Konica Minolta Security White Paper

Security Basic Policies and Technologies

Provided by Konica Minolta

Version 8.0.4

August 26, 2014

Notice: This White Paper is for KM subsidiaries.

In the White Paper, there is information of specifications that are supported only for unreleased models. When explaining to users, please refer to the attached list of security specifications on each model.

Version 1	August 2004	First release
Version 1.1	September 2004	Added description of applicable models
Version 2.0	February 2005	Added description of applicable models
Version 2.1	February 2005	Corrected Version2.0
Version 2.2	March 2005	Corrected Version2.1
Version 3.0	October 2005	Revised functions and description of applicable models
Version 4.0	May 2007	Revised functions and description of applicable models
Version 5.0	October 2007	Revised functions and description of applicable models
Version 5.1	August 2008	Addition of applicable models
Version 5.2	January 2010	Addition of functions and applicable models
Version 5.3	September 2010	Addition of functions and applicable models
Version 5.4	May 2011	Added description of applicable models
Version 5.5	February 2012	Addition of functions and applicable models
Version 5.6	April 2012	Addition of functions and applicable models
Version 5.6.1	May 2012	Addition of applicable models
Version 6.0	November 2012	Addition of descriptions and applicable models
Version 7.0	February 26, 2013	Addition of descriptions and application models
Version 7.1	October 18, 2013	Addition of descriptions
Version 8.0.1	Jun 10, 2014	Addition of descriptions and application models
Version 8.0.3	July 14, 2014	Addition of descriptions for TPM
Version 8.0.4	August 26, 2014	Addition of applicable models(C3110、C3100P、4700P、4000P、3300P)

Konica Minolta products come with various security technologies. However, these technologies work effective only when customers use their products based on the Konica Minolta's security policies. We appreciate your understanding that you use Konica Minolta products based on the contents described here. For each setting, please see User's Manual of the products. Also, please understand that this document does not assure a complete security.

Active Directory is the trademark of Microsoft Corporation.
VxWorks is the registered trademark of Wind River Systems, Inc.
Adobe Acrobat is the registered trademark of Adobe Systems Incorporated.
Felica is the registered trademark of Sony Corporation.
Linux is the registered trademark or trademark of Linus Torvalds in Japan and other countries.

Table of Contents

2. ID & Print (Secured printing by “One Touch”)

VI. Extended functions in cooperation with PageACSES

1. Scan with authentication
2. Print with authentication
3. Access control per file (only Page ACSES Pro)

VII. PKI Card authentication system

1. The login that PKI Card is used
2. LDAP Search that PKI Card is used
3. SMB sender that PKI Card is used
4. E-mail sender（S/MIME）that PKI Card is used
5. PKI Card Print
6. Scan To Me / Scan To Home

VIII. Security about MFP self-protection

1. Verify Function for Firmware

IX. Security about CS Remote Care

1. Security when public lines (modem, FAX) are used
2. E-mail security
3. Security on HTTP communication
4. Product authentication
5. Security at DCA

X. Security about bizhub Remote Panel

1. Communication, Connection trigger
2. Authentication
3. Access Code
4. Audit log

XI. Security about bizhub Remote Access

1. Communication, Connection trigger
2. Auto cut-off due to timeout
3. Security on administrator mode
4. Security when cut off during remote operation
5. Security when used in both user authentication and account authentication

In the current market where network infrastructure has been developed and IT is widely spread, huge amount of information is distributed. And at the center of business, information is gathered in diverse ways and translated into higher-level information assets. It is a significant task for every company to protect these information assets for risks management.
This document introduces basic security functions provided with Konica Minolta bizhub, Sitios, and DiALTA series.

I. Security Basic Policies

1. Equipment of Latest Security Technologies

Konica Minolta develops and provides all possible and latest security functions from every angle, in order to protect customers' information assets from various threats that are categorized below.

(1) Unauthorized access and/or information leak via network
(2) Unauthorized use and/or information leak by direct operation on device
(3) Alteration, copying and/or erasing of electronic and/or paper information
(4) Information destruction by human disaster or device failure
(5) Trace function with logs, etc.

2. Certification from 3rd party company

Konica Minolta has been certified according to ISO15408 on almost all the MFP products (A4/20 or higher PPM) released from March 2004, to objectively prove equipment of security functions.

ISO15408 certification is obtained based on the initial Firmware.
When ROM such as maintenance release is released, we don't use the guarantee continuous system anymore, but we will support so that the security functions can be maintained.

And MES (RSA BSAFE Micro Edition Suite) Encrypted modules installed in the machine acquired the certification of FIPS140-2.
Thereby, it certify that software is strong and safe and it is possible to sell to the organization which makes the certification of FIPS140-2 indispensable.

I. Security from public telephone line

1. Security from FAX line

Communication with FAX line uses only FAX protocol and does not support other communication protocols.

If somebody attempts to intrude from outside with a different protocol via public line or send data that cannot be decompressed as FAX data, Konica Minolta products handle that kind of event as error by software and blocks off the communication.

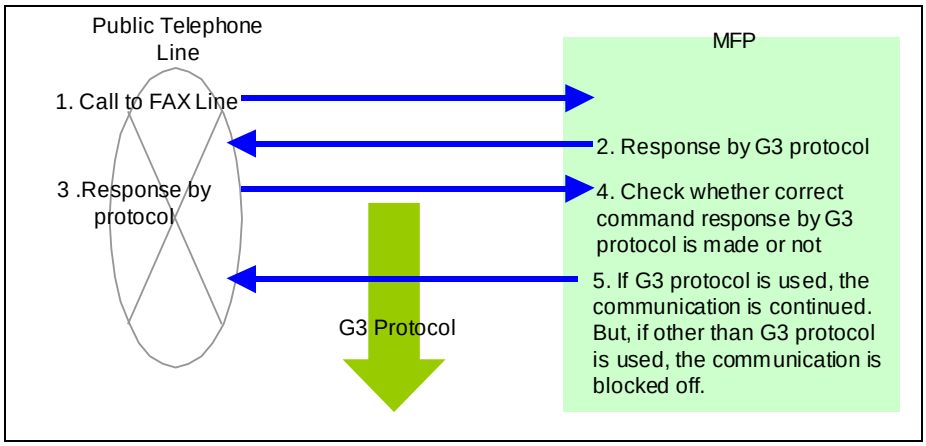


Figure 1-1

2. Putting number twice

When putting the address of fax by use of telephone number, you have to put the number again. By confirmation of matching these two numbers, miss-send from wrong number can be prevented.

Also when you register the speed dialing, you have to put the number twice. The correct number can be registered.

3. Putting regular number and abbreviation number for preventing miss-sending

For putting address to send fax, combination of speed dialing and direct ten/key can be used. Wrong number can prevented by registering speed dials for area codes.

4. Display for address confirmation

When you enter the destination address (e.g. speed dialing, telephone number etc.), the address will be displayed on the operation panel. Then you confirm and send the fax. By this procedure, you can prevent from sending to wrong address.

5. Selecting one address per sending

By allowing to set only one address, when sending fax it can be prevented to send to unintentional destination.

6. Confirmation of telephone number of fax system to send

When the fax transmission starts, the telephone number of the device to send fax will be confirmed by use of the fax protocol signal (CSI) received from the device. When the numbers are matched, fax will be sent. By this way fax can be sent more safely.

II. Security with LAN connection

1. Security with network protocol

Operation can be enabled/disabled for each port.

Invasion from outside can be prevented by disabling unnecessary ports.

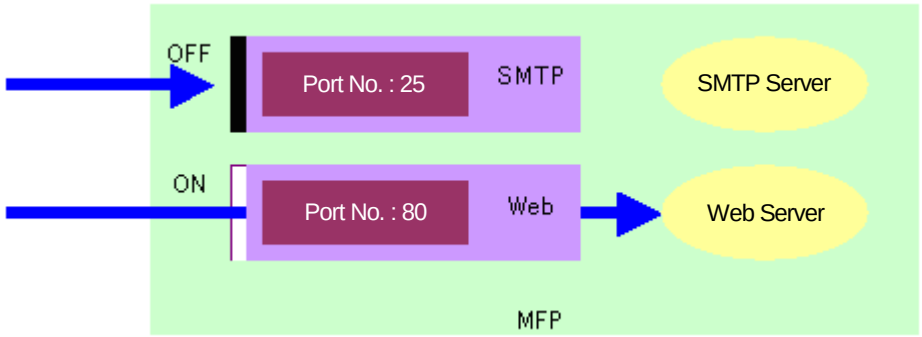


Figure 2-1

Filtering function of IP address enables selection of access to devices on the network by setting the addresses.

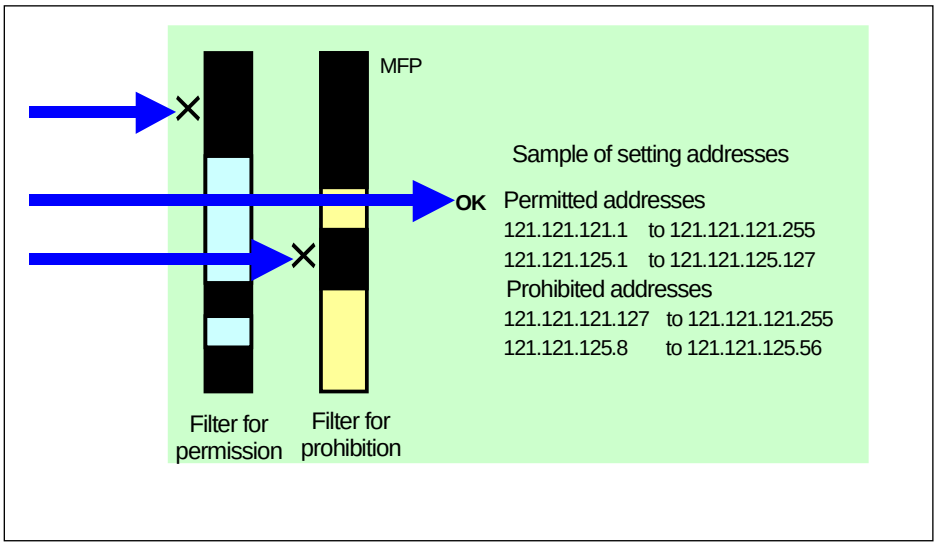


Figure 2-2

2. User authentication

This is available for network related functions using the network authentication function provided by Active Directory service. And not only for network function but also for device function, authentication by Active Directory is available.

Authority to use is given by combination of pre-registered user ID and password. Internal data is protected since only the pre-registered users can use the devices.

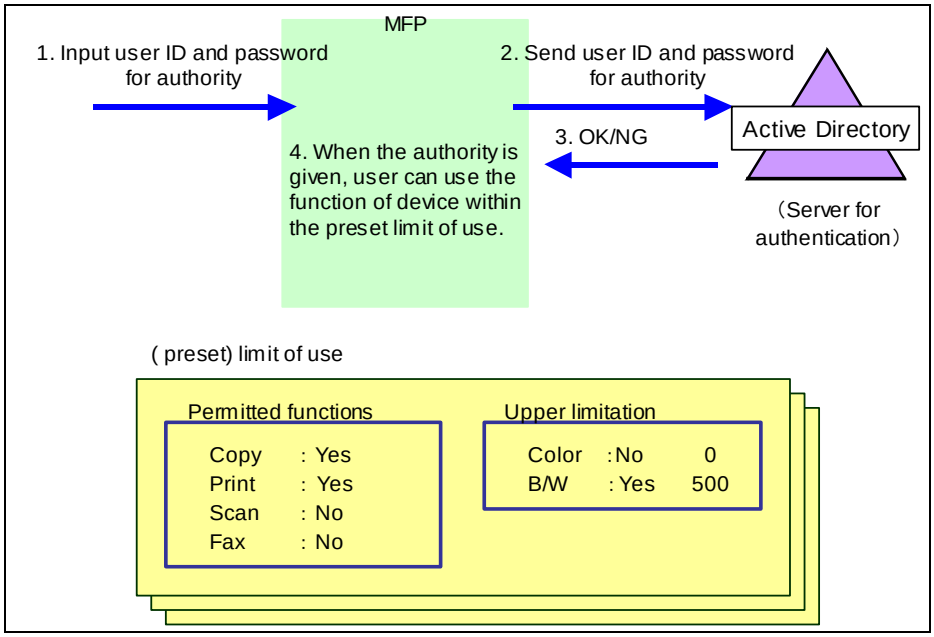


Figure 2-3

3. Security of device control from network

(1) Security on address book data import from network

Input of device administrator's password is required to import address book data collectively from network. If wrong password is input, data cannot be registered. Since the data registration is password-protected, there is no chance to alter the existing address book data at a time.

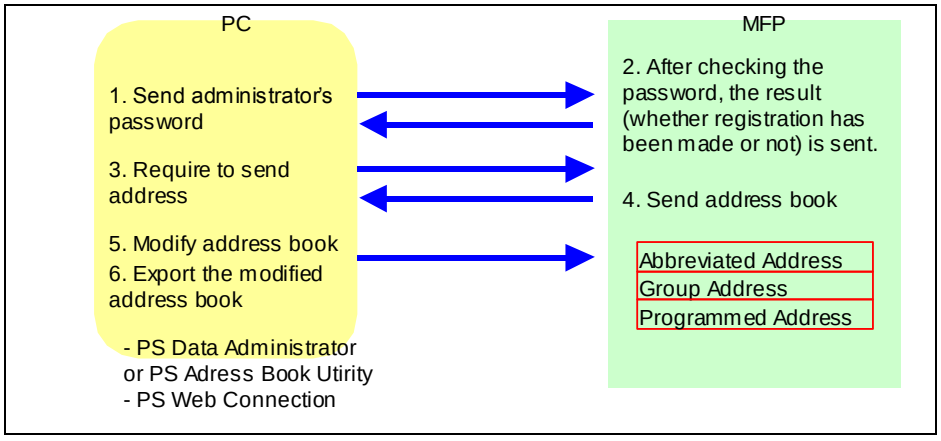


Figure 2-4

(2) bizhub OpenAPI

bizhub OpenAPI acquires and sets the data of devices via network by SSL encryption protocol. And by using its original password, communication will be made more safely.

When managing the important data of the device (e.g. setting information of user authentication) by PageScope Data Administrator, the data is safely protected by bizhub OpenAPI.

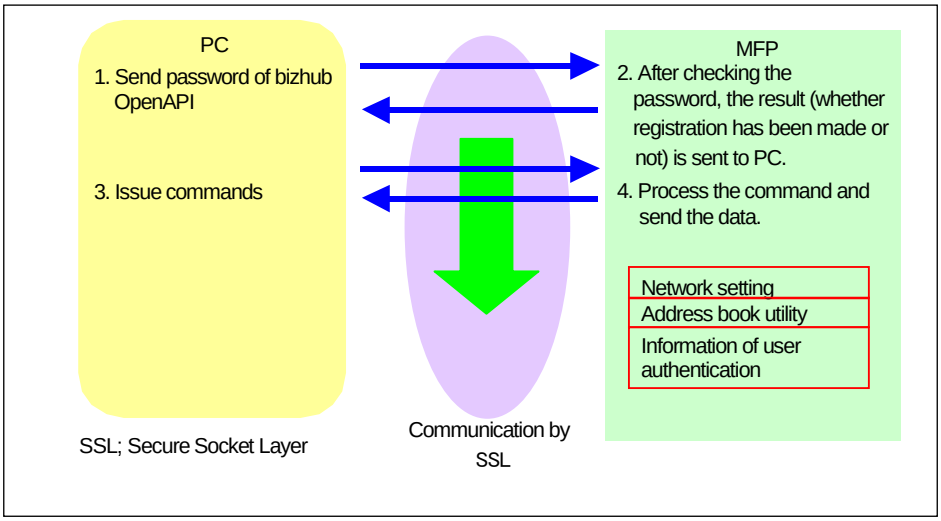


Figure 2-5

4. Encryption of data communication

SSL encryption protocol is used for data communications between LDAP server, PageScope Data Administrator or Address Book Utility, and PageScope Web Connection, and the main body. Data is protected as it is encrypted during communications between networks. IPsec that can be encrypted data without communication protocol is adopted for carrying out the communication encrypt corresponding to IPv6.

5. Quarantine Network Support

The IEEE802.1x feature allows you to authenticate the device against the RADIUS (Remote Access Dial in User System) server in order to connect to the quarantine network. The connection is carried by the switching hub corresponded. These networks will only allow devices into the network if the RADIUS server approves the authentication

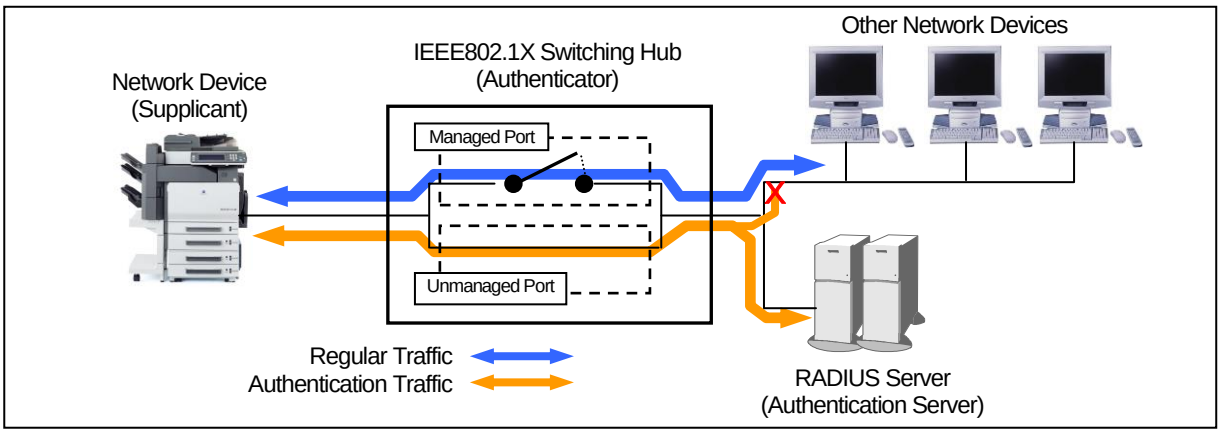


Figure 2-6

6. Certificate verification by dual direction

Conventional type of MFP have the certificate in there device, and they transmit it to the devices of destination. The validity of MFP can be certificate in this way. Our MFP products verify the validity of the device of the destination by themselves. And transmission is controlled by confirming the validity by dual direction, we can prevent "Spoofing" adequately this way.

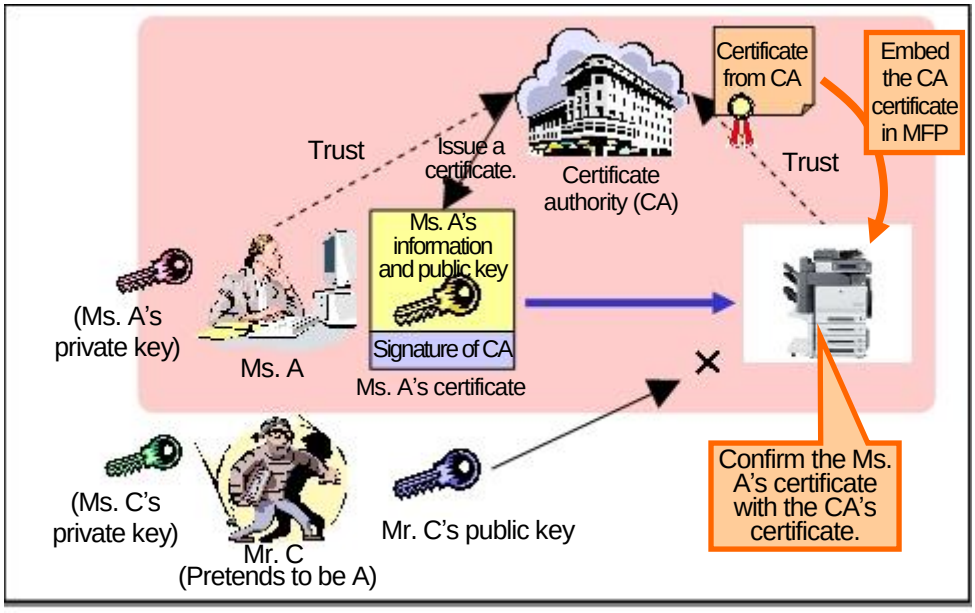


Figure 2-7

7. Action against virus

Differently from usual PCs, controllers that are built-in Konica Minolta products use VxWorks for OS. Therefore, it is considered to be rare that controllers are affected by viruses via LAN.

Server typed Fiery controllers made by EFI use Windows for OS. However, the vulnerability of Windows is covered by providing necessary Windows security patch on a timely basis.

8. Protection against virus from USB memory

Virus infection from USB memory is caused by program files automatically executing when the USB memory is inserted in the device. Konica Minolta devices do not support functionality to automatically execute files by inserting the USB memory. Therefore, Konica Minolta devices are not affected by these types of viruses.

Konica Minolta devices support capability to print image data stored in USB memory, as well as store scanned data and User Box data in the USB memory. However, these tasks are done through user operation and not through automatic execution.

9. Monitoring of the security of Linux kernel

Concerning Linux kernel, R&I division of Konicaminolta is constantly monitoring the information of the security vulnerability and security patch. And it is confirmed whether the public information of vulnerability will effect the function of MFP or not.

10. Separation from USB I/F path

The path of USB I/F and the path of network are separated system structurally. If MFP is connected to USB of the PC connected to the Internet, MFP cannot be accessed from the Internet environment through the PC.

III. Security of data stored in MFP

1. Security on image processing and printing

Data read with the scanner is image-processed, compressed, and then written onto main body memory（volatile DRAM）. Further, print data is decompressed, sent to printer and then output on paper. Data is overwritten by page on memory. Therefore, re-output of data is not possible.

Since job data (compressed data) is deleted from the memory at the same time when it is output or transferred, re-output or retransfer of the data by 3rd person is prevented.

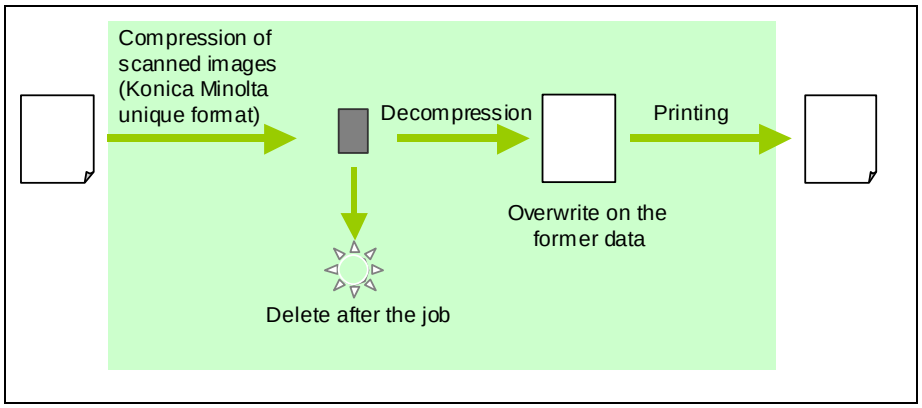


Figure 3-1

Job data is stored on DRAM or HDD in Konica Minolta unique compression format. Therefore, even if somebody reads out the internal data, it is extremely difficult to analyze it. And even if HDD is taken out, security of data in HDD is protected because the data in HDD is encrypted when stored. (Option)
If a lock password is used, even if HDD is taken out, the security of HDD is protected.

Further, when using Secure Print function, print job is once stored on the main body memory and print operation takes place after the assigned password is input from the main body operation panel. This function prevents the output from being taken by other people.

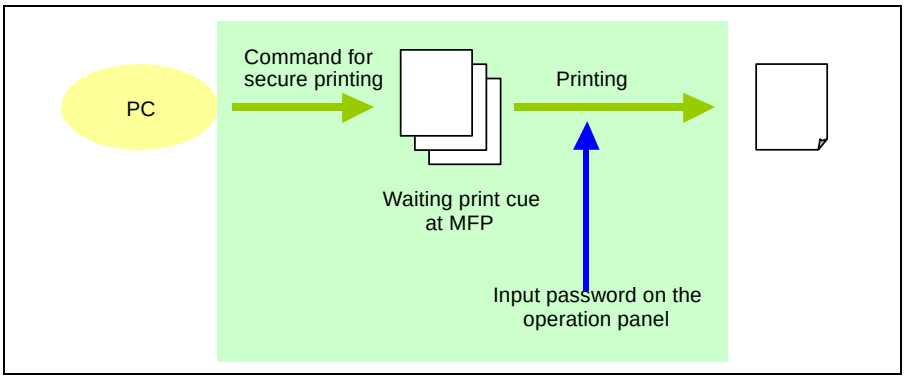


Figure 3-2

2. User authentication

The engine supports the user authentication feature. Users can authenticate against the MFP, external authentication server such as Active Directory, or PageScope Authentication Manager. Authentication can be done by entering the User ID and PW, or by using IC Cards/Biometrics.
Users can limit functions such as copy/print/scan/fax as well as limit the usage of color by user. Also, access to destinations (such as fax or e-mail destinations) can be limited according to authorization levels.

(1) Authentication can be done by using external authentication server, however, even if the customer does not have an external authentication server in their network, users can still authenticate by using the authentication feature embedded within the device.
(2) Usage of copy/print can be managed per user by presetting upper limit on the device.
(3) It is possible to set authentication and upper limitation per user by color and B/W.

3. Box security

In addition to the user authentication, access to the data inside of the box can be protected by password.

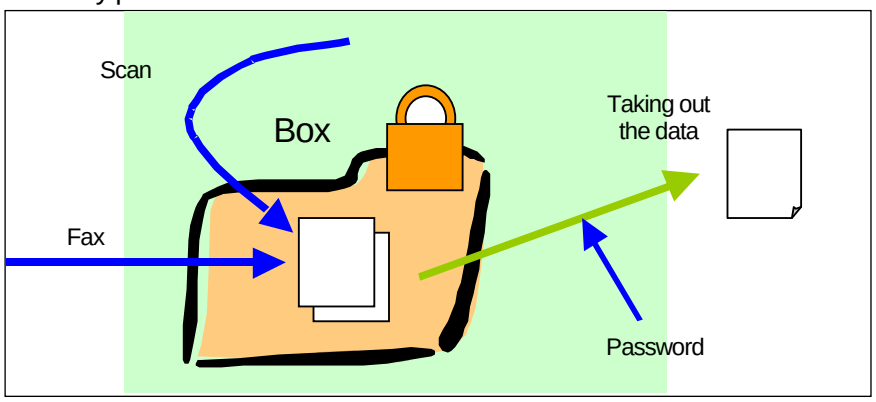


Figure 3-3

4. Complete data deletion when discarding HDD

There is a function to erase the internal data of HDD by overwriting with a certain pattern of numbers and/or random numbers.
Using this function, customers can prevent confidential data from leaking after MFP main body is disposed.

5. Protection of data in HDD by password and encryption

HDD can be locked by password. When HDD is locked, even if HDD is taken out of the MFP main body and set with PC, without password, access to the data becomes not possible.
And, the data in HDD can be encrypted with AES. Even if the data is taken out, the data cannot be decrypted without the key of encryption.

6. Access management by audit log

All history of MFP operations for security can be stored into audit log data.
With this log data, it is possible to trace unauthorized accesses.

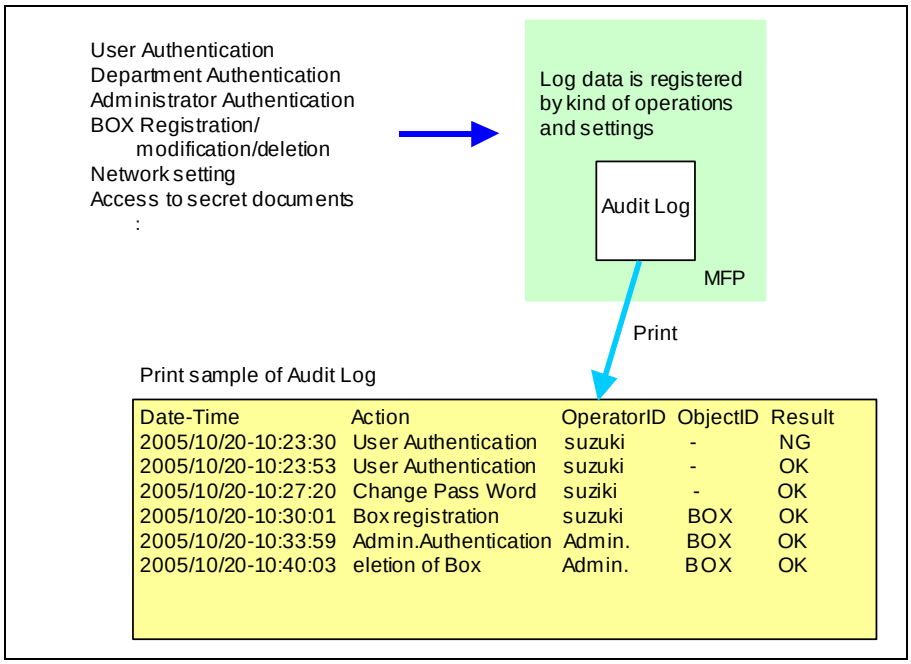


Figure 3-4

7. Encryption of data in PDF file

When storing scanned data as a PDF file, the data can be encrypted by using the common key. In order to open the PDF file with Adobe Acrobat, it is necessary to input the common key.

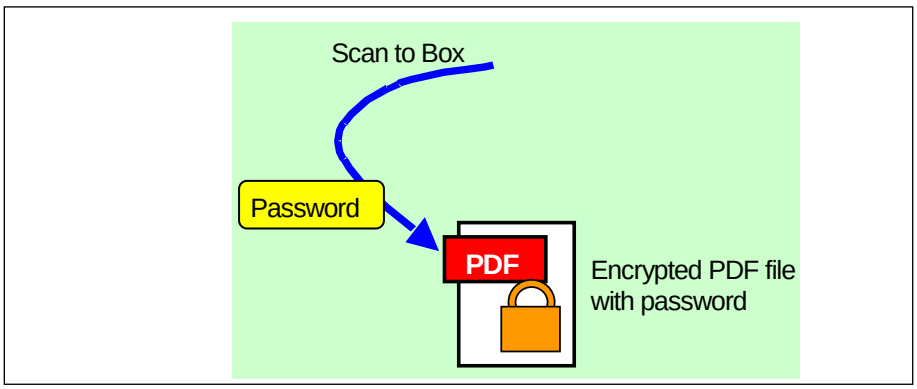


Figure 3-5

8. Encryption of the data in e-mail

When an e-mail is sent from MFP, the data in the mail can be encrypted by the recipient's certificate (public key, which can be registered in the address book in MFP), and the recipient can decrypt the data in the mail by his private key. By this procedure, the data in the mail cannot be interrupted by others and secured correspondence will be available. The certificate registered in the LDAP server can be used for the public key on the network.

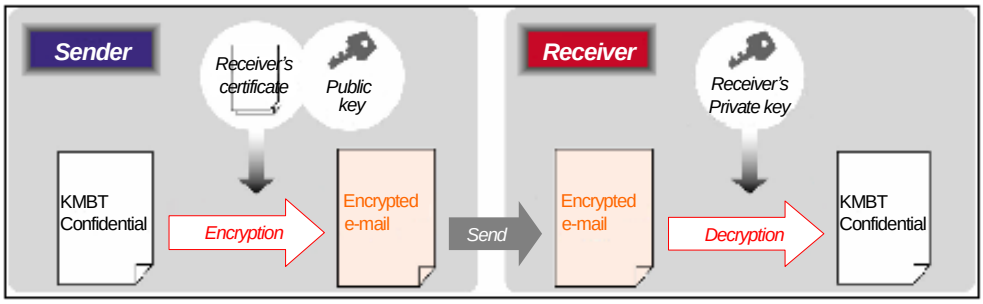


Figure 3-6

9. Digital signature on the e-mail

When an e-mail is sent from MFP, digital signature can be made by use of the private key of MFP, and the recipient can verify the signature by the public key and check whether the data on the mail has been modified illegally or not.

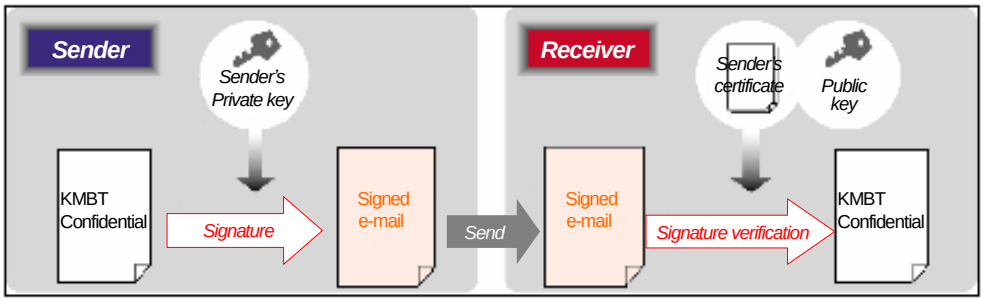


Figure 3-7

10. Scan to Me, Scan to Home & Scan to Authorized Folder

This function allows you to scan data easily back to yourself. When user authentication feature is turned ON, the “Me” button will appear in the Address Book. Also, by enabling in Administrator Mode, the “Home” button can be displayed in the Address Book.

By selecting the “Me” button as the scan destination, users can send the scanned data to their own e-mail address. By selecting the “Home” button as the scan destination, users can send the scanned data to their pre-registered PC folder.

When registering the SMB destination, by leaving the User ID and PW blank, the login User ID and PW can be carried over to be used as the User ID and PW to access the registered SMB destination. This will prevent the SMB destination to be used by unauthorized users.

Also, the administrator can limit/prohibit users from registering destinations in the Address Book, or manually entering the destination, allowing the administrator to be able to manage destinations that can be sent from the device.

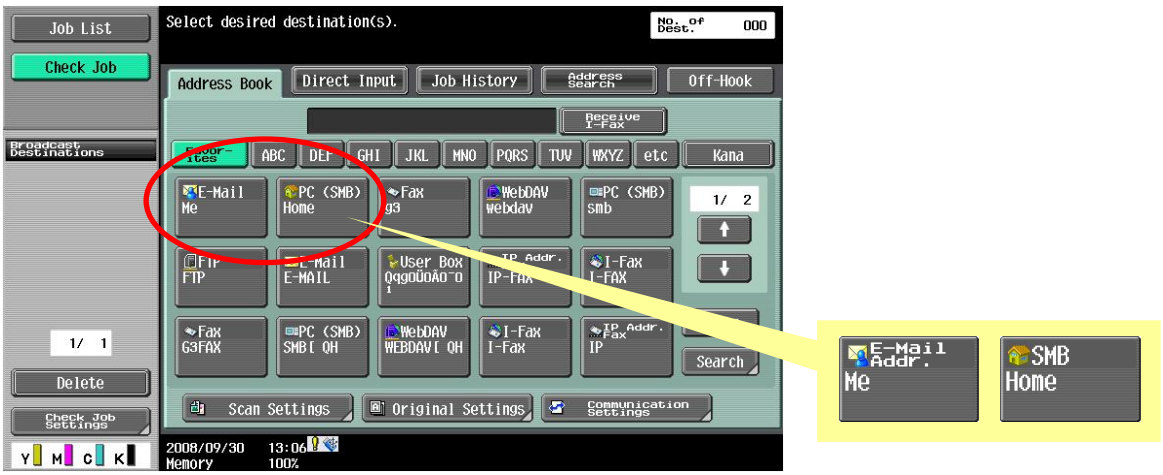


Figure 3-8

11. Overwrite to delete the temporary data (HDD data).

When the setting of Overwrite to delete the temporary data (HDD data) is "On", MFP overwrite to delete the data saved temporarily at the hard disk at the time of the end of use of image data, for example, completion of jobs such as a print and a scan, deletion operation of a box document.
The risk of the unnecessary image data on a hard disk being reused is reduced.

12. Adoption of the Encrypted modules which received authorization

Encryption and the authentication function have been attained by installing Encrypted modules, such as OpenSSL / MES（RSA BSAFE Micro Edition Suite）, in MFP.

The main functions to use the MES Encrypted modules which received authorization of FIPS140-2 are the following item.

1. Encrypted communication at the time of sending scanning data
   At the time of SSL communication of can to WebDAV, TWAIN etc
   At the time of S/MIME transmission of Scan to E-Mail
2. At the time of SSL communication of PSWC
3. PDF encryption file generating function

13. Data protection by using TPM

(1) Purpose

When the MFP is physically analyzed or the network packet is eavesdropped, the password and other information may be in danger of being leaked into a

vicious user. It is possibly that the MFP is accessed illegally resulting in a leakage of the important internal data.

Since a root key created inside the TPM cannot be taken out of the TPM, a TPM chip is required for decrypting the data encrypted with the root key. Therefore, by using the TPM, the password and other information are protected from leakage.

[Data to be protected]

1. Certificate to be registered by an administrator
2. An administrator password and a password to be set by an administrator
3. A password to be set when the MFP provides services as a server

(2) Structure of the protection by using TPM

Normally, to prevent the password and other information in an MFP from leakage, a 256-bit AES key and a 2048-bit RSA key were used. To efficiently use a TPM for protecting data, use the root key of the TPM to encrypt the RSA key as shown below.

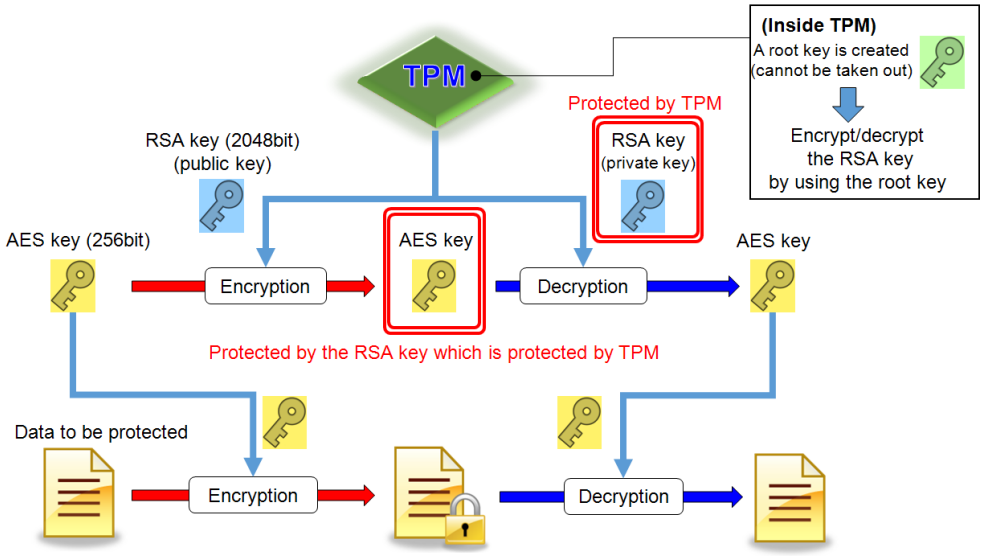


Figure 3-9

Since the root key cannot be taken out of the TPM, a TPM chip is required for decrypting the RSA key. If the RSA key is failed to be decrypted, also the AES key cannot be decrypted, that makes decryption of the password and other encrypted data disabled.

Therefore, even when a vicious user tends to analyze or eavesdrop on the password and other information, no leakage of the password and other information will occur, since they are protected by the TPM and disabled to be decrypted despite of using a TPM chip.

(3) Backup of the TPM key

The RSA key shall be backed up to a USB memory or other storage devices beforehand to relieve the encrypted data at occurrence of defect on a TPM chip. (Concerning security, the RSA key shall be stored safely by encryption and etc.)

IV. Security of output data

1. Copy Security Function

(1) Copy Protect Function

This function is putting the woven pattern on the copied or printed image as the original document. When the original document is copied, the woven pattern of message (e.g. “Copy”) comes up and by that message the copied document can be clearly distinguished from the original one.

Besides the message, serial No. of MFP and copied date and time can be set for the pattern. Combination of the information on the woven pattern and audit log helps to trace the person who copied illegally.

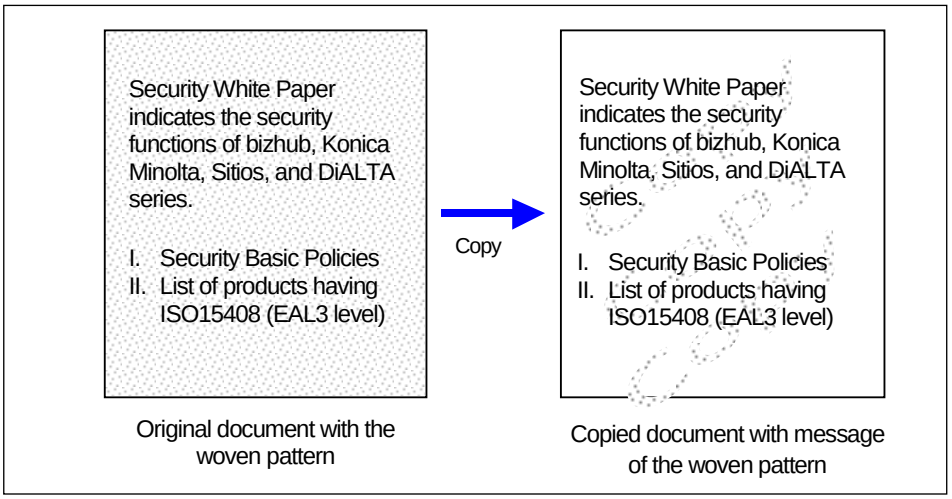


Figure 4-1

(2) Copy Guard Function/Password Copy Function

This function allows you to embed a Copy Guard security pattern on the output so that when a user tries to make a secondary copy of the output, the device will display a message that says “Copying Prohibited” and will prohibit copying. Also, the Password Copy Function allows you to set a password so that by entering the correct password, the Copy Guard security pattern embedded document can be copied.

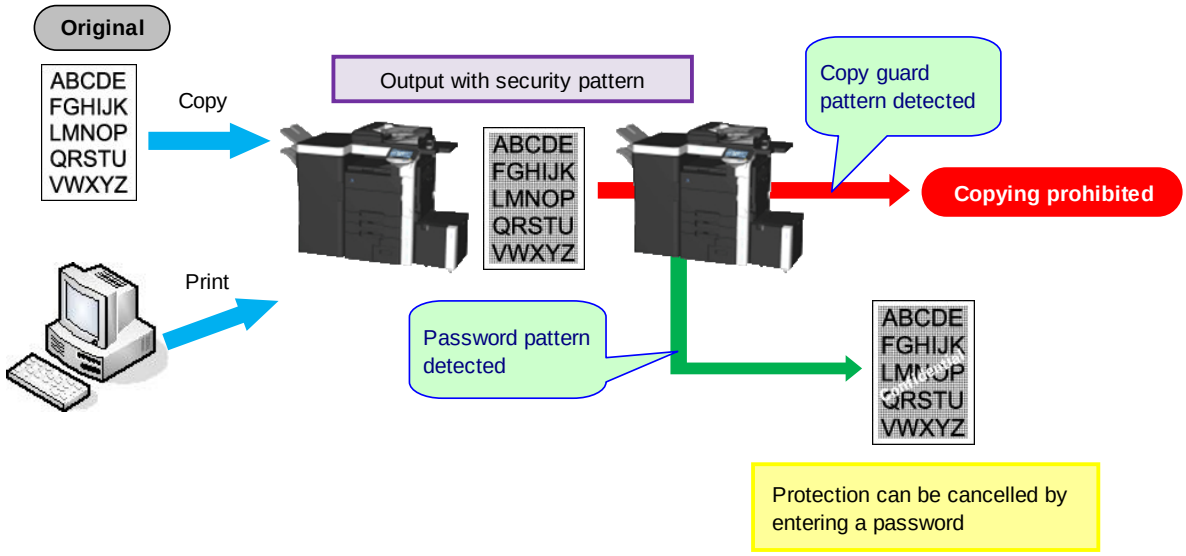


Figure 4-2

V. Authentication Devices

1. Security of the data for the biometric authentication device

The data for the biometric authentication device, AU-101 is handled in a very secure manner, and cannot be used illegally.

The Vein on the finger as the biometric data

The vein is located in the body and it cannot be scanned/read without notice unlike fingerprint. So, it is very difficult to forge.

The way of process hired by this system

This system implements the security guide line based upon “U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (BVMPP-MR) Version 1.0”*

Some of the important security/privacy specifications supported by this system are as follows:

<Reconstruction of the biometric data>

The data registered into the HDD is the random numbers calculated based on the feature of the scanned data. And it is theoretically impossible to reconstruct the original vein data from the data in the HDD.

<Structure of the data in the HDD>

The structure of the data in the HDD is not made public. So, it is impossible to forge and pretend somebody.

<Erase of the data in the authentication device>

The data left in the device is encrypted when storing in the RAM temporarily, and is erased after transferring to MFP.

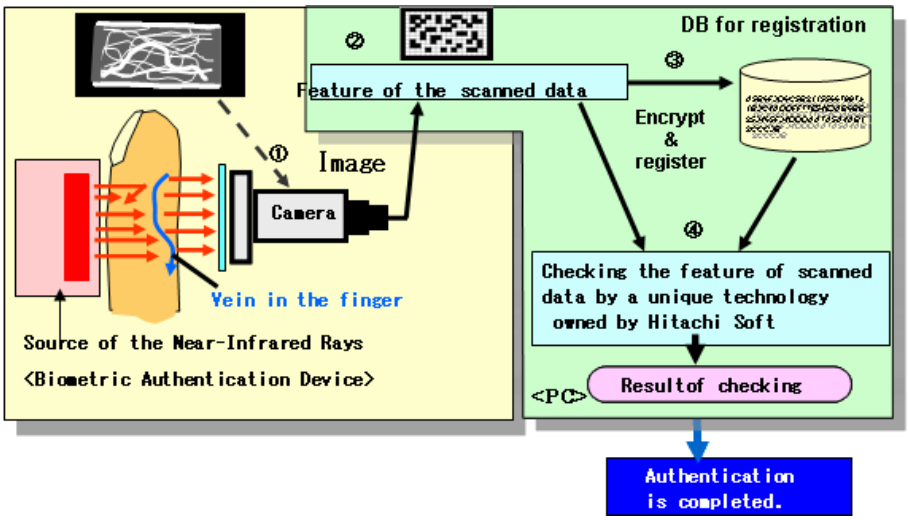
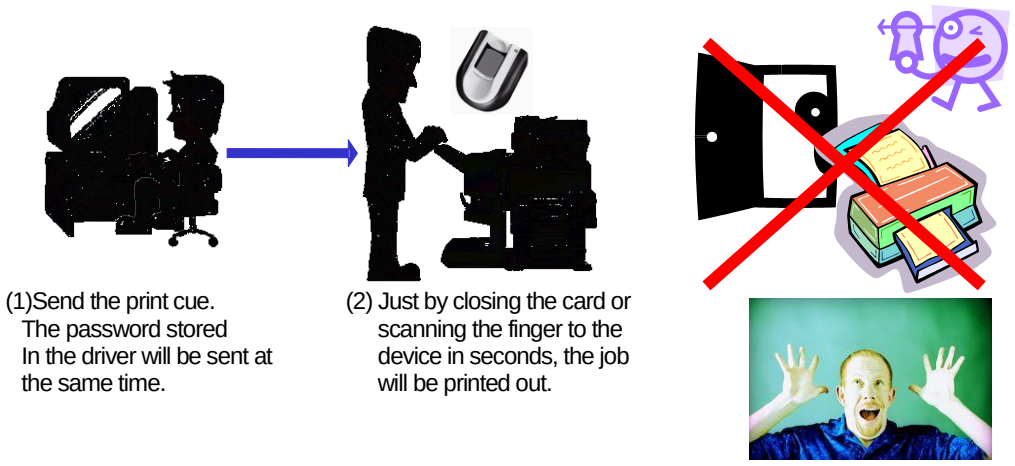


Figure 5-1

U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (BVMPP-MR) Version 1.0 :
Please refer to http://www.commoncriteriaportal.org/public/files/ppfiles/PP_VID10140-PP.pdf

2. ID & Print (Secured printing by “One Touch”)

By equipped with the biometric authentication device –AU-101-, or with the IC card authentication device –AU-201-, not only easy authentication but also simple and high secured print job (ID & Print) will be available. “ID & Print” will prevent the print from being taken away and also from being intermingled with other prints.



(1)Send the print cue. The password stored In the driver will be sent at the same time.

(2) Just by closing the card or scanning the finger to the device in seconds, the job will be printed out.

Figure 5-2

By cooperation with PageACSES, the security function of MFP will be extended and the usability will be improved.

<Overview>

Authentication functions by file (only PageACSES Pro version)

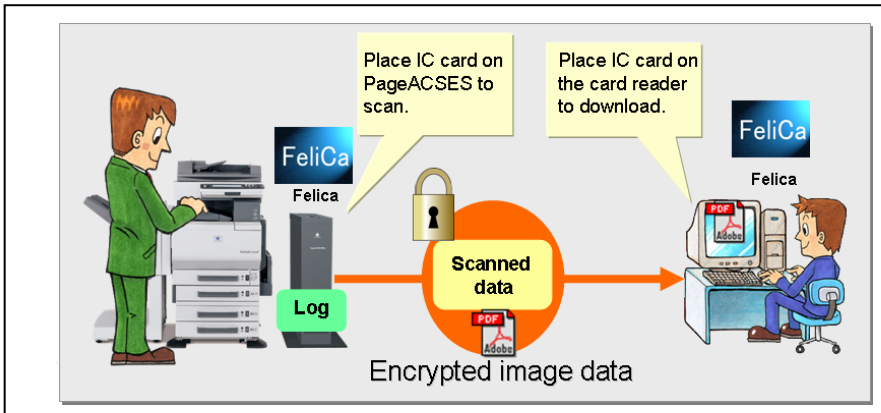
Authorization settings for browse, correction, and printing can be configured per file for respective users. External leakage and falsification of important documents scanned by MFP is prevented by this authentication function and the encryption of image file.

User authentication using IC cards

User authentication using a noncontact IC card (FeliCa) allows logging in MFP without entering the password.

1. Scan with authentication

It prevents direct external sending of scan data as it is. The data that was encrypted by IC card information and was sent to the client PC is taken out using the IC card. At the same time, you can log operation records about copy, print, and scan.



1. Prevention of improper scan by a member without scan authorization
2. Inhibition of improper scan by a member by means of log monitoring
3. Prevention of flow of information by network hacking
4. Prevention of improper acquisition of scan data

Figure 6-1

2. Print with authentication

Printed data is encrypted when printing, and you can take out the print job you sent using your IC card.

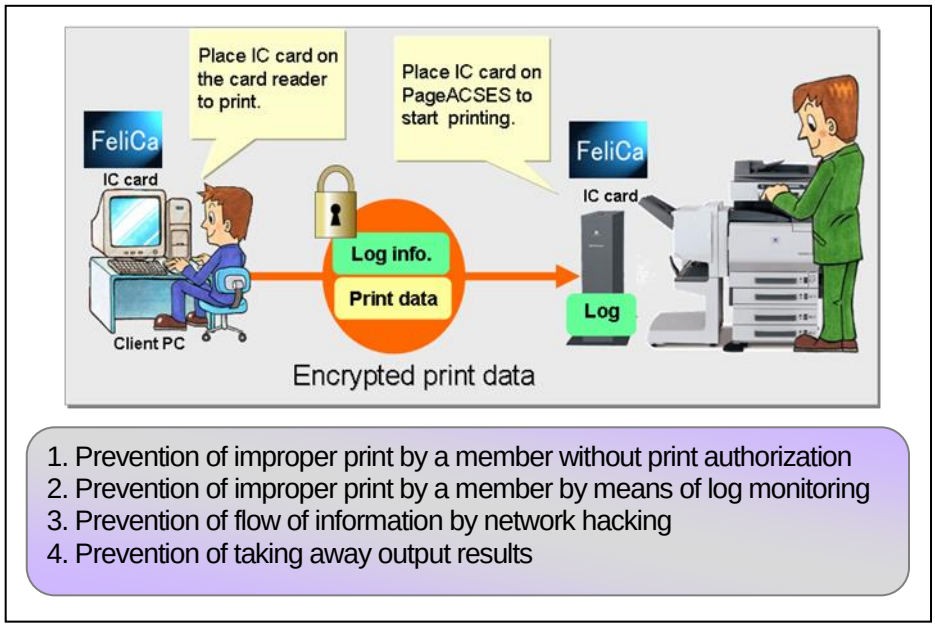


Figure 6-2

3. Access control per file (only Page ACSES Pro)

Right of access per PDF file can be set with PageACSES Pro. Even if the file is carried out illegally, the data is encrypted and cannot be read.

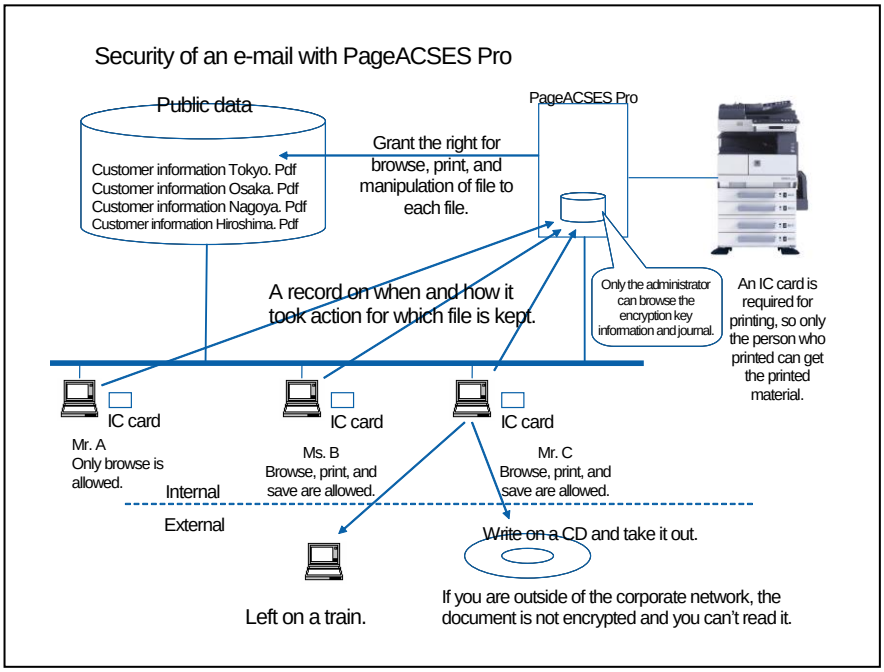


Figure 6-3

<Summary>

PKI Card has the function of Coding/ Decoding, E-signature. You can build the MFP environment of the high security level by using MFP function and PKI card.

1. The login that PKI Card is used

When you insert a PKI card in a card reader and input PIN, MFP carries out the certification to Active Directory. Then, the digital certificate which has been sent to MFP from Active Directory can be inspected in MFP.

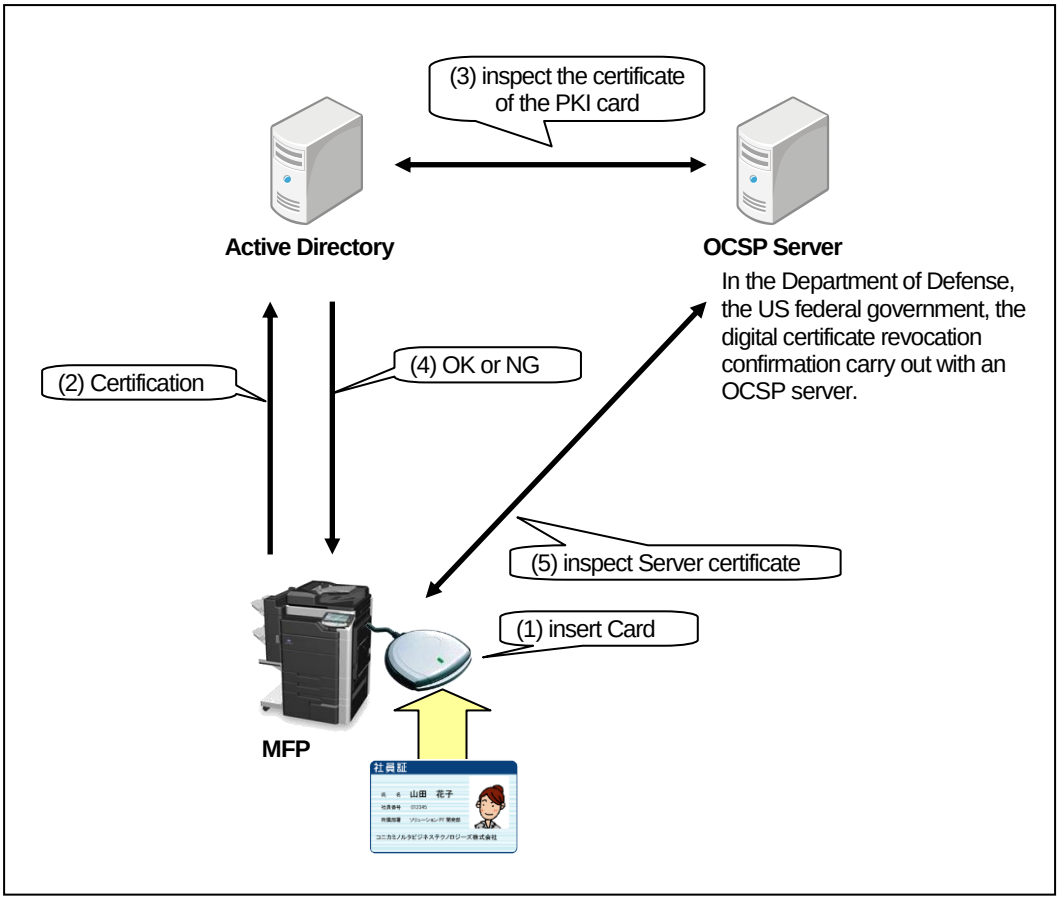


Figure 7-1

2. LDAP Search that PKI Card is used

When you search address with an LDAP server, you log in to an LDAP server with the Kerberos certification ticket which you acquired by the Active Directory certification. Because you can access it by one certification, you can build the Single Sign-On environment where the convenience is high.

