Version 1.0

Xerox® B1022/B1025
Multi-Function Printer
Contents

1.0 INTRODUCTION ........................................................................................................... 5
1.1 Purpose ....................................................................................................................... 5
1.2 Target Audience ......................................................................................................... 5
1.3 Disclaimer .................................................................................................................... 5

2.0 DEVICE DESCRIPTION .............................................................................................. 6
2.1 Security-relevant Subsystems ..................................................................................... 7
  2.1.1 Physical Partitioning ............................................................................................... 7
2.2 Controller .................................................................................................................... 8
  2.2.1 Purpose .................................................................................................................... 8
  2.2.2 Memory Components ............................................................................................. 9
  2.2.3 External Connections ............................................................................................ 12
2.3 Optional Fax Module (for the B1025 only) ................................................................. 15
  2.3.1 Purpose ................................................................................................................... 15
  2.3.2 Hardware ................................................................................................................. 15
2.4 Scanner ....................................................................................................................... 15
  2.4.1 Purpose ................................................................................................................... 15
  2.4.2 Hardware ................................................................................................................. 15
2.5 Graphical User Interface (GUI) ................................................................................... 15
  2.5.1 Purpose ................................................................................................................... 15
2.6 Marking Engine (Image Output Terminal or IOT) ......................................................... 16
  2.6.1 Purpose ................................................................................................................... 16
  2.6.2 Hardware ................................................................................................................. 16
2.7 System Software Structure ......................................................................................... 16
  2.7.1 Software Installation ............................................................................................. 16
  2.7.2 Verification Test ..................................................................................................... 16
  2.7.3 Operating System Layer in the Controller ............................................................. 16
  2.7.4 Software Verification Test ...................................................................................... 18
  2.7.5 Software Installation ............................................................................................. 18
  2.7.6 Network Protocols ............................................................................................... 19
2.8 Logical Access ............................................................................................................ 20
  2.8.1 Network Security .................................................................................................. 20
  2.8.2 Ports ....................................................................................................................... 22

Ver. 1.0 June 2018
3.0 System Access
3.1 Authentication Model
3.2 Login and Authentication Methods
3.3 Scan To
3.4 Device log on
3.5 Device User Database

4.0 Security aspects of Selected Features
4.1 SMart eSolutions
4.2 Encrypted Partitions
4.3 Email Signing and Encryption to Self
5.0 Security @ Xerox (www.xerox.com/security)

APPENDICES

Appendix A – Abbreviations
1.0 Introduction

This document describes the locations, capacities and contents of volatile and non-volatile memory devices within the Xerox® B1022 and Xerox® B1025.

1.1 Purpose

The purpose of this document is to disclose information for the Xerox® B1022 and Xerox® B1025 products 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 networked environment, and how the product may be accessed, both locally and remotely. Please note that the customer is responsible for the security of their network and the Xerox products do not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Xerox® B1022 and Xerox® B1025 products relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or Xerox® B1022 and Xerox® B1025 products features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics. However, a number of references are included in the Appendix. Additional information also available in the Xerox® B1022 and Xerox® B1025 System Administrator guide.

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 Corporation 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 Corporation has been advised of the possibility of such damages.
2.0 Device Description

This product consists of an input document handler and scanner, marking engine including paper path, controller, and user interface.

Figure 1 - Xerox® B1025 Multi-Function System
2.1 Security-relevant Subsystems

2.1.1 Physical Partitioning

The security-relevant subsystems of the product are partitioned as shown in

Figure 2 - B1022 System functional block diagram
2.2 Controller

2.2.1 Purpose

The controller provides both network and direct-connect external interfaces, and enables copy, print, email, network scan, and fax functionality. The controller also incorporates a web server that exports a Web User Interface (WebUI) through which users can submit jobs and check job and machine status, and through which system administrators can remotely administer the machine.

The controller contains the image path, which uses proprietary hardware and algorithms to process the scanned images into high-quality reproductions. Scanned images may be temporarily buffered in DRAM to enable electronic pre-collation. When producing multiple copies of a document, the scanned image is processed and buffered in the DRAM in a proprietary format. The buffered bitmaps are then read from DRAM and sent to the Image Output Terminal (IOT) for marking on hardcopy output. For long documents, the production of hardcopy may begin before the entire original is scanned, achieving a level of concurrency between the scan and mark operations.

The controller operating system is VxWorks 6.9. Unnecessary services such as rsh, telnet and finger are disabled in the Operating System. Ramona Supports Scan To Service (Scan to FTP/SMB/HTTP/HTTPS/SFTP).

The controller works with the Graphical User Interface (GUI) assembly to provide system configuration functions. A System Administrator can access these functions.
The controller software can be updated via USB or WebUI.

