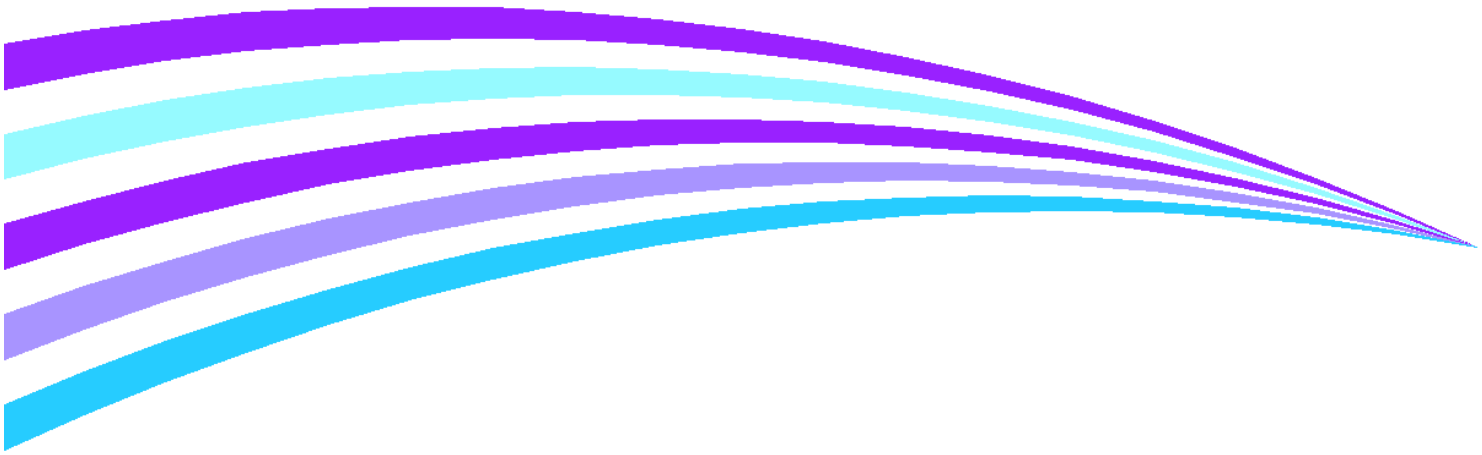
WorkCentre 3335/3345
Phaser 3330

Information Assurance Disclosure

Version 1.0

Document Version: 1.0 (August 2016)



Introduction

This document describes the locations, capacities and contents of volatile and non-volatile memory devices within the WorkCentre 3335/3345.

1.1. Purpose

The purpose of this document is to disclose information for the WorkCentre 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 WorkCentre 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 WorkCentre products relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or WorkCentre 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.

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.

Device Description

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

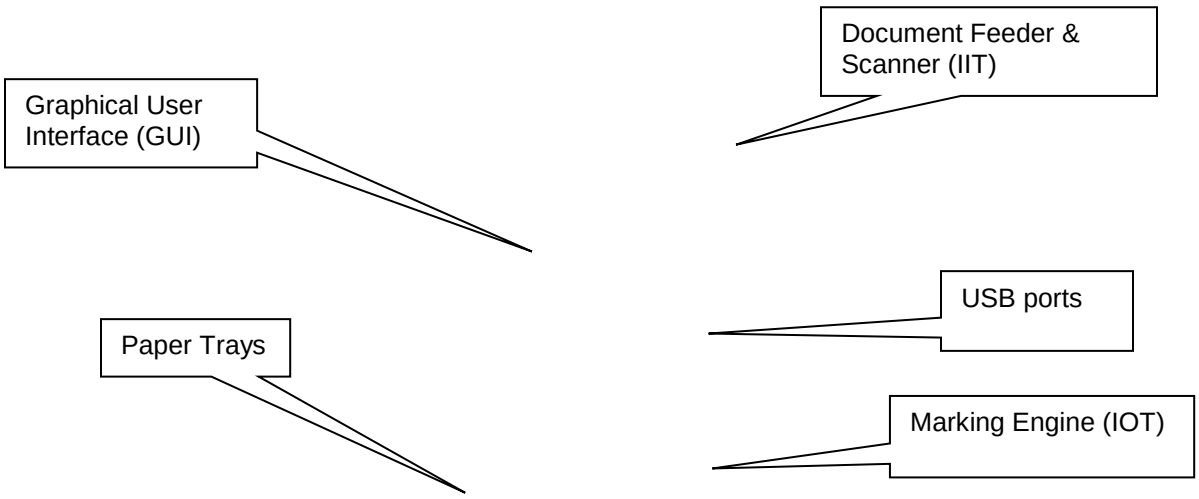


Figure 0-1 WorkCentre 3335 and 3345 Multifunction System

2.1. Security-relevant Subsystems

2.1.1. Physical Partitioning

The security-relevant subsystems of the product are partitioned as shown in Figure 0-2.

