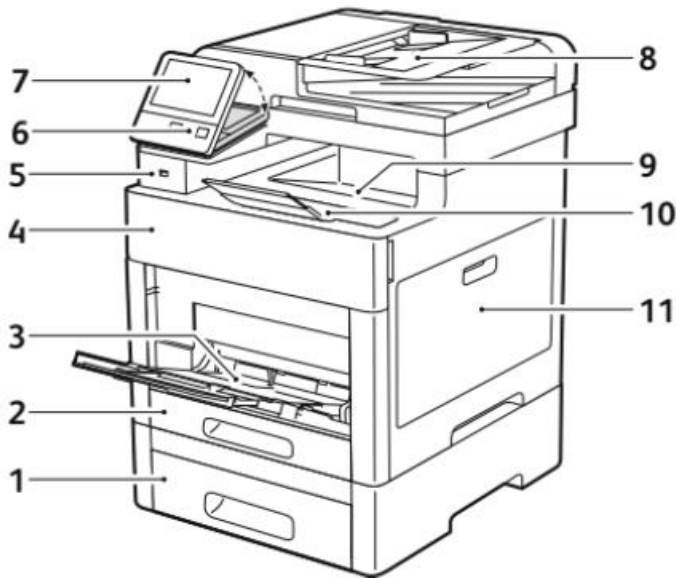
Figure 1: 6510/6515 (Front)
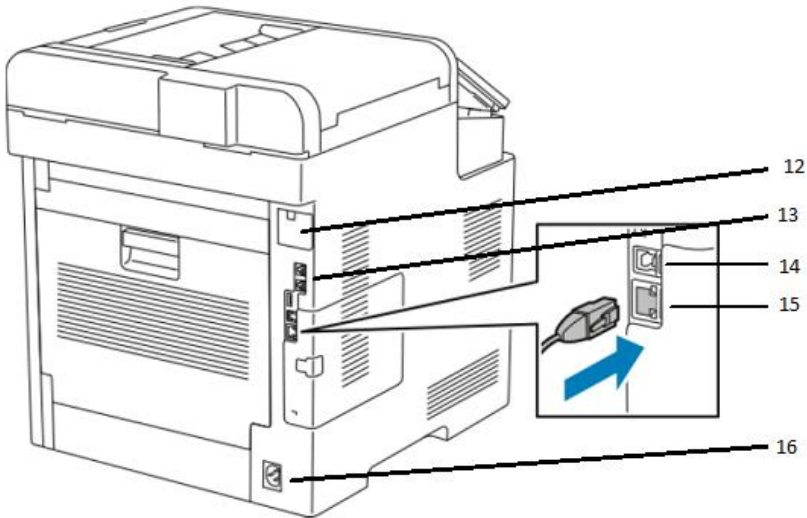
Figure 2: 6510/6515 (Back)

1. Lower Paper Tray
2. Upper Paper Tray
3. Special Paper Feed
4. Front Bezel
5. USB 3.0 (A)
6. Power Button and Optional NFC
7. Touch Screen User Interface
8. Document Feeder
9. Catch Tray
10. Catch Tray Extension
11. Side Panel
12. Optional Wireless Adapter Connector
13. RJ-11 Fax and Telephone Connector
14. USB 3.0 (B)
15. RJ-45 Ethernet Connector
16. AC Power

Please note that the Phaser 6510 SFP has no front USB connection (5), Document Feeder (8) and that the Touch Screen User Interface (7) is replaced with a 2 line LCD User Interface.

2.1   Connector Layouts

The connectors shown below are set on the back of the product.

