Print Controller Design Guide for Information Security:

Model A-P4

Model MT-P2

Model G-P2

Model AP-P1

TABLE OF CONTENTS

Overview

This document describes the structural layout and functional operations of the hardware and software for the laser printers listed below (herein referred to as the LP), 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 LP internal and peripheral devices.

The explanations will primarily focus on the following, with particular attention to demonstrating how unauthorized access to data stored in the LP is not possible.

- Operational Summaries
- Data Flow
- Data Security Considerations

Products to Which This Document Applies

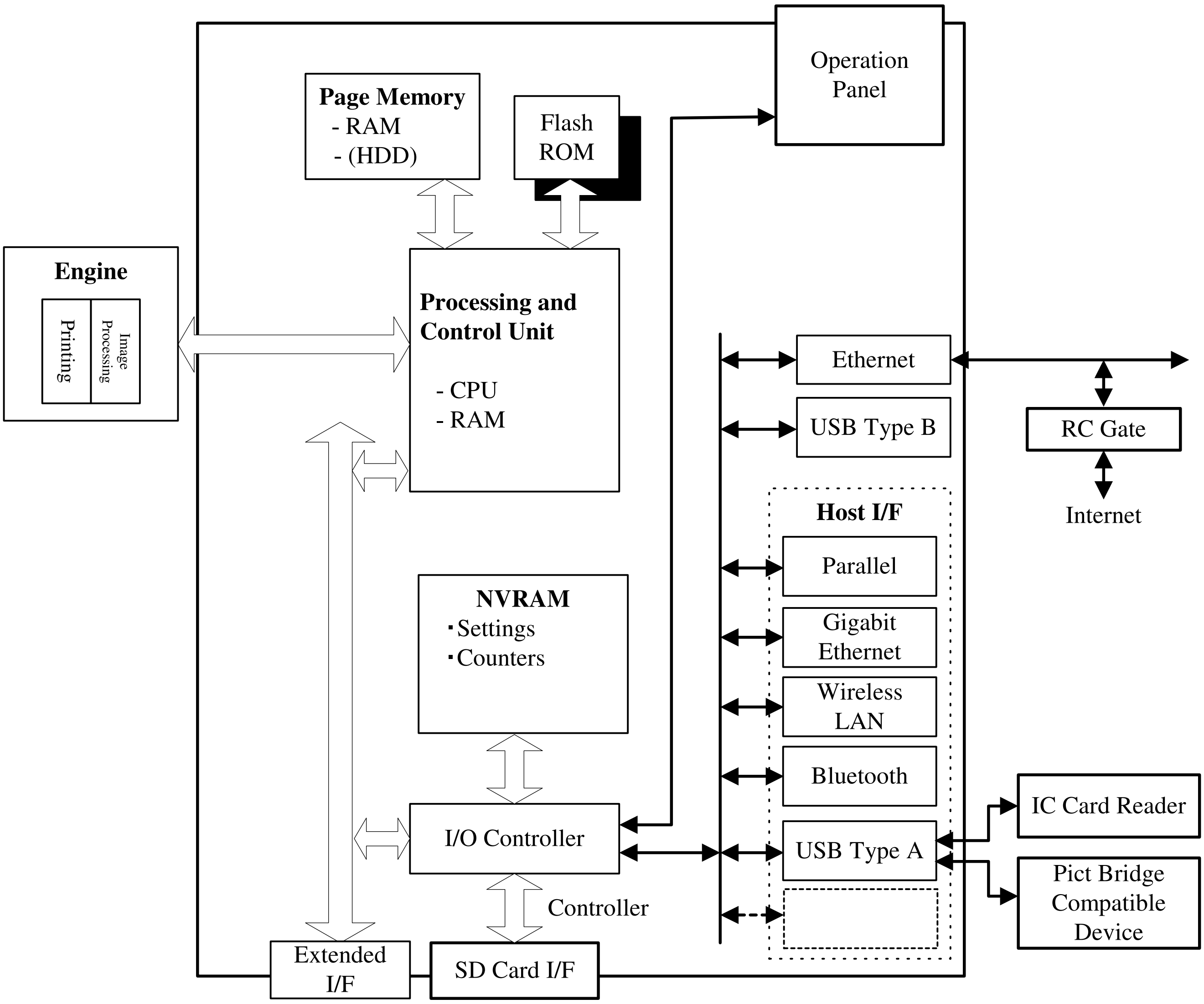
This document applies to the following LPs designed and developed by Ricoh:

- *Model A-P4*
- *Model MT-P2*
- *Model G-P2*
- *Model AP-P1*

Note: Some of the hardware (e.g. external I/F) and functions described in this document may not be supported by the end user's machine. For these details, please refer to the Operating Instructions for the specific machine in question.

1 Internal System Configuration

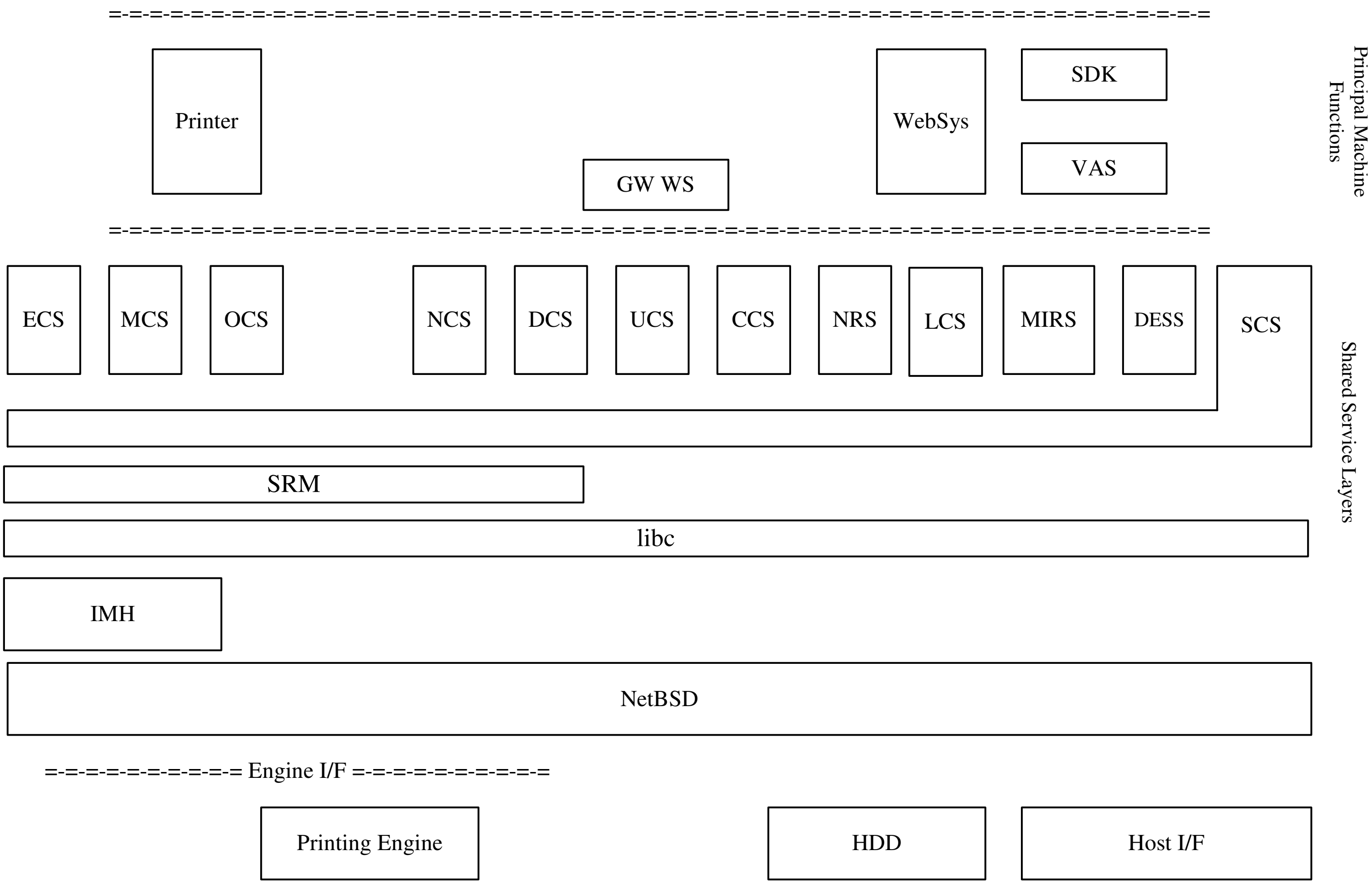
1.1 Hardware Configuration



Hardware Configuration

- Image Memory area: Also performs image-processing functions such as data compression and decompression.
- RC Gate: Intermediary device connected to the LP 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 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).

