Xerox® Versant®
80 / 180 Press

Information Assurance Disclosure Paper
Version 1.0

Document Version: 1.0 (March 2017).

Preface

The purpose of this document is to disclose information for the Xerox Versant 80/180 Press products (hereinafter called as “the product”) 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 (IA).

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. **Target Audience**

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

2. **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 Fuji 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 Fuji Xerox has been advised of the possibility of such damages.

Contents

1. Device Description

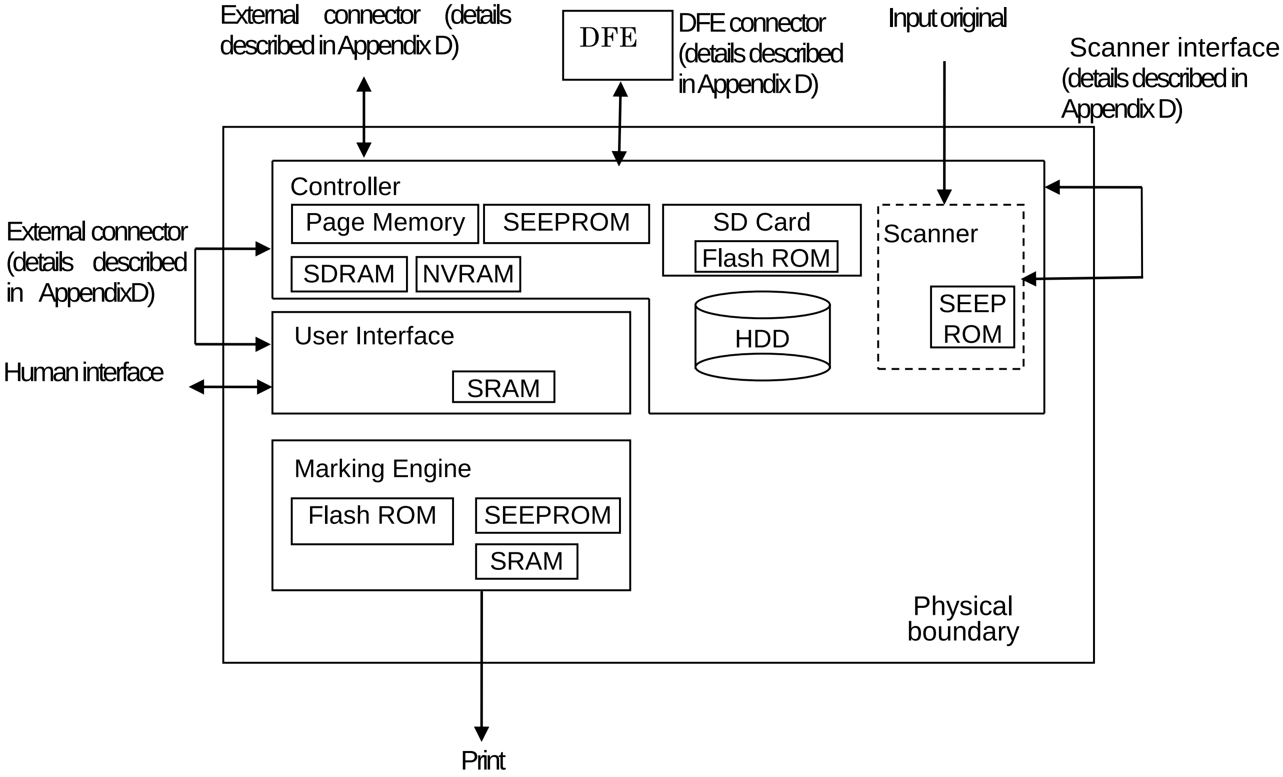
The product provides the copy and DFE print functions and features, and consists of the following subsystems: a controller module, marking engine, user interface, and scanner.

1.1 Security-relevant Subsystems

This section describes the physical methods to access the product and the relationship of the subsystems. It also describes the main security features and the subsystems that provide them. The next section describes the purpose of each subsystem as well as the memory components, which may possibly store user information.

1.1.2 Physical Partitioning

The figure below shows the physical methods to access the product as well as the relationship of the subsystems. The figure also includes the memory components of each subsystem described in the next section.