WiFi Dongle
Mounting Portion

Ethernet
1000Base-TX

USB3.0
Device

Serial I/F for
Engineering
(Debug Serial)
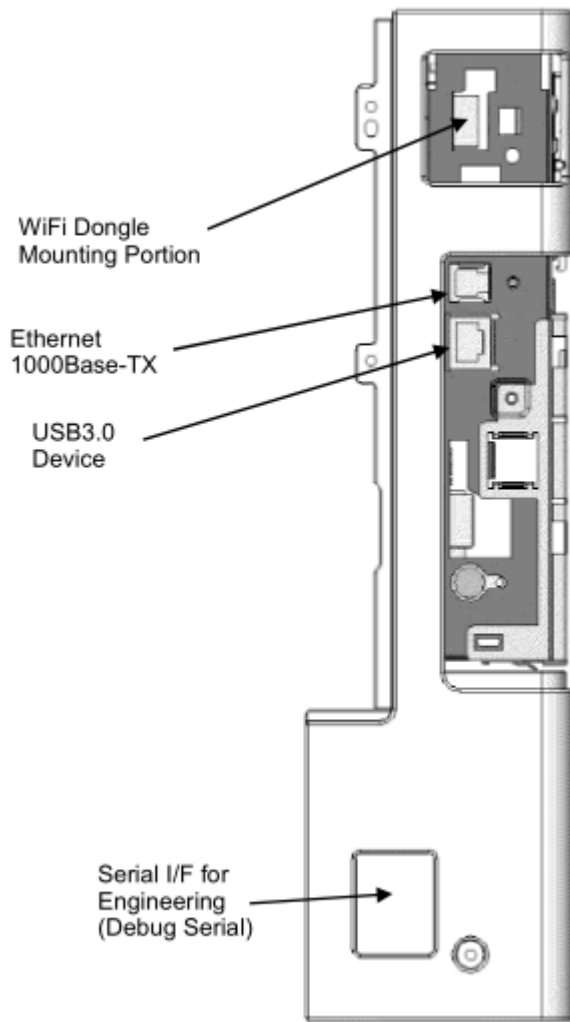
Figure 3:Back Panel Connectors

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:
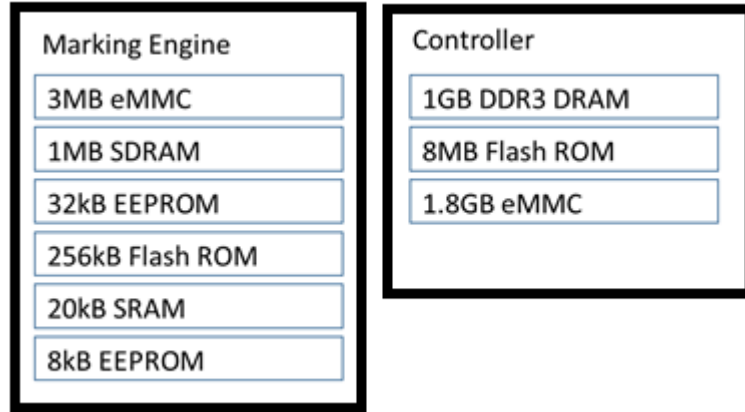
Figure 4: Memory Diagram

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.

2.2.1.1 Volatile Memory - Marking Engine

Size	Type	Use	User Data	How To Clear	Volatile
20kB	SRAM	Secondary Marking Engine Process	No	Power Off	Yes
1MB	SDRAM	Marking Engine Process RAM	No	Power Off	Yes

2.2.1.2 Non-Volatile Memory - Marking Engine

Size	Type	Use	User Data	How To Clear	Volatile
3MB	eMMc	Marking Engine Operating System	No	NA	No
32kB	EEPROM	Marking/Alignment Offset Values	No	NA	No
256kB	FLASH	Marking Engine Control Values	No	NA	No
8kB	EEPROM	Secondary User Marking/Alignment Offset	No	NA	No

Table 2: Marking Engine Memory Details

2.2.2   Controller

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

2.2.2.1 Volatile Memory - Controller

Size	Type	Use	User Data	How to Clear	Volatile
1GB	DDR3 DRAM	Controller Operating System, Swap space and Temporary Job Information	Yes	Power Off	Yes

2.2.2.2 Non-Volatile Memory - Controller

Size	Type	Use	User Data	How to Clear	Volatile
8MB	FLASH ROM	System Configuration Data	Yes	NA	No
1.8GB	eMMC	Spooled Documents in PDL format Spooled Document Metadata Job and Audit Logs Encrypted using an AES-256 algorithm	Yes	NA	No

Table 3: Controller Memory Details

2.3   Operating Systems

The Marking Engines for the product contains the VxWorks 6.8.2 operating system.