SCS (System Control Service) Manages the status of all internal operations performed on or by the system as a whole, and controls the switching of the LCD screen as well as the operational link between SP settings and machine operations.

SRM (System Resource Manager) In addition to managing hardware resources, this module mediates control of the printer engine and memory resources during the image creation process.

DCS (Delivery Control Service) Controls email transmission and reception.

MIRS (Machine Information Report Controls the sending of machine configuration data by email

Service)

UCS (User Control Service) Manages the Address Book data.

CCS (Certification Control Service) Mediates 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).

LCS (Log Control Service) Controls the LP's access logs (e.g. Address Book, LP functions).

DESS (Data Encryption Security Service) Controls the encryption and decrytption functions.

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.

GW WS As a server, GWWS provides some LP functionality to specific network-connected PC utilities. GWWS also acts as a client to external Web services.

WebSys Controls Web-based access to the LP and allows machine configuration settings to be viewed and changed via a Web interface.

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

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

1.3 Data Security

1.3.1 External I/F

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

- Serial I/F for connection of peripheral devices (e.g. Finisher, LCT).
- Standard IEEE 1284 parallel I/F
- 100BASE-TX and 10BASE-T compatible network I/F
- Gigabit Ethernet-compatible network I/F
- Standard IEEE802.11b wireless LAN network I/F
- Bluetooth I/F
- USB2.0 Type B I/F, USB2.0 Type A I/F

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

1. All of the above principal 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 LP, thereby preventing access by any module outside this pre-determined set.
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 pre-determined modules in the LP itself. This arrangement ensures that the data stored in the LP cannot be accessed illegally via an external I/F.
4. Communication between the LP 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 LP has recognized the peripheral device. If the LP receives illegal data from the peripheral, it will judge that a perhiperal device failure has occurred or that the device is not connected. This prevents any illegal access to internal programs or data.
5. With the @Remote function, the LP is connected via the network to a Ricoh-developed device known as RC Gate, which is then connected to the @Remote Center, or to the @Remote Center directly. When connecting to the center directly, the LP communicates via a LAN connection over the Internet. Before transferring any data, mutual authentication is performed using digital certificates between the LP and RC Gate or LP and @Remote Center, which ensures that the LP cannot connect to any device other than RC Gate or to its single, pre-assigned @Remote Center. Communication between RC Gate/@Remote Center and the LP 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 LP settings to prohibit @Remote communication.

6. The standard IEEE1284 parallel I/F, USB I/F (Type B), and Bluetooth I/F treat all incoming data as print data. This print data can only be sent to pre-specified modules responsible for executing printing operations. In addition, using LP settings, it is possible to disable each interface individually.
7. The USB I/F (Type A) only allows connection with devices that support PictBridge printing functions. After confirming the identity of the connected PictBridge device, the interface and device will only exchange pre-defined commands and data. Access to data stored inside the LP is not possible. It is possible to disable PictBridge printing for the USB I/F (Type A) using the LP settings.

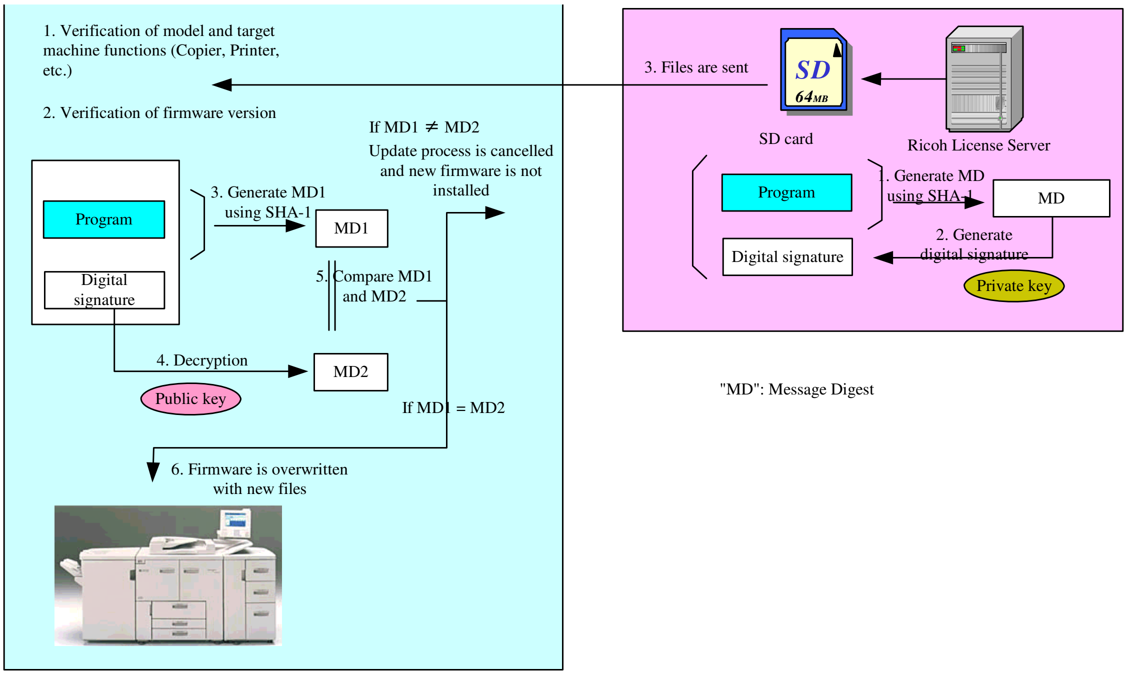
1.3.3 Firmware Update

It is possible to update the firmware and application programs stored in the LP 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 LP via this storage media. Briefly stated, a license server assigns a digital signature to the software, which is then used by the LP 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 LP from the SD card slot.
  3. The LP 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 LP 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 LP 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 LP 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 LP main power suddenly turns off. After recovery is initiated, the LP checks to see that the data in the SD card has not been altered, and then resumes the update.


1. Verification of model and target machine functions (Copier, Printer, etc.)
2. Verification of firmware version
If MD1 ≠ MD2
Update process is cancelled and new firmware is not installed
Program
Digital signature
3. Generate MD1 using SHA-1
MD1
5. Compare MD1 and MD2
4. Decryption
MD2
Public key
If MD1 = MD2
6. Firmware is overwritten with new files
3. Files are sent
SD 64MB
SD card
Ricoh License Server
Program
Digital signature
1. Generate MD using SHA-1
MD
2. Generate digital signature
Private key