External connector (details described in Appendix D)
DFE
DFE connector (details described in Appendix D)
Input original
Scanner interface (details described in Appendix D)
External connector (details described in AppendixD)
Human interface
Controller
Page Memory
SEEPROM
SDRAM
NVRAM
SD Card
Flash ROM
HDD
Scanner
SEEP ROM
User Interface
SRAM
Marking Engine
Flash ROM
SEEPROM
SRAM
Physical boundary
Print

1.1.3 Security Functions allocated to Subsystems

Key security functions	Subsystems
Security Audit Log	Controller
Xerox Standard Accounting	Controller
Data Encryption	Controller
Image Overwrite	Controller
Email Signing and Encryption to Self	Controller
Self Test	Controller

1.2 Controller

1.2.1 Purpose

The controller provides interfaces for the network, user interface, marking engine, and scanner and thus enables such functionalities as copy, DFE print, and network scan. The Image Overwrite feature, which overwrites hard disc data that has already been used, and a Data Encryption feature, which encrypts data when it is stored to the hard disk, are also provided.

A scanned document image can be stored in a hard disk. By sending this data out to the marking engine, multiple copies can be made of the same image in one scan.

A PIN must be entered for a key operator to access the product via a network or the user interface.

1.2.2 Memory Components

Name	Purpose / Explanation
SDRAM	The executable software is loaded in this memory and is run. This memory is also used for temporary storage of user data such as data files and images. Such data is not backed up and is deleted when a job is completed. In addition, all data is lost when the power to the product is removed.
Flash ROM (SD Card)	This Flash memory contains the code necessary to boot the system, all executable code (operating system, PostScript interpreter, network protocols, document scheduler, etc.), installed fonts, and a backup of NVRAM data. A power-on self-test is performed and the bootstrap OS is loaded. This memory never contains any user data or document data. Operating System and application executable control code resides here. All codes except for the code of boot loader are compressed and are extracted into DRAM to be executed. No user image data is stored in this memory.

NVRAM	This non-volatile memory has no image data stored in it. User data such as system setting information, mailbox information, speed dial information, job memory, user management information, and various types of logs are recorded in it. The data is written in the memory after it is encrypted.
Controller Hard Disk	This device contains numerous types of data including user data: 1) Data of the documents scanned in upon copying. 2) Data of the scanned-in documents 3) Job logs For the formatting of the hard disk, the file system included in VxWorks is used. The format, however, is not accessible even when the hard disk is connected to PC. When a job is completed, its reference in the directory table is deleted but the image data remains on the disk until overwritten by a subsequent job. Image Overwrite feature enables an overwrite of the used data with meaningless data. Also, Data Encryption feature enables a data encryption of the HDD data.
Page Memory	This is a volatile memory used to store image data temporarily.
SEEP ROM	This memory contains the system's setting information.
RFID (Radio Frequency Identification)	No RFID Devices are contained in the device

1.3 Scanner

1.3.1 Purpose

The scanner scans a document and converts it to electronic data.

1.3.2 Memory Components

Name	Purpose / Explanation
SEEPROM	This non-volatile memory has no user data stored in it. This memory contains: ・Mode setting information on image processing and mechatronics control, and data on the parts usage status associated with recycling.

1.4 User Interface

1.4.1 Purpose

The user interface displays menus for users to provide input using hard or soft buttons, which the UI detects.

1.4.2 Memory Components

Name	Purpose / Explanation
Flash ROM	This flash memory stores the user interface control software. This memory never contains any user data.
SRAM (Static RAM)	This volatile memory temporarily stores the control data necessary to run the user interface control software. This memory never contains any user data.

1.5 Marking Engine

1.5.1 Purpose

The marking engine fuses images onto paper in copying and printing jobs.

1.5.2 Memory Components

Name	Purpose / Explanation
Flash ROM	All operating system and application executable control code related to Marking Engine resides here (e.g. boot loader, paper path, and xerographic).
DDR2 SDRAM	This is a Work RAM used to develop the program and parameters in the above-mentioned Flash ROM. No user data is stored in this memory.
RFID (Radio Frequency Identification)	RFID (Radio Frequency Identification) is used to identify each toner cartridge.

1.6 DFE (Digital Front End)

DFE is a controller equipped with features for importing data of scanned images and for requesting printing. This document does not provide any detailed description about this controller. FreeFlow Print Server and Fiery are examples of DFEs.

1.7 Other Memory Devices

The product has other memory devices, but such devices are used solely as accessory devices that control I/O of paper. Examples of this distributed control are:

- Finisher, ADF(Document Feeder), Duplex, and Tray Module

No user data is stored in any of these memory devices.

1.8 Program Downloading

The programs stored in the Flash ROM listed below are downloadable from external sources.

- Controller
- Marking Engine
- User interface
- ADF
- Finisher (Option for processing printed paper. No description on Finisher is provided in this document because user's image data will not be stored in it.)
- High capacity feeder (No description on High capacity feeder is provided in this document because user's image data will not be stored in it.)

This program-downloading 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 download file is legitimate.

1.9 Logical Access

1.9.1 Network Protocols

The network protocols supported by the product are IP (IPv4/IPv6), BOOTP, DHCP, SNMP(v1/v2c/v3), NETBIOS over TCP/IP, SMTP, SSDP, SNTP, HTTP, Kerberos, LDAP, SLP v1, and so on. These protocol specifications are implemented based on standard specifications such as RFC issued by IETF.

1.9.2 Ports

A number of TCP/IP and UDP/IP ports exist. The following table summarizes all ports that can be opened, and subsequent sections discuss each port in detail for when the product uses them.

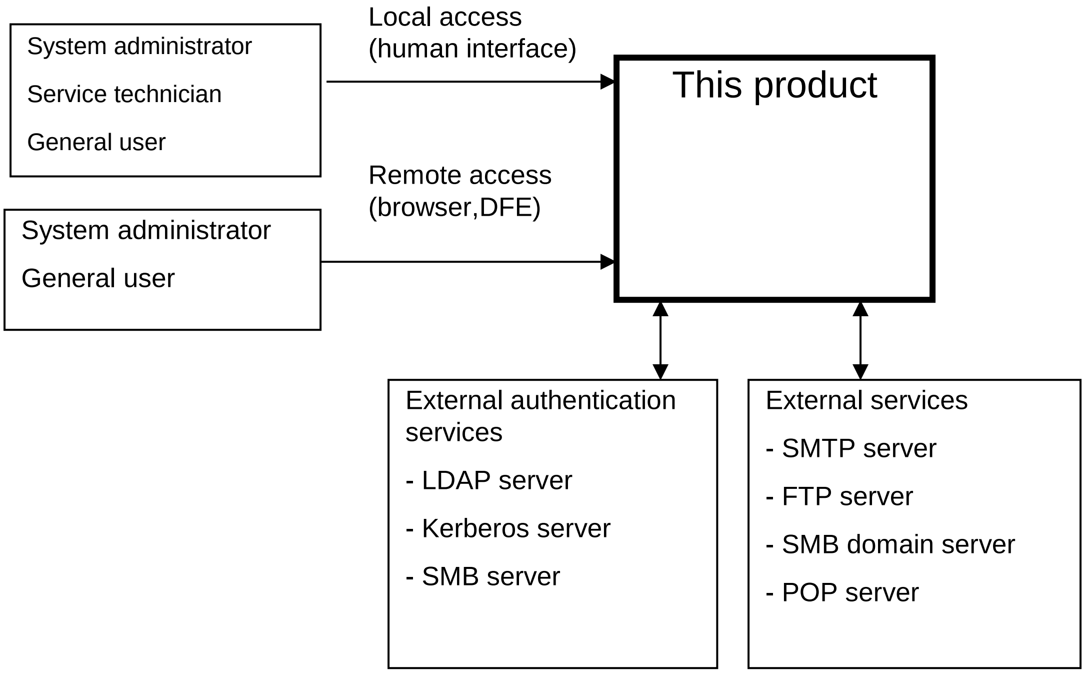
Port #	Type	Service Name
20	TCP	• FTP data (Active) - Client -
21	TCP	• FTP – Client -
25	TCP	• SMTP
53	TCP/UDP	• DNS – Client -
67	UDP	• BOOTP/DHCP – Client
80	TCP	• HTTP(CWIS)
80	TCP	• HTTP(SESAMi Manager)
80	TCP	• HTTP(WebDAV)
88	UDP	• Kerberos – Client -
110	TCP	• POP3 – Client -
123	UDP	• SNTP – 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	• HTTP(CWIS)
443	TCP	• HTTP(WebDAV)
443	TCP	• HTTP(Authentication Agent)
445	TCP	• Direct Hosting
465	TCP	• SMTPS – Client -

500	UDP	• ISAKMP
547	UDP	• DHCPv6 – Client
636	TCP	• LDAPS – Client -
995	TCP	• POPS – Client -
1824	TCP	• HTTPS(OffBox Validation) – Client -
1824	TCP	• Xerox Secure Access
1900	UDP	• SSDP
5353	UDP	• Mdns
9100	TCP	• raw IP
15000	TCP	• Loopback port for the control of SMTP server

“- 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.

2. System Access

2.1 Authentication Model



2.2 Log-in and Authentication Methods

The product provides a number of authentication methods for different types of users.
The definition of each user type is as follows.
- Key operator: This user has special rights for operating the machine. Only one account is assigned as the key operator for the product. This user can change the user ID and password, but cannot add another key operator account or delete the existing account.
- System administrator privilege (SA): By changing the machine management settings on the user settings screen, machine management rights can be given to a user, and the user becomes a system administrator privilege.
- System administrator: This is a term that refers to both the key operator and system administrator privilege. It is expected that the administrators will not perform any illicit operations.
- Service technician: A service engineer that performs maintenance on the product.
- General user: This user does not have any special rights that an administrator may have.

In addition, the product also logs into remote servers according to the features to use. Details of the operations follow.

2.2.1 Key Operator Authentication

The following authentication information is stored in the product NVM. At the shipment, a default password is set. Xerox strongly recommends that this password is changed from the default value immediately upon product installation.

2.2.1.1 Local Access

To access the product from the local user interface, a User ID and password are required. The User ID must be 1 to 32 characters and the password must be 4 to 12 characters.

2.2.1.2 Remote Access

To access the product from Xerox software products, DFE or CentreWare Internet Services, the same User ID and password used to access the local user interface are required.

2.2.2 Service Technicians Authentication

Authentication is also required for Xerox Service Technicians.

2.2.3 General Users and SA Authentication

The product provides the authentication function for general users. A user can be assigned to be a system administrator privilege that holds similar rights as a key operator. The settings can be changed in the user settings screen so that a user can have machine management rights and thereby becoming a system administrator privilege. The authentication method is the same as that of general users.

2.2.3.1 LOCAL ACCESS

To access the product from the Local User Interface, authentication is required per the authentication method as shown below.

Authentication Method	Operation
No authentication	No authentication is required for general users.
Authentication on the product (without password)	When Authentication on the product is in enabled state, the User ID (PIN) is required for general users.
Authentication on the product (with password)	When Authentication on the product is in enabled state, the User ID and 4 to 12 characters password are required for general users.
Card Auditron	General user is required to insert the authentication card. Either of the following IC cards can be used: - IC Card Gate 2 that is connected to accessory interface - Built-in IC card reader that is connected to a USB port
Secure Access Authentication	General user is authenticated using Secure Access Authentication server. This method is explained later in detail.

Remote authentication	When remote authentication is in enabled state, general users access remote authentication function for local access such as for copy / scan. The following are the remote authentication functions, and input of the User ID and password is required. 1) Kerberos authentication 2) SMB authentication 3) LDAP authentication Description of each authentication function follows.

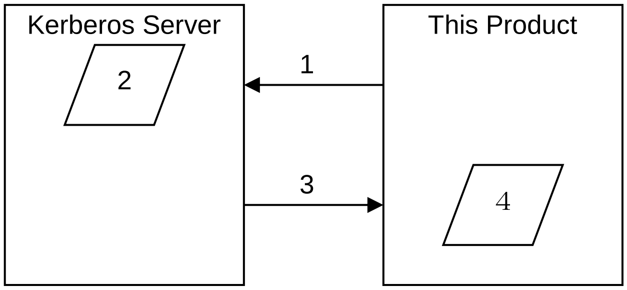
2.2.3.2 REMOTE ACCESS

Authentication Method	Operation
No authentication	No authentication is required for general users.
Authentication on the product	When Authentication on the product is in enabled state, the user ID and 4 to 12 character password are required for general users.
Remote authentication	When remote authentication is in enabled state, general users are authenticated using remote authentication functions. The following are remote authentication functions, and they require user ID and password. • Kerberos authentication • SMB authentication • LDAP authentication Description of each authentication function follows.

2.2.3.3 KERBEROS AUTHENTICATION

Kerberos authentication can avoid password interception and replay attack by using Kerberos protocol. The authentication steps using Kerberos are:

1. A user enters the User ID and password from the Local User Interface on the product. The product encrypts the entered User ID and time stamp into authentication identifier using the password, and sends the authentication identifier to the Kerberos server.
2. The Kerberos server decrypts the authentication identifier using the stored user password, to authenticate and obtain the included time stamp. Then, the server checks the validity of the time stamp. When the time stamp is correct, the Kerberos server creates a Session Key and encrypts it using the user password.
3. The Kerberos server sends back the Initial Ticket that includes the encrypted Session Key to the product.
4. The product decrypts the Session Key included in the Initial Ticket that the product received, using the entered password. When the decryption completes in success, the user is authenticated.



2.3.3.4 SMB AUTHENTICATION

In SMB authentication, only NTLMv2 authentication is supported. The user selects the pre-registered SMB domain name and enters the user ID and password to execute the authentication.

SMB Authentication method	Operation
NTLMv2 authentication	This is supported by Windows OS of Win XP and later. By challenge/response, authentication is executed without sending a password directly to the network.

2.3.3.5 LDAP AUTHENTICATION

The following modes are supported as the authentication methods in LDAP authentication. Since authentication on LDAP server is executed through Simple Bind using plain text, there is a risk of interception of User ID and password on network when LDAP protocol (port 389) is used. When LDAP server supports LDAPS protocol that uses secure channel using SSL, interception of User ID and password on network can be avoided by using LDAPS.

LDAP Authentication Mode	Operation
Direct Login	Executes authentication (ldap_bind) on LDAP server using User ID and password entered by user on local UI.

Search & Login	Searches user's Login ID from LDAP server using the User ID entered by user on local UI as a specific attribute (such as ID number), and executes authentication (ldap_bind) on LDAP server using the searched user's Login ID and entered password.

2.3.3.6 SECURE ACCESS AUTHENTICATION

In Secure Access Authentication, since a secure channel communication using Secure Access Authentication server and SSL is performed, interception of User ID and password on network can be avoided. Communication between Secure Access card reader and Secure Access Authentication server is encrypted by the supplier's unique code (e.g. Equitrac Corporation).
Sequence of authentication performed by inserting card to Secure Access card reader is as follows:

1. The information on the card inserted to Secure Access card reader is read and notified to the Secure Access authentication server. Then, the request for password confirmation is notified to the product from the Secure Access authentication server. When the User ID is entered from the local UI, the User ID is notified to the Secure Access authentication server from the product, and the request for password confirmation is notified to the product from the Secure Access authentication server.
2. The product sends the entered password to the Secure Access Authentication server, and the Secure Access Authentication server sends back the validation result to the product.

2.2.4 Login to External Servers

To use the following features, the product logs into the external servers.

Feature to use	Operations of the product
ScanToMail / MailboxToMail	To use this feature, the product accesses the SMTP server set to the product. The following authentication methods are supported: *SMTP authentication (AUTH-PLAIN / AUTH-LOGIN / AUTH-CRAM-MD5/GSSAPI) *POP before SMTP (basic authentication / APOP) Also, to use the remote Address Book in this feature, the product accesses the LDAP server set on the product. In this case, a bind by SIMPLE authentication will be conducted, using the User ID and password set on the product.
ScanToFTP / MailboxToFTP	To use this feature, the product accesses the FTP server registered in the Address Book. The following authentication method is supported: * basic authentication
ScanToSMB / MailboxToSMB	To use this feature, the product accesses the SMB domain server registered in the Address Book. The following authentication methods are supported. For the

	authentication method, the product automatically selects the most powerful method through the negotiation with the server. * GSSAPI * LM authentication * NTLM v1/v2
Mail receive (POP3)	To use this feature, when the receive protocol is set to POP3, the product accesses the POP3 server set on the product. The following authentication methods are supported: * basic authentication * APOP

2.2.5 Single Sign ON (SSO)

SSO is a feature that enables a user who has already logged into the device to access the external server without performing authentication again. The authenticated user’s user ID and password are used to access the external server. SSO is available in the following services when the authentication method is remote authentication.

Service	Operations Description
Remote Address Book	Authenticated user’s user ID and password that were used for remote authentication are used for authentication to access the LDAP server using ldap_bind. When the remote authentication method is Kerberos, the product obtains a service ticket and accesses the LDAP server using SASL protocol.
ScanToMail	Authenticated user’s user ID and password that were used for remote authentication are used for authentication to access the SMTP server. When the remote authentication method is Kerberos, the product obtains a service ticket and accesses the SMTP server.
ScanToMyFolder	Authenticated user’s user ID and password that were used for remote authentication are used for authentication to access the server. When the remote authentication method is Kerberos and the product transfers the scanned information to the SMB server, it obtains a service ticket and accesses the SMB server.
ScanToPC	Authenticated user’s user ID and password that were used for remote authentication are used for authentication to access the server. When the remote authentication method is Kerberos and the product transfers the scanned information to the SMB server, it obtains a service ticket and accesses the SMB server.

Centerware ScanServices	Authenticated user’s user ID and password that were used for remote authentication are used when the Login Source described in Job Template is “UserLogin / DomainUser / PromptIfNecessary.” When the remote authentication method is Kerberos and the product performs ScanToHTTP, it obtains a service ticket and accesses the HTTP server.

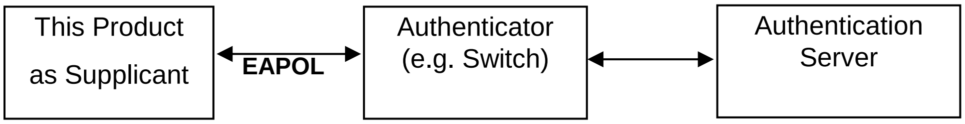
2.3 Device Authentication Method

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

Device Authentication Method	Operation
802.1X	Wired 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.

2.3.1 802.1X Authentication

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



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

802.1X Authentication Method	Operation
MD5	Performs authentication using the ID information in plain text and MD5 hashed password.
MS-CHAPv2	Performs authentication using the ID information in plain text and MD5 hashed password that is encrypted using a key generated from random numbers.

PEAP/MS-CHAPv2	Performs authentication in the SSL-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 SSL-encrypted channel established between the product and the authentication server, using the SSL client certificate of the product. ID information and password are not used.

3. Security Aspects of Selected Features

3.1 Audit Log

This feature is enabled when the system administrator sets “Audit Log Settings”. By enabling this Security Audit Log feature, the following information can be kept track of.
- When, by whom (user), and what was done (task) using the product
- Important events on the product (e.g. error, setting change, user operation, etc.)

Up to 15,000 events can be stored in the hard disk. When the number of events exceeds 15,000, audit log files 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 browser. Access from the control panel is not possible. When the user accesses the product through Web browser, there is an ”Export as text file” button. By pressing that button, audit logs can be downloaded as tab-delimited text files. When a user downloads audit log data, SSL/TSL communication must be enabled.

3.2 Data Encryption

Data Encryption feature is the feature to encrypt any data to be written to the Controller hard disk before writing the data to the hard disk.

3.2.1 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, based on the encryption key set by the system administrator and stored in the DRAM. The key is deleted by a power-off, due to the physical characteristics of the DRAM.

3.2.2 Special Behavior

This feature is enabled at the time of shipment, but in order to change the encryption key, the following is to be performed.
The menu to set Data Encryption feature is displayed in the setting items for the system administrator on the Control Panel.
The system administrator sets the Data Encryption feature in accordance with the policy. When setting this feature, the system administrator is asked to enter an encryption key and he/she can enter any 12 alphanumeric characters. The setting becomes valid when the product is started up again.
The Data Encryption feature is valid on all the data stored on the Controller hard disk, and the data is encrypted before it is stored in the hard disk. Whenever the data is read out from the hard disk, decryption of the data is performed.

3.3 Image Overwrite

Image Overwrite feature is the feature to delete the already used document data that still resides on the Controller hard disk by an overwrite, after the completion of Copy, Print, and Scan operations.

3.3.1 Algorithm

The system administrator can select the overwrite algorithm from the following:

"Off"

Image overwrite is not conducted.

"On (once)"

Image overwrite is conducted once with "the data set to all 0".

"On (thrice)"

Image overwrite is conducted thrice with "the random data",

" the random data", and then "the data set to all 0".

3.3.2 Special Behavior

The system administrator sets the number of times to overwrite in accordance with the policy. The setting will become valid when the product is started up again.

The Image Overwrite feature is operated when the document data in the Controller hard disk is abandoned after the Copy, Print or Scan feature is used. (See "Chapter 4: Data Flow" for the abandon timing of the document data.)

The user confirms at the Confirmation screen on the Control Panel whether image Overwrite operation is under way; "In Progress" indication is displayed during the image overwrite operation, and "Standby" indication is displayed when the image overwrite operation is not under way.

If the Image Overwrite does not complete due to causes such as power being cut off during the image overwrite process, the Image Overwrite is performed at the next start up.

3.4 FIPS

FIPS140 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 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 non-approved mode	The algorithms that are specified in FIPS and/or are recommended by NIST, and other algorithms operate in this mode.

The following are the approved algorithms that operate in FIPS140 approved Mode.

Algorithm approved by FIPS140
AES 3DES DH DSA FIPS 186-2 PRNG RSA X9.31, PKCS#1 V.1.5 RSA SHA-1 HMAC-SHA1

Although SMB, NetWare, SNMPv3, and PDF Direct Print Service use encryption algorithms that are not approved by FIPS140, they can operate in FIPS140 approved Mode in order to maintain compatibility with conventional products

3.5 Email Signing and Encryption to Self

By S/MIME encrypting mail function, the document data being transmitted to/from the outside by E-mail are protected from interception. By S/MIME signature mail function, the document data are protected from interception and alteration.
A cryptographic key is generated at the time of starting mail encryption and lost at the time of completion of the encryption or powering off the MFD main unit.

Secret-key cryptographic method generated as S/MIME for every mail.

Cryptographic Method and Size of Secret Key
3Key Triple-DES/168 bits
AES / 128 bits
AES / 192 bits
AES / 256 bits

Hash method generated as S/MIME for every mail

Hash method
SHA1
SHA256

3.6 Self-Test

The product can execute a Self-Test feature to verify the integrity of executable code and setting data.
The product verifies the area of NVRAM and SEEPROM including setting data at initiation, and displays an error on the control panel at error occurrence.
However, an error is not detected for the data on audit logs and time and date as these are not included in the target.
Also, when Self-Test feature is set at initiation, the product calculates the checksum of Controller ROM to confirm if it matches the specified value, and displays an error on the control panel at error occurrence.
If any abnormal condition such as internal program modification is found during the program diagnosis, the product stops starting up and records the information in the audit log.
The information may not be recorded in the audit log depending on the status of program malfunction.

4. Responses to Known Vulnerabilities

4.1 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

5. APPENDICES

Appendix A – Abbreviations

API	Application Programming Interface
CE	Customer Engineer
CWIS	CentreWare Internet Services
DADF	Duplex Automatic Document Feeder
DFE	Digital Front End
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DRAM	Dynamic Random Access Memory
EEPROM	Electrically erasable programmable read only memory
EP	Electronic Partnership
HTTP	Hypertext transfer protocol
IETF	Internet Engineering Task Force
IIT	Image Input Terminal (the scanner)
IT	Information Technology
IOT	Image Output Terminal (the marking engine)
IP	Internet Protocol
LAN	Local Area Network
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
RFC	Request for Comments
SNMP	Simple Network Management Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
USB	Universal Serial Bus

Appendix B – External management interface 2: SESAMi Service Management Interface

The SSMI (SESAMi Service Management Interface), which provides the following features as the device management interface is supported.

Supported Feature	Description
Status/Config Management	Provides the means to obtain and set the information subject to management. To be more precise, the feature to obtain the description on the various setting values and status values of the device (GetDescription), to obtain the attributes (GetAttribute), and to set the attributes (SetAttribute).
Job Management	Provides the means to manage processing jobs and completed jobs. To be more precise, the means to obtain job information (logs) (GetJobList), to control jobs in process (OperateJob), and to obtain job information (logs) including parent-child job relationships (GetJobListEx).

Exclusive Control	A control service used for exclusive access to features provided by SSMI. To be more precise, the feature to start exclusive control by creating context for access (CreateExclusiveContext) and to end exclusive control by releasing context for access (ReleaseExclusiveContext).
Service State Management	Instructs the state transition of the service (device) (OperateService). (e.x. instructs rebooting.)
User Management	Manages users. To be more precise, provides the features to add (AddUser), delete (DeleteUser), obtain (GetUser), and set (SetUser) users managed by the product.
User Information Management	Manages the information associated with users (Service use counter / use restriction, per user). To be more precise, provides the features to obtain (GetUserInformation) and set (SetUserInformation) user information.
Account Management	Manages the Account ID. To be more precise, provides the features to obtain (GetAccountID), set (SetAccountID), and delete (DeleteAccountID) Account ID.
Address Book Management	Manages the Address Book, which contains information such as the speed dials and server addresses. To be more precise, provides the features to add (AddAddress), delete (DeleteAddress), obtain (GetAddress)/, and set (SetAddress) such information.
Job Flow Sheet Management	Manages the Flow Sheets (i.e. Job Flow Sheets). To be more precise, provides the features to add (AddJob Flow Sheet), delete (DeleteJob Flow Sheet), obtain (GetJob Flow Sheet), and set (SetJob Flow Sheet) Job Flow Sheets.
Job Flow Sheet Owner Management	Manages the owners of each Flow Sheet (Job Flow Sheet). To be more precise, provides the features to obtain (GetJob Flow SheetOwner) and set (SetJob Flow SheetOwner) the owner of Job Flow Sheet.
Mailbox Management	Manages the Mailboxes. To be more precise, provides the features to add (AddMailbox) and delete (DeleteMailbox) Mailbox, and obtain (GetMailbox) and set (SetMailbox) the Mailbox setting information.
Key Management	Manages the certificates. To be more precise, provides the features to add (AddKey), delete (DeleteKey), obtain (GetKey), and assign (AssignKey) key.
Local Key Management	Generates the self-certificates. To be more precise, provides the features to generate (Generate) self-certificates.
Chain-Link Management	Manages Chain-Link. To be more precise, provides the features to obtain(GetChainLink) and set (SetChainLink) Chain Link.
Job Log Management	Manages the job logs. To be more precise, provides the features to obtain the job log information (GetJobLogInfo) and obtain the job log (GetJobLog).
Accounting Relation Management	Manages the relation between the Account ID and User ID. To be more precise, provides the features to add (AddAccountingRelation), delete

	(DeleteAccountingRelation), and obtain (GetAccountingRelation) the accounting relations.
Custom Service Management	Provides management features of registering, changing, and deleting custom service scripts, and obtaining list of custom service scripts. To be more precise, provides folder management, script file management, and service management features. [Folder management] Create folder to register custom service script files (CreateCsvFolder) / Obtain list of names of folders to register custom service scripts (ListCsvFolder) / Delete folder to register custom service script files (DeleteCsvFolder) [Script file management] Register custom service script to folder (StorCsvFiles) / Delete custom service script from folder (DeleteCsvFiles) [Service management] Register folder in which custom service script is stored to custom service (AddCsv) / Change content of registered items in custom service (SetCsv) / Obtain list of custom services (ListCsv) / Delete registered items from custom service (DeleteCsv)
Stored Document Management	Provides features to manage stored documents. Specifically, it provides features to obtain and delete information of the stored documents.
Embedded Plugin Management	Provides features to manage the plugin to be embedded. Specifically, the following features are provided: - Register, delete, and update the files for the embedded plugin - Obtain information on the embedded plugin - Start and stop the embedded plugin
Function Layout Management	Provides management features for allocating functions to positions where functions can be allocated (e.g. screens or buttons). Specifically, the following features are provided: - Obtain information on the available functions and positions - Obtain information on function layout - Configure function layout
ExecuteJobTemplate	Provides a feature to execute job flow sheets that exist in a device and a feature to execute a job sheet as soon as it is input. - Execute job flow sheet (ExecuteJobTemplate)
Batch	Provides features to process various SSMI messages in batches.

	- Request a batch - Obtain batch process result (GetBatchResult) - Release batch process result (ReleaseBatchResult)
GroupDial	Provides features to manage Group Dials. - Add a Group Dial (AddGroupDial) - Update a Group Dial (SetGroupDial) - Delete a Group Dial (DeleteGroupDial) - Obtain a Group Dial (GetGroupDial) - Add a member to a Group Dial (AddGroupDialMember) - Remove a member from a Group Dial (DeleteGroupDialMember)
BoxSelector	Provides features to manage the Box Selector. - Add a Service Box Selector (AddServiceBoxSelector) - Update a Service Box Selector (SetServiceBoxSelector) - Delete a Service Box Selector (DeleteServiceBoxSelector) - Obtain a Service Box Selector (GetServiceBoxSelector) - Configure a Line Box Selector (SetLineBoxSelector) - Obtain a Line Box Selector (GetLineBoxSelector)
WindowControl	Provides the following feature to control the window. - Display a window (DisplayWindow)
FaxLog	Provides the following feature to manage the fax log. - Obtain fax log (GetFaxLog)