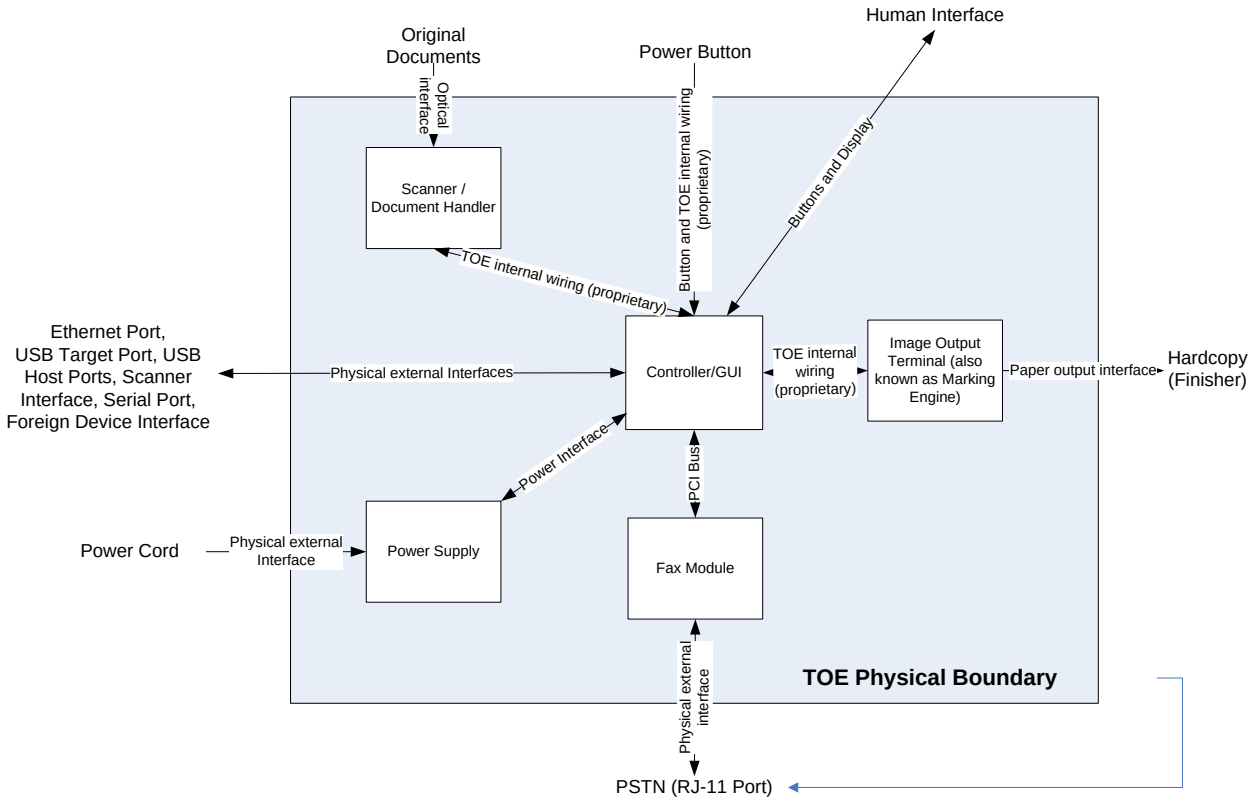


Figure 0-2 System functional block diagram

2.2. Controller

2.2.1. Purpose

The controller provides both network and direct-connect external interfaces, and enables copy, print, email, network scan, server fax, and LanFAX functionality. Network scanning, and LanFax, are standard features. The controller also incorporates an open-source web server (Apache) 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, sometimes referred to as scan-once/print-many. When producing multiple copies of a document, the scanned image is processed and buffered in the DRAM in a proprietary format. Extended buffer space for very large documents is provided on the network disk. 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 version 6.9. Unnecessary services such as rsh, telnet and finger are disabled in the Operating System. FTP is used in client-only mode by the network-scanning feature for the filing of scanned images; however, the controller does not contain an FTP server.

The controller works with the Graphical User Interface (GUI) assembly to provide system configuration functions. A System Administrator has the ability to access these functions.

2.2.2. External Connections

The controller printed wiring boards are physically mounted in a tray with external connections available at the right rear of the machine. The tray contains a single controller board. An optional fax board may also be installed.

Below the controller tray are other connectors that distribute power and communications to external options such as a finisher or high-capacity paper tray.