### 2.2.2 Memory Components

#### 2.2.2.1 Controller Module

**Program Memory**: B1022/B1025 model uses NAND Flash as a Program memory which stores System Program and can be upgraded through USB Device Interface.

Capacity: 128MB for B1022 and 512MB for B1025

#### 2.2.2.2 General Memory Information

##### 2.2.2.2.1 Volatile Memory

All volatile memory listed is cleared after power is removed (decay occurs generally within 20 seconds at room temperature).

All volatile memory listed is required for normal system operation and during service and diagnostic procedures.

Removal of any volatile memory will void the warranty.

##### 2.2.2.2.2 Non-Volatile Memory

All non-volatile memory listed is required for normal system operation and during service and diagnostic procedures.

Removal of any non-volatile memory will void the warranty.

Non-volatile memory in the system cannot be accessed by accidental keystrokes.

#### 2.2.2.3 Controller Module

**B1022 Volatile Memory**

<table>
<thead>
<tr>
<th>Type (SRAM, DRAM, etc.)</th>
<th>Size</th>
<th>User Modifiable (Y/N)</th>
<th>Function or Use</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDR3 SDRAM 1333MHz, 16bit</td>
<td>256MB</td>
<td>N</td>
<td>Executable code, Printer control data, temporary storage of job data</td>
<td>Power Off System</td>
</tr>
</tbody>
</table>

Additional Information:
B1022 uses DDR3 SDRAM for Swath Buffer in Printing, Scan Buffer in Scanning, System Working Memory Area.
### B1025 Volatile Memory

<table>
<thead>
<tr>
<th>Type (SRAM, DRAM, etc.)</th>
<th>Size</th>
<th>User Modifiable (Y/N)</th>
<th>Function or Use</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDR3 SDRAM 1333MHz , 16bit</td>
<td>1.5Gbbytes</td>
<td>N</td>
<td>Executable code, Printer control data, temporary storage of job data</td>
<td>Power Off System</td>
</tr>
</tbody>
</table>

Additional Information:
B1025 model uses DDR3 SDRAM for Swath Buffer in Printing, Scan Buffer in Scanning, System Working Memory Area

### B1022 Non-Volatile Memory

<table>
<thead>
<tr>
<th>Type (Flash, EEPROM, etc.)</th>
<th>Size</th>
<th>User Modifiable (Y/N)</th>
<th>Function or Use</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAND</td>
<td>128Mbytes</td>
<td>Via Diagnostics</td>
<td>Flash as a Program memory which stores System Program and can be upgraded through USB Device Interface.</td>
<td>NA</td>
</tr>
<tr>
<td>EEPROM</td>
<td>64Kbytes</td>
<td></td>
<td>Frequently used data, Network Settings, MAC Address, Serial Number etc is stored in EEPROM,</td>
<td></td>
</tr>
</tbody>
</table>

Additional Information:

### B1025 Non-Volatile Memory

<table>
<thead>
<tr>
<th>Type (Flash, EEPROM, etc.)</th>
<th>Size</th>
<th>User Modifiable (Y/N)</th>
<th>Function or Use</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD CARD</td>
<td>8Gbbytes</td>
<td>via Diagnostics</td>
<td>Control set points, configuration settings, Boot Memory</td>
<td>NA</td>
</tr>
<tr>
<td>NAND</td>
<td>512Mbytes</td>
<td>Via Diagnostics</td>
<td>Flash as a Program memory which stores System Program and can be upgraded through USB Device Interface.</td>
<td>NA</td>
</tr>
<tr>
<td>EEPROM</td>
<td>64Kbytes</td>
<td></td>
<td>Frequently used data, Network Settings, MAC Address, Serial Number etc is stored in EEPROM,</td>
<td></td>
</tr>
</tbody>
</table>

Additional Information:
Non-Volatile Hard Disk Memory

<table>
<thead>
<tr>
<th>Drive / Partition (System, Image):</th>
<th>Removable Y / N</th>
<th>Size:</th>
<th>User Modifiable: Y / N</th>
<th>Function:</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional Information: No hard disks on Xerox B1022/B1025 devices

RFID Devices

<table>
<thead>
<tr>
<th>RFID Device and location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>No RFID Devices are contained in the device</td>
</tr>
</tbody>
</table>

Media and Storage Descriptions

<table>
<thead>
<tr>
<th>Type (disk drives, tape drives, CF/SD/XD memory cards, etc.):</th>
<th>Removable Y / N</th>
<th>Size:</th>
<th>User Modifiable: Y / N</th>
<th>Function:</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Marking Engine Modules