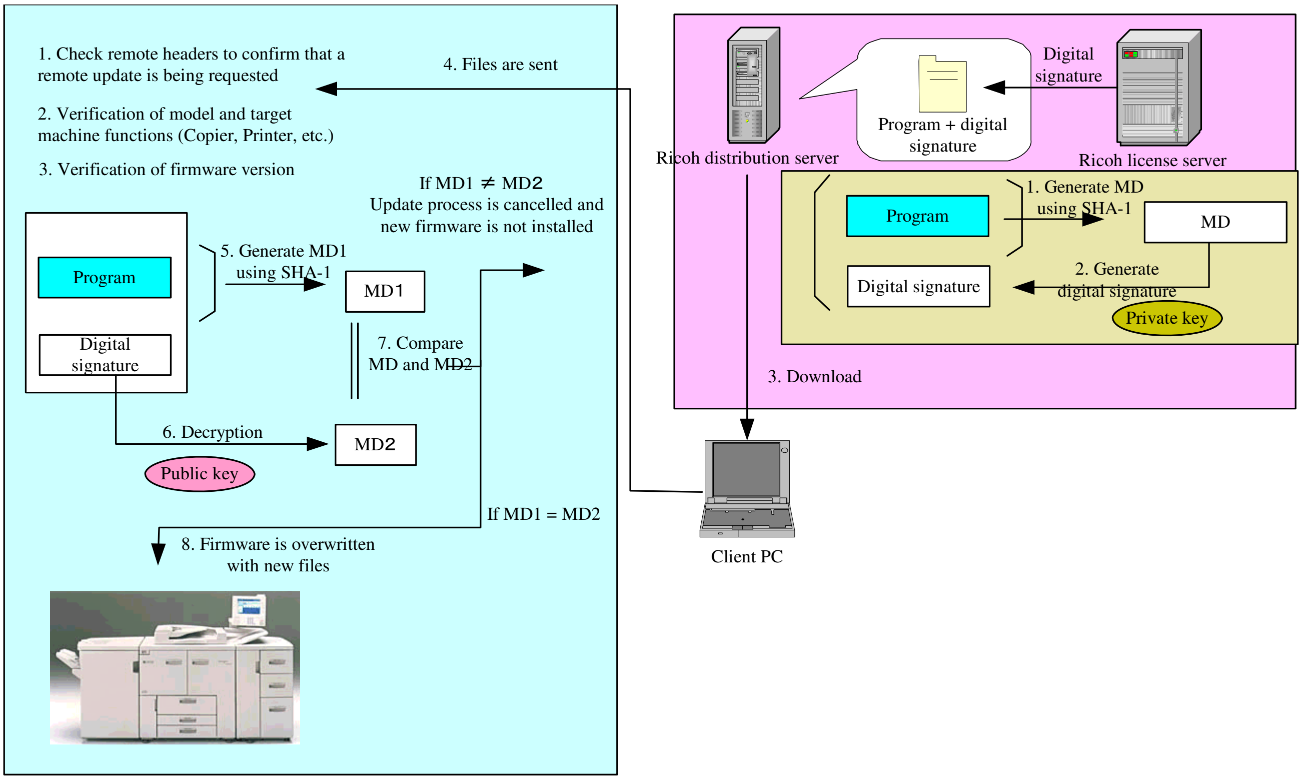
"MD": Message Digest

Firmware Installation Using an SD Card

Remote Firmware Installation

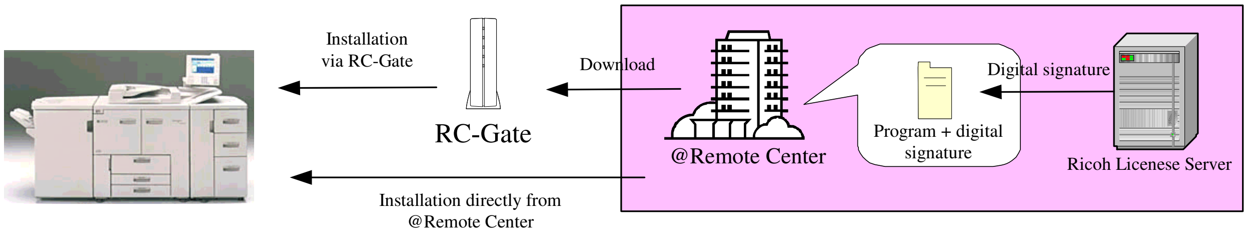
- In addition to using an SD card, it is also possible to update the firmware by transmitting the firmware files to the LP via a remote connection. Since these files are transmitted over public Internet communication paths in some cases, routed through multiple servers before reaching their destination, 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 LP.
  - 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 three main scenarios in which a remote firmware update is 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 using the @Remote function, normally by an individual with access rights to the @Remote Center GUI
  - The update is performed via Web SmartDeviceMonitor for Admin, usually by the end user

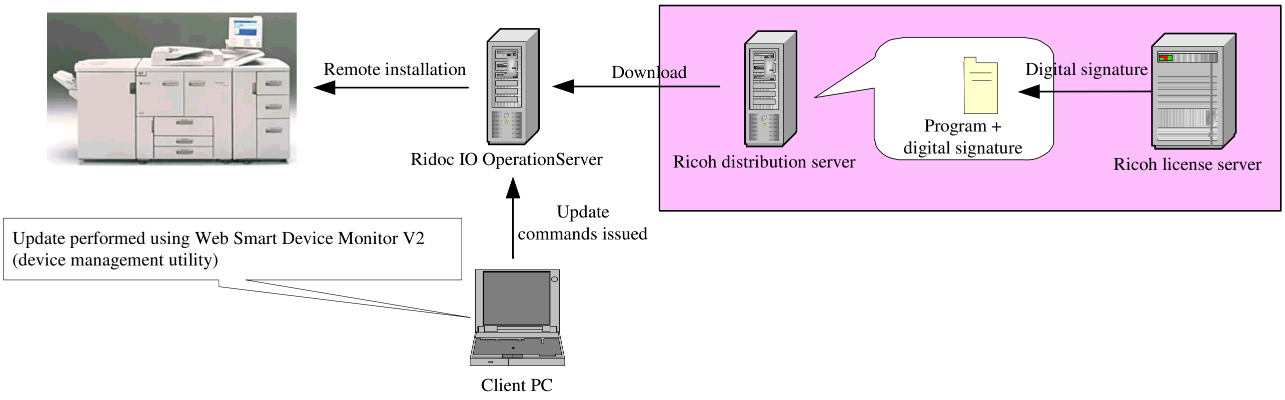

1. Check remote headers to confirm that a remote update is being requested
2. Verification of model and target machine functions (Copier, Printer, etc.)
3. Verification of firmware version
4. Files are sent
If MD1 ≠ MD2 Update process is cancelled and new firmware is not installed
Program
Digital signature
5. Generate MD1 using SHA-1
MD1
7. Compare MD and MD2
6. Decryption
MD2
Public key
If MD1 = MD2
8. Firmware is overwritten with new files
Ricoh distribution server
Program + digital signature
Digital signature
Ricoh license server
Program
1. Generate MD using SHA-1
MD
Digital signature
2. Generate digital signature
Private key
3. Download
Client PC

Remote Firmware Installation Performed by a CE

(from a client PC)



Remote Firmware Installation from the @Remote Center



Remote Firmware Installation via Web SmartDeviceMonitor for Admin

(performed by the end user)

1.4 Authentication, Access Control

1.4.1 Authentication (LP)

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

- There are five types of User Authentication:
  - Basic Authentication
  - Windows Authentication
  - LDAP Authentication
  - User Code Authentication
  - Integration Server Authentication

- As the authentication server, the LP can be used for Basic Authentication, a Windows NT4.0 server, Windows 2000 server or Server2003 can be used for Windows Authentication, and an LDAP server can be used for LDAP Authentication. In addition, when "Integration Server Auth" is selected from the User Authentication menu, the LP connects to the actual authentication server via an Integration Server. In this case, the authentication is performed using the User Authentication functions of ScanRouter, ScanRouter Document Server, Web SmartDeviceMonitor for Admin or ScanRouter Web Navigator.

  Note: See "Windows Authentication, LDAP Authentication" and "Integration Server Authentication" diagrams below.

- Usernames:
  - Format: US-ASCII, WinLatin1, WinLatin2, WinCyrillic (except 2-byte characters used for display languages such as Chinese, Japanese, Taiwanese and Korean).
  - Length: Maximum 32 characters.

    Note: Although usernames longer than 32 characters are invalid, the input field will accept up to 128 characters in order to make the 32-character limit more difficult to surmise.

- Passwords:
  - Format: US-ASCII, WinLatin1, WinLatin2, WinCyrillic (except 2-byte characters in languages such as Chinese, Japanese, Taiwanese and Korean).
  - Length: Maximum 128 characters (general users), 32 characters (administrators).