The Controller uses the Wind River Linux 6.0 real time operating system.

Neither of these operating systems are user accessible.

2.4   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.

2.5　Feeders and Finishers

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

Section 3 System Access

3.1 Physical Access

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

3.1.1 User Interface

The User Interface is the two line control panel on the front of the product.
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

Table 4: Wireless Details

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.

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.

3.2   Logical Access

3.2.1   Network Protocols

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

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, FQDN

UUID is a unique identifier on the NFC client (mobile device – phone or tablet, etc,)

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   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 -
67	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 added port)
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 the control of SMTP server

Table 5: Network Ports

"- 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 Methods

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.

3.4   Device Authentication Method

The product provides the device authentication feature that is required for network connection to LAN port / 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.

Table 6: Network Authentication of Device

3.4.1   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.
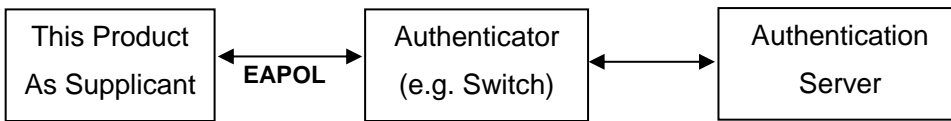
Figure 5: Network Authentication Diagram

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.

Table 7: 802.1X Authentication Methods

Section 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 (eMMC) 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.

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

(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 spool mode only.
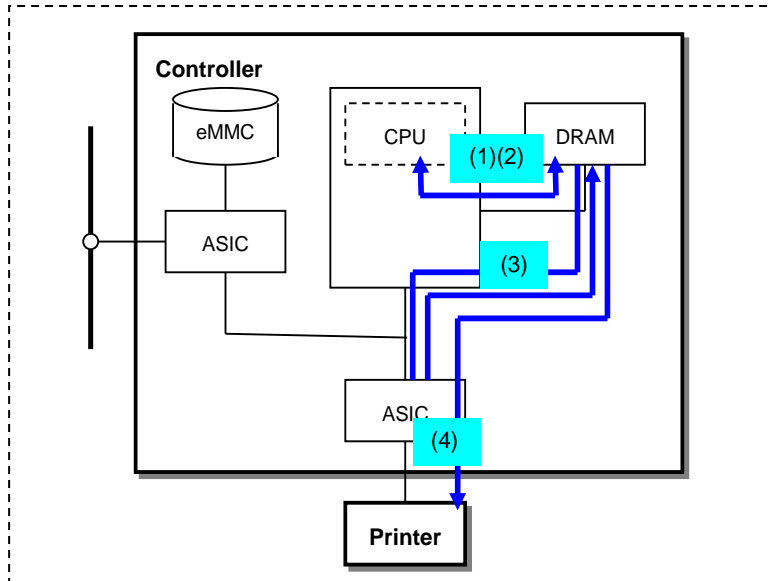
Figure 6: Data Flow of Direct Print

4.1.2   EPC Print

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

<Operation>

Step1

    (1) Stores the received PDL in the spool area (DRAM or eMMC).

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

    (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 the eMMC.

      Deletes the information in the page buffer after page image is transferred to the eMMC.

Step2

    (6) Reads out the compressed image from the eMMC and transfers to the DRAM.

    (7) Outputs the compressed image read out from the DRAM to the printer through decompression.

    (8) Deletes the received PDL data when printing of all data is completed.

* In spool mode only.

Password in Security Print

In the case of security print, the user ID and password is included in the received PDL and stored in the eMMC with the page image.

When printing, the user ID and password input from the control panel are compared with that stored in the eMMC. Printing is conducted only when the two matches.

Deletes the user ID and password recorded in the eMMC when printing for all data is completed.