Volatile Memory

<table>
<thead>
<tr>
<th>Type (SRAM, DRAM, etc.)</th>
<th>Size</th>
<th>User Modifiable (Y/N)</th>
<th>Function or Use</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAM (MCU PWBA)</td>
<td>32M x 16 bit</td>
<td>N</td>
<td>Temporary Storage of variables</td>
<td>Power Off System</td>
</tr>
<tr>
<td>RAM (UI PWBA)</td>
<td>1kbyte</td>
<td>N</td>
<td>Temporary Storage of variables</td>
<td>Power Off System</td>
</tr>
</tbody>
</table>

Non-Volatile Solid State Memory
Media and Storage

<table>
<thead>
<tr>
<th>Type (disk drives, tape drives, CF/SD/XD memory cards, etc.):</th>
<th>Removable: Y / N</th>
<th>Size:</th>
<th>User Modifiable: Y / N</th>
<th>Function:</th>
<th>Process to Clear:</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2.2.3 Feeder and Finisher Modules

No additional memory for feeder and finishing modules.

**Feeder Modules**

The standard tray along with the optional tray does not have memory.

**Finisher Modules**

NA

### 2.2.3 External Connections

The controller printed wiring boards are physically mounted in the device. An optional fax board may also be installed (for the B1025 only).

#### B1022 Rear View

![B1022 Rear View Diagram]

**Figure 4**

- 1. Power Receptacle
- 2. USB Port, B-Type
- 3. Ethernet Connection
- 4. USB Port, A-Type
B1025 Rear View

1. Power Receptacle
2. USB Port, B-Type
3. Ethernet Connection
4. USB Port, A-Type
5. Fax Line Connection, option

Figure 5

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description / Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Target Port</td>
<td>Diagnostics and service; Xerox Copier Assistant</td>
</tr>
<tr>
<td>Dual USB Host Ports</td>
<td>SW upgrade; USB Printing; Scan to USB</td>
</tr>
<tr>
<td>Ethernet Port</td>
<td>Network Connectivity</td>
</tr>
<tr>
<td>Optional FAX (Single or Dual)</td>
<td>Allows insertion of optional “Land Line” Fax card</td>
</tr>
</tbody>
</table>
2.2.3.1 USB Ports

The Xerox® B1022 and Xerox® B1025 contains a host connector for a USB flash drive, enabling upload of software upgrades and download of network logs or machine settings files and scan jobs. Autorun is disabled on this port. No executable files will be accepted by the port.

Modifying the software upgrade, network log or saved machine settings files will make the files unusable on the Xerox® B1022 and Xerox® B1025

<table>
<thead>
<tr>
<th>USB port and location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front panel – 1 Host port</td>
<td>User retrieves print ready files from Flash Media or stores scanned files on Flash Media. Physical security of this information is the responsibility of the user or operator. Upload of software upgrades, download of network logs, download and upload of machine settings for setup cloning.</td>
</tr>
<tr>
<td>Rear panel – 1 Host ports</td>
<td>User retrieves print ready files from Flash Media or stores scanned files on Flash Media. Physical security of this information is the responsibility of the user or operator. Upload of software upgrades, download of network logs, download and upload of machine settings for setup cloning.</td>
</tr>
<tr>
<td>Rear panel – 1 Target port</td>
<td>User PC direct connection for printing,</td>
</tr>
</tbody>
</table>
| Additional Information      | A number of devices can be connected to the 3 USB Host ports. Once information has been copied (either as a back-up data set or as a transfer medium, physical security of this information is the responsibility of the user or operator.)
2.3 Optional Fax Module (for the B1025 only)

2.3.1 Purpose
The embedded FAX service uses the installed embedded fax card to send and receive images over the telephone interface. The FAX card plugs into a custom interface slot on the controller.

2.3.2 Hardware
The Fax Card is a printed wiring board assembly containing a fax modem and the necessary telephone interface logic. It connects to the controller via a serial communications interface. The Fax Card is responsible for implementing the T.30 fax protocol. All remaining fax-specific features are implemented in software on the controller. The fax telephone lines are connected directly to the Fax Card via RJ-11 connectors.

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Purpose / Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODEM #1</td>
<td>NA</td>
<td>Optional Fax modem 2 ports</td>
</tr>
</tbody>
</table>

Fax Module components

2.4 Scanner

2.4.1 Purpose
The purpose of the scanner is to provide mechanical transport to convert hardcopy originals to electronic data.

2.4.2 Hardware
The scanner converts the image from hardcopy to electronic data. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images. All other image processing functions are in the copy controller.