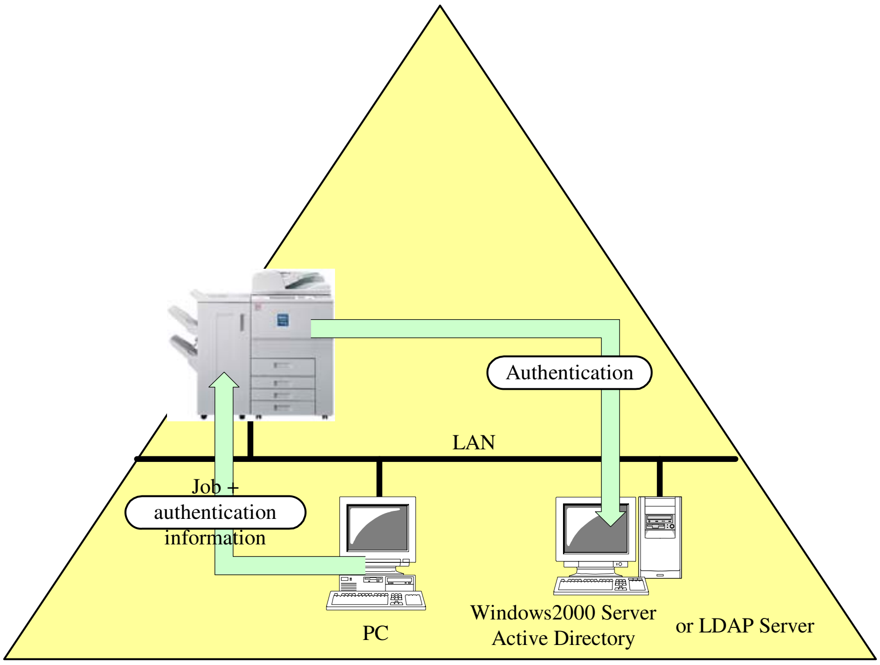
- Before authentication at the LP operation panel can be performed, uses must be pre-registered in the LP. The communication path can be encrypted using SSL, however for environments that do not support SSL protocol, the password itself is encrypted using an encryption key provided by the user. To do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

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

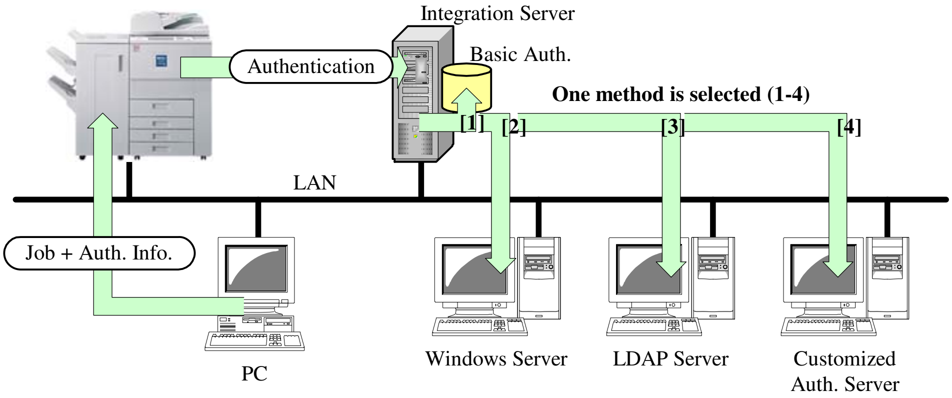
- The information for performing the authentication of administrators is encrypted and then stored in the LP in non-volatile memory. Therefore, it is always possible to perform authentication on administrators even when a failure occurs with the LP HDD or one or more of the external authentication servers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

- Active sessions will expire under the following conditions:
  - When the "Logout" button is pressed in User Tools
  - When the LP enters Low-power Mode or Energy Saver Mode
  - After a pre-determined amount of time has passed (automatic logout)


Authentication
LAN
Job + authentication information
PC
Windows2000 Server Active Directory
or LDAP Server

Windows Authentication, LDAP Authentication



Integration Server Authentication

1.4.2 Authentication (IC Card)

Overview

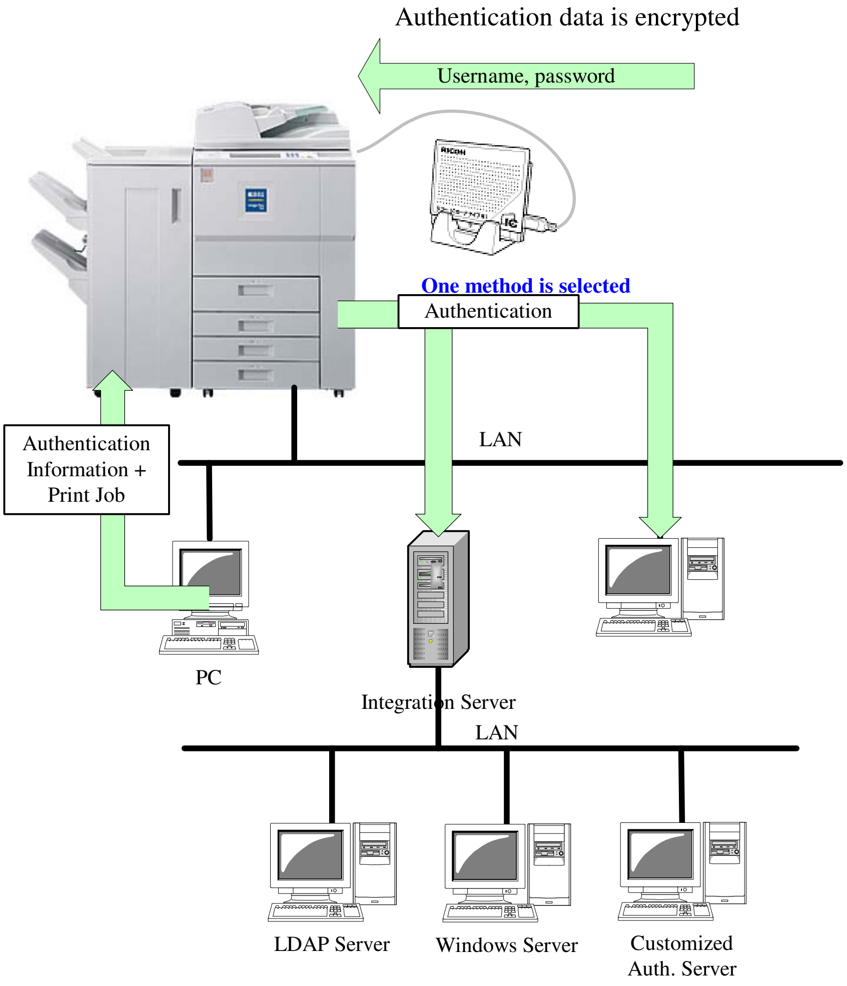
- IC Card Authentication is provided to the field in the form of an optional IC card. The information necessary to perform the authentication functions described in section 1.4.1 above (username and password) can be stored to this IC card and then used to authenticate LP users.

- To use this option, it is necessary to install the "ADK" (Authentication Development Kit), a local customization solution.

Data Flow

- IC Authentication using the username and password (Ricoh IC cards):

When the IC card is placed in the reader, if it contains a function release code, the user will be prompted to enter this code in order to proceed with the authentication. The CSC compares the code entered with the one stored in the IC card, and if these two match, it then obtains the username and password stored in the card and begins the authentication process. If the IC card does not contain a function release code, the CSC simply reads the username and password stored in the IC card and begins the authentication process automatically.



1.4.3 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 LP 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.
- It is possible to prohibit unauthenticated users as well as general users from viewing or making any changes to the User Tools settings.
- A numeric password of 4-8 digits can be assigned to each stored document. If the password entered by the operator does not match the password stored in the LP, no operations can be performed on that document. In addition, it is possible to create a group or user-based access control list (ACL) for each document.

1.5 Administrator Settings

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

1. **Machine Administrator:** Manages the User Tools settings and ensures that the LP 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 privileges 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 LP 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 LP 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. The NVRAM also stores various data, such as User Tools settings. Data stored on the magnetic media of the LP is normally "erased" by overwriting it with a fixed value (normally, this is performed once).

- However, in the case of a print job, for example, although the LP completely erases the page location data (the storage location information necessary to access image data on the HDD), the image data itself remains in the temporary storage stored area of the HDD. The Data Erase/Overwrite feature, provided to the field as optional software stored on an SD card, renders this image data indecipherable. Even in the unlikely event that the HDD were removed from the LP, a third party would not be able to reconstruct 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, the optional Data Erase/Overwrite feature employs the following methods, which ensure that data 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 DoD and NSA methods automatically perform three passes, using a different pattern each time (the number of passes is unchangeable). The Ricoh randomized value method performs three passes by default, using a different set of randomly-generated numbers each time, however the number of passes can be set from 1-9. Comparing the DoD method, NSA method and Ricoh randomized value method (set at three or more passes), no single method is any safer than the other two. Under these conditions, all three methods render the data equally indiscernible. Regardless of which method is selected, the more passes are made, the more indiscernible the original data becomes (although performing more passes requires more time).

- Before the Data Erase/Overwrite option can be run on the LP, a service technician must perform the setup procedure. If the SD card is removed from the slot at any time after installation, the option will cease to function and an error message will be displayed on the operation panel, however the machine will continue functioning normally. Also, it is not possible to remotely verify whether or not the option is installed or actually running.

- To execute the overwrite, the operator can choose from two options: "Auto Erase Memory" and "Erase All Memory" (detailed descriptions below).

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 LP 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 LP.

- In addition, it is also possible to manually erase data that was intentionally saved to the HDD.

Note: If the LP receives a request to perform a print job or other operation that requires writing data to the HDD in between the time the operator initiates the overwrite and the time the machine actually begins the overwrite, the area of the HDD in question may be used to store the incoming image data.

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. Since this operation makes it impossible to retrieve or reconstruct the contents of the HDD in addition to initializing the NV-RAM 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 privileges to individual users as well as to groups. Users who have not been assigned any access privileges are not able to view the contents of Address Book entries.
- There are four levels of access privileges: View, Edit, Edit/Delete, and Full-Access. These settings can be changed by Group and User Administrators, users with Full-Access privileges 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 LP HDD. This data can be encrypted before it is stored.

			General Users Groups	Owner of the Entry (User)	User Administrator
General Info.	Reg. No.	00001	R	RW	RW
	Name	Taroh Ricoh			
			Use ACL		
	…	…			
Detailed User Info.	Login password*	**********	–		RW/W*
Admin. Data	Login Username	Taroh	–	R	RW
	Authorized Usage	Usage allowed			
	…	…			
ACL Information		00002=R--- 00003=RW-- 00004=RW-O 00005=RWDO …	Use ACL	RW	RW

Access Privilege Management Structure for the Address Book

***Note:** This password can only be changed by users with Write privileges. As the user inputs the password, it is displayed as asterisks.

		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 Privileges and Operations for the Address Book

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 individual users from registering or making changes to Address Book entries.
- Change the complexity and minimum number of characters required to set a valid password (from 1 to 32 characters) for both Basic Authentication and Administrator Authentication. A password's complexity can be increased by requiring the use of two or more (or three or more) types of alphanumeric characters out of the four types available (capital letters, lower-case letters, numbers, and symbols).

  Note: When users log in via the Integration Server, the LP does not check the password policy (e.g. length, complexity). Therefore, in such cases, the password policy must be managed by configuring the Integration Server settings.

1.9 Job/Access Logs

- Job logs and access logs for the principal machine functions in sections 2.1-2.7 contain entries for job status-related events (initiation, completion, any changes during the job), while the access log contains entries for LP operational events (authentication, operations performed on documents, administrator operations). Therefore, not every single operational or status-related event is recorded in the log.

- Both logs are saved to the HDD by the LCS, and contain a date and time for each entry. By saving the data to the log along with the time and date of the operation performed, it is possible to then retrace the sequence of operations performed leading up to a machine failure. In addition, making it known that the time and date are recorded together with the operations can serve as a deterrent to unauthorized use.

- The specific events for which log entries are created vary slightly with each principal machine function. The events common to all principal machine functions are: SMC printout, log-in, log-out, HDD format, storage or deletion of a file in HDD storage, deletion of all log entries in a single operation, and changes to log settings. For the events that are unique to each principal machine function, please refer to sections 2.1-2.3 below.

- It is then possible to have the LP send the log data to Web SmartDeviceMonitor for Admin (a log data server utility) whenever any of the events described above occurs, after which the data is stored in an MSDE or SQL Server database. Only users who are registered with an administrator-level User Account in Web SmartDeviceMonitor for Admin can access the contents from a Web SmartDeviceMonitor for Admin client station. In addition, these administrators are the only persons who can perform any changes to the log data transfer settings.

  The log data is encrypted before being saved to the HDD, which prevents any illegal acquisition or alteration of the data through unauthorized access to the HDD. In addition, the encrypted data is sent via the LCS and NFA to Web SmartDeviceMonitor for Admin over an SSL connection.

- Before log data can be transferred from the LP to Web SmartDeviceMonitor for Admin, it is necessary to assign LP administrator types 1-4 described in section 1.5 Administrator Settings to a single account, and then create an administrator-level Access Account in Web SmartDeviceMonitor for Admin with the same name and password. It is also necessary to enable the settings for log data sending in the LP and in Web SmartDeviceMonitor for Admin.
  Note: For more information on the transfer of this data, please refer to 2.5 Netfile.

- The LP does not allow any changes to be made to the log data itself, i.e. the data can only be transferred to Web SmartDeviceMonitor for Admin in an unaltered, encrypted state. Therefore, the data cannot be overwritten or modified in any way, even by those with administrator-level access rights.

- When the log reaches its capacity, the oldest entries are then overwritten one by one by each new entry. To ensure that this data is not lost, it must be sent to Web SmartDeviceMonitor for Admin before it is overwritten. As mentioned above, the LP sends the data to Web SmartDeviceMonitor for Admin only when an operational or access event has occurred.

  Note: With LPs that do not have an HDD installed, the log data is stored in volatile RAM. The data is therefore erased when the LP main power is turned off. In addition, since the RAM capacity is not as large as that of the log area in the HDD, the oldest log entries will be overwritten sooner.

- The time it takes for the log to reach its capacity and begin overwriting from the oldest entry depends on the log capacity, as well as the rate at which operational events (e.g. print jobs) are recorded.

  - **Job log**

    <u>Capacity</u>:

✧ With HDD:	2000 entries
✧ Without HDD:	500 entries

    <u>Time to full condition</u>:

✧ With HDD:	2000/N minutes
✧ Without HDD:	500/N minutes

    Note:

    - One job = one log entry
    - N = Average number of jobs (log entries) generated in one minute

    Example: An HDD is installed, and the LP receives an average of five (5) jobs per minute.

    2000 / 5 = 400 minutes (6 hours, 40 minutes)

  - **Access log**

    <u>Capacity</u>:

✧ With HDD:	6000 entries
✧ Without HDD:	500 entries

    <u>Time to full condition</u>:

✧ With HDD:	6000/M minutes
✧ Without HDD:	500/M minutes

    Note:

    - One job = one event
    - M = Average number of events (log entries) generated in one minute

    Example: An HDD is installed, and an average of eight (8) events occur per minute.

    6000 / 8 = 750 minutes (12 hours, 30 minutes)

2 Principal Machine Functions

2.1 Printer

2.1.1 Overview of Printer Operations

- The Printer function can be divided in to main processes: 1) Converting the printer language data received by the LP 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.

2.1.2 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 LP 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 WebImageMonitor, or “Spooling Job” list on the LP operation panel. The data is developed page by page in the order in which it was converted (beginning from page 1), however the actual printing order of the pages 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 and then stored to the HDD. Once this is completed for all pages, the data is then sent to the printing engine for printing out.
  Note: The order in which jobs are printed out is same whether Image Spooling is enabled or disabled.

- From the printer driver, it is possible to select the following printing methods: Normal Print, Sample Print, Locked Print, Hold Print, Stored Print, and Store and Print. 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 WebImageMonitor or the LP operation panel, after which the page location data is deleted at the conclusion of the job.

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

- When Stored Print is selected as the job type, the image data is saved directly to the HDD as a Stored Print document, without being printed out. When Store and Print is selected as the job type, the image is saved to the HDD and is also printed out. Just as with the above, the documents stored in the HDD can also be printed out from WebImageMonitor or the LP operation panel, however these documents remain in HDD memory even after the conclusion of the print job.

- 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, Locked Print, Hold Print, Stored Print or Store and Print is selected as the print job, the necessary bibliographic information for the document is stored in the HDD along with the image data itself. This information and data is preserved even when the machine main power is turned off.

- 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, Locked Print, Hold Print and Stored Print printing methods, and also appears in the printing history. In addition, it is also possible to set the passwords for Locked Print and Stored Print documents.

- 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 LP. The username and password are sent along with the printing data as authentication data. If authentication fails, the printing data sent to the LP 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 LP 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 WebImageMonitor or the LP 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 LP 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 LP to prohibit the printing of PDF files. PDF files for which this setting is used cannot be printed out when received by the LP, as the LP resets the job and deletes the data.

2.1.3 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 LP will only accept printing data that contains a username and password (or User Code in the case of User Code Authentication) 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 LP 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 LP. When performing the encryption, it is possible to use a key that is common to both the driver and the LP, 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 LP is disabled, the LP will only accept passwords that have been encrypted using the driver encryption key. Therefore under these conditions, even when the LP 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 any authenticated user can view the "Spool Printing" list (WebImageMonitor), printer job history and error log, it is possible to display other users' information in the 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 LP from the operation panel or WebImageMonitor, 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.

- When User Authentication is not enabled, it is possible to view the list of Locked Print documents created by all users, however all filenames are displayed as asterisks ("****"). When User Authentication is enabled, the user cannot view any information on this list until authenticated. However, even after successfully logging in, the user can only view a list of his or her own Locked Print documents (the filenames for which are displayed as is, without asterisks).

- Stored Print or Store and Print documents in the HDD can be printed out from WebImageMonitor or the LP operation panel, as described earlier, and can be protected with a password. If a password has been assigned to the document, the operator will be prompted when attempting to print it out. The document cannot be opened unless the correct password is entered, which prevents illegal access to the document.

- It is possible to make a Stored Print or Store and Print document available for printing out by any authenticated user by selecting “Share” in the printer driver’s Advanced Options settings when the job is sent. It is also possible to change the access privileges setting for the document from WebImageMonitor. Normally, this is set in the printer driver to grant access to either all authenticated users or to the creator of the document alone. However the user can change this setting to grant access to specific user(s) or group(s).

- In addition, it is possible to enable the Document Lock feature, whereby the LP 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. The operator can also change the password at any time, making it much more difficult to surmise. This is particularly helpful in cases where documents are stored in the HDD for extended periods of time.

- The language processing system is only capable of processing legal data in pre-defined formats. Therefore, even in the case that illegal fonts or firmware were downloaded to the LP on-board memory, such data could not be executed as a program nor be processed by any of the LP’s internal 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 LP operation panel or from WebImageMonitor, 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 LP, 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 LP 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 LP that printing of this file is prohibited. Since the LP will reject such data, it is not possible for the data to introduce any illegal programs or be processed by any LP modules.

2.2 NetFile (GWWS)

2.2.1 Overview of NetFile Operations

- NetFile operates via communication with the following applications installed on a network-connected client PC: SmartDeviceMonitor for Admin, Web SmartDeviceMonitor for Admin for Admin, DeskTopBinder, SmartDeviceMonitor for Client

Viewing and Changing User Information Stored in the LP

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

Viewing and Changing Machine Settings Stored in the LP

- Some machine settings stored in the LP can be viewed and changed from inside Web SmartDeviceMonitor for Admin. The operator must be authenticated as a Machine Administrator, Network Administrator or User Administrator, depending on the specific setting.

Transferring Job Log and Access Log Data to Web SmartDeviceMonitor for Admin

- The Netfile job log contains data related to job status (initiation, completion, any changes during the job), while the access log contains data related to operational events (authentication, operations performed on documents, administrator operations). Both logs are saved to the HDD by the LCS, and contain a date and time for each entry. As mentioned in 1.9 Job/Access Logs, it is possible to have the LP send the log data to Web SmartDeviceMonitor for Admin whenever any of the events described above occurs.

  Note: See "**Supplementary**" below for a list of the specific events for which Netfile job log entries are created.

- Only users who are registered with an administrator-level User Account in Web SmartDeviceMonitor for Admin can access the contents from a Web SmartDeviceMonitor for Admin client station.

Deleting Print Jobs

- From inside SmartDeviceMonitor for Client, it is possible to delete, pause, or resume any individual print job sent from the printer driver. From inside Web SmartDeviceMonitor for Admin, it is possible to delete all print jobs at once or the job in progress.

2.2.2 Data Flow

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

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

Viewing and Changing User Data Settings Stored in the LP

- From SmartDeviceMonitor for Admin, it is possible to view and change the user data settings stored in the LP. 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 LP 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 LP 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 1.7 Data Protection.

- Even in cases in which SSL is not used, GWWS encrypts the user's password using the DESS module (but does not encrypt any other part of the user data). The DESS module also communicates directly with the UCS to encrypt the Address Book data when performing an Address Book backup.

Viewing and Changing Machine Configuration Data Stored in the LP

- In order to view or change the machine configuration settings obtained by Web SmartDeviceMonitor for Admin, users must have an administrator-level User Account registered in this utility. The machine configuration data is managed by multiple modules, including the 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 SmartDeviceMonitor for Admin.

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

Transferring the Job Log and Access Log Data

- To send log data from the LP to Web SmartDeviceMonitor for Admin, GWWS communicates with the LCS, which uses its internal modules to load the necessary information out of HDD memory. GWWS then encrypts the data using the DESS module and sends it as a Web SmartDeviceMonitor for Admin client over an SSL connection.

Note: For an overview of the contents and operations of the Netfile job/access logs, please refer to 1.9 Job/Access Logs and "**Transferring Job Log and Access Log Data to Web SmartDeviceMonitor for Admin**" above.

Deleting, Pausing, and Resuming Print Jobs

- The operator can delete, pause, or resume a print job from SmartDeviceMonitor for Client. To do this, SmartDeviceMonitor for Client sends Netfile the request along with a specific track ID, which it manages internally for each job. Netfile in turn forwards this on to the Printer function.

- When deleting a print job from Web SmartDeviceMonitor for Admin, only the request is sent. A track ID is unnecessary in this case, as the operator may only select the job in progress or all jobs for deletion.

2.2.3 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 (LP) via a unique session ID. Only after the LP 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 LP 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 LP.

Viewing and Changing User Information Stored in the LP

- As mentioned above, user data stored in the LP can be captured, added to, deleted, and changed from inside SmartDeviceMonitor for Admin, however this requires User Administrator access rights (see 1.7 Data Protection for more details).

Viewing and Changing Machine Settings Stored in the LP

- As mentioned above, in order to view or change the machine configuration settings obtained by Web SmartDeviceMonitor for Admin, 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. These administrators are the only individuals who can view the user counter values.

Sending the Log Information to Web SmartDeviceMonitor for Admin

- Please refer to 1.9 Job/Access Logs.

Deleting, Pausing or Resuming Print Jobs

- To delete the current job or all active jobs at once, the operator must have Machine Administrator-level access privileges. In addition, the operator must have already logged in to Web SmartDeviceMonitor for Admin as a Machine Administrator.

- As mentioned above, the operator can delete, pause, or resume a print job from SmartDeveiceMonitor for Client. Netfile allows the operation only if the request from SmartDeveiceMonitor for Client is accompanied by the track ID for the specific job in question. This prevents the unauthorized deletion of print jobs by other users.

2.3 Web Applications

2.3.1 Web Server Framework

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

Encrypted Communication Support

- The Web server installed on the LP supports SSL communication. Since the LP 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 WebImageMonitor and the LP. It is possible to set the LP 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

- WebImageMonitor supports the access restriction functions described in section 1.5 of this document. These functions provide greater security by prohibiting unauthenticated users from changing any settings as well as limiting the number of items that can be viewed.

Protection Against Cross-site Scripting (XSS)

- “Cross-site scripting” is a security threat that refers to the introduction of malicious script into the data stored on a Web server with the purpose of causing the following damage when a valid user accesses a Web page associated with that server.
  - 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 LP settings can be made from WebImageMonitor. This ensures that users without valid accounts are not able to introduce script containing malicious data.

- The LP sanitizes all HTML data that is sent from an LP Web application to WebImageMonitor. One of the strongest known countermeasures against cross-site scripting, data sanitizing deletes or neutralizes selected character strings designed to function as HTML tags or script.

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. WebImageMonitor 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” refers to when the session ID stored in a cookie is obtained in order to illegally access or otherwise use a session for malicious purposes.

- Web Image Monitor employs the following countermeasures to minimize the threat of session hijacks:
    - The session ID is randomized, which makes it very difficult for third parties to surmise its value
    - Communication is protected by SSL, preventing theft of any data or messages exchanged
    - The above-mentioned countermeasures for cross-site scripting prevent cookies from being illegally accessed

- In addition, there are also security measures to minimize any potential threat to the LP in the unlikely event the session ID were somehow stolen:
    - The session ID is given an expiration date
    - The session ID contains no information whatsoever that could be linked to individual user data stored in the LP

Protection Against the Setting of Illegal URLs

- The optional URL setting in Web Image Monitor can only be changed by users authenticated as Network Administrators.

3 Optional Features

3.1 @Remote

3.1.1 Overview of @Remote Operations

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

- When communicating as a "client", the LP continually monitors its own status and informs RC Gate or @Remote Center when action is required, such as when parts have reached their periodic replacement limit or an abnormal machine condition is detected. When communicating as a "server", the LP receives requests from RC Gate or @Remote Center for machine status information, after which it provides this information to whichever has requested it.

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

3.1.2 Data Flow

- The communication protocol used is different depending on whether the LP is communicating with the @Remote center directly, or via the RC Gate. The NRS module controls all primary @Remote functions inside the LP.

Communicating with the @Remote Center via RC Gate

- **When the LP communicates with RC Gate as a client (e.g. notifying the center of a malfunction)**

  When the SCS detects an abnormal condition in the LP 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 LP sends the relevant information to RC Gate in an encrypted state via the host I/F.

- **When the LP communicates with RC Gate as a server (e.g. taking a counter reading)**
  Requests for information sent by RC Gate to the LP 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 LP 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.

Communicating with the @Remote Center Directly (via the Internet)

Functionally, the server/client relationship between the LP and @Remote Center is two-way, as described below. However in terms of actual data flow, the LP is always an HTTPS client of the @Remote Center.

- **When the LP communicates with the @Remote Center as a client (e.g. notifying the center of a malfunction)**
  When the SCS detects an abnormal condition in the LP 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 SSL-encrypted and sent to the @Remote Center via the NCS module.

  The NCS module communicates with the @Remote Center via the host I/F over an SSL connection. Both the LP and @Remote center perform a bi-directional, digital certificate-based SSL authentication process to verify that the other is a valid @Remote communication terminal, after which the NRS module accesses the DESS module and compares the @Remote Center ID information sent from the center with the ID information already stored in the LP. (As the @Remote Center ID is unique, each LP is only able to connect to one @Remote Center). If both judge that the other is the legitimate communication terminal, SSL encrypted communication is established, whereby the LP sends the relevant information to the @Remote Center in an encrypted state via the host I/F.

- **When the LP communicates with the @Remote Center as a server (e.g. taking a counter reading)**
  In order to enable the LP to poll the @Remote Center, the NRS module sends the necessary polling information to the NCS module. The NCS module then communicates with the @Remote Center via the host I/F over an SSL connection. The authentication process is the same as described in the paragraph above.

  Requests from the @Remote Center sent as polling responses are received by 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 SSL-encrypted and then sent to the @Remote Center via the NCS module.

3.1.3 Data Security Considerations

- As mentioned above, communication between the LP 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 LP can be connected.

- The LP's digital certificate for the @Remote function is embedded in the LP 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 LP, 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 LP to be mistakenly sent to the @Remote Center.

3.2 The “Copy Data Security” Feature

3.2.1 Overview of Copy Data Security Operations

- The Copy Data Security feature acts to discourage unauthorized copying of confidential documents. There are two aspects to the feature:
  - Marking the copy/print with a visible, embedded pattern

    Note: The marking aspect is a standard feature on LP models.
  - Detecting the pattern if a copy is attempted, and then graying out the entire image

    Note: The detection aspect is provided as an optional feature on MFP models only (Copy Data Security Unit).

- Marking:

  If the user selects the Copy Data Security feature when making the first copy of a document or printing out the document for the first time from the printer driver, a pre-defined pattern will be embedded in the background area of the resulting image to demarcate that copying of the image is prohibited. Users can select from among several patterns, as well as add a text string such as “Copying of this document is prohibited” or the date, time or name of the user who created the original document (details below).

- Detection/Graying:

  If a user then attempts to make a copy of an image containing the embedded pattern (or store the image to the MFP Document Server), and the optional Copy Data Security Unit is installed on that MFP, the pattern will be detected and a buzzer will sound. The image is then grayed-out to hide the original contents and then exited to the tray. In addition, a log entry of the event will be added to the Access Log, along with the date, time and username.

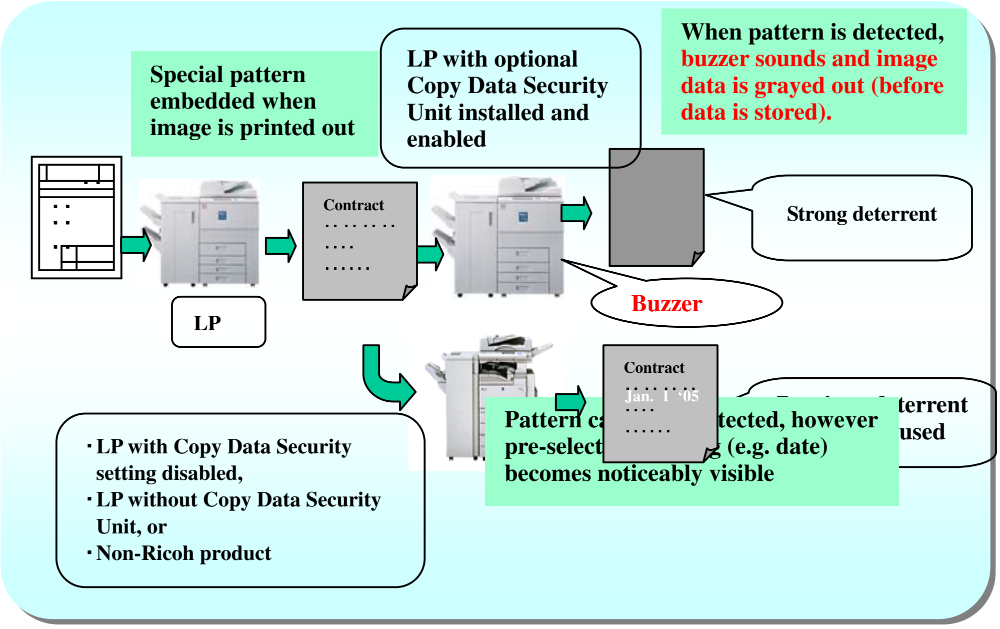
  If a user attempts to make a copy of an image containing the embedded pattern on an MFP without the optional Copy Data Security Unit, including products of another make, the resulting image will not be grayed out. However, it will be much more indecipherable due to the superimposition of the pattern on the original image. In addition, if the user entered a text string to be embedded into the pattern when printing out the original document, the text will be made visible when a copy of the document is made. This optional text field can be set to a number of different character strings to suit the operator’s needs, such as “Copying of this document is prohibited”, the date on which the document was created or the name of the user who created the document By making this information visible, it is possible to further deter the unauthorized copying of documents.