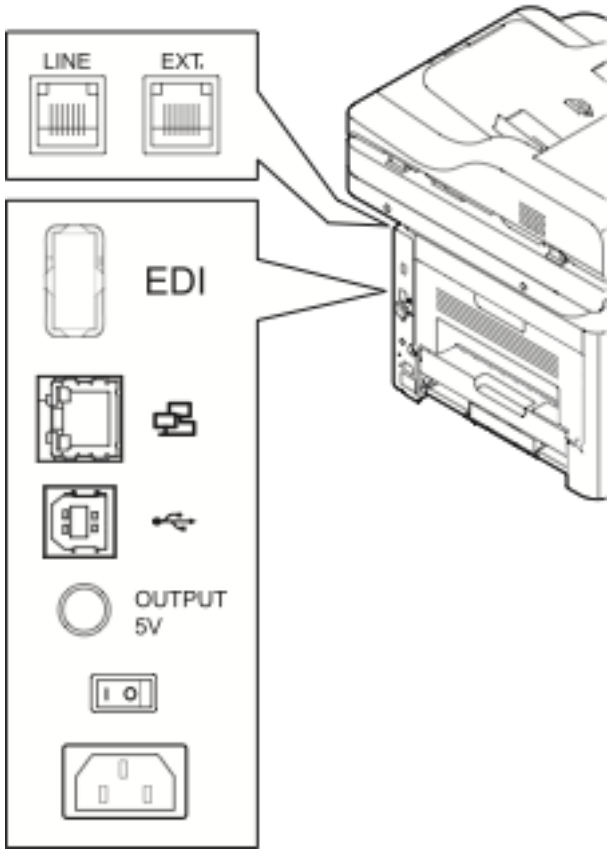


Figure 0-3 WorkCentre 3335 and 3345 Back panel connections

Interface	Description / Usage
USB Target Port	Diagnostics and service; Xerox Copier Assistant
Dual USB Host Ports	Card readers; SW upgrade; USB Printing; Scan to USB
Ethernet Port	Network Connectivity
Diagnostic LED Readout	Displays status codes for Diagnostics
Foreign Device Interface (FDI)	Allows connection of optional access control hardware.

Table 1 Controller External Connections

2.2.3. USB Ports

The WorkCentre 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 logging or saved machine settings files will make the files unusable on a WorkCentre.

The data in the network logging file is encrypted and can only be decrypted by Xerox service personnel at a Xerox location.

The machine settings that can be saved and restored by a service technician are limited to controller and fax parameters that are needed for normal operation. For example, the fax address book can be saved and restored by a service technician.

USB Port(s)	
USB port and location	**Purpose**
Front panel – 2 Host port	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.
Rear panel – 2 Host ports	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. Optional security devices, such as a card reader, communicate with the machine via this port. No job data is transmitted across this interface when an optional security device is connected.
Rear panel – 1 Target port	User PC direct connection for printing, Xerox Customer Service Engineer PWS connection for problem diagnosis. The optional Copy Assistant kit communicates with the machine via this port. No job data is transmitted across this interface.
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.)	

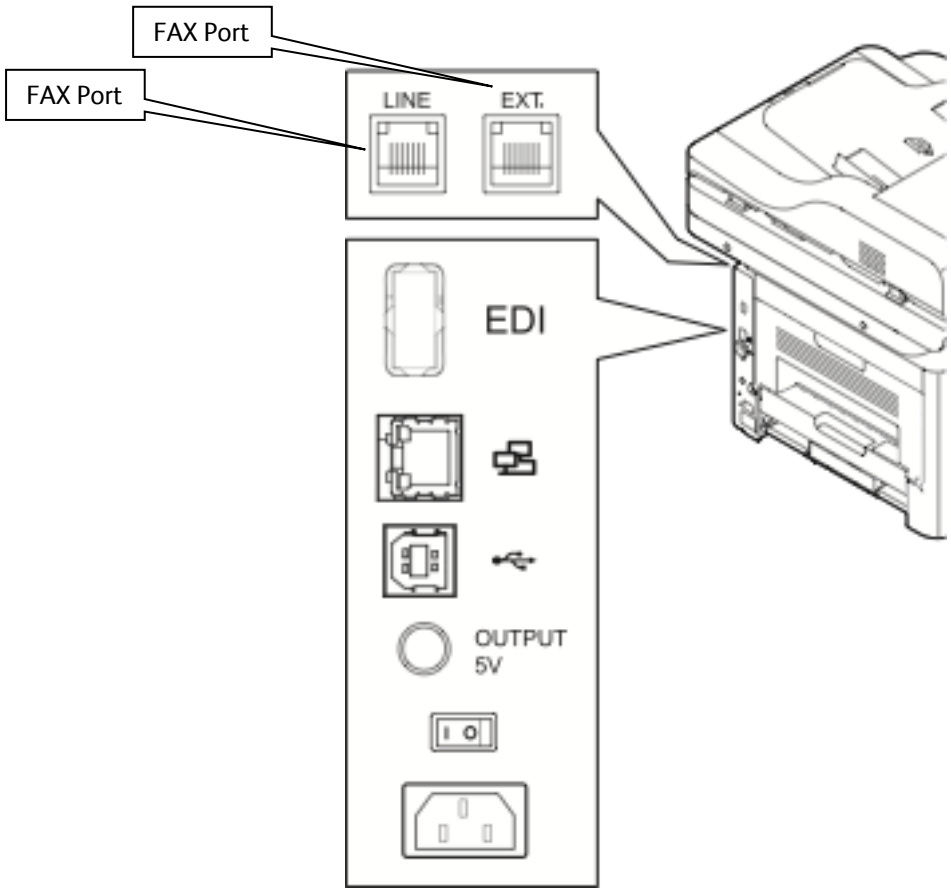
2.3. Fax Module

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.