* User can set the product to keep the user ID and password in the eMMC even after printing is completed.
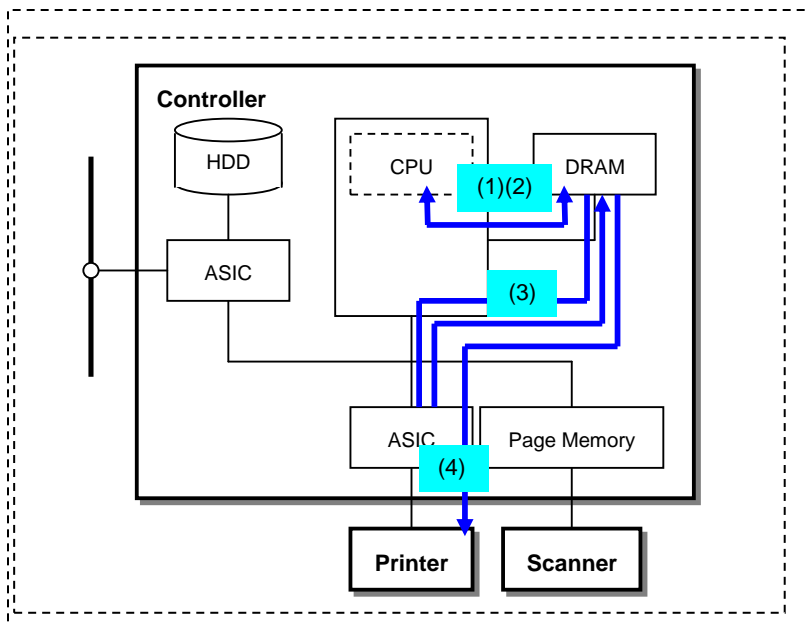
Figure 7: Data Flow of EPC Print

4.2

4.3   Fax Service

4.3.1   IP Fax (SIP) Receive

In IP Fax Receive, the received image data is stored in the eMMC after compression is performed.

<Operation>
   (1) Reads out the image data (JBIG/MH/MR/MMR) received via the Ethernet and stores it in the DRAM.
   (2) Reads out the image data from the DRAM, decompresses the data at the CPU, and stores it in the DRAM.
   (3) Reads out the uncompressed image data from the DRAM, performs JBIG compression at the CPU, and stores it in the eMMC.
   (4) Deletes all the page images in the DRAM after they are transferred to the eMMC.
Repeats the operations (1) to (4) for the number of times that equals to the number of pages stored.

* Operations of outputting the image data stored in the eMMC to the Printer is the same as described in section "4.1.2 EPC Print."
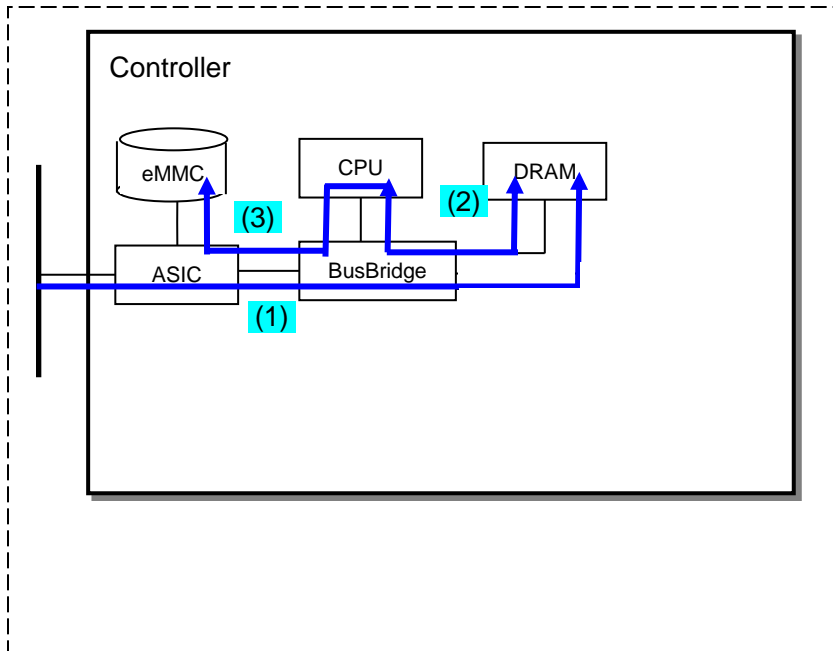
Figure 8: Data Flow of Fax Service

4.4   Report Service

4.4.1   Report Print

In report print, the compressed image data of Report is stored in the eMMC, then the image data is output to the printer after read out from the eMMC.

<Operation>

Step1

(1) Creates PDL to be reported from the system information (NVRAM) and stores in the DRAM.

(2) Reads out the PDL stored in the DRAM.

(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 in the eMMC.
    Deletes the page image in the DRAM after transferring of the data is completed.

Step2

(6) Reads out the compressed image from the eMMC and transfers to the DRAM.

(7) Outputs the compressed image read out from the DRAM to the printer through decompression.

Conducts the operations (6) to (7) for the number of times that equals to the number of pages stored in the eMMC.

(8) Deletes the document image in the eMMC and page image in the DRAM after printing is completed.
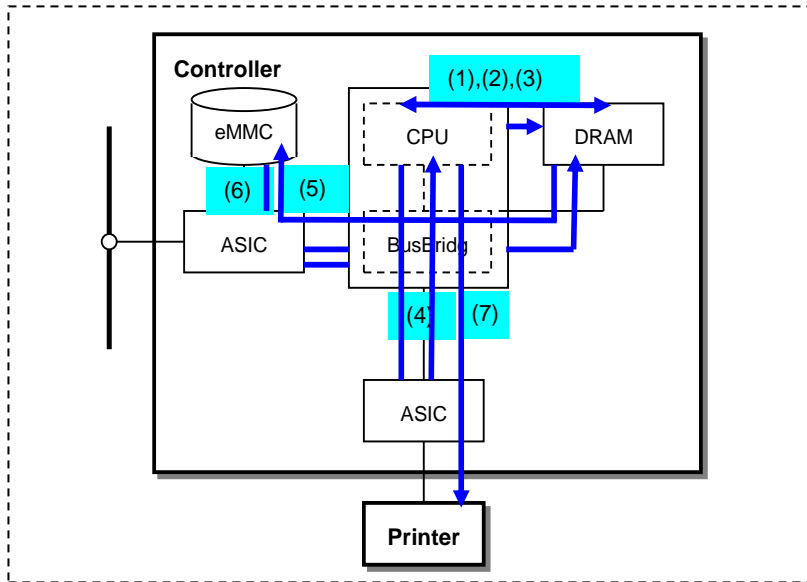
Figure 9: Data Flow of Report Printing

Section 5 Security Aspects of Selected Features

5.1   Data Encryption

By default any data to be written to the Controller eMMC 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.

5.2   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

Table 8: IPsec Implementation Details

5.3　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

Table 9: S/MIME Protocols

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.

Table 10: S/MIME Algorithms

5.4　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.

Table 11: Possible FIPS140-2 Modes

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.

5.5   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 eMMC. 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.

5.6   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.

5.7   Audit Log Entries

The following table lists the events that are recorded in the log where applicable:

ID	Category	User Name	Description	Status	Optional Information
0x0101	System Status	-	Started normally (cold boot)	-	
0x0101	System Status	-	Started normally (warm boot)	-	
0x0101	System Status	-	Started (NVM initialized)	-	
0x0101	System Status	-	Started (Hard Disk initialized)	-	
0x0101	System Status	-	Shutdown requested	-	
0x0101	System Status	-	Image Overwriting started	Successful Failed	Scheduled On Demand
0x0101	System Status	-	Image Overwriting finished	Successful Failed	
0x0101	System Status	-	Self-Test	Successful Failed	Checksum of Image1 ROM
0x0201	Login/Logout	CE Guest User Name -	Login	Successful Failed (Invalid User ID) Failed(Invalid Password) Failed	Local Web User Interface Hostname Authentication Method Role
0x0201	Login/Logout	CE Guest User Name -	Logout	Successful Failed	
0x0201	Login/Logout	-	Locked System Administrator Authentication	-	Countdown to Access Denied due to authentication failure
0x0201	Login/Logout	User Name -	Detected Continuous Authentication Fail	-	Web User Interface SNMPv3 - Number of failed attempts
0x0301	Audit Policy	CE Guest User Name -	Audit Log	Enabled	
0x0301	Audit Policy	CE Guest User Name -	Audit Log	Disabled	
0x0401	Job Status	User Name -	Print	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0401	Job Status	User Name -	Copy	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0401	Job Status	User Name -	Scan	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0401	Job Status	User Name -	Fax	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0401	Job Status	User Name -	Mailbox	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0401	Job Status	User Name -	Print Reports	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details