2.5 Graphical User Interface (GUI)

2.5.1 Purpose
The GUI detects soft and hard button actuations, and provides text and graphical prompts to the user. The GUI is sometimes referred to as the Local UI (LUI) to distinguish it from the WebUI, which...
is exported by the web service that runs in the controller. Images are not transmitted to or stored in the GUI.

2.6 Marking Engine (Image Output Terminal or IOT)

2.6.1 Purpose
The Marking Engine performs copy/print paper feeding and transport, image marking and fusing, and document finishing. Images are not stored at any point in these subsystems.

2.6.2 Hardware
The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographics, and paper output and finishing. The marking engine contains a CPU, BIOS, RAM and Non-Volatile Memory.

2.7 System Software Structure

2.7.1 Software Installation
Software can be installed by the customer via 2 different methods, USB and CenterWare Web (Web UI). The most current release of software can be found on Xerox.com Software.

2.7.2 Verification Test
This test can be executed in CWIS. This test verifies the software integrity by confirming the installed software has not been modified.

2.7.3 Operating System Layer in the Controller
The OS layer includes the operating system, network and physical I/O drivers. The controller operating system is VxWorks 6.9 (UI 4.3 touch screen is O.S. Linux kernel v. 2.6.35 and Android version 2.3 which is known as Gingerbread).
IP Filtering is provided by the kernel.
<table>
<thead>
<tr>
<th>Open Source Software Module Name</th>
<th>Open Source Software Version</th>
<th>Type of the Open Source license</th>
<th>Obligation</th>
</tr>
</thead>
</table>
| uboot                            | 101                         | GPL v2                         | 1) Insert the full license text in the manual (or product)  
2) State use of the GPL software (software title, license) in the manual (or product).  
3) Provide a written offer that is valid for at least 3 years for provision of the GPL source code. |
| Linux Kernel                     | 2.6.35                      | GPL v2                         | 1) Insert the full license text in the manual (or product)  
2) State use of the GPL software (software title, license) in the manual (or product).  
3) Provide a written offer that is valid for at least 3 years for provision of the GPL source code. |
| iptables                         | 1.3.7                       | GPL v2                         | 1) Insert the full license text in the manual (or product)  
2) State use of the GPL software (software title, license) in the manual (or product).  
3) Provide a written offer that is valid for at least 3 years for provision of the GPL source code. |
| Android                          | Gingerbread                 | Apache 2.0                     | Insert the full license text in the manual (or product) |
| libxml                           | Not Available               | MIT                            | none |
| freetype                         | Not Available               | FreeType Project LICENSE       | acknowledge somewhere in your documentation that you have used the FreeType code |
| JPEG                             | 6b                          | Independent JPEG Group License| State the acknowledgment in the manual (or product): "This software is based in part on the work of the Independent JPEG Group." |
| Expat                            | 1.95.8                      | MIT                            | none |
| xpm                              | Not Available               | MIT                            | none |
| tiff                             | 3.8.0                       | TIFF License                   | none |
| png                              | 1.2.6                       | libpng license                 | none |
| zlib                             | 1.2.3                       | zlib license                   | none |
| mDNS                             | Not Available               | Apache 2.0                     | Insert the full license text in the manual (or product) |
| AUTH1X                           | Not Available               | BSD                            | Insert the full license text in the manual (or product) |
| Kerberos 5                       | 1.6.3                       | MIT                            | none |
| OpenLDAP                         | Not Available               | OpenLDaP Public License        | Insert the full license text in the manual (or product) |
| OpenSLP                          | Not Available               | Open SLP License               | Insert the full license text in the manual (or product) |
| OpenSSL                          | 1.1.0c                      | OpenSSL Combined License       | State acknowledgment in the manual (or product): "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)", "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)." |
| PCRE                             | Not Available               | BSD                            | Insert the full license text in the manual (or product) |
| uIP                              | Not Available               | BSD                            | Insert the full license text in the manual (or product) |
| InfoZIPLib                       | Not Available               | InforZIPLib license            | Insert the full license text in the manual (or product) |
2.7.4 Software Verification Test
This test can be executed in CWIS. This test verify's the software integrity by confirming the installed software has not been modified.

2.7.5 Software Installation
Software can be installed by the customer via 2 different methods, USB and CenterWare Web (Web UI). The most current release of software can be found on Xerox.com.
2.7.6 Network Protocols

Interface diagrams depicting the IPv4 and IPv6 protocol stacks supported by the device, annotated according to the DARPA model.

Figure 6

IPv4 Network Protocol Stack

Figure 7
2.8 Logical Access

2.8.1 Network Security

A variety of network protocols is supported. There are no ‘Xerox unique’ additions to these protocols.

2.8.1.1 IPSec

The device supports IPSec tunnel and transport mode. The print channel can be secured by establishing an IPSec association between a client and the device. A shared secret is used to encrypt the traffic flowing through a tunnel.

2.8.1.2 802.1x

IEEE 802.1X is a security standard for port based network access control. It secures Ethernet and/or Wi-Fi networks against unauthorized access by requiring device authentication with a central server before network access and data transmissions are allowed.

2.8.1.3 IP Filtering

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address and/or port number. Filtering rules can be set by the SA using the WebUI. An authorized SA can create rules to (Accept / Reject / Drop) for ALL or a range of IP addresses. In addition to specifying IP addresses to filter, an authorized SA can enable/disable all traffic over a specified transport layer port.
2.8.2 Ports

The following table summarizes all potentially open ports and subsequent sections discuss each port in more detail. All ports can be disabled if not needed under control of the system administrator.

2.8.2.1 Port 22, SSH
SSH is used to encrypt ftp data being transferred to a network server/repository.

2.8.2.2 Port 23, SNTP
This port is used to retrieve the time from a network server.

2.8.2.3 Port 25, SMTP
This unidirectional port is open only when Scan to E-mail is exporting images to an SMTP server, or when email alerts are being transmitted. SMTP messages & images are transmitted to the SMTP server from the device.

2.8.2.4 Port 53, DNS
Designating a DNS server will allow the device to resolve domain names. This can be configured via the WebUI.

2.8.2.5 Port 68, DHCP
This port is used only when performing DHCP, and is not open all of the time. To permanently close this port, DHCP must be explicitly disabled. This is done in User Tools via the Local User Interface or via the TCP/IP page in the Properties tab on the WebUI.

2.8.2.6 Port 80, HTTP
The embedded web pages communicate to the machine through a set of unique APIs and do not have direct access to machine information:

![Diagram](image)

Figure 9

The HTTP port can only access the HTTP server residing in the controller. The embedded HTTP server is Apache 2.0. The purpose of the HTTP server is to:
• Give users information of the status of the device;
• View the job queue within the device and delete jobs;
• Allow users to upload print ready files

The HTTP server can only host the web pages resident on the memory of the device. It does not and cannot act as a proxy server to get outside of the network the device resides on. The server cannot access any networks (or web servers) outside of the customer firewall.

When the device is configured with an IP address, it is as secure as any device inside the firewall. The web pages are accessible only to authorized users of the network inside the firewall.

This service (and port) may be disabled in User Tools via the Local User Interface or via the TCP/IP page in the Properties tab on the WebU. Please note that when this is disabled, IPP Port 631 is also disabled.

HTTP may be configured to use HTTPS for all traffic.

2.8.2.7 Proxy Server
The device can be configured to communicate through a proxy server. Features that can make use of a proxy server include the Automatic Meter Read feature, and scanning to a remote repository.

2.8.2.8 Port 88 Kerberos
This port is only open when the device is communicating with the Kerberos server to authenticate a user, or to request a TGT/TGS to access the LDAP server. To disable this port, authentication must be disabled, and this is accomplished via the Local User Interface.

This version of software has Kerberos 5-1.6-3 with DES (Data Encryption Standard), 3DES and AES encryption. The Kerberos code is limited to user authentication, and is used to authenticate a user with a given Kerberos server as a valid user on the network. Please note that the Kerberos server (a 3rd party device) needs to be set up for each user. Once the user is authenticated, the Kerberos software has completed its task. This code will not and cannot be used to encrypt or decrypt documents or other information.

This feature is based on the Kerberos program from the Massachusetts Institute of Technology (MIT). The Kerberos network authentication protocol is publicly available on the Internet as freeware at http://web.mit.edu/kerberos/www/.

Please note:
The device does not require much of the information provided by Kerberos for authenticating. For the most part, the device only uses information that indicates whether authentication has passed. Other information that the server may return (e.g. what services the user is authenticated for) is ignored or disabled in the Xerox implementation. This is not an issue since the only service a user is being authenticated for is access to an e-mail directory. No other network services are accessible from the Local UI.

Xerox has received an opinion from its legal counsel that the device software, including the implementation of a Kerberos encryption protocol in its network authentication feature, is not subject to encryption restrictions based on Export Administration Regulations of the United States Bureau of Export Administration (BXA). This means that it can be exported from the United States to most destinations and purchasers without the need for previous approval from or notification to BXA. At the time of the opinion, restricted destinations and entities included terrorist-supporting
states (Cuba, Iran, Libya, North Korea, Sudan and Syria), their nationals, and other sanctioned
entities such as persons listed on the Denied Parties List. Xerox provides this information for the
convenience of its customers and not as legal advice. Customers are encouraged to consult with
legal counsel to assure their own compliance with applicable export laws.

2.8.2.9 Ports 137, 138, 139, NETBIOS
For print jobs, these ports support the submission of files for printing as well as support Network
Authentication through SMB. Port 137 is the standard NetBIOS Name Service port, which is used
primarily for WINS. Port 138 supports the CIFS browsing protocol. Port 139 is the standard
NetBIOS Session port, which is used for printing. Ports 137, 138 and 139 may be configured in
the Properties tab of the device’s web page.

For Network Scanning features, ports 138 and 139 are used for both outbound (i.e. exporting
scanned images and associated data) and inbound functionality. In both instances, these ports
are only open when the files are being stored to the server. For these features, SMB protocol is
used.

2.8.2.10 Port 161, SNMP
This port support the SNMPv1, SNMPv2c, and SNMPv3 protocols. Please note that SNMP v1
does not have any password or community string control. SNMPv2 relies on a community string
to keep unwanted people from changing values or browsing parts of the MIB. This community
string is transmitted on the network in clear text so anyone sniffing the network can see the
password. Xerox strongly recommends that the customer change the community string upon
product installation. SNMP is configurable, and may be explicitly enabled or disabled in the
Properties tab of the device’s web pages.

SNMPv3 provides a secure channel to transmit SNMP data. It can be configured to use MD5
authentication with DES encryption. SNMP can also be secured using IPSec.

2.8.2.11 Port 389, LDAP
This is the standard LDAP port used for address book queries in the Scan to Email
feature.

2.8.2.12 Port 427, SLP
When activated, this port is used for service discovery and advertisement. The device will
advertise itself as a printer and listen for SLP queries using this port. It is not configurable. This
port is explicitly enabled / disabled in the Properties tab of the device’s web pages.

2.8.2.13 Port 443, HTTPS – HTTP over TLS
This is the default port for Secure HTTP communication. This can be configured via the device’s
web pages.

SSL/TLS version 1.2 is used and compliant to the SSL 3.0 IETF specification. SSL can be
disabled through within the IPP protocol section of properites.

HTTPS may be enabled so that the device can be securely administered from the web UI. SSL
(now TLS) uses X.509 certificates to establish trust between two ends of a communication
channel.

To administer the device securely, the user’s browser must be able to verify the certificate
supplied by the device. A certificate signed by a well-known Certificate Authority (CA) can be
installed on the device, or the device can generate a self-signed certificate. In the first instance,
the device creates a Certificate Signing Request (CSR) that can be downloaded and forwarded to
the well-known CA for signing. The signed device certificate is then installed on the device.
Alternatively, the device will generate a self-signed certificate. In this case, the generic Xerox root CA certificate may be downloaded from the device and installed in the certificate store of the user’s browser.

The device supports only server authentication.

2.8.2.14 Port 445, SMB 2.0, 3.0 (Microsoft – DS)
This port is open and used only when SMB (Microsoft Networking/Active Directory) is enabled.

2.8.2.15 Ports 500/4500, ISAKMP
ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation (e.g. denial of service and replay attacks). ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations. ISAKMP can be implemented over any transport protocol. All implementations must include send and receive capability for ISAKMP using UDP on port 500. Port 500 will only be open on the device if the IPsec service is enabled.

2.8.2.16 Port 515, LPR
This is the standard LPR printing port, which only supports IP printing. It is a configurable port, and may be explicitly enabled or disabled in the Properties tab of the device’s web pages.

2.8.2.17 Port 631, IPP
This port supports the Internet Printing Protocol. It is not configurable. This is disabled when the http (web) server is disabled.

2.8.2.18 Port 1900, SSDP
This port behaves similarly to the SLP port. When activated, this port is used for service discovery and advertisement. The device will advertise itself as a printer and listen for SSDP queries using this port. It is not configurable. This port is explicitly enabled/disabled in the Properties tab of the device’s web pages.

2.8.2.19 Port 3702, WSD Discovery, WS Discovery Multicast
This is the default port for WS-Discovery (the discovery of services in an ad hoc network with a minimum of networking services (for example, no DNS, UDDI or other directory services). It does this by announcing or advertising the existence of the printer and its services on the network when it becomes available, and announcing its departure when unavailable. The default state is selected (enabled).

2.8.2.20 Port 4500 ISAKMP
See Port 500. Port 4500 is an alternate port for port 500.

2.8.2.21 Port 5353 Multicast DNS, 5354 Multicast DNS Responder IPC
Multicast DNS provides the ability to address hosts using DNS-like names without the need of an existing, managed DNS server. The Multicast DNS Responder is a client in the printer that replies to multicast DNS requests for services on the local network. The multicast DNS requests and replies conform to RFC 1034 and RFC 2782 and are broadcast to the destination IP address 224.0.0.251 on port 5353. These ports will only be open if the Multicast DNS service is enabled.

2.8.2.22 Port 9100, raw IP
This allows downloading a PDL file directly to the interpreter. This port has limited bi-directionality (via PJL back channel) and allows printing only. This is a configurable port, and may be disabled in the Properties tab of the device’s web pages.

2.8.2.23 Ports 53202, 53303, 53404, WSD

Transfer Web Service (53202) and Print Web Service (53303 and 53404) for Microsoft WSD support.
3.0 System Access

3.1 Authentication Model

Authentication is the process of confirming user identities. If you enable authentication, the printer compares the information that users provide to another source of information, such as an LDAP directory. If the information is valid, the users are considered authenticated.

There are several ways to authenticate a user:

• **Passcode**: This option enables a passcode. To access the printer, at the control panel, users type a passcode. The printer compares the passcode to the stored information.

• **Local Authentication**: The option enables local authentication. To prove their identity, users type their user name and password at the control panel or in Xerox® CentreWare® Internet Services. The printer compares the user credentials to the information stored in the user database. If you have a limited number of users, or do not have access to an authentication server, use this authentication method.

• **Network Authentication**: This option enables network authentication. To prove their identity, users type their user name and password at the control panel or in Xerox® CentreWare® Internet Services. The printer compares the user credentials to the information stored on an authentication server.

**Note**
The printer can use one of the following authentication server types:
- Kerberos for UNIX, Linux, or Windows ADS
- SMB for Windows ADS or LDAP

3.2 Login and Authentication Methods

There are 3 methods and 4 selections available to Authentication. The following selection are available:
1) No Authentication – setting up a new
2) Passcode
3) Local Authentication
4) Network Authentication

3.3 Scan To

Scan To may require the device to log into a server. The instances where the device logs into a server are detailed in the following table. Users may also need to authenticate for scanning. This authentication is detailed in subsequent sections.
3.4 Device log on

<table>
<thead>
<tr>
<th>Scanning feature</th>
<th>Device behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan to File, Public Template</td>
<td>The device logs in to the scan repository as set up by the SA in the Properties tab on the WebUI. The credentials may be the user’s credentials or system credentials.</td>
</tr>
<tr>
<td>Scan to E-mail</td>
<td>The device logs into an LDAP Server as set up by the SA in User Tools. It will log into the Server when a user is authenticated and the device is configured for Remote Authorization or Personalization is enabled, and when the user attempts to access LDAP based scan-to-email address books. At the time the LDAP server must be accessed, the device will log into (bind to) the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>The device uses a simple bind to the LDAP server unless the device was able to obtain a TGS for the LDAP server from the Kerberos Server. In this case, a SASL (GSSAPI) bind is performed... A network username and password may be assigned to the device. The device logs in as a normal user, with read only privileges. User credentials may be used if configured by the SA for this authentication step.</td>
</tr>
<tr>
<td></td>
<td>The device then logs into the SMTP server as set up by the SA in the Properties tab on the WebUI. The credentials may be the user’s credentials or system credentials.</td>
</tr>
</tbody>
</table>

Please note that when the device logs into any server the device username and password are sent over the network in clear text unless one or more of the following have been enabled:

- HTTPS has been enabled
- IPSec has been configured to encrypt the traffic
- The device is logging into an SMB Server in which case the credentials are hashed.

3.5 Device User Database

The Device User Database stores user credential information for local authentication. When you configure local authentication, the printer checks the credentials that users provide against the information in the database. You can export the database for use on other printers.

Managing the Device User Database

1. In Xerox® CentreWare® Internet Services, click Properties > Login / Permissions.
2. Click Device User Database.
3. Select an option:

   Add New: Select this option to add users to the database. To add more than one user, select Add Another User. Add the user information and password, then click Save.

   Import from file: Select this option to import user information from a .csv file. Select a file to import, then click Apply.

   Export to File: Select this option to export the Device User Database to a .csv file. Select location to store the file. To edit or delete a user, for the user, click the appropriate icon.
4.0 Security aspects of Selected Features

4.1 SMart eSolutions

SMart eSolutions provides the ability to transmit data to Xerox to be used for billing (Meter Assistant) and toner replenishment (Supplies Assistant). The Systems Administrator sets up the attributes for the service via the Web UI, including enable/disable participation in SMart eSolutions, and time of day for the daily polling to the Xerox Communication Server. The device can be set to communicate via a proxy server on the customer’s network. The proxy server may be set to auto detect proxy settings or to manually set proxy address using the Web UI.

Meter Assistant

Once the connection with the Xerox Communication Server has been established, the Meter Assistant service will poll the Xerox Communication server daily over the network. The server will check whether it is time in the billing cycle to update the meter readings. If so, the server will request reads from the device, and the device will then respond by sending the meter reads back to the server.

Supplies Assistant

Once the connection with the Xerox Communication Server has been established, the Supplies Assistant service will be automatically enabled by request from the Xerox Communication Server. The device will then automatically send supplies data over the network to the Xerox Communication server at a regular interval.

Maintenance Assistant

Once the connection with the Xerox Communication Server has been established, the Maintenance Assistant service will be automatically enabled by request from the Xerox Communication Server. The device will then automatically send device fault codes and log data over the network to the Xerox Communication server at a regular interval.

4.2 Encrypted Partitions

All memory that store customer data are encrypted with AES256. Encryption keys are encrypted and stored per current relevant US government standards, specifications and guidelines for the SD card.

4.3 Email Signing and Encryption to Self

The device is capable of encrypting emails when the user is authenticated to the device. The device allows encryption to the authenticated user only, supporting 3DES and AES encryption.
5.0 Security @ Xerox (www.xerox.com/security)

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-article-whitepapers/enus.html
## APPENDICES

### Appendix A – Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>AMR</td>
<td>Automatic Meter Reads</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application-Specific Integrated Circuit. This is a custom integrated circuit that is unique to a specific product.</td>
</tr>
<tr>
<td>CAT</td>
<td>Customer Administration Tool</td>
</tr>
<tr>
<td>CSE</td>
<td>Customer Service Engineer</td>
</tr>
<tr>
<td>DADF/DADH</td>
<td>Duplex Automatic Document Feeder/Handler</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server. A centralized database that maps host names to static IP addresses.</td>
</tr>
<tr>
<td>DDNS</td>
<td>Dynamic Domain Name Server. Maps host names to dynamic static IP addresses.</td>
</tr>
<tr>
<td>DRAM</td>
<td>Dynamic Random Access Memory</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrically erasable programmable read only memory</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>HP</td>
<td>Hewlett-Packard</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext transfer protocol</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IFAX</td>
<td>Internet Fax</td>
</tr>
<tr>
<td>IIO</td>
<td>Immediate Image Overwrite</td>
</tr>
<tr>
<td>IIT</td>
<td>Image Input Terminal (the scanner)</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IOT</td>
<td>Image Output Terminal (the marking engine)</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPX</td>
<td>Internet Protocol Exchange</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Lightweight Directory Access Protocol Server. Typically, the same server that is used for email. It contains information about users such as name, phone number, and email address. It can also include a user’s login alias.</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LPR</td>
<td>Line Printer Request</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>n/a</td>
<td>not applicable</td>
</tr>
<tr>
<td>NDPS</td>
<td>Novell Distributed Print Services</td>
</tr>
<tr>
<td>NETBEUI</td>
<td>NETBIOS Extended User Interface</td>
</tr>
<tr>
<td>NETBIOS</td>
<td>Network Basic Input/Output System</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>NOS</td>
<td>Network Operating System</td>
</tr>
<tr>
<td>NVRAM</td>
<td>Non-Volatile Random Access Memory</td>
</tr>
<tr>
<td>NVM</td>
<td>Non-Volatile Memory</td>
</tr>
<tr>
<td>ODIO</td>
<td>On-Demand Image Overwrite</td>
</tr>
<tr>
<td>PCL</td>
<td>Printer Control Language</td>
</tr>
<tr>
<td>PDL</td>
<td>Page Description Language</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PWBA</td>
<td>Printed Wire Board Assembly</td>
</tr>
<tr>
<td>PWS</td>
<td>Common alternative for PSW</td>
</tr>
<tr>
<td>RFC</td>
<td>Required Functional Capability</td>
</tr>
<tr>
<td>SA</td>
<td>System Administrator</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SLP</td>
<td>Service Location Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SRAM</td>
<td>Static Random Access Memory</td>
</tr>
<tr>
<td>SSDP</td>
<td>Simple Service Discovery Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TIFF</td>
<td>Tagged Image File Format</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>WebUI</td>
<td>Web User Interface – the web pages resident in the WorkCentre Pro. These are accessible through any browser using the machine’s IP address as the URL.</td>
</tr>
<tr>
<td>XCMI</td>
<td>Xerox Common Management Interface</td>
</tr>
<tr>
<td>XSA</td>
<td>Xerox Standard Accounting</td>
</tr>
</tbody>
</table>