Name	Size	Purpose / Explanation
MODEM #1	NA	Optional Fax modem 2 ports

Table 2 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. The Start hard button is located on the GUI panel.

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. Open-source components

Open-source components in the connectivity layer implement high-level protocol services. The security-relevant connectivity layer components are:

- Apache 2.0x
- OpenSSL 1.0.2d (TLS)
- OpenLDAP 2.8
- Kerberos 5 v1.6-3

These components may be updated as necessary via software updates.

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.

An IPSec tunnel can be established between a client and the machine, for example, to secure administration with SNMPv2 tools (HP Open View, etc.), providing security for SNMP SETs and GETS with an otherwise insecure protocol. SNMP Traps may not be secure if either the client or the device has just been rebooted. IP Filtering can be useful to prevent SNMP calls from non-IPSec clients.

Once an IPSec channel is established between two points, it stays open until one node reboots or goes into power saver. Only network clients and servers will have the ability to establish an IPSec tunnel with the WorkCentre device. Device-initiated operations (like scanning) cannot assume the existence of the tunnel unless a print job (or other client-initiated action) has been previously run since the last boot at either end of the connection.

2.8.1.2. 802.1x

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

802.1X allows network access decisions to be made at the port level, on a per-port basis (where a port is defined as a point of attachment to a network).

The device can be configured to use 802.1X for either Ethernet or WiFi network connections. The 802.1X configuration requires selection and configuration of an authentication frameworks or EAP (Extensible Authentication Protocol) method. For Ethernet, 802.1X is an optional, standalone configuration. For WiFi, 802.1X configuration is embedded within the wireless configuration for WPA/WPA2 Enterprise WiFi Security Modes.

These configurations may be done through the Web UI under the Properties tab in the Connectivity, Setup, and Network area.

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

This may be done through the Web UI under the Properties tab in the Security area.

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.

Default Port #	Type	Service name
68	UDP	DHC ACK Response to DHCP
80	TCP	HTTP
88	UDP	Kerberos
137	UDP	NETBIOS- Name Service
138	UDP	NETBIOS-Datagram Service; SMB filing
139	TCP	NETBIOS Session Service - SMB Authentication, SMB filing
161	TCP/UDP	SNMP
427	UDP	SLP
443	TCP	HTTPS – HTTP over TLS
445	TCP	Microsoft-DS
500	TCP	ISAKMP
515	TCP	LPR
631	TCP	IPP
1900	UDP	SSDP
1901	UDP	SSDP
3702	TCP/UDP	WSD Discovery
4500	TCP/UDP	IKE Negotiation Port for IPSec
5353	TCP/UDP	Multicast DNS
5354	TCP	Multicast DNS Responder IPC
9100	TCP	raw IP
28002	TCP	WS: Scan Extension, Convenience Authentication, Authentication & Authorization Configuration, Device Configuration
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

Table 3 Network Ports

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

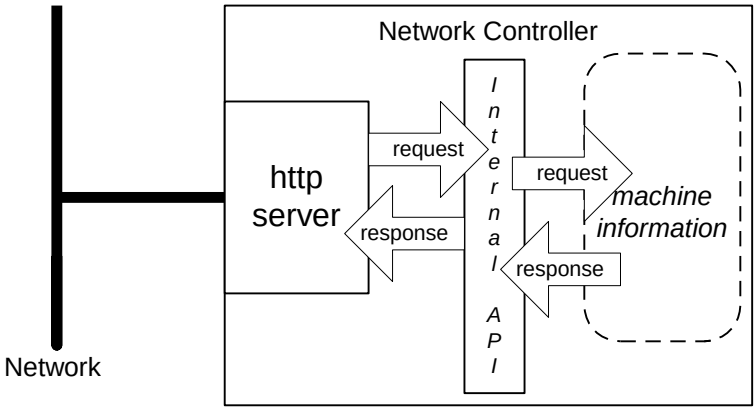
Designating a DNS server will allow the device to resolve domain names. This can be configured via the WebUI.

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:



The HTTP port can only access the HTTP server residing in the controller. The embedded HTTP server is Apache. 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 hard disk 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.

2.8.2.5.1. 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.

2.8.2.7. 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 5-1.8-3 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.

2.8.2.8. 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.