0x0401	Job Status	User Name -	Job Flow Service	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0401	Job Status	-	-	Completed Completed with Warnings Canceled by User Canceled by Shutdown Aborted Unknown	Job Details
0x0501	Device Settings	-	Adjust Time	Successful Failed	Previous Date and Time
0x0501	Device Settings	CE User Name -	Add User	-	User Name
0x0501	Device Settings	CE User Name -	Edit User	-	User Name (previous if User Name is changed) Attributes
0x0501	Device Settings	CE User Name -	Delete User	-	User Name
0x0501	Device Settings	CE User Name -	Create Mailbox	-	Host Name Box Number
0x0501	Device Settings	CE User Name -	Delete Mailbox	-	
0x0501	Device Settings	CE User Name -	Switch Authentication Mode	Successful	Local Remote Convenience Custom Off Previous Setting
0x0501	Device Settings	CE User Name -	Change Security Setting	Authentication Accounting Image Overwrite eMMC Encryption TLS S/MIME IPSEC SNMPv3 802.1x Certificate Verify Mode Maintainer Password SmartCard FIPS140-2 Self-Test Auto Clear Timer Service Rep. Restricted Operation Print Reports Button External Code Integrity Check Authorization NFC	
0x0501	Device Settings	CE User Name -	View Security Setting	Local Web User Interface	Host Name
0x0501	Device Settings	User Name -	Change Contract Type	Successful Failed Aborted	
0x0501	Device Settings	-	Change Geographic Region	-	
0x0501	Device Settings	-	Enter Activation Code	Successful	
0x0501	Device Settings	CE	Change Job Setting	Successful	Delay Print Private Print
0x0601	Device Data	-	Change Billing Impression Mode	Successful Failed	Mode Set to A3 Mode Mode Set to A4 Mode Billing Meter Values

0x0601	Device Data	CE User Name -	Import Certificate	Successful Failed	RootCA DeviceEE SSCEE Key Size IssuerDN Serial Number
0x0601	Device Data	-	Delete Certificate	-	
0x0601	Device Data	-	Add Address Entry	-	Host Name Registration Number
0x0601	Device Data	-	Delete Address Entry	-	
0x0601	Device Data	-	Edit Address Entry	-	
0x0601	Device Data	-	Import Address Book	-	Host Name
0x0601	Device Data	-	Export Address Book	-	
0x0601	Device Data	-	Clear Address Book	-	Host Name
0x0601	Device Data	-	Export Audit Log	-	
0x0601	Device Data	-	Install Custom Service	Failed	Host Name Custom Service Name
0x0601	Device Data	-	Install Embedded Plug-in	-	Host Name Plugin File Name
0x0601	Device Data	-	Export Cloning Data	Successful Failed	Apps Contacts Connectivity Permissions System
0x0601	Device Data	-	Import Cloning Data	-	
0x0701	Device Config	-	Important Parts	Replaced	
0x0701	Device Config	-	Hard Disk	Installed Removed Replaced	
0x0701	Device Config	-	Software	Updated	Rom Type New Version Previous Version
0x0801	Communication	-	Trusted Communication	Failed	Protocol Name

Table 12: Audit Log Entries

Please note that 'CE' refers to a 'Xerox Customer Service Engineer' performing service.

5.8   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.

Please contact Xerox support to recover from a failed self-test condition.

5.9   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.

5.10   IP Address Filtering

When enabled all traffic is prohibited regardless of interface (wired/wireless) unless enabled by IP filter rule.

IPv4 and IPv6 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.

5.11   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.

Section 6 Responses to Known Vulnerabilities

6.1   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