  Note: The exact appearance of this optional text string (size, image density, etc.) will depend on the type and condition of the machine making the copy.

3.2.2 Data Flow

- Marking:

  The data flow for when the Copy Data Security feature is selected at the time a print job is performed is virtually the same as that of regular print jobs (see 2.2 Printer). 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. It is then combined with the background pattern selected by the user and stored temporarily in the Page Memory in binary bitmap format.



Special pattern embedded when image is printed out

LP with optional Copy Data Security Unit installed and enabled

When pattern is detected, buzzer sounds and image data is grayed out (before data is stored).

Strong deterrent

- LP with Copy Data Security setting disabled,
- LP without Copy Data Security Unit, or
- Non-Ricoh product

Pattern ca tected, however pre-select g (e.g. date) becomes noticeably visible

terrent
used

4 Device SDK Applications (DSDK)

4.1 Overview of Operations

- DSDK applications developed by Vendors are able to make use of the printing and other LP functions by calling the VAS (Virtual Application Service), which wraps the GW-API for the standard principal functions of the LP. 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 LP: 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 (Compact Virtual Machine) Java core developed by Sun Microsystems. The GW system regards the CVM Java core itself as a single Type 1 SDK application.
  Note: The required CVM version is ver1.01/J2SE1.3 (or equivalent).

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

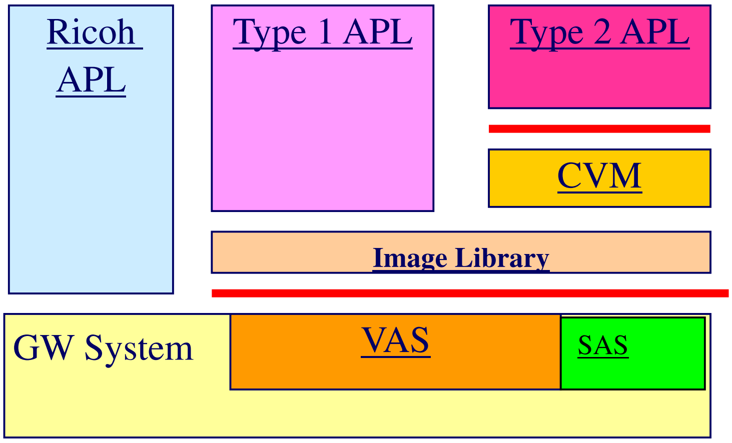


Fig. 1

4.1.1 Installation

- DSDK applications are installed via Type 1 or Type 2 SD cards into partitions and directories in the LP HDD or SD card itself that are specifically allocated 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 4.3.2 Authentication of SDK Applications at Installation below.

4.1.2 Overview of SDK Application Functions

- As mentioned above, Vendors can create their own DSDK applications for installation on the LP. Vendors are provided with an image library, which simplifies complex internal LP operational flows into concise, predefined methods for simple execution. This allows Vendors to develop their applications relatively easily. One example would be a method that searches for a file stored on the LP HDD and then retrieves or prints out the file.

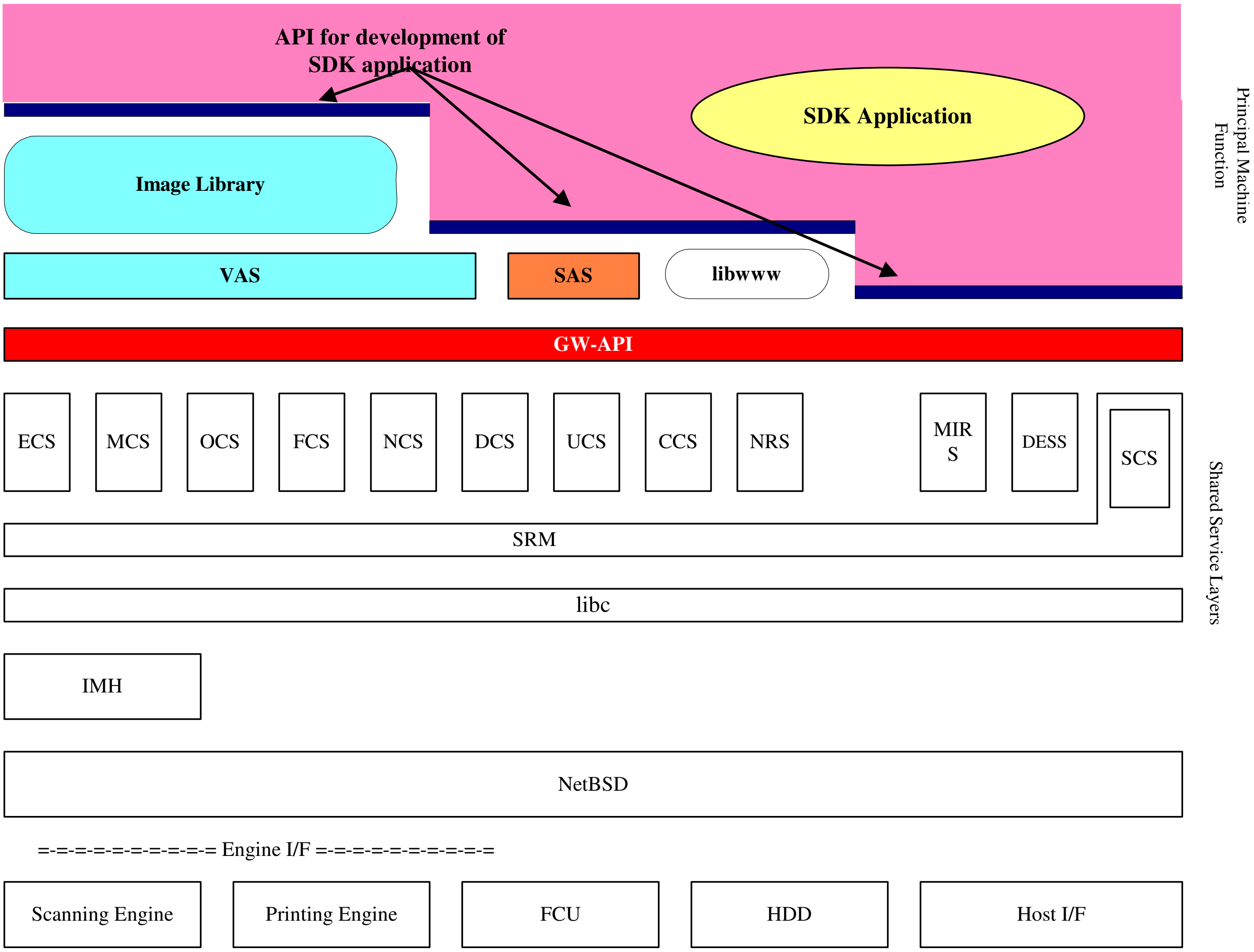


Fig. 3: DSDK/LP Hardware Configuration

4.2 Data Flow

4.2.1 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.

4.2.2 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 LP, 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 LP 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 section 2.2 and is printed out by the printing engine.

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 LP:
  - 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 LP, 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 below, without the correct product ID, there is no way to install the SDK application on the LP.

- The LP 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 LP, 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 LP 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 LP 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 LP.

- As demonstrated above, it is not possible to install an SDK application on the LP 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 LP 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 LP 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 LP 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 LP in question, and having determined that the application poses no security threat to the LP, 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, 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 LP Functions, Prevention of Damage to the System

Buffer Overflow Attacks on the LP 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 LP 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 LP 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

- 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). In the latter case, all communication including the content of all messages and data exchanged is encrypted, and specialized protocols and authentication procedures are employed. As a result, these safeguards protect the LP from any attacks 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 functional 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 (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.

- If the Vendor then makes any changes to the application after receiving the authentication files from Ricoh, this Vendor must go through the entire certification process again to obtain new authentication files. It is therefore impossible for an SDK application to be successfully installed on the LP 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.