2.8.2.9. 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.

2.8.2.10. Port 389, LDAP

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

2.8.2.11. 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.

2.8.2.12. 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.

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.

2.8.2.13. Port 445, SMB 2.0, 3.0 (Microsoft – DS)

This port is open and used only when SMB (Microsoft Networking/Active Directory) is enabled.

2.8.2.14. 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.

2.8.2.15. 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.

2.8.2.16. Port 631, IPP

This port supports the Internet Printing Protocol. It is not configurable. This is disabled when the http (web) server is disabled.

2.8.2.17. 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.

2.8.2.18. 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).

2.8.2.19. Port 4500 ISAKMP

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

2.8.2.20. 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.

2.8.2.21. 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.

2.8.2.22. Ports 53202, 53303, 53404, WSD

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

System Access

3.1. Authentication Model

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 (see the discussion in Chapter 4 of Xerox Standard Accounting) 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 such as Copy, Fax, Server Fax, Reprint Saved Jobs, Email, and Workflow Scanning Server.

Also, users can be authorized to access one or any combination of the following machine pathways: Services, Job Status, or Machine Status.

User Permissions, the new authorization method determines your authorization be Role. 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. Assignment of users to the System Administrator role or the Accounting Administrator is also managed via User Permissions.

Figure 0-1 provides a schematic view of the authentication and authorization subsystem. Use of the local accounts database or a network database can be set independently for both authentication and authorization, meaning that it is possible to enable network authentication and local authorization, or vice versa. Usually authentication and authorization will be configured to use the same database.

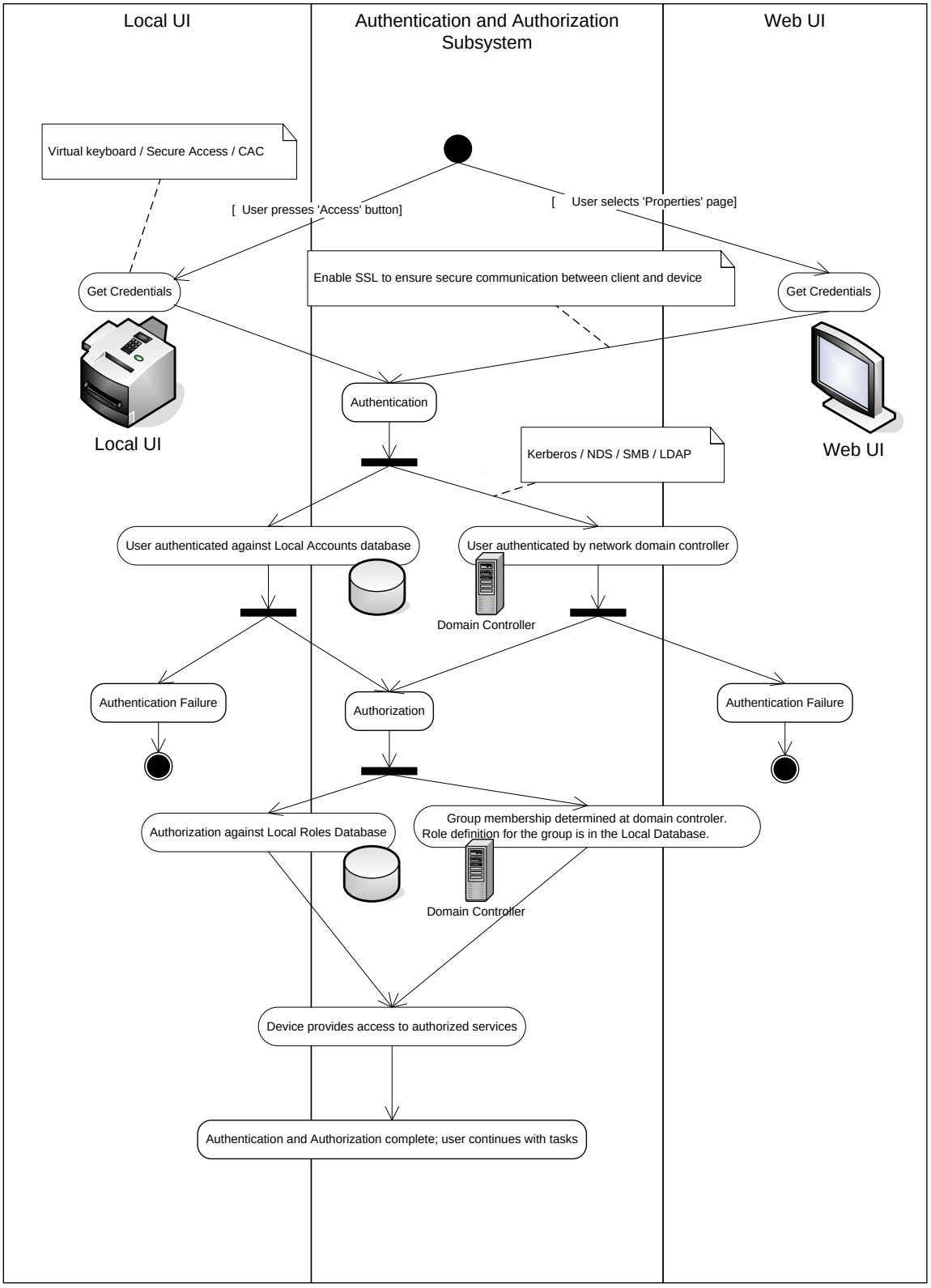


Figure 0-1 Authentication and Authorization schematic

3.2. Login and Authentication Methods

There are a number of methods for different types of users to be authenticated. In addition, the connected versions of the product also log into remote servers. A description of these behaviors follows.

3.2.1. System Administrator Login [All product configurations]

System Administrator Login and access to Tools requires use of either a reserved account “admin”, or login into an account with SA privileges defined in the role. It is highly recommended that the default password be changed to a strong alphanumeric password for the “admin” account. The same name and password is used to access the device via CWIS.

3.2.2. User authentication

Users may authenticate to the device using Kerberos, LDAP, or SMB Domain. For Kerberos and SMB the WebUI allows an SA to set up a default authentication domain and as many as eight additional alternate authentication domains.

3.2.2.1. Kerberos Authentication (Solaris or Windows)

The authentication steps are:

1) A User enters a user name and password at the device in the Local UI. The device sends an authentication request to the Kerberos Server.
2) The Kerberos Server responds with an encrypted key for the user attempting to sign on.
3) The device attempts to decrypt the key using the entered password. The device sends the decrypted key back to the server. The user is authenticated if the credentials were properly decrypted. The server responds by granting a Ticket Granting Ticket to the device.
4) The device then logs onto and queries the LDAP server trying to match an email address against the user’s Login Name. The user’s email address will be retrieved if the personalization option has been selected on the Authentication Configuration page.
5) If the LDAP Query is successful, the user’s email address is placed in the From: field. Otherwise, the user’s login name along with the system domain is used in the From: field.
6) The user may then add recipient addresses by accessing the Address Book on the LDAP server. Please see the User Manual for details. Each addition is a separate session to the LDAP server.

3.2.2.2. SMB Authentication (Windows 2000/Windows 2003/Windows 2008)

The authentication steps vary somewhat, depending on the network configuration. Listed below are three network configurations and the authentication steps.

Basic Network Configuration: Device and Domain Controller are on the same Subnet

Authentication Steps:

1) The device broadcasts an authentication request that is answered by the Domain Controller.
2) The Domain Controller responds back to the device whether or not the user was successfully authenticated.

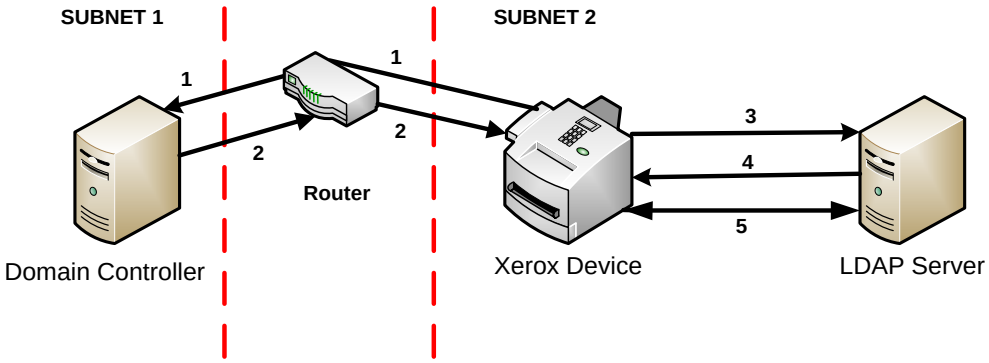
If (2) is successful, steps 3 – 5 proceed as described in steps 4 – 6 of the Kerberos section.

Device and Domain Controller are on different Subnets, SA defines IP Address of Domain Controller

Authentication Steps:

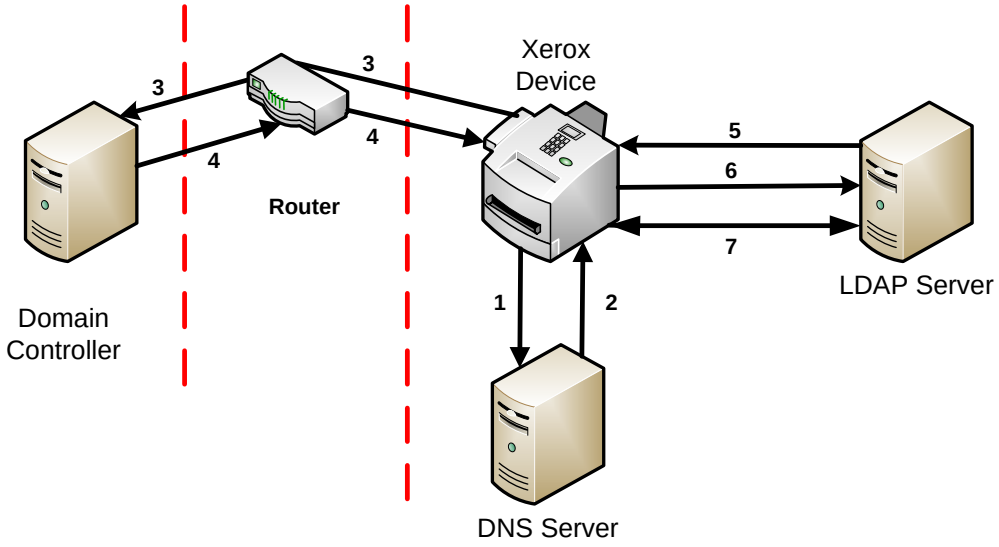
1) The device sends an authentication request directly to the Domain Controller through the router using the IP address of the Domain Controller.
2) The Domain Controller responds back to the device through the router whether or not the user was successfully authenticated.

If (2) is successful, steps 3 – 5 proceed as described in 4 - 6 of Kerberos section.



Device and Domain Controller are on different Subnets, SA defines Hostname of Domain Controller

Authentication Steps:



1) The device sends the Domain Controller hostname to the DNS Server.
2) The DNS Server returns the IP Address of the Domain Controller
3) The device sends an authentication request directly to the Domain Controller through the router using the IP address of the Domain Controller.
4) The Domain Controller responds back to the device through the router whether or not the user was successfully authenticated.

If (4) is successful, steps 5 – 7 proceed as described in steps 4 - 6 of the Kerberos section.

3.2.2.3. Convenience Authentication

Via Convenience Authentication, a customer can enable additional authentication methods to the device with minimal impact on the system software. By using a Web Service and 3rd party equipment, any authentication method that complies with the established interface into the device can be used. This includes biometric and card access.

Convenience Authentication is a Web Service that allows a 3rd party to use its own mechanisms, including accessing the customers authentication servers, to authenticate a user. The device can also take in additional information about the user to allow for two-factor authentication.

The Web Service interface allows the 3rd party to tell the device that someone was successfully logged in, who logged in and inform the device of logon issues using error messages.

The authentication steps are:

1) The device presents the appropriate screens to tell the user what needs to be done to authenticate.
2) The user follows the authentication instructions like swiping a card and/or entering a PIN or password.
3) User is authenticated and the device will complete any Authorization and Personalization as would have been done if the user authenticated using a system supplied solution.

3.3. System Accounts

3.3.1. Printing

The device may be set up to connect to a print queue maintained on a remote print server. The login name and password are sent to the print server in clear text. IPSec should be used to secure this channel.

4.1. Xerox Standard Accounting

Xerox Standard Accounting (XSA), intended primarily for use as an accounting service, can be used as an internal authorization service. XSA tracks copy, scan (including filing and email), print and fax usage by individual user[1]. The system administrator can enable/disable the feature by service (Copy, Print, Scan, or Fax via the LUI or Web UI, add or delete users, and set usage limits by service for each user. If XSA is enabled, a walk-up user must enter a valid XSA ID before being allowed access to the service for which XSA has been enabled at the device. The device will confirm that the entered XSA ID matches an authorized user, and that the usage limits for the selected service have not been exceeded. In this sense, XSA acts as an authorization service. The system administrator can limit access to device services by setting the usage limits on specific services to zero for users that should not have rights to use the feature. After each job is performed, the user's balance is updated by the number of impressions or scans performed. Services become unavailable to the user when the usage limits are exceeded.

When XSA is enabled in the print driver or on the Web UI or Local UI for print, before a print job is submitted, an XSA ID must also be entered. The ID is sent to the controller for validation. If the submitted ID is valid, the job will print, and the user's balance will be updated by the number of impressions performed. If the submitted ID is invalid, the job is deleted and an error sheet is printed in its place.

The Systems Administrator can chose to track all services (Print, Copy, Scan and Fax) or can choose to permit specific accounting IDs only for color print and color copy.

On demand, the SA will be able to download a report that shows activity for all of the users. The SA can add, modify or remove users and their allocations at any point.

An end user will be able to review their balances by entering a User ID at the Local UI or Web UI.

[1] On color machines, XSA can track color copy or color print usage.

4.2. 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.

Summary

The SMart eSolutions communication process means that the device initiates all communication between it and Xerox. Only device ID, device configuration, current firmware versions, meter read and supplies information is transferred. The information is sent encrypted using https (TLS).

4.3. Software Self Test

The Software Self Test features allows an administrator to initiate a test from CentreWare Internet Services (Web UI) to ensure that none of the static files on the device have been altered since they were installed. The Administrator will receive a Pass/Fail response. The test will take into account any Software Upgrades that have been performed. The test is based on a checksum generation of the files.

5.1. Responses to Known Vulnerabilities

5.1.1. 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-articles-whitepapers/enus.html

.

APPENDICES

Appendix A – Abbreviations

API	Application Programming Interface
AMR	Automatic Meter Reads
ASIC	Application-Specific Integrated Circuit. This is a custom integrated circuit that is unique to a specific product.
CAT	Customer Administration Tool
CSE	Customer Service Engineer
DADF/DADH	Duplex Automatic Document Feeder/Handler
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server. A centralized database that maps host names to static IP addresses.
DDNS	Dynamic Domain Name Server. Maps host names to dynamic static IP addresses.
DRAM	Dynamic Random Access Memory
EEPROM	Electrically erasable programmable read only memory
EGP	Exterior Gateway Protocol
GB	Gigabyte
HP	Hewlett-Packard
HTTP	Hypertext transfer protocol
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IIO	Immediate Image Overwrite
IIT	Image Input Terminal (the scanner)
IT	Information Technology
IOT	Image Output Terminal (the marking engine)
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX	Internet Protocol Exchange
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAP Server	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.
LED	Light Emitting Diode
LPR	Line Printer Request
MAC	Media Access Control
MIB	Management Information Base
n/a	not applicable
NETBEUI	NETBIOS Extended User Interface
NETBIOS	Network Basic Input/Output System

NOS	Network Operating System
NVRAM	Non-Volatile Random Access Memory
NVM	Non-Volatile Memory
PCL	Printer Control Language
PDL	Page Description Language
PIN	Personal Identification Number
PWBA	Printed Wire Board Assembly
PWS	Common alternative for PSW
RFC	Required Functional Capability
SA	System Administrator
SFTP	Secure File Transfer Protocol
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol
SRAM	Static Random Access Memory
SSD	Solid State Drive
SSDP	Simple Service Discovery Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TIFF	Tagged Image File Format
UI	User Interface
URL	Uniform Resource Locator
UDP	User Datagram Protocol
WebUI	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.
XCMI	Xerox Common Management Interface
XSA	Xerox Standard Accounting

Appendix B –Standards

Controller Hardware

PCI Specification (PCI Local Bus Specification Revision 2.1)
100 Megabit Ethernet (IEEE 802.3)
Universal Serial Bus 1.1
Parallel (IEEE 1284)
IEEE 1394a (FireWire)

Controller Software

Function	RFC/Standard
Internet Protocol	950
Internet standard subnetting procedure	919
Broadcasting internet datagrams	922
IP Version 6	2460
IP Version 6 Addressing Architecture	2373
ICMP Version 6 Protocol	2463
Transition Mechanisms for IPv6 Hosts and Routers	1933
Transmission Control Protocol (TCP)	793
User Datagram Protocol	768
Standard for the transmission of IP datagrams over Ethernet networks	894
Standard for the transmission of IP datagrams over IEEE802 networks	1042
ICMP – ICMP Echo, ICMP Time, ICMP Echo Reply, and ICMP Destination Unreachable message.	792
Reverse Address Resolution Protocol (RARP)	903
Bootstrap Protocol (BOOTP)	951
Clarifications and Extensions for the Bootstrap Protocol (BOOTP)	1542
X.500 Distinguished Name RFC references	1779, 2253, 2297, 2293
SLP	2608
Dynamic Host Configuration Protocol (DHCP)	2131
DHCP Options and BOOTP Vendor Extensions	2132
X.509 Certificate RFC references	2247, 2293, 2459, 2510, 2511, 3280
Hyper Text Transfer Protocol version 1.1 (HTTP)	2616
Line Printer Daemon (LPR/LPD)	1179
File Transfer Protocol (FTP)	959
SNMPv1	1157
SNMPv2	1901, 1905, 1906, 1908, 1909
SNMPv3	1902, 2572, 2574
Structure of Management Information (SMI) for SNMPv1	1155, 1212
Structure of Management Information (SMI) for SNMPv2	1902, 1903, 1904

Function	RFC/Standard
IETF MIBs: MIB II Host Resources RFC 3805 (Printer), Printer MIB V2	 1213 2790 3805
SNMP Traps	1215
Document Printing Application (DPA)	10175

Printing Description Languages

Postscript Language Reference, Third Edition
PCL6 (PCL5C + PCL XL class 3.0 emulation)
XPS
TIFF 6.0
JPEG
Portable Document Format Reference Manual Version 1.3

Appendix C – References

Kerberos FAQ http://www.cmf.nrl.navy.mil/krb/kerberos-faq.html

IP port numbers http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml