Print Controller Design Guide for Information Security:

Model MT-C2

Model Th-C1

Model J-C2

Model V-C1

Ricoh Company, Ltd.

Octber 31, 2005

TABLE OF CONTENTS

Overview

This document describes the structural layout and functional operations of the hardware and software for the multi-functional products listed below (herein referred to as the MFP), which were designed and developed by Ricoh Co. Ltd. (herein referred to as Ricoh), as well as the security of image data and related information handled by MFP internal and peripheral devices.

The explanations will primarily focus on the following, with particular attention to demonstrating how unauthorized access is not possible via the CSS and FAX telecommunications lines to local network environments and to data stored in the MFP.

- Operational Summaries
- Data Flow
- Data Security Considerations

Products to Which This Document Applies

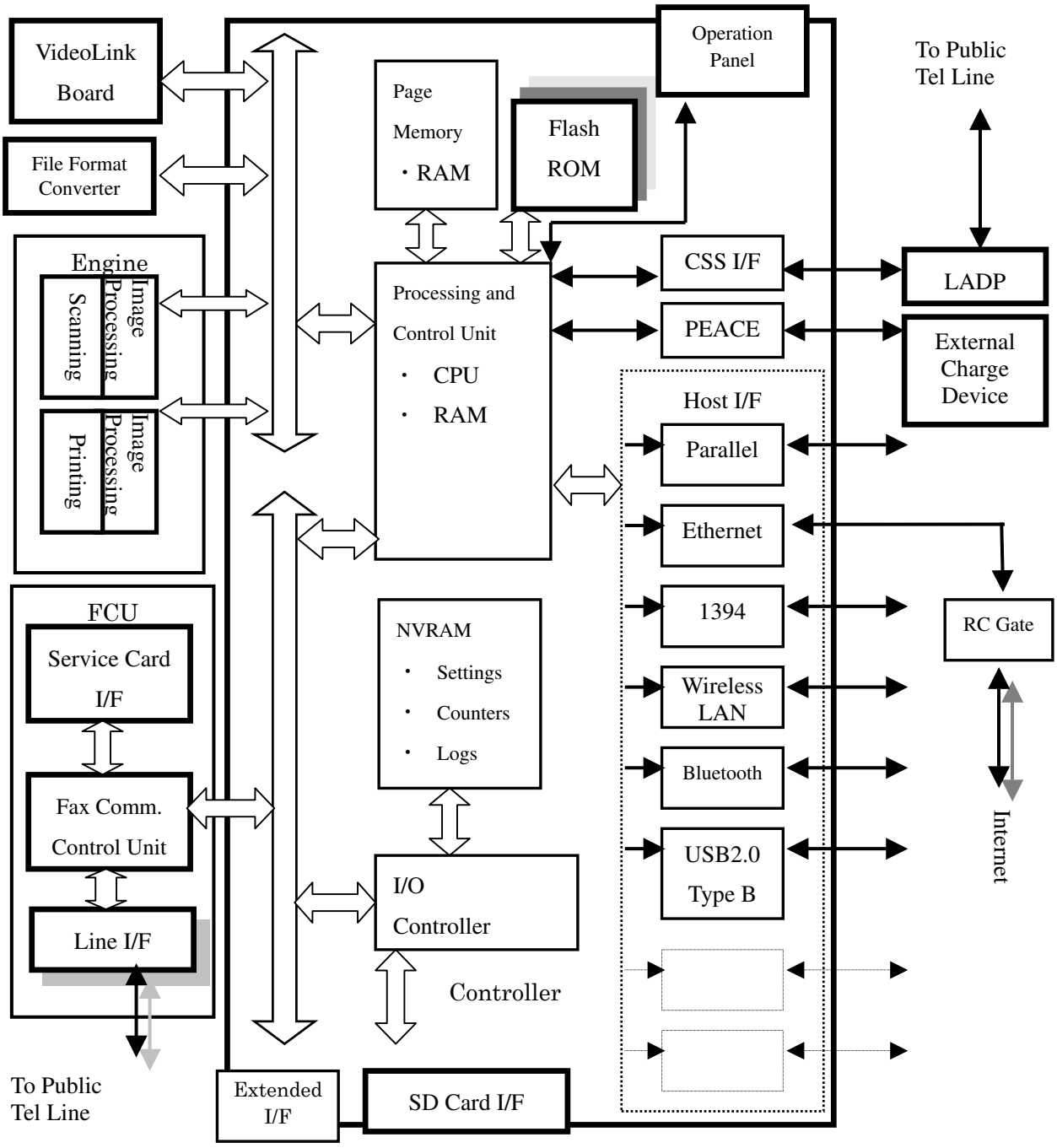
This document applies to the following MFPs designed and developed by Ricoh:

- *Model MT-C2(*)*
- *Model Th-C1*
- *Model J-C2*
- *Model V-C1(*)*

(*) Please note that the description related to fax function is not beapplicable as these MFP do not its function..

1 Internal System Configuration

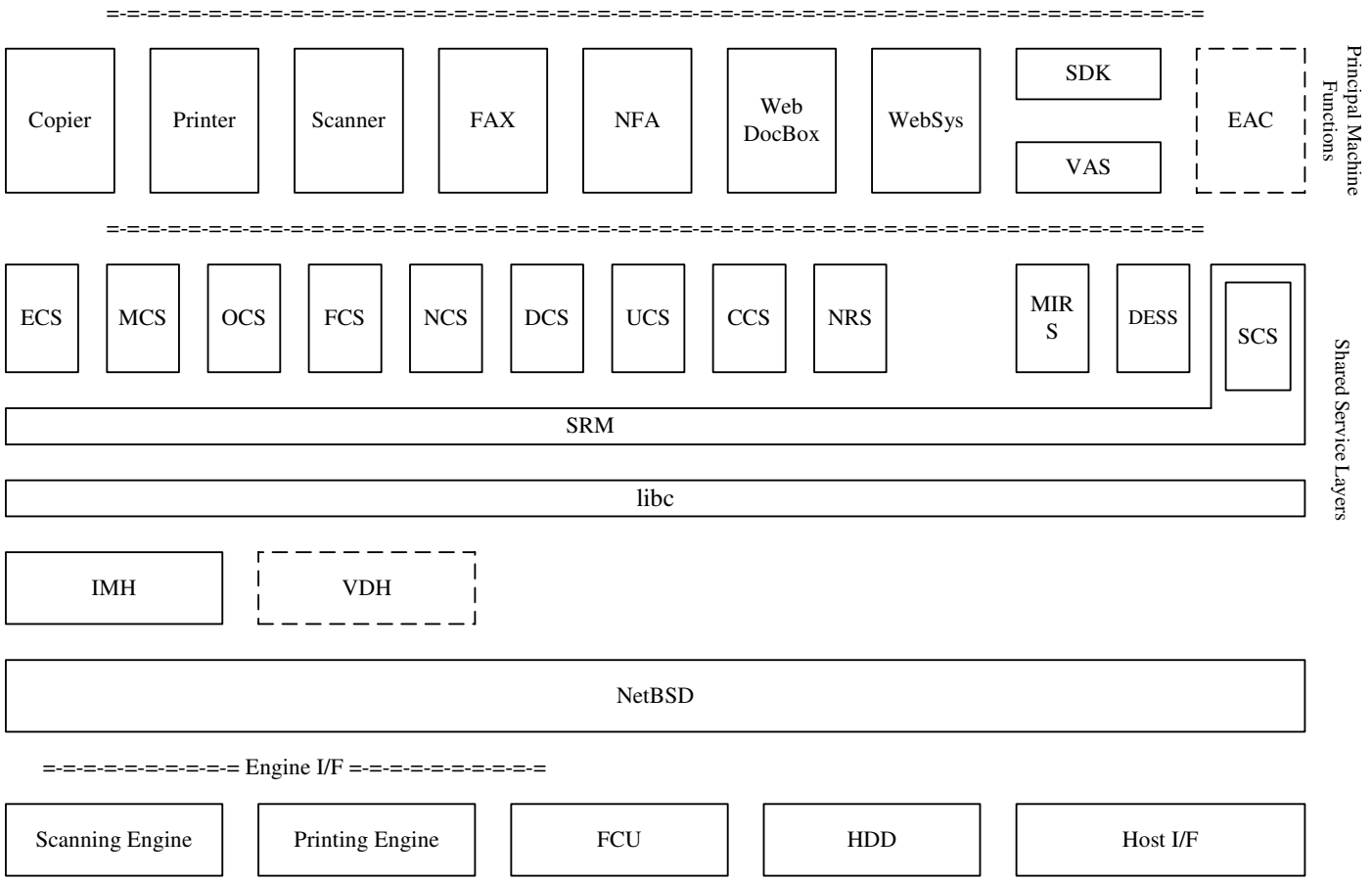
1.1 Hardware Configuration



Hardware Configuration

- Serial communication between the CSS (Customer Support System) I/F and LADP (Line Adapter).
- Serial communication between PEACE (coin/card-operated device I/F) and external coin/card-operated devices.
- Image Memory area: Also performs image-processing functions such as data compression and decompression.
- Video Link Board: Acts as the interface between the MFP and external controller.
- File Format Converter: Converts the file format of image files.
- RC Gate: Intermediary device connected to the MFP via an Ethernet connection for performing remote diagnostic operations including firmware updates and settings changes.
- SD card I/F: Used for performing service maintenance and as an interface for firmware storage media.

1.2 Software Configuration



Software Configuration

1.2.1 Shared Service Layers

ECS (Engine Control Service)	Controls engine operations for scanning and printing.
MCS (Memory Control Service)	Manages the memory in the Image Memory area (incl. the HDD), as well as compression/decompression.
IMH (Image Memory Handler)	Transfers data between the controller and engine.
OCS (Operation Panel Control Service)	Controls the panel LEDs, monitors panel keys and manages panel objects and display messages.
NCS (Network Control Service)	Controls host I/F and protocol control (transport, session).
FCS (FAX Control Service)	Exchanges data and commands with the FCU (FAX Control Unit), which manages and controls FAX communication and telecommunications lines.
SCS/SRM (System Control Service/ System Resource Manager)	Manages machine settings and counter/log data.
DCS (Delivery Control Service)	Controls all non-FAX transmission/reception of email as well as the forwarding of image data to servers and folders.

MIRS (Machine Information Report Service)	Controls the sending of machine configuration data by email
UCS (User Control Service)	Manages the Address Book data.
CCS (Certification Control Service)	Mediates the communication between the principal machine function and external charge device during the authenitcation process, as well as the charge-related processing (e.g. counters).
NRS (New Remote Service)	Controls remote correspondence with RC Gate (e.g. diagnostics, firmware update, settings changes).
DESS (Data Encrytion Security Service)	Controls the encryption and decrytption functions.
VDH (Video Device Handler)	Transfers image data between the MFP engine and external controller. **Note:** This layer exisits only on models capable of supporting an external controller.

1.2.2 Principal Machine Functions

Copier	Activates the scanning engine, which reads the original and then sends the data on to the controller to be printed out from the printing engine. Secondary data, such as that used for access control, is handled from the operation panel.
Printer	Receives image data through the host interface, which then sends the data to the controller. Also contains a printer language processing subsystem (e.g. RPCS) that converts the printer language into image data, which is then printed out from the printing engine. Secondary data is handled via the connection protocols between the driver UI and the host I/F.
Scanner	Activates the scanning engine, which reads the original and then sends the data to a PC via the host I/F. Scanning can be initiated from both the operation panel and from a PC via a TWAIN driver.
FAX	Activates the scanning engine, which reads the original and then sends the data to the FCU to be sent as a FAX via a telecommunications line. Also receives FAX data and prints it out from the printing engine.
NFA (NetFile)	Accesses and performs operations on documents stored on the Document Server through the four principal machine functions above via a PC utility or server software.
WebSys	Controls Web-based access to the MFP and allows machine configuration settings to be viewed and changed via a Web interface.
WebDocBox	Allows operations to be peformed on Document Server documents stored in the MFP (viewing, downloading, printing, deleting) via a Web interface.

SDK/VAS SDK: Applications provided by third-party vendors designed to function with MFP pricipal machine functions developed by Ricoh.

VAS: An MFP API that standardizes the meanings of simplified commands used by SDK applications when communicating with the MFP.

EAC The module which controls the serial command flow of the external controller connected via the VideoLink Board, making it possible for the external controller to initiate MFP operations such as print jobs, as well as the storage, deletion, and capturing of Document Server documents. In addition, this module also controls the display content of the MFP LCD for each operation initiated by the controller.

Note: This is only available on models capable of supporting an external controller.

1.3 Data Security

1.3.1 External I/F

The MFP is equipped with the following interfaces for connection with external devices:

- Serial I/F for LADP connection.
- Serial I/F for connection of external coin/card-operated devices.
- Serial I/F for connection of peripheral devices (e.g. DF, Finisher, LCT).
- Analog G3 FAX I/F (public telecommunications line), G4 FAX I/F (ISDN).
- Standard IEEE 1284 parallel I/F, Standard IEEE 1394 I/F.
- 100BASE-TX and 10BASE-T compatible network I/F
- Standard IEEE802.11b wireless LAN (option) network I/F
- Wireless LAN I/F
- Bluetooth I/F
- USB2.0 Type B I/F

1.3.2 Protection of Program Data from Illegal Access via an External Device

1. All of the above principle machine functions, as well as software for all shared service layers, run on the UNIX operating system as independent processes (data/program modules). Memory space is allocated specifically for each module, which makes it impossible for one module to directly access the memory space of any other.
2. Data transfer between modules is Unix socket-based, whereby communication is performed along ID-protected communication paths. This ensures exclusive connections among the modules present in the MFP, thereby preventing access by any module outside this predetermined set. For example, incoming CSS data will only be sent to those modules designed to perform CSS data operations. This arrangement prevents illegal access to networks and internal programs from an outside line.
3. All image data stored on the HDD or stored temporarily in the Image Memory is managed by a memory control module called the MCS (Memory Control Service), which ensures that the data can only be accessed by specified machine function(s). In addition, this arrangement prevents illegal access to this data from an outside line.

User data stored in the HDD, such as the Address Book data, is managed by the UCS module. Access to this data is not possible by any module except those predetermined modules in the MFP itself. This arrangement ensures that the data stored in the MFP cannot be accessed illegally via an external I/F.

4. Communication between the MFP and its peripherals is conducted via the peripheral I/F using Ricoh-unique protocols. These exchanges are limited to pre-determined commands and data, and only take place after the MFP has recognized the peripheral device. If the MFP receives illegal data from the peripheral, it will judge that a perhiperal device failure has occurred or that the device is not connected.
5. The MFP communicates with external coin/card-operated devices through the PEACE I/F in accordance with the same protocols used for its peripherals described in #4 above. It is possible to utilize such external devices in tandem with restrictions on the Available Functions for each individual user, in which case the device and MFP exchange the relevant information (e.g. User Code data).
6. With the @Remote function, the MFP is connected via the network to a Ricoh-developed device known as RC Gate, which is then connected to the @Remote Center. Before transferring any data, the MFP and RC Gate perform a two-way authentication process based on digital certificates, which ensures that the MFP cannot connect to any device other than RC Gate. Communication between RC Gate and the MFP modules responsible for @Remote operations is performed over exclusive socket-based connections, as described in #2 above. In addition, it is also possible to change the MFP settings to prohibit @Remote communication.
7. Communication with an external controller is performed via the VideoLink board over a serial connection, which uses a Ricoh-original communication protocol. The internal arrangement is designed such that the external controller cannot gain access to the MFP internal modules until after it has successfully cleared the device registration process.

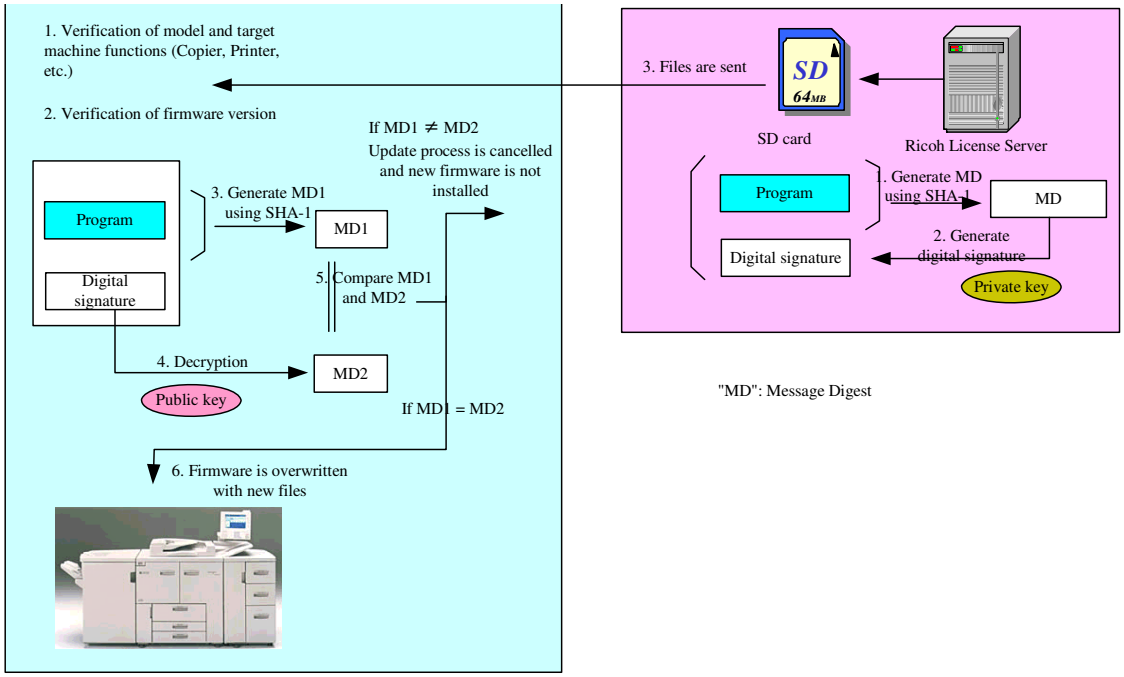
   In addition, although the external controller is capable of operations such as issuing printing instructions, sending data for storage in the MFP Document Server and downloading/restoring data to and from the MFP, the controller is not able to alter any of the original files already stored in the MFP. (e.g. When the controller restores a file back to the MFP, it is always saved as a separate file).

1.3.3 Firmware Update

It is possible to update the firmware and application programs stored in the MFP using an SD card or via a remote connection.

Firmware Installation Using an SD Card

- Since SD cards themselves are generic items that are widely available for purchase in the field, the following process is used to prevent the illegal introduction of data and programs into the MFP via this storage media. Briefly stated, a license server assigns a digital signature to the software, which is then used by the MFP to authenticate the program.
  1. The Ricoh license server applies the SHA-1 algorithm (Secure Hash Algorithm 1) to the program to generate the value MD1. A private key is used to encrypt this value, which is then used as the firmware's digital signature.
  2. The firmware in the SD card is introduced into the MFP from the SD card slot.
  3. The MFP checks the firmware to identify the type (e.g. Printer, FAX, Copier), verify that the model name is the same as its own, and verify that the firmware version is newer that the one already installed.
  4. The MFP then applies SHA-1 to the program to generate MD1, after which it uses a public key to decrypt the digital signature to generate MD2.
  5. If MD1 = MD2, the firmware update process begins.
- This use of a public key to decrypt the digital signature allows the MFP to verify that that there has been no illegal alteration of the data.
- The basic identifying information of the firmware (version, type, etc.) is stored in the MFP as the update is being performed. Therefore it is possible to retry the update with the same SD card in the event that the update is interrupted, e.g. if the MFP main power suddenly turns off. After recovery is initiated, the MFP checks to see that the data in the SD card has not been altered, and then resumes the update.

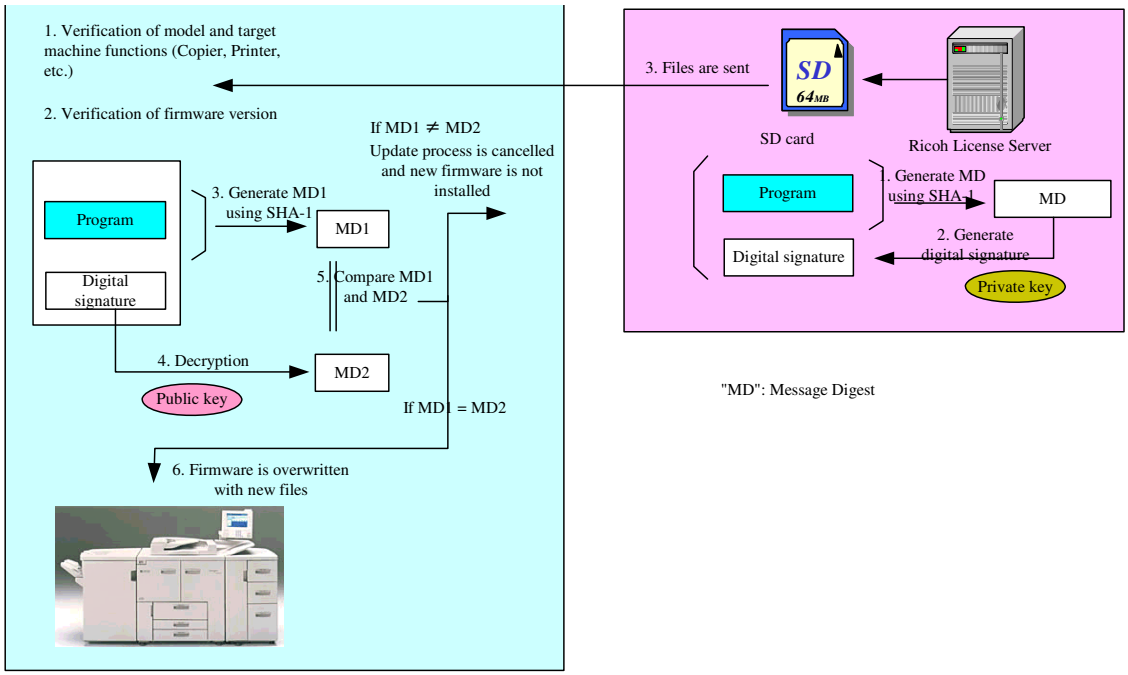


Firmware Installation Using an SD Card

Remote Firmware Installation

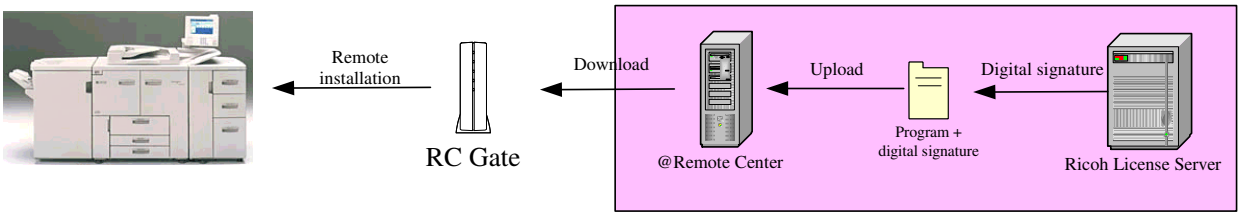
- In addition to using an SD card, it is also possible to update the firmware by transmitting the firmware files to the MFP via a remote connection. Since these files are transmitted over public Internet communication paths in some cases, routed through multiple servers before reaching their destination, it is necessary to use the authentication process described above for remote update as well. The process for remote updates is virtually the same as that for the SD card-based update described above, with the following differences:
  - Remote headers are attached to the digital signature before sending the files to the MFP.
  - If the update is interrupted for some reason, e.g. a power cut before the update is completed, it is possible to retry the update by resending the file.

- There are two scenarios in which a remote firmware update can be performed, the process for which is the same (see illustrations below). In addition, all of the security features described above are used in each case.
  - The update is performed by a customer engineer (CE) in the field via a PC.
  - The update is performed from the @Remote Center, usually by center personnel or a CE



Remote Firmware Installation From a Client PC

(performed by a CE)



Remote Firmware Installation From the @Remote Center

1.4 Authentication, Access Control

1.4.1 Authentication

- The MFP requires all users to go through a username and password-based authentication process before MFP operations can be performed. This is true in cases where the user attempts to access MFP functions via the operation panel as well as via a network connection.

- There are four types of User Authentication:
  - Basic Authentication
  - Windows Authentication
  - LDAP Authentication
  - User Code Authentication

- As the authentication server, the MFP can be used for Basic Authentication. A Windows NT4.0 server, Windows 2000 server or server2003 can be used for Windows Authentication. Finally, an LDAP server can be used for LDAP Authentication.

- Usernames are in US-ASCII format, and therefore cannot contain spaces, colons or double quotation marks. The maximum length is 32 characters. The password is also in US-ASCII format, with a maximum length of 128 characters for general users and 32 characters for administrators.

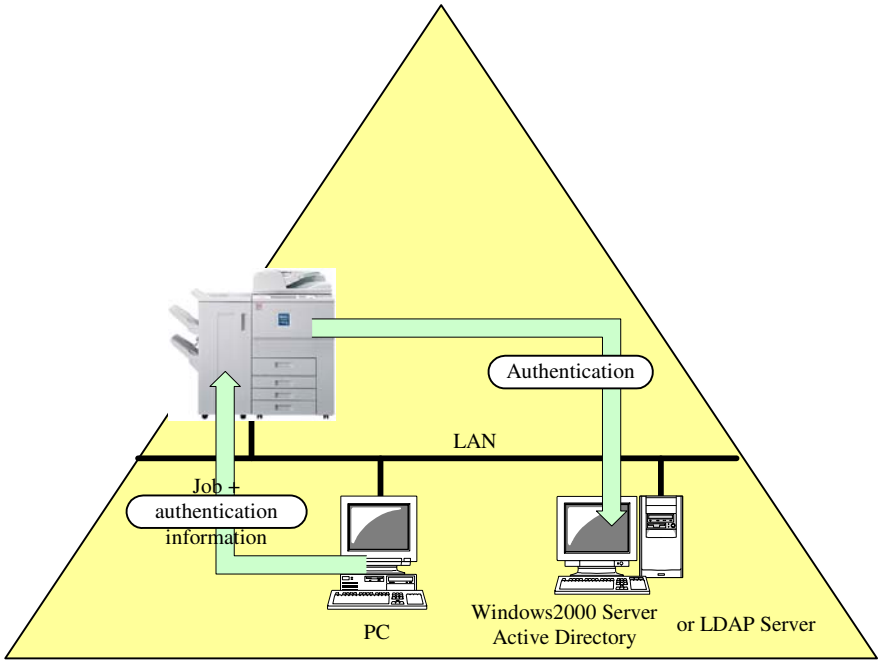
- Before authentication at the MFP operation panel can be performed, uses must be pre-registered in the MFP. The communication path can be encrypted using SSL, however for environments that do not support SSL protocol, the password itself is encrypted using an encryption key provided by the user. To do this, however, the Printer/Scanner option must be installed.

- To minimize the impact of brute-force attacks, the MFP will delay sending the authentication results back to the originator in cases where authentication has failed.

- The information for performing the authentication of administrators is encrypted and then stored in the MFP in non-volatile memory. Therefore, it is always possible to perform authentication on administrators even when a failure occurs with the MFP HDD or one or more of the external authentication servers is down.

- With Windows Authentication, NTLM Authentication is performed with the specified domain controller, after which an attempt is made to establish an LDAP connection with the active directory. The email address, FAX number and GUID are then obtained for users who successfully clear the authentication. The same NTLM Authentication process is performed for LDAP Authentication as well, after which an LDAP search is performed to obtain the user's email address, FAX number and GUID.

- Active sessions will expire under the following conditions:
  - When the “Logout” key is pressed in User Tools
  - When the MFP enters Low-power Mode or Energy Saver Mode
  - After a pre-determined amount of time has passed



Windows Authentication, LDAP Authentication

1.4.2 Access Control

Users logged in as administrators are able to make changes to the following security-related settings:

- Access restrictions for individual users: Access to each principal MFP function can be controlled for each individual user. In the case of Windows Authentication, it is also possible to set such restrictions for global groups as well as individual users.
- To prevent the impersonation of the user by a third party, it is possible to set the MFP so that the email address of the logged-in user is set as the “From” field whenever an email is sent. Users who do not have a registered email address would not be able to send email.
- It is possible to prohibit the sending of email to any address except those that have been approved. This is true for addresses that are entered manually as well as those registered in the address book.
- It is possible to prohibit unauthenticated users as well as general users from viewing or making any changes to the User Tools settings.
- An 8-digit protection code can be assigned to each individual address book entry to protect its contents, so that users cannot freely select addresses to send email and/or impersonate other users as the sender. If the code entered by the operator does not match the one in the MFP, no operations can be performed on the address. In addition, it is possible to create an ACL for each individual address book entry and Document Server document at both the individual user and group levels.

1.5 Administrator Settings

In order to spread the risk of malicious operations by a single individual with administrator-level access rights, the MFP allows the following five types of administrators to be registered.

1. **Machine Administrator:** Manages the User Tools settings and ensures that the MFP is always in good working order.

2. **Network Administrator:** Manages the network-related User Tools settings and ensures that protections against illegal remote access are properly maintained.

3. **Document Administrator:** Manages the document storage-related User Tools settings, access rights for stored documents and the stored documents themselves.

4. **User Administrator:** Manages the user information stored in the address book, as well as the access rights to this information.

5. **Supervisor:** Manages the passwords of the four administrators listed above.

- Each individual administrator is able to change their own username and password, however they are not able to change the usernames and passwords of other administrators.

- It is possible to assign two or more (or all) of the above titles to the same individual user.

- If the Supervisor forgets any of the passwords, the information cannot be retrieved by customer engineers or any other technical personnel. The only way to retrieve the information is to initialize the MFP back to its factory shipment condition. If this is done, all of the user information, document data and settings performed since machine installation are initialized (erased).

1.6 Data Erase/Overwrite

1.6.1 Overview

- A wide variety of data is stored in MFP memory both permanently and temporarily. The HDD stores data such as image data, email destinations, and address book data containing various types of user information. In addition, the NVRAM stores data such as User Tools settings, while the FCU stores FAX reception image data. Data Erase/Overwrite refers to the actual erasing or overwriting of data stored on the magnetic media of the MFP with a combination of 0's and random values, so as to effectively "erase" the original data by making it completely indecipherable. Although the MFP does erase the page location data, i.e. storage location information that is absolutely necessary to access image data on the HDD, the image data itself remains in the temporary storage stored area of the HDD. However, the Data Erase/Overwrite feature renders this image data indecipherable, even in the unlikely event that the HDD were removed from the MFP and an analysis performed by a third party with the intent of reconstructing the original data. .

- In rare cases, performing the overwrite just once may not be enough to completely alter the magnetic pattern of the data to an indecipherable level, leaving the possibility of partial reconstruction of the original data. Because of this, Data Erase/Overwrite is performed using the following methods, which overwrite the data three times to ensure that reconstruction is not possible.
  - The DoD method, developed and required by the U.S. Department of Defense
  - The NSA method, developed by the U.S. National Security Agency
  - The Ricoh randomized-value method, a Ricoh-original method which overwrites data using randomly-generated values

  Note: The first two methods automatically perform the overwrite three times. The Ricoh method can be set to "three times," in which case the effectiveness is the same as the first two methods.

- There are two main types of Data Erase/Overwrite: Auto Erase Memory and Erase All Memory. Auto Erase Memory overwrites the data at the end of each job, whereas Erase All Memory overwrites the entire contents of the temporary and management areas of the HDD as well as the data in the NV-RAM and FCU (details below). Both functions are provided to the field as optional software stored on SD cards, which must be inserted in the MFP slot at all times in order to use the function. If the card is taken out of the slot, Data Erase/Overwrite cannot be used.

1.6.2 Auto Erase Memory

- The main purpose of this feature is to automatically overwrite data stored to the processing region of the HDD, i.e. data that is saved to the HDD for purposes of MFP internal processing only, of which users are normally unaware. Auto Erase Memory prevents this unnecessary data from remaining in the HDD by overwriting it as soon as it is no longer used by the MFP.

- In addition, it is also possible to manually erase data that was intentionally saved to the HDD, such as Document Server documents.

Note: If the timing of the Auto Erase Memory overwrite coincides with a command received by the MFP for any other operation, this other operation is given priority. The data overwrite is then performed once this other operation is completed.

1.6.3 Erase All Memory

- This function overwrites the contents of every region of the HDD and initializes the contents of the NV-RAM and FCU. Since this operation makes it impossible to retrieve or reconstruct the contents of the HDD in addition to initializing the FCU data, Erase All Memory is primarily used at machine disposal or at the conclusion of a machine lease or rental contract. It is therefore necessary to back up the information mentioned above or send it to a PC for storage before executing Erase All Memory.

- By initializing the contents of the NVRAM to their default values, this feature prevents information that is unique to a particular installation environment from being released to third parties (e.g. IP address, control lists and other administrative information).

- The execution of this feature does not clear engine-related information such as the value of the total counter, or engine-related adjustment settings contained in SP mode and UP mode.

1.7 Data Protection

1.7.1 Protection of Address Book Data

- The tables below show the various types of data stored in address book entries as well as the operations that general users/groups, owners and User Administrators can perform on this data. It is possible to assign general user access rights to individual users as well as to groups. Users who have not been assigned any access rights are not able to view the contents of address book entries.
- There are four types of access rights: View, Edit, Edit/Delete and Full-Access. These settings can be changed by Group and User Administrators, users with Full-Access rights and the user who registered the entry. User Administrators are also able to change user passwords.
- The data in the address book is stored in the MFP HDD. This data can be encrypted before it is stored if the Printer/Scanner option is installed.

			General Users Groups	Owner of the Entry (User)	User Administrator
General Info.	Reg. No.	00001	R	RW	RW
	Name	Taroh Ricoh			
	Email address	taroh@ricoh.co.jp	Use ACL		
	FAX No.	1234-5678			
	…	…			
Detailed User Info.	Login password	**********	–		R
	Authent. Username	Taroh			
	Authent. Password	**********			
	Protection Code	****			
Admin. Data	Login Username	Taroh	–	R	RW
	Authorized Usage	Copier			
	…	…			
ACL Information		00002=R--- 00003=RW-- 00004=RW-O 00005=RWDO …	Use ACL	RW	RW

Access Rights Management Structure for the Address Book

		View	Make Changes	Delete Entries	Change ACL Settings
R	View	Yes			
RW	Edit	Yes	Yes		
RWD	Edit/Delete	Yes	Yes	Yes	
RWDO	Full-Access	Yes	Yes	Yes	Yes

Access Rights and Operations for the Address Book

1.7.2 Document Server Documents

- The tables below show the various types of data stored in Document Server management files, as well as the operations that general users/groups, owners and User Administrators can perform on this data. It is possible to assign general user access rights to individual users as well as to groups. Users who have not been assigned any access rights are not able to view the contents of these files.
- There are four types of access rights: View, Edit, Edit/Delete and Full-Access. These settings can be changed by Group and User Administrators, users with Full-Access rights and the user who registered the entry.
- A password can be assigned to each document (4–8 numeric characters long), ensuring that the document cannot be accessed unless the correct password is entered first. In addition, by enabling the Document Lock feature, the MFP will deny any attempt to access a given document if an incorrect password is entered ten times consecutively. This setting can be enabled and disabled in System Settings by the Document Administrator.
- The Document Administrator can also change the passwords for individual documents without having to clear a password-based authentication process.

			General Users	Document Owner (User)	Document Administrator
General Info.	Document No.	00001	Use ACL	RW	RW
	Document Name	Meeting files			
	Thumbnails				
	Bibliographic Info.				
	Pg. 1 Image Data				
	Pg. 2 Image Data				
	・・・	・・・			
Detailed User Info	Document Password	********	—	W	W
ACL Information		00002=R--- 00003=RW-- 00004=RW-O 00005=RWDO ・・・	Use ACL	RW	RW

Access Rights Management Structure for Stored Documents

		View Bibliog. Information	View Thumbnails	Printing, Sending	Edit Image	Delete Pages	Delete Doc.	ACL Settings
R	View	Yes	Yes	Yes				
RW	Edit	Yes	Yes	Yes	Yes	Yes		
D	Edit/Delete	Yes	Yes	Yes			Yes	
RWOD	Full-Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Access Rights and Operations for Stored Documents

1.8 Additional Methods for Increased Security

In addition to the above, administrators can also perform the following settings as needed to provide additional security.

- Prohibit the viewing or changing of all security-related settings from inside SP Mode (Service Program Mode).
- Prohibit access to SP Mode without authorization from the user.
- Prohibit any operations from being performed on jobs in progress by any user except the one who initiated the job.
- Prohibit individual users from registering or making changes to address book entries.
- Allow only registered email addresses to be set as the destination when sending email from the MFP (prohibit the sending of email to destinations which were manually entered).
- Specify the encryption key that will be used to encrypt the password when sending the information over communication paths that do not support SSL protocol.

2 Principle Machine Functions

2.1 Copier

2.1.1 Overview of Copier Operations

- When a copy job is initiated, the scanning engine scans the original and forwards this data to the controller to be printed out from the printing engine. If “Store File” is selected at this time, the image data is also stored in the HDD.

- The Document Server function can also be used to scan images and store them directly to the HDD without printing them out, as well as to print out documents already stored in the HDD. In addition, a password can also be assigned when scanning a document for storage to the HDD, requiring the operator to input the correct password to print out the document.

- User Codes can be enabled to restrict access to the Copier function.

2.1.2 Data Flow

- A copy job is initiated from the Copier function, which sends a job start command to the ECS. In turn, the ECS instructs the scanner engine to begin scanning and the MCS to secure the necessary amount of memory in the volatile RAM (Image Memory RAM). The scanned image data is then temporarily stored in the Image Memory by the IMH, after which the ECS instructs the IMH to retrieve the data and send it on to the printing engine. The data is printed out according to the specified number of pages, after which the ECS erases the image data via the MCS.

- When scanning documents for direct storage to the HDD or for simultaneous storage and copying, the data is sent via the MCS and saved to HDD memory. When using the Document Server function to print out documents already stored in memory, the operator selects from among the documents displayed, i.e. only those MCS-managed documents stored in the HDD using the Copier function. The start command is then sent to the ECS and the document is printed out.

- The Copier function keeps track of how many copies have been made in each copy mode by storing these values in the non-volatile RAM (NV-RAM). These counters are incremented after each page is printed and at the conclusion of every job. These values can be viewed on the operation panel from inside SP mode or in machine service reports.

2.1.3 Data Security Considerations

- Since the page location data is erased at the conclusion of every copy job, it is not possible to perform a job re-print on the same data. In addition, since the Copier function itself does not have any external I/F and does not perform any data exchanges or communication with external devices, it is not possible for any illegal external data to be introduced through the Copier function.

2.1.4 Copy Job Protection

- When User Authentication is enabled, if one user attempts to cancel a copy job in progress that was initiated by a different user who had logged out before the end of the job, the MFP will prompt the operator for the username and password of the user who originally initiated the job. The only individuals who can successfully cancel the job are the Machine Administrator and the user who initiated the job. Also, the Machine Administrator always has the ability to perform operations on copy jobs in progress (e.g. job cancel).

2.1.5 Protection of Document Server Documents

- When User Authentication is enabled, it is possible to assign specific access rights to individual documents when storing them to the HDD, which limits what operations can be performed on them (e.g. View, Edit, Delete, Full-Access).

- Users who have viewing access rights can view and print out documents but cannot delete or make any changes to the document (incl. filename). Users who have Full Access rights can perform all operations on the document including printing, sending, editing and deleting the document, as well as making changes to access rights settings. Users who have not been assigned any of these access rights cannot perform any of these operations, and are also prohibited from selecting documents in the document list screen.

- Refer to section 1.8.2 for details on the Document Lock feature.

2.1.6 Protection of Copier/Document Server Features

- When Machine Administrator Authentication is enabled and the Menu Protect setting in Copy/Document Server Features is set to “Level 2”, changes to the Copy/Document Server Features can only be performed by the Machine Administrator. With a setting of “Level 1”, users are able to change a select number of items, while a setting of “None” allows users to change all items.

2.1.7 Restricting the Available Functions for Each Individual User

- When User Authentication is enabled, it is possible to then allow or prohibit the use of specific Copier functions for each individual user. For example, with color products, it is possible to allow or prohibit the use of B/W, full-color, two-color and single-color modes for each user. Therefore, if a user were assigned restrictions that limited him or her to B/W copies, even after having successfully logged in, they would not be able to make color copies.

- It is also possible to increase the level of security by using the above features in tandem with an external charge device or key counter. This is because operators would not only be prompted to enter a user name and password, but would also be required to clear the usage restrictions imposed by the external charge device or key counter itself (card, currency, etc.).

2.2 Printer

2.2.1 Overview of Printer Operations

- The Printer function can be divided in to main processes: 1) converting the printer language data received by the MFP into image data, and 2) printing out this image data onto the paper in accordance with the specified job settings. The former is performed by the printer language processing subsystem, while the latter is performed by the printing subsystem.

- Once the data sent from the host computer is accepted, and the processing subsystem begins processing the new print job, a print job log entry is created (temporary entry). The entry is registered as soon as the job is completed.

2.2.2 Data Flow

Printing Unencrypted Image Data

- As stated above, the printer language-encoded data sent from the host computer is interpreted by the language processing subsystem, after which it is converted into image data and then stored temporarily in the Page Memory in binary bitmap format. Once this is done, the data is compressed in Ricoh original compression format, and stored in the HDD page by page. If the MFP does not have an HDD, the compressed data remains in the Page Memory and is treated the same as data written to the HDD.

- When Spooling is enabled, the incoming data is stored directly to the spooling area of the HDD. Following this, the data is sent to the language processing subsystem, where it is interpreted and converted to image data page by page. Before it is printed out, the spooled data can be deleted from the “Spool Printing” list in Web Image Monitor, or “Spooling Job” list on the MFP operation panel. The data is developed page by page in the order in which it was converted (beginning from page 1), however the physical orientation of each page on the paper may differ depending on the job settings received from the printer driver (e.g. duplex vs. simplex, usage of Booklet or Stapling features, etc.).

- When Image Spooling in enabled, all pages of the incoming data are converted to image data before being stored to the HDD. The data stored in the HDD is then printed out via the printing engine.

- From the printer driver, it is possible to select the following printing methods: Normal Print, Sample Print, Locked Print, and Save to Document Server. The data processing flow varies depending on the method used, since some operations are not supported with some printer languages (see below).

- With Normal Print, the page location data for the image data stored in the HDD is erased at the conclusion of the print job or when the main power is turned off. When Sample Print is selected as the job type, the document will remain in the HDD as a Sample Print document even after the sample set is printed out. Additional sets of this document can then be printed out from Web Image Monitor or the MFP operation panel, after which the page location data is deleted at the conclusion of the job.

- When Locked Print is selected as the job type, the image data is saved directly to the HDD as a Locked Print document, without being printed out. Locked Print documents stored in the HDD can then be printed out from Web Image Monitor or the MFP operation panel, after which the page location data is deleted at the conclusion of the job.

- When Save to Document Server is selected as the job type, the image data is stored directly to the HDD as a Document Server document, without being printed out. The necessary bibliographic information for the image data is stored in the HDD along with the image data itself. The bibliographic information is part of the print management data, and includes information such as the page size, paper type and number of sets.

  Document Server documents stored in the HDD can then be printed out from the MFP operation panel or from Web Image Monitor, after which they remain stored in the HDD. These documents remain stored in the HDD even if the main power is turned off.

- When Normal Print is selected as the print job, the print management data[*1] for the image data stored in the HDD is stored in volatile RAM memory in Ricoh original format. It is erased at the conclusion of the job, together with the page location data.

- When Sample Print or Locked Print is selected as the print job, the necessary bibliographic information for the image data is stored in the HDD along with the image data itself.

- The user ID can be registered in the printer driver UI, which machine operators can then use as a unique marker for documents to differentiate them from one another. Once a user ID is registered, it is used for the Sample Print and Locked Print printing methods, and also appears in the printing history. In addition, it is also possible to set the password for Locked Print documents as well as the username and password for Document Server documents in the printer UI.

- Once the necessary username and password have been set in the printer driver, it is possible to perform User Authentication when sending data to the MFP. The username and password are sent along with the printing data as authentication data. If authentication fails, the printing data sent to the MFP is destroyed and the job is cancelled.
  Note: See section 1.82 for details on how to assign a password to individual documents after they are stored.

- The print job history is stored in volatile memory and is therefore deleted when the MFP main power is turned off. The information stored includes the username, number of pages, the time the print job was performed, and job status/results. The print job history can be accessed from SmartDeviceMonitor for Client, which retrieves the information via a Ricoh-original MIB over an SNMP connection.

- [*1]: The “print management data” is managed and maintained by the Printer function itself, and contains information such as the size of the paper for printing, job settings (simplex or duplex, etc) and general job data (time, username, etc.). This is not the same as the “page location data” for the image data stored in the HDD.

Printing Encrypted Image Data

- With PDF Direct Print, it is possible to print out an encrypted PDF file. The password is registered in the Printer function via Web Image Monitor or the MFP operation panel, or is set inside DeskTopBinder (incl. the Function Pallet). When the printer receives the file, the printer language processing subsystem (PDF interpreter) temporarily stores the file directly to the HDD. Once the file is recognized as an encrypted PDF file, the password registered in the MFP is compared to the password sent along with the file. If they do not match, the data itself will not be decrypted correctly, causing an error to occur and the job and data to be erased. If they do match, the data will be decrypted correctly. After this, the decrypted data is converted to image data, stored to the HDD and then follows the normal process described above.

- When Spooling is enabled, the incoming encrypted data is stored directly to the spooling area of the HDD. Following this, the first page of the data is then sent to the PDF interpreter to be interpreted.

- It is also possible to set the MFP to prohibit the printing of PDF files. PDF files for which this setting is used cannot be printed out when received by the MFP, as the MFP resets the job and deletes the data.

2.2.3 Data Security Considerations

Printing Unencrypted Image Data

- The language processing subsystem only allows data in legal format to be processed. In the event that illegal data is received, the subsystem will declare an error and cancel the processing session.

- When User Authentication is enabled, the MFP will only accept printing data that contains a username and password that matches those of a pre-registered user. Any such data is destroyed, preventing the introduction of illegal data. When the Printer's authentication mode is set to Simple Authentication, the MFP does not perform authentication on data sent from users that have been given "Guest" status.

- The password necessary for authentication is encrypted before the printer driver sends it to the MFP. When performing the encryption, it is possible to use a key that is common to both the driver and the MFP, known as the driver encryption key. It is also possible to encrypt the password using Simple Encryption, which does not use the driver encryption key. If the "Permit Simple Encryption" setting in the MFP is disabled, the MFP will only accept passwords that have been encrypted using the driver encryption key. Therefore under these conditions, even when the MFP receives data with passwords encrypted using Simple Encryption, the job will be reset and the data will not be printed out. It is therefore recommended to use a stronger encryption method, which ensures that a third party attempting to tap into the communication path will not be able to surmise the actual password and impersonate the password holder.

- In addition the printing data itself, it is also possible to encrypt the communication path by selecting “IPP over SSL” as the network communication protocol.

- Although the printer job history can be accessed by any individual, it is possible to set the MFP to display user information in the form of asterisks (“****”).

- When Locked Print is selected as the job type, and the operator wishes to print out a Locked Print document stored in the MFP from the operation panel or Web Image Monitor, it is necessary to enter a password before the job can be performed. If this password does not match the pre-registered password, the operator is not allowed to retry. This prevents illegal access to Locked Print documents.

- In addition, it is possible to enable the Document Lock feature, whereby the MFP will deny any attempt to access a given document if an incorrect password is entered ten times consecutively. This protects documents from attempts to crack the password via brute-force attacks.

- Although it is possible to download illegal fonts and firmware for storage to the HDD, the language processing system is only capable of accepting legal data in pre-defined formats. Since the MFP will reject such data, the data is not able to introduce any illegal programs or be processed by any MFP modules.

Printing Encrypted Image Data

- As stated above, PDF Direct Print handles the sending of encrypted PDF files. The main use of this function is for sending encrypted PDF files in cases where it is not possible to encrypt the communication path itself. Once the password for opening the file has been programmed from the MFP operation panel or from Web Image Monitor, it is possible to then safely send the printing data over the communication path. Even if the PDF file sent as printing data were intercepted on its way to the MFP, the contents of the data are secure since the data is already encrypted.

- As stated above, the password for opening the file can also be programmed from inside DeskTopBinder. Since this allows the user to assign unique passwords to each individual PDF file, this function can be used to distribute confidential documents. Since both the printing data and distributed PDF file itself are sent along the communication path in an encrypted state, their contents are secure. Even if the PDF file were intercepted at the PC or server point, the contents of the file cannot be accessed. In addition, the password itself is also protected since it is encrypted using the group password already programmed in DeskTopBinder.

- As stated above, the PDF interpreter cross-references the password programmed in the MFP with the encrypted password sent from the PC, and destroys the incoming data when these passwords do not match. In addition, the incoming data is also destroyed if accompanying information alerts the MFP that printing of this file is prohibited. Since the MFP will reject such data, it is not possible for the data to introduce any illegal programs or be processed by any MFP modules.

2.3 Scanner

2.3.1 Overview of Scanner Operations

- Depending on the settings selected, the Scanner function does one of the following:
  1) Saves the scanned image to the HDD and then sends it via the network I/F as an email (via an SMTPserver), to a folder (FTP server, client PC with Windows 98 or newer), or forwarding server (via ScanRouter V2/EX),
  2) Saves the scanned image to the HDD alone without forwarding it, or
  3) Temporarily stores the image to the HDD and then forwards it to one of the destinations mentioned above.

  With the third option, the page location data for the data temporarily stored to the HDD is deleted once the destination receives the transmission, or after the maximum number of transmission attempts has been reached.

- With the TWAIN I/F, the TWAIN driver can initiate a scanning job under specified conditions from a network-connected client PC, after which the image is sent back to the TWAIN driver.

- Access to the Scanner function itself or to specific features can be restricted with the use of User Authentication, the Available Functions settings for each individual user, and an external coin/card operated device. Use of the TWAIN feature is only allowed after a crosscheck with the User Code, User ID and password pre-programmed in the TWAIN driver U/I.

- Operational log entries are created for both scanning and forwarding jobs. The forwarding results can be printed out or viewed directly from the operation panel (“Scanned File Status”). These results are stored in non-volatile memory, i.e. the data is preserved even after the MFP main power is turned off.

2.3.2 Data Flow

- The raw image data sent to the RAM managed by the IMH goes through MH/MR/MMR/JPEG compression or is left uncompressed, depending on the operator’s settings. TIFF headers are attached to all data except JPEG-compressed files. The data is then sent over the network in a commonly used image file format. In addition, it is also possible to convert these files to multi-TIFF or PDF format before they are sent.

- When authenticating with User Codes, the User Code data is sent from the TWAIN driver in binary format (unencrypted). However when using User Authentication with the TWAIN driver, the password is encrypted before being sent. In addition, the password set from the MFP operation panel for accessing Document Server documents is not sent to DeskTopBinder or DeskTopEditor for Production. This password is only used for authentication when downloading the requested Document Server documents to these PC applications, or for access control with remote forwarding.

2.3.3 Data Flow Security Considerations

- Forwarding operations are unidirectional, sending image data to pre-programmed email addresses, folders and forwarding servers only. Since there is no receiving aspect, it is not possible for the Scanner function to receive any illegal data from an external I/F.

- When sending image data to an SMTP server, it is possible to introduce an authentication process at the POP server before making the connection to the SMTP server (POP before SMTP), and at the SMTP server itself (SMTP authentication).

- When sending image data to an SMTP server or Windows PC (SMB), it is possible to encrypt the password using a DIGEST-MD5 or CRAM-MD5 algorithm.

- The TWAIN driver will not process any binary data that does not conform to the predetermined protocol of the command I/F. The protocols used are SNMPv1, v2 and v3.

2.3.4 Protection with Scanning, Sending Operations

- It is possible to set the MFP/related software to perform the following operations:

  Require user identification when sending to a forwarding server. By requiring the operator to select from pre-registered email destinations and then input a protection code, it is possible to protect against sender impersonation.

  Require user ID and password authentication before data is forwarded to an SMTP server or folder (Basic Authentication). This makes it possible to control the sending of data for each registered user.

  Require a numerical protection code (up to 8 digits long) when the operator selects a document stored in the MFP for sending, which protects against unauthorized email sending.

  Perform user access restrictions and further prevent any impersonation of the sender:

  When User Code Authentication or Basic Authentication is enabled, and a successfully logged-in user performs a sending operation, this user is automatically set as the sender of the email. If this user does not have an email address, it is not possible to send the email.

  Limit the sending of email to destinations that have already been programmed in the MFP. This can be done using the "Restrict use of destinations" setting of the Extended Security feature.

  Require user ID and password authentication when attempting to retrieve email addresses from an LDAP server.

  Set the MFP so that it is not possible to register email addresses in the MFP, whether obtained from an LDAP server or entered manually.

- In order for the MFP Scanner to retrieve the address book data of individual registered users from the forwarding server, Basic Authentication must be enabled at the MFP and the forwarding server software must be ScanRouter V2/EX or later. In all other cases, the MFP Scanner is either able to obtain shared address book data only via port 3670 (Basic Authentication disabled, all versions of ScanRouter), or is not able to obtain any data at all (Basic Authentication enabled, ScanRouter V1). The data obtained from the forwarding server is then deleted at the MFP when the user logs out.

  Note: Administrators cannot perform these operations.

- By enabling Basic Authentication, it is possible to protect the destination information. For each destination, it is possible to assign an access level to each registered user (View, Edit, Delete, Full-Access). Users who have Viewing access rights for a particular destination can select the destination for forwarding, but cannot edit or delete the data. Users who have Full-Access rights can perform all functions including sending to the destination, editing and deleting data, and making changes to access rights settings. Users who have not been assigned any of these access rights cannot even view the destination list. Even when all of the above restrictions are enabled, User Administrators have Full-Access rights for all registered destinations. However since User Administrators cannot use the Scanner function, they are not able to send any data.

- When logged in with Basic Authentication, users are able to perform operations with either the forwarding feature or the TWAIN driver feature, not both. However with User Code Authentication, there are conditions in which one operator can utilize the Scanner via the TWAIN driver even while another operator is already logged in from the MFP operation panel (i.e. before the user logged in from the operation panel actually initiates a job).

- With the TWAIN feature, the user is logged out automatically as soon as scanning is complete. Also, the authenticated user and Machine Administrator are the only individuals who can interrupt a scanning job in progress. When the Stop key is pressed to interrupt the job, the MFP prompts the operator with the authentication dialog.

2.3.5 Protection of Document Server Documents

- When Basic Authentication is enabled, it is possible to assign access rights to individual documents when scanning them for storage in the Document Server (View, Edit, Delete, Full-Access). These access rights are applied even when accessing the document from DeskTopBinder or DeskTopEditor for Production. Users who have Viewing access rights can send the document but cannot delete or make any changes to the document (incl. filename). Users who have Full-Access rights can perform all functions including sending, editing and deleting the document, as well as making changes to access rights settings. Users who have not been assigned any of these access rights cannot perform any of these operations, and are also prohibited from selecting documents in the document list screen. Even when all of the above restrictions are enabled, Document Administrators have Full-Access rights for all registered documents. However since User Administrators cannot use the Scanner function, they are not able to send or store any data.

- It is also possible to assign a password to individual documents when scanning them for storage in the Document Server. After this, the document cannot be sent unless the correct password is entered. Additionally, when the Document Protect feature in System Settings is enabled, the MFP will deny any attempt to access a given document if an incorrect password is entered ten times consecutively.

2.3.6 Protection of Sending Results and Status Information

- When Basic Authentication is enabled, authenticated users are only able to view the sending results for the jobs that they performed. Results for jobs that other users performed are displayed as asterisks ("***"), preventing any leakage of information to third parties. The information is hidden in this way when displayed on the LCD, as well as when the results report is printed out. When Basic Authentication is enabled, entries in the sending results report can only be deleted by the user who performed the particular job. This prevents operations from being performed on these entries by third parties.

- Even when all of the above restrictions are enabled, Machine Administrators have Full-Access rights for all log entries. Machine Administrators are able to view and print out all entries.

- By default, the sending results log is automatically printed out when the maximum number of entries has been reached. It is possible to disable the automatic printing out of this log in Scanner Features, which ensures that the information on the log is not leaked to unauthorized third parties, and also allows administrators to keep a record of every transmission job performed. However, when the log reaches the maximum number of entries (with this setting disabled), the MFP displays an alert message to this effect and gives the Machine Administrator the option of printing out the log.

2.3.7 Protection of the Scanner Features Settings

- When User Authentication or Administrator Authentication is enabled, users and administrators must be authenticated before they are allowed to make any changes to the settings in Scanner Features. When Machine Administrator Authentication is enabled and the Menu Protect setting is set to "Level 2", changes to the Scanner Features settings can only be performed by the Machine Administrator. With a setting of "Level 1", users are able to update the delivery server destination list as well as change the file compression and email display language settings (System Settings). With a setting of "None", users are able to change all items in Scanner Features.

- As explained above, the email forwarding feature sends data from the MFP to external destinations via the network. By changing the network traffic-related settings, which can only be performed by Network Administrators, it is possible to prohibit or limit the conditions under which emails from the MFP are actually forwarded to their destinations.

2.3.8 Terminology

- **SMTP** (Simple Mail Transfer Protocol) [RFC2822]: A protocol used for the transmission of email over the Internet.
- **SMTP-AUTH** (SMTP AUTHentication) [RFC2554]: The protocol used for authentication when connecting to an SMTP server.
- **POP3** [RFC1939]: An email transfer protocol used when receiving email.
- **POP Before SMTP**: An authentication mechanism using POP3 protocol, developed to guard against SPAM mail (email sent indiscriminately to a large number of destinations).
- **SASL** (Simple Authentication and Security Layer) [RFC2222]: A framework that provides a common authentication processing mechanism for protocols that may require authentication, such as SMTP, POP3 and LDAP.
- **CRAM-MD5** [RFC2195]: A message digest functional algorithm that uses the MD5 algorithm to encrypt the challenge string and password.
- **DIGEST-MD5** [RFC2831]: A message digest functional algorithm developed as a countermeasure to dictionary and brute-force attacks. DIGEST-MD5 also supports realm designation (FQDN).
- **LDAP** (Lightweight Directory Access Protocol) [RFC1777], [RFC2251]: A protocol used for accessing directory services that manage items such as user address books.
- **SMB** (Server Message Block): A protocol used to enable file sharing between Windows PCs.
- **FTP** (File Transfer Protocol): A protocol used when transferring files over a TCP/IP network.

2.4 FAX

2.4.1 Overview of FAX operations

- The FAX function sends the scanned image data from the scanner engine to the other party's machine via a telecommunications line as a G3 or G4 FAX. Conversely, the MFP will only accept incoming FAX data that conforms to G3/G4 standards. The incoming document is then forwarded on to the printer engine for printing out.

- For Internet FAX transmission, the scanned image data is sent to the DCS, where it is converted into file attachment format for email transmission, after which it is sent to its destination via the network I/F. Conversely, the email FAX data received as an Internet FAX is converted into image data and then forwarded on to the printer engine for printing out.

- It is possible to store transmission files in the Document Server for sending at a later time. The file is saved to the HDD, after which commands can be issued from the operation panel or through the network to send the file to its destination. Conversely, incoming FAX data can be stored in the Document Server for printing out at a later time. The incoming FAX is saved to the HDD, after which commands can be issued from the operation panel or via the network to print out the file.

- With PC FAX transmission, the image data received from the PC is then sent to its destination via a telecommunications line or network I/F.

- With all FAX transmission features, including Internet FAX, it is possible to restrict individual user access with the use of User Codes. For reception, it is possible to configure the MFP to receive only those transmissions accompanied by a predetermined code. Operational log entries are made for each transmission and reception job. This data is stored in non-volatile memory on the FCU, and can be viewed by printing out the Journal.

2.4.2 Data Flow

- After FAX transmission is initiated, the scanning command is sent to the ECS via the FCS, and the scanner engine is activated. At the same time, the data retrieval and transmission commands are sent to the FCU via the FCUH. The image data in memory is then sent from the scanning engine to the FCU, after which it is sent to its destination via the telecommunications line.

- With FAX reception, the incoming data is received by the FCU, which then sends the printing command to the FAX function via the FCUH and FCS. The FAX function then forwards the printing command to the ECS via the FCS, and the printing engine is activated. The FAX image data is then sent from the FCU to the printing engine for printing out.

- With Internet FAX transmission, the image data is sent from the FCU to the HDD and then on to the host I/F, which sends the data to its destination via the network. With Internet FAX reception, the image data is sent to the MFP over the network, after which it is sent to the FCU via the HDD and then stored in FCU memory. After this, the printing process is the same as described above.

- When sending a FAX that will also be stored to the Document Server, the image data is first stored in the HDD and then sent to its destination via the network or telecommunications line. Conversely, when receiving a FAX for storage to the Document Server, the image data is saved to the HDD.

- With PC-FAX transmission, the data sent from the PC is stored in the HDD, or in the FCU if the MFP does not have an HDD. After this, the transmission flow is the same as described above.

- With IP-FAX transmission, the data flow is the same as with normal FAX transmission described above, except that instead of being sent via the telecommunications line, the image data is sent from the FCU to the FCS and then transmitted over the IP network via the network I/F of the controller. Similarly, IP-FAX reception does not receive incoming data through the telecommunications line, but rather through the network I/F of the controller. After this, the data is sent from the FCS to the FCU and then printed out.

2.4.3 Data Security Considerations

- The FCU supports only G3 and G4 FAX protocols. Therefore, even if an initial connection is established with a terminal that does not use these protocols, the MFP will view this as a communication failure and terminate the connection. This prevents access via telecommunications lines and the FCU to internal networks, and ensures that no illegal data can be introduced via these lines.

- Internet FAX supports TIFF files and text-based email only, which is true for both reception and transmission. If the data received through this function is in any other format, a communication error will result.

- Internet FAX can also be set to forward incoming FAX data to specific destinations that have been preset in the MFP. With servers using SMTP reception/delivery, the receiver can set the server to prohibit the delivery of incoming Internet FAX documents from specific senders, restricting SMTP access.

- With PC FAX transmission, the language processing subsystem is only able to process data that conforms to PC-FAX standards. If any other type of data is received, an error will result and the processing will be terminated.

- IP-FAX uses SIP for session initiation. SPI is a protocol that conforms to the H.323 and RFC326-1 standards prescribed by the ITU-T Recommendations. If any data is introduced which does not conform to these standards during transmission or reception, it will not be possible to establish SIP-based communication and the connection will then be terminated. Once a session is successfully established, communication is only performed in accordance with ITU-T recommended G3 FAX protocol. Since the MFP does not support any other type of communication protocol, if it attempts to connect to another machine that is not a FAX, it will not be possible to establish G3-based communication and the connection will then be terminated.

- When User Authentication is enabled, it is possible to set the authenticated user as the “Sender” of the FAX data. Similarly, for Internet FAX transmission, it is possible to set the authenticated user as the “Sender” of the email, i.e. the user who appears in the “From” field of the email.

- It is possible to restrict the use of the FAX function to specific users as well as to specific Document server documents, preventing any unauthorized access to this information.

- In order to guard against the reception of unnecessary or unwanted data, such as SPAM email, it is possible to register a list of authorized senders so that the MFP only accepts incoming data from these senders. Conversely, it is also possible to register a list of unauthorized senders, so that the MFP rejects any incoming data from these senders.

- For more details, please refer to section 2.3.

2.4.4 Protection of the Journal and Documents in Document Server Storage

- When User Authentication is enabled, only authenticated users are permitted to perform any changes to the documents they transmitted, including deleting or canceling a transmission job or adding address(es). When the Journal is printed out, only the results for the authenticated user are shown on the printout.

- The only operation Machine Administrators are capable of performing on FAX jobs is job cancellation. They are not authorized to perform other operations such as adding or deleting destinations. Also, when the Machine Administrator prints out the Journal, the communication results for all users are printed out on the report.

2.4.5 Protection of FAX Transmission Operations

- By setting restrictions on address book destinations in addition to enabling User Authentication, it is possible to limit access to the destinations listed in the address book. After clearing authentication, general users are able to select only those destinations that have been set to allow this. In addition, the MFP can be set so that users can only transmit data to destinations registered in the MFP.

- It is possible to assign access restrictions to individual Document Server documents, so that only users with the required access rights can perform operations on the document. Since this feature requires a specific access level to perform specific operations, it prevents unauthorized operations from being performed on the document (e.g. viewing, deleting). Also, documents that have not been assigned any access level cannot be sent as a FAX or printed out.

2.4.6 Protection of FAX Features Settings

- When Administrator Authentication or User Authentication is enabled, authentication is required in order to view or change any of the settings in Fax Features.

- Administrators can set the MFP so that general users are unable to make changes to the Fax Features settings, preventing any unauthorized alteration of these settings.

2.4.7 The “Extended Security” Feature

- It is possible to set Extended Security to prohibit the transfer or forwarding of data, preventing any unauthorized sending of data to external destinations.

Note:

- The access control used for SMTP reception/delivery operates in accordance with RFC2305.
- The SMTP-AUTH feature operates in accordance with RFC2554.

2.5 NetFile

2.5.1 Overview of NetFile Operations

- NetFile operates via communication with the following applications installed on a network-connected client PC: DeskTopBinder, DeskTopEditor for Production, SmartDeviceMonitor for Admin, ScanRouter V2/EX, Web Smart Device Monitor.

Performing Operations on Document Server Documents

- From DeskTopBinder or DeskTopEditor for Production, it is possible to print out Document Server documents that were stored using the Copier, FAX and Scanner functions or those that were edited and then returned to the MFP from one of the two DeskTop applications mentioned above. Commands issued from these applications allow documents stored using the FAX function to be sent as FAX data, and those stored using the Scanner function to be forwarded to ScanRouter V2/EX. In addition, it is also possible to make changes to or delete the bibliographic information files for the stored image data from inside DeskTopBinder or DeskTopEditor for Production. Documents stored using each principal machine function can be protected with a password. Users are prompted for this password, even when attempting to perform the above operations from inside DeskTopBinder or DeskTopEditor for Production.

Restoring Files Back to the MFP

- When Copier or Printer files which were originally downloaded from the MFP to DeskTopEditor for Production in TIFF or JPEG format are then restored to the MFP, the data is saved to the HDD as a separate file from the original one.

Viewing and Changing User Information Stored in the MFP

- User data stored in the MFP can be captured, added to, deleted, and changed from inside SmartDeviceMonitor for Admin, however this requires User Administrators access rights.

Viewing and Changing Machine Settings Stored in the MFP

- Some machine settings stored in the MFP can be viewed and changed from inside Web Smart Device Monitor. At present, it is possible to change a portion of the System Settings that can be changed from the MFP operation panel, however these operations require authentication as a Machine Administrator, Network Administrator or User Administrator.

2.5.2 Data Flow

- Netfile supports two protocols for the sending and receiving of XML messages: Netfile Protocol and SOAP.

- With SOAP, once the PC client initiates the session, Netfile begins the appropriate processing operations in accordance with the specific request received.

Creating Thumbnails

The MFP creates thumbnail images in JPEG format for the first page of the image files stored in the HDD. The thumbnails themselves are also stored in the HDD as well. The specific operations performed by the MFP to create the thumbnails depend on whether or not the File Format Converter is installed.

- When the File Format Converter is not installed:
  When the image data is saved to the HDD, the MCS uses its modules to create a thumbnail of the first page of the image data.

- When the File Format Converted is installed:
  When the image data is saved to the HDD, the IMH uses its modules to create a thumbnail of the first page of the image data. The first page is read into memory, after which the File Format Converter compresses it and converts it into image data. The MFP software then creates the thumbnail from this data. If a request is received for thumbnails for page 2 or onward, Netfile sends the request to the IMH via the MCS. The IMH then generates the thumbnail for the requested page(s) in the same way as described above for page 1.

Viewing Thumbnails

Netfile loads the requested thumbnail data directly from its storage location on the HDD, and then sends it to the PC via the NCS.

Deleting Thumbnails

When the number of thumbnails for pages 2 and onward created at the request of DeskTopEditor for Production reaches a certain limit, Netfile will choose the oldest thumbnail and send a request to the MCS to delete it. The MCS then deletes the specified thumbnail from HDD memory. Also, the MCS deletes all thumbnails for pages 2 and onward from HDD memory whenever the main power is turned on or a system reset is performed.

Downloading Document Server Files to the PC

From DeskTopBinder or DeskTopEditor for Production, it is possible to view full images of documents stored on the MFP HDD. Netfile loads the requested image data stored in the HDD via the MCS, and then sends it to the PC via the NCS. Since documents created using the Copier and Printer functions are saved to the HDD in a Ricoh-original data format, the File Format Converter is necessary to convert the data into a commonly used data format (JPEG, JPEG2000 or TIFF). To do this, the IMH uses its own internal modules in tandem with the File Format Converter.

Printing out Document Server Files

When printing out documents stored in the MFP from DeskTopBinder or DeskTopEditor for Production, Netfile sends the printing command to the ECS. Working in tandem with the IMH, the ECS then loads the specified document out of HDD memory and sends it along to the printing engine for printing out.

Transmitting FAX Document Server Files

When the MFP receives instructions from DeskTopBinder or DeskTopEditor for Production to transmit a file that was stored to the HDD using the FAX function, Netfile sends the FAX transmission command for the specified file to the FCS. Working in tandem with the IMH, the FCS then loads the specified document out of HDD memory and sends it along to the FCU for FAX transmission.

Downloading FAX Reception Documents to the PC

Netfile loads the image data out of HDD memory via the MCS, after which the data is sent to the PC via the NCS.

Forwarding Stored Scanner Documents

When the MFP receives instructions from DeskTopBinder or DeskTopEditor for Production to forward a Scanner document, Netfile sends a forwarding command for the specified file to the DCS. Working in tandem with the MCS and IMH, the DCS then loads the specified document out of HDD memory and sends it along to the PC. The transmission protocol used is FTP.

Restoring Images Back to the MFP

When Copier or Printer files which were originally downloaded from the MFP to DeskTopEditor for Production in TIFF or JPEG format are then restored to the MFP, Netfile sends the data to the NCS, which then sends it to the HDD for storage via the MCS. This pathway is the reverse of that used to send stored images to the PC. Before storage, the IMH uses its modules and the File Format Converter to convert the file format from TIFF/JPEG2000 to a Ricoh-original format. These “restored” files are actually separate files than their originals, and are stored in the HDD in a separate location.

Viewing and Changing User Data Settings Stored in the MFP

From SmartDeviceMonitor for Admin, it is possible to view and change the user data settings stored in the MFP. Only users authenticated as User Administrators are able to change these settings. User data is stored in the HDD and is managed by the UCS.

When the MFP receives a request to view this data, the UCS loads the data out of HDD memory, after which Netfile obtains the information via communication with the UCS and related modules. Netfile then sends the data to SmartDeviceMonitor for Admin via the network. When the MFP receives a request to make changes to some of the data, Netfile obtains the new settings from SmartDeviceMonitor for Admin, after which it communicates with the UCS and related modules. The UCS then saves the new data to the HDD. In cases where data is received from SmartDeviceMonitor for Admin for an address book data backup or restore, the data is encrypted before it is sent. For more details on the UCS internal management of the address book data, please see section 1.8.

Viewing and Changing Machine Configuration Data Stored in the MFP

In order to view or change the machine configuration settings obtained by Web Smart Device Monitor, users must have an administrator-level User Account registered in this utility. The machine configuration data is managed by multiple modules, including the FCS, NCS, DCS and SCS. The main storage location of the data is the NV-RAM. When a request is received to view configuration data, these modules directly assess the NV-RAM. Netfile then communicates with these modules to load the data out of memory and send it on to Web Smart Device Monitor.

When making changes to the current settings, Netfile receives the new settings from Web Smart Device Monitor and forwards them on to the appropriate module(s). The settings are then saved to the NV-RAM.

Supplementary: Protection of Passwords for Stored Documents

No operations can be performed on password-protected stored documents unless the correct password is entered, even when attempting to do so from DeskTopBinder or DeskTopEditor for Production on a network-connected PC. Communication between the MFP and these applications is performed using text written in http and XML format, for both sending and receiving. The password is embedded in this text data when it is sent to the MFP. User Codes and passwords are encrypted before being sent.

2.5.3 Data Security Considerations

SOAP Communication Sessions

- SOAP communication supports SSL (Secure Sockets Layer), ensuring the proper security during communication sessions. Even in cases where SSL is not used, the client (PC) identifies the server (MFP) via a unique session ID. Only after the MFP identifies the client through this session ID will it accept any requests from the client. This session ID is a randomly generated value, making it extremely difficult for third parties to surmise its contents and use it to impersonate the client. The session time limit of 30 seconds provides additional security against this type of threat.

- To increase the level of security even further, it is possible to use usernames and passwords stored in the MFP to authenticate clients, so that any clients who do not know this information will be unable to perform remote Netfile operations. As mentioned above, this password is encrypted before being sent over the network, preventing third parties from accessing or altering any information stored in the MFP.

Usage of Documents Stored in the MFP

- The protections provided for documents stored in the MFP are the same, regardless of the access method (over the network versus from the MFP operation panel). The ACL operates in accordance with the settings in the MFP.
  Note: Please refer to section 2.1.5.

- For password-protected documents, it is not possible to perform any operations on the file unless the correct password is entered. As described above ("Protection of Passwords for Stored Documents"), communication between the MFP and DeskTopBinder or DeskTopEditor for Production is performed using text written in http and XML format, for both sending and receiving. The password is embedded in this text data when it is sent to the MFP. Since User Codes and passwords are encrypted before being sent, the information itself would be indecipherable even if it were intercepted along the communication path.

- For each individual user, it is possible to restrict the use of specific functions of DeskTopBinder and DeskTopEditor for Production. To use any of these functions, however, users need to be pre-registered in the MFP.

- User access control can also be performed for FAX reception documents stored in the MFP. Operations on these documents can only be performed by users already registered in the FAX function as individual users or as part of a group.

Restoring Files Back to the MFP

- Netfile will reject any data it receives that does not conform to preset formats, regarding it as illegal data. If the operator attempts to restore image data from DeskTopEditor for Production to the MFP, and the data does not conform to the standard format, the File Format Converter will not be able to convert the file and the data will be destroyed without any adverse effect on data stored in the MFP. It is therefore not possible to introduce illegal data when restoring data to the MFP.

  Note: Since Netfile treats the data it receives through this process as a separate file from the one originally sent to the PC, the destruction of such illegal data does not affect the original file

Viewing and Changing User Information Stored in the MFP

- As mentioned above, user data stored in the MFP can be captured, added to, deleted, and changed from inside SmartDeviceMonitor for Admin, however this requires User Administrator access rights (see Fig. 1-12 in section 1.81 for more details).

Viewing and Changing Machine Settings Stored in the MFP

- In order to view or change the machine configuration settings obtained by Web Smart Device Monitor, users must have an administrator-level User Account registered in this utility. Similarly, the network settings can only be changed by users logged in as Network Administrators, and the user settings can only be changed by those logged in as User Administrators. The access control settings for an individual user can only be viewed by the user who is registered with that account, or by any of the administrators mentioned above. Additionally, these administrators are the only individuals who are able to view the user counter values

2.6 Web Applications

2.6.1 Web Server Framework

The MFP Web Server was developed exclusively by Ricoh, Co. Ltd.

Encrypted Communication Support

The Web server installed on the MFP supports SSL communication. Since the MFP is accessed via an HTTPS connection, all input/output data is encrypted (incl. authentication ID, password, cookie). This allows for safe and secure communication between Web Image Monitor and the MFP. It is possible to set the MFP so that it will reject HTTP-based communication, which does not encrypt the data mentioned above, such that it will only accept HTTPS-based communication.

User Authentication Support

Web Image Monitor supports the access restriction functions described in section 1.2 of this document. These functions provide greater security by prohibiting Guest users from changing any settings as well as limiting the number of items that can be viewed. In addition, the communication path is encrypted when using SSL, providing an even higher level of security.

Protection Against Cross-site Scripting (XSS)

Cross-site scripting, also known as XSS, refers to the introduction of malicious content into a Web application, which can occur just by accessing a Web page. This can have the following results:

- User information is accessed, such as data stored in cookies
- Files stored on the PC are accessed or destroyed
- URL redirection to malicious Web sites

As mentioned above, authentication is required before any changes to the MFP settings can be made from Web Image Monitor. Users who do not have valid accounts are therefore not able to introduce script containing malicious data. In addition, the MFP performs sanitizing on all valid HTML/JavaScript characters before sending HTML file updates to the PC.

Protection Against URL Buffer Overflows

URL buffer overflow attacks occur when intentionally oversized URL strings are sent to a Web server with the intent of overflowing the buffer's storage capacity, causing the server to shut down. Web Image Monitor prevents such trouble by limiting the length of the URL strings it will accept, rejecting any requests that exceed this limit.

In addition, authentication is performed before any settings can be changed, ensuring that malicious data cannot be introduced via illegal access.

Protection Against Session Hijacks

A session hijack occurs when the session ID stored in a cookie is obtained to illegally access or otherwise use the session for malicious purposes. With Web Image Monitor, information necessary to clear authentication is not stored in session files analogous to cookies, which provide “automatic” authentication. Instead, authentication is performed at the initiation of each individual session, such that even if a third party did obtain the session ID, it would not be possible to gain illegal access to user information.

Protection Against the Setting of Illegal URLs

Network Administrator Authentication prevents the resetting of the optional “URL” field in Web Image Monitor, providing protection against URLs that link to malicious Web sites. To change this optional field, it is necessary to successfully log on as a Network Administrator.

2.6.2 WebDocBox

Overview of WebDocBox Operations

- WebDocBox allows users to issue commands via a Web browser to view, capture, print and delete Document Sever image files and thumbnails saved to the MFP HDD using the Copier, Printer, FAX functions, or those that were restored to the MFP using DeskTopEditor for Production.

Data Flow

- WebDocBox supports HTTP, a protocol used by Web browsers installed on network-connected computers. The session is initiated when the first request for connection is received from the Web browser, after which WebDocBox sends commands to the shared service layers in accordance with the specific operations requested. If 30 minutes passes with no additional access attempts from the same browser, the session is terminated. To initiate a new session, it is then necessary to access the WebDocBox top page, i.e. the main screen that displays the list of Document Server files.

- **Viewing Thumbnails of Stored Image Data**

  The MCS creates thumbnails of the Document Server image files that were stored in the HDD using each machine principal function, after which the thumbnails are stored in the HDD. When the MFP receives a request from the Web browser to view a thumbnail, WebDocBox instructs the NFA to send the requested thumbnail to the PC. The NFA loads the thumbnail directly from HDD memory and then sends it to the PC via the NCS.

- **Viewing and Changing the Properties of Stored Image Data**

  By sending a request from the Web browser to view the properties of stored image data, it is possible to view information such as the date/time at which the file was stored and the size of the original for the first page. By sending a request to change the property settings, it is possible to change such items as the filename, document name and password. These operations are carried out by the NFA and MCS, after which the requested information or results of the requested operation are sent to the PC via the NCS.

- **Sending Stored Image Data to the PC**

  When the MFP receives a request from the Web browser to send stored image data to the PC, WebDocBox instructs the NFA to send the requested data. The NFA loads the requested data from HDD memory via the MCS and then sends it to the PC via the NCS. Since Copier and Printer documents are saved to the HDD in Ricoh-original file format, it is necessary to use the File Format Converter to convert the data to JPEG or TIFF format.

- **Printing Out Stored Image Data**

  When the MFP receives a request from the Web browser to print out stored image data, WebDocBox instructs the ECS to print out the requested data. The ECS, in tandem with the IMH, loads the requested data from HDD memory and sends it to the printing engine for printing out.

Data Security Considerations

- As a security feature common to all Web applications, it is possible to perform access control by allowing connection only with users who provide a specific IP address when the session is initiated. Users who do not provide an authorized IP address are not even able to view Document Server data. In addition, it is possible to prevent the viewing and altering of data through the use of encrypted communication (HTTPS over SSL).

- With the use of User Authentication, it is possible to limit the conditions under which remote operations can be performed on Document Server files. Only users who have been pre-approved for access and clear the authentication process are allowed to perform the remote operations. Additionally, it is possible to place limits on the specific operations that each registered user is capable of performing. Users are unable to perform operations that have been prohibited, even if they clear the authentication process. This prevents any potential leakage or alteration of image data.

- It is possible to protect individual Document Server documents with a password (see section 1.52 for more details).

- It is possible to restrict remote access to stored documents using the same ACL mentioned in section 1.52. Users logged in as Document Administrators are able to disable the password lock as well as view, edit and delete all documents. However, Document Administrators are not able to capture or print out the documents.

3 Optional Machine Functions

3.1 @Remote

3.1.1 Overview of @Remote Operations

- "@Remote" refers to a remote machine management service that manages and monitors the MFP status from a remote location called the @Remote Center. Information and commands are exchanged between the MFP and @Remote Center via an intermediary device called RC Gate, which is connected to the MFP in the same LAN.

- As an RC Gate client, the MFP continually monitors its own status and informs RC Gate when action is required, such as when parts have reached their periodic replacement limit or an abnormal machine condition is detected. As a server, the MFP receives requests from RC Gate for status information such as the amount of toner remaining in the MFP, after which it provides RC Gate with this information.

- @Remote communication to and from the MFP is only possible when the relevant SP mode switch has been turned ON. It is therefore possible to prohibit communication with RC Gate by turning this switch OFF.

3.1.2 Data Flow

- As mentioned above, the MFP functions as either a client or server when communicating with RC Gate. Communication between the MFP and RC Gate is controlled by the NRS module.

  - **When the MFP communicates with RC Gate as a client**

    When the SCS is informed of an abnormal condition in the MFP or other status-related notification, it will notify the NRS module. After this, the NRS module obtains more detailed information via the SCS and then converts it into a special format for transmission to the @Remote Center. Finally, the data is sent to RC Gate via the NCS module, and then on to the @Remote Center.

    The NCS module communicates with RC Gate via the host I/F over an SSL connection. The authentication process uses the information on the relevant digital certificates to verify the identity of both machines. To do this, the NRS module uses the DESS module and checks the information contained in the digital certificates. If both machines judge that the other is the legitimate server/client, SSL encrypted communication is established, whereby the MFP sends the relevant information to RC Gate in an encrypted state via the host I/F.

- **When the MFP communicates with RC Gate as a server**

  Requests for information sent by RC Gate to the MFP are received by the host I/F and then forwarded to the NCS module. Before establishing the communication session, the NCS module initiates a two-way authentication process whereby the contents of both machines' digital certificates are verified. To do this, the NRS module uses the DESS module and checks the information contained in the digital certificates. As described above, if both machines judge that the other is the legitimate server/client, SSL encrypted communication is established. The MFP receives the information request from RC Gate, after which the information is decrypted by the NCS module and then sent along to the NRS module. The NRS module retrieves the required information from the SCS module, converts the data into @Remote-transmission format, and then forwards the data to the NCS module. The NCS module encrypts the data for SSL transmission and sends it to RC Gate.

3.1.3 Data Security Considerations

- As mentioned above, communication between the MFP and RC Gate is conducted on an SSL-encrypted communication path. Since digital certificate-based authentication takes place before any data exchange is performed, this ensures that RC Gate is the only remote device to which the MFP can be connected.

- The MFP's digital certificate for the @Remote function is embedded in the MFP during the last stage of factory assembly.

- With the use of SSL communication, symmetric key cryptography ensures that the data being transferred cannot be leaked to third parties. Security is increased even further by the fact that the symmetric key used is not a static key, but rather one that is generated every time a new session is initiated.

- The internal layout of the modules is such that the NRS module must always exchange machine information with RC Gate via the SCS module. Although it is possible for RC Gate to obtain specific machine information stored in the MFP, there is no route possible that would allow access to the image data. It is therefore not possible for any image data stored in the MFP to be mistakenly sent to the @Remote Center.

3.2 CSS (Customer Support System)

3.2.1 Overview of CSS Operations

- The CSS control center sends a request for service-related information to the MFP across a telecommunications line, which is then received by the LADP (line adapter telephony box). The LADP then obtains the requested information via the CSS I/F and sends it back to the CSS control center. The service-related information requested by the CSS control center includes data related to external charge devices (e.g. serial number, counter values), as well as other data.

- If an abnormal condition is detected in the MFP, the MFP sends a command to the LADP via the CSS I/F to inform the CSS control center of the condition. The LADP then contacts the CSS control center via a telecommunications line and reports the information.

3.2.2 Data Flow

- The SCS module extracts the information requested by the LADP out of the pre-defined RAM location, and then sends it to the LADP via the CSS I/F. When an abnormal condition is detected in the MFP, the SCS module reports this information to the LADP via the CSS I/F.

3.2.3 Data Security Considerations

- For MFP products that support the CSS function, a single-chip microcontroller is used to control all CSS-related communication, including protocol conversion and the destruction of any illegal data. On the structural layout diagram, this chip is located at the CSS I/F. The actions that the MFP CPU can perform are limited to three types of pre-defined commands: Read, Write and Execute. These are the only commands that can pass through the CSS I/F, i.e. the only actions that the external source (CSS control center) can instruct the MFP CPU to perform. Through these commands, the MFP performs the same processing tasks as when receiving the commands from the operation panel, making it impossible for the operator to execute external programs or freely read/write to a memory area of their choosing.

- Through this filtering, the CSS I/F will destroy any command other than the three pre-defined commands mentioned above. In addition, the firmware for the single-chip microcontroller is stored in a Mask ROM, making it impossible for its contents to be overwritten.

4 Device SDK Applications (DSDK)

4.1 Overview of Operations

- DSDK applications developed by Vendors are able to make use of the scanning, printing and other functions of the MFP by calling the VAS (Virtual Application Service), which wraps the GW-API for the standard principal functions of the MFP. This arrangement allows SDK applications to run as additional principal functions themselves once installed.

- There are two types of DSDK applications that are able to run on the MFP: Type 1 and Type 2. Type 1 applications are written in the C programming language, and are usually developed for use with productivity-oriented principal machine functions. Type 2 applications are Java-based, and are composed of main program files (JAR files) which run on top of a CVM Java core developed by Sun Microsystems (Compact Virtual Machine ver1.01, J2ME1.3 or newer). The GW system regards the CVM Java core itself as a single Type 1 SDK application.

- Type 2 applications initiate MFP scanning and printing operations by calling an extended class (called an MFP class), which then uses the JNI (Java Native Interface) to call the VAS directly or libraries provided by a Type 1 application.

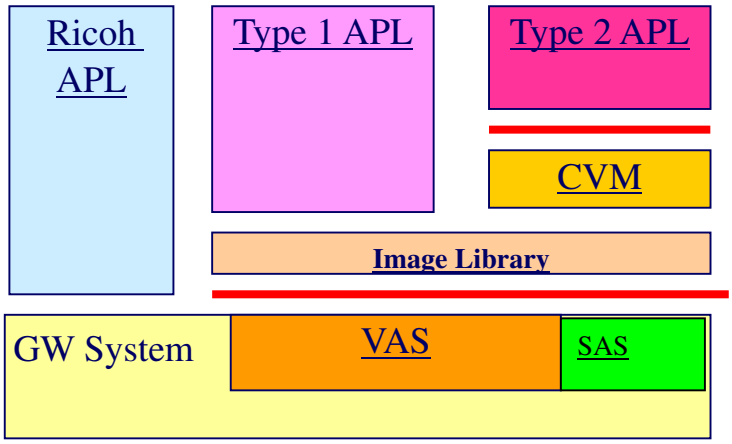


Fig. 1

4.1.1 Installation

- DSDK applications are installed on the MFP via Type 1 or Type 2 SD cards into partitions and directories in the MFP HDD allocated exclusively for DSDK applications.

- The SAS (SDK Application Service) in the MPF contains an installer for DSDK applications. When the main power is turned ON, the SDK installer inside the SAS checks the pre-defined area in the SD card for the necessary installation files and then performs the installation. For more details on the authentication process performed at installation, see section 3.1 below.

- Type 2 applications can be further divided into Xlet applications and Servelet applications. Xlet applications have the capability of displaying their own screens on the MFP operation panel, whereas Servelet applications do not.

- A maximum of three Type 1 applications can be installed on the MFP at one time, depending on the amount of virtual memory (VM) that the applications require. As mentioned above, the GW system regards the CVM Java core itself as a single Type 1 application. Therefore if one Xlet and one Servelet application are installed at the same time, the MFP will allow one additional Type 1 application to be installed (see Fig. 2 below).

- A maximum of seven Xlet applications and four Servelet applications can be installed on the MFP at one time, depending on the amount of VM that the applications require.

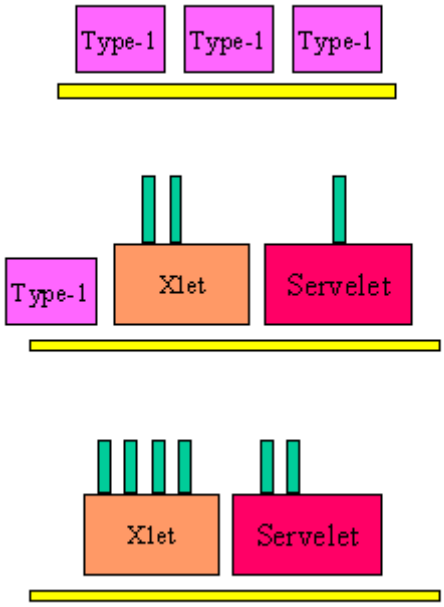


Fig. 2: Three Examples of Simultaneous Installation of Type 1 and 2 Applications

4.1.2 Overview of SDK Application Functions

- As mentioned above, Vendors can create their own DSDK applications for installation on the MFP. Vendors are provided with an image library, which simplifies complex machine operations into concise, predefined methods for major operational flows of the MFP, allowing Vendors to develop their applications relatively easily.

  Examples of such operations include:

  - Scanning the original according to specified conditions, and then storing the image on the MFP HDD.
  - Searching for an image file stored on the MFP HDD, and then retrieving or printing out the file.

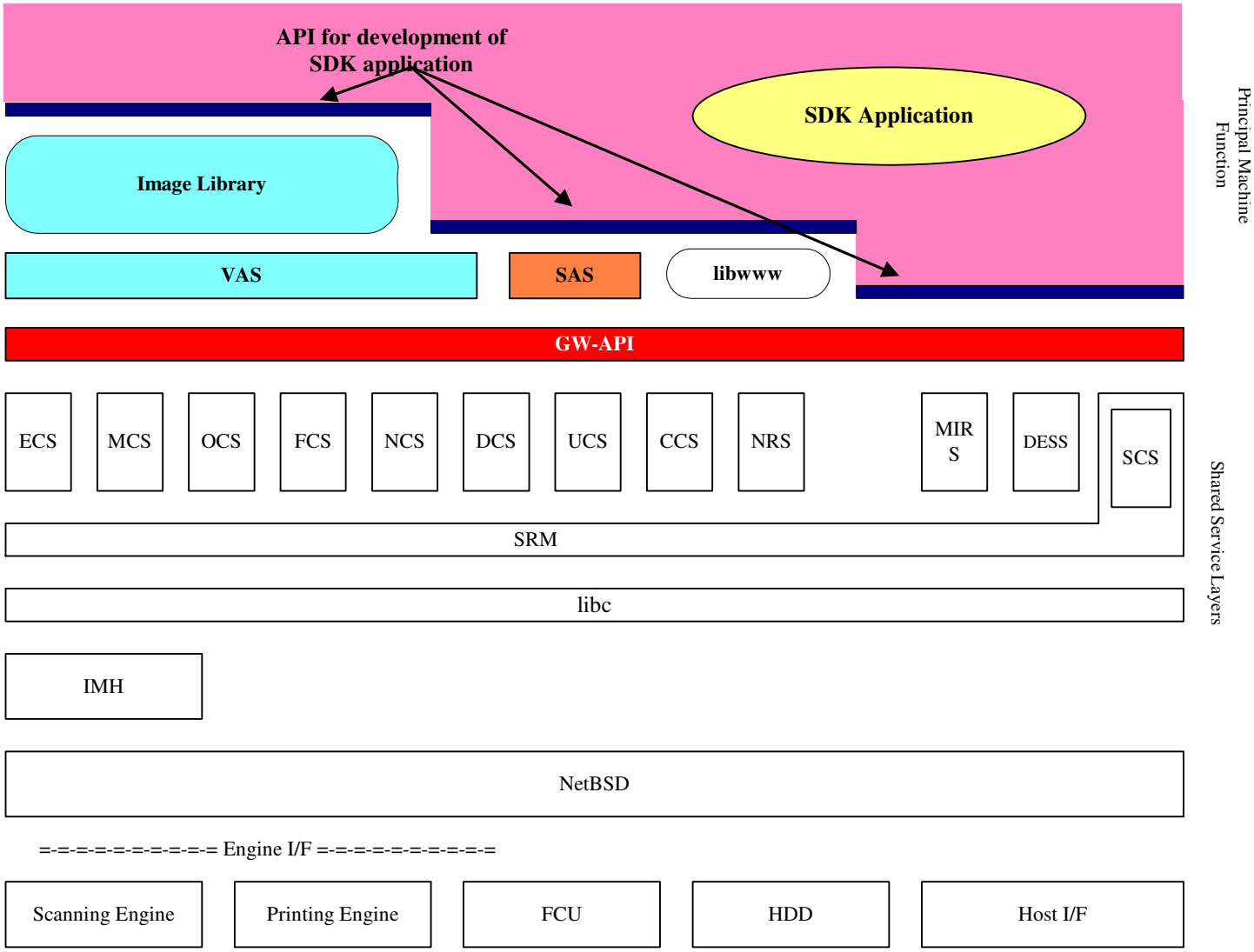


Fig. 3: DSDK/MFP Hardware Configuration

4.2 Data Flow

4.2.1 Scanning Functions: Sending Data Over the Network with the Copier and Scanner

- DSDK applications are capable of utilizing the scanning features of the MFP Copier and Scanner. For an overview of the MFP Copier and Scanner operations, please refer to sections 2.1 and 2.3 of the Main Document.

- The Image Library calls the ECS, MCS (IMH) and SCS service layers via the VAS and GW-API, after which Scanner or Copier operations are initiated (e.g. Scanning→ HDD storage→ Loading from memory→ Printing). The Image Library is a static library, and is contained within the SD card along with the SD application(s). The application generates and controls its user interface by calling the operation panel control I/F (OCS).

- When sending a scanned image stored in the machine over the network to a network-connected server or client station, the raw file is read out of HDD memory and then converted from Ricoh-original format to Unix FFS (Fast File System) format. The image data is converted to TIFF, JPEG or PDF format, after which the SDK application transmits the entire file over the network using the NCS (Type 1) or by opening its own unique socket (Types 1 and 2).

4.2.2 FAX Functions

- Of the several FAX transmission features provided by the FCS (Fax Control Service), SDK applications are allowed to utilize the PC FAX feature only. Therefore, as the MFP only allows PC-FAX to send to one destination at a time, the SDK application is not able to utilize such features as Broadcasting or Batch Transmission.

- With FAX reception, SDK applications are able to access FAX images that have been received and stored in the MFP HDD, and then transfer them to DeskTopBinder or DeskTopEditor for Production.
  Note: Incoming FAX images are automatically stored to the HDD when "Store Incoming Faxes" is enabled.

- When the FCU (Fax Control Unit) receives an incoming FAX, a notification is sent to the FCS, which then writes the incoming data to the work area of the HDD. The FCS informs libFAX that a transmission has been received, after which libFAX is able to access the file and retrieve it from the HDD. If the file is to be transferred to DeskTopBinder or DeskTopEditor for Production, it is converted to TIFF format and then sent to its destination.

4.2.3 Network Functions

- As mentioned above, a Type 1 SDK application is able to perform network communication either by using the NCS or by opening and closing its own unique socket. Since Type 2 applications are Java-based, they must use the network classes provided by Sun Microsystems, and are therefore restricted to socket-based network communication.

4.2.4 Printer Functions

- SDK applications are able to make use of a printer data filter, which allows the application to edit the incoming printing data received by the MFP, convert it to a different PDL, and change job control commands such as the paper tray selection or printing mode. Following this, the SDK application sends the edited PDL data to the printer port of the loop-back address (the 127.0.0.1 local address), which the MFP Printer function then receives just as if the PDL data had come directly from an external source. The data then follows the normal flow described in the Main Document and is printed out by the printing engine.

4.2.5 Machine Administrative Functions

- In addition to the principal machine functions of the MFP (e.g. Copier, Scanner), once installed, the SDK application can be selected in the “Function Priority Setting” so that it its screen is displayed when the main power is turned ON and the MFP reaches the Ready condition.

- It is possible to create a user interface for communication with a network-connected authentication server in order to authenticate individual machine users, thereby restricting the use of the application. The user interface can be customized for each individual user, and will automatically log out the user and return to the default screen if no operations have been performed after a certain amount of time has passed.

- It is also possible to maintain a machine usage log. The SDK application creates the log files and writes them to the SDK area of the HDD.

4.3 Data Security Considerations

4.3.1 Preventing the Installation of Illegal Applications

- The following are used to prevent the installation of illegal SDK applications or altering of authorized SDK applications already installed in the MFP:
  - Product ID (comprised of a vendor code, country code and code representing the application type)
  - SDK Authentication (Types 1 and 2)
  - Digital Authentication (Type 2)

- When the Vendor begins developing an SDK application for installation on the MFP, a contract is created between the Vendor and Ricoh. In addition to the necessity for strict confidentiality of information, this contract also specifies the scope of responsibilities regarding product quality, as well as all the details of sales-related agreements made between both sides.

- Having agreed to the terms of the contract, the Vendor requests Ricoh to assign and provide a product ID for the proposed application. In addition to being a completely unique number by which the Vendor can be identified should the need arise, the product ID is also used by the Vendor to create an installation directory for the SDK application and by Ricoh to authenticate the application through SDK Authentication. As explained in section 3.1.1 below, without the correct product ID, there is no way to install the SDK application on the MFP.

- The MFP is designed so that each SDK application, once authenticated, is installed in its own unique directory on the HDD. This ensures that the objects, data files and other contents of one SDK application can never be overwritten or accessed by another.

4.3.2 Authentication of SDK Applications at Installation

The following two processes are performed in order to authenticate SDK applications, which ensures that only authorized applications can be installed in the MFP, as well as to control the range of operations and access of the applications once installed.

SDK Authentication (Types 1 and 2)

- Once the development of the SDK application has been completed, and Ricoh has authorized its installation on the MFP model(s) in question, Ricoh provides the Vendor with 1) a file containing the unique product ID mentioned above in its raw form, and 2) a "key file," which contains two hash values generated from the product ID and SDK application object code, which are then embedded inside randomly-generated data. The locations of these hash values inside the key file are not disclosed to the Vendor.

- Using a special tool, Ricoh generates a unique key file for every SDK application that is approved. Among the entire group of specialists at Ricoh engaged in SDK application-related activities, only a select number of engineers have been granted the access rights to use and manage this special tool.

- When the SD card is inserted in the MFP slot, the SAS reads the raw form of the product ID contained in the product ID file, as well as the hash value for the ID contained in the key file. The SAS then applies a unique hash function to the raw form of the product ID, and compares the resulting value with the hash value read from the key file.

- If these two values match, the SAS then reads the raw form of the SDK application object code stored in the SD card, as well as the hash value for the code contained in the key file. The SAS applies a unique hash function to the entire code, and then compares the resulting value with the hash value read from the keyfile. If these two values match, the name of the SDK application appears on the installation screen and the application can be installed on the MFP.

- As demonstrated above, it is not possible to install an SDK application on the MFP unless both of the following conditions have been satisfied:
  - The SD card contains the key file and raw form of the product ID provided by Ricoh, as well as the raw form of the application object code developed by the Vendor, AND
  - The two hash values generated by the MFP for the product ID and application object code match those contained in the key file on the SD card.

Digital Authentication (Type 2 only)

- For Type 2 applications, Ricoh embeds a digital signature inside the JAR files received from the Vendor, assigns an appropriate access level, and then returns the files to the Vendor. This allows the MFP to authenticate the application as well as restrict its operations once installed.

- As a general rule, Ricoh assigns relatively restricted access privileges to Type 2 applications. These applications are normally prohibited from performing operations such as file storage to MFP media or opening and closing sockets to communicate over the network. Vendors who wish to utilize such functions must make this request to Ricoh when applying for the digital signature. After having fully ascertained all relevant details on the proposed SDK application, including the Vendor's specific purpose for using the application on the MFP in question, and having determined that the application poses no security threat to the MFP, Ricoh approves the application and assigns the appropriate access level.

4.3.3 Prevention of Access to Address Book Data and Machine Management Data

- Regardless of the access level granted by Ricoh, SDK applications are not able to access Address Book data (phone numbers, email addresses), internal log data or machine settings stored in the NV-RAM. It is therefore not possible for the SDK application to perform any operations whatsoever on this data, such as making unauthorized copies of the data, transmitting it over the network or saving it to an SD card or other media.

4.3.4 Protection Against Attacks on Principal MFP Functions, Prevention of Damage to the System

Buffer Overflow Attacks on the MFP VM

- After completing the development of the SDK application, the Vendor must apply to Ricoh for the items necessary to carry out the SDK Authentication and/or Digital Authentication processes described above, and at that time declare the expected VM consumption of the application. The proper method for measuring VM is described in the SDK Development Kit provided by Ricoh to the Vendor. Ricoh then performs tests on the proposed application to verify that the actual VM consumption matches that which the Vendor has stated on the application form, and then makes a judgment as to whether or not to approve the application and provide the Vendor with the requested authentication items.

Alteration or Deletion of MFP Principal Function Program Objects

- As mentioned above in section 3.1, each SDK application is installed in its own unique directory on the HDD, which is determined by its unique product ID. It is impossible for the application to access any other areas.

- Even in the event that an SDK application attempted to write a large amount of data to the SD card or MFP HDD, e.g. with the aim of rendering machine principal functions unable to write data, this would not succeed since the application cannot access any area aside of its own isolated partition on the HDD. In addition, as a general rule, Ricoh prohibits SDK applications from writing to any machine media or SD cards. Even in cases where Ricoh has given the application writing capabilities upon request from the Vendor, the application is only able to write to a specialized SD card for SDK applications.

4.3.5 Protection Against Attacks from External Sources

SDK applications are able to perform input/output exchanges via FAX and network connections.

- FAX communication, as explained in section 2.4 of the Main Document, can only be performed using predefined FAX protocols and standards. In addition, the SDK application simply instructs the MFP to initiate a FAX job, after which the actual operations for transmission and reception are performed by the CCU module, FCU and other MFP elements that comprise the FAX function itself.

- As mentioned in section 2.3, an SDK application is able to perform network communication either by using the NCS (Type 1) or by opening and closing its own unique socket (Types 1 and 2). For the latter case, in addition to using predefined protocols and authentication procedures, the communication channel itself can be encrypted. This precludes the possibility of attack from external sources.

4.3.6 Certification of the SDK Application

- Having completed the development of the production-level (product release) version of the SDK application, the Vendor must then request Ricoh to certify the application. When applying for Ricoh certification, the Vendor must provide Ricoh with the application's specifications, entire object code and all relevant evaluation results.

- Following this, Ricoh examines the information provided by the Vendor to ascertain in detail the full scope of the operations of the application, as well as to what extent the application has already been tested. These results are then documented in written form. (If deemed necessary, Ricoh may perform further testing on the application). As mentioned in section 3.1, if Ricoh determines that the application poses no particular issues or problems, the Vendor is provided with the necessary authentication files. By providing these files, Ricoh is certifying the application.

- It is therefore impossible for an SDK application to be successfully installed in the MFP without the correct authentication files described in section 3.1. Ricoh utilizes this system to manage and control the specifications, operations and quality of SDK applications developed by Vendors, preventing the illegal installation of any SDK application that has not been fully certified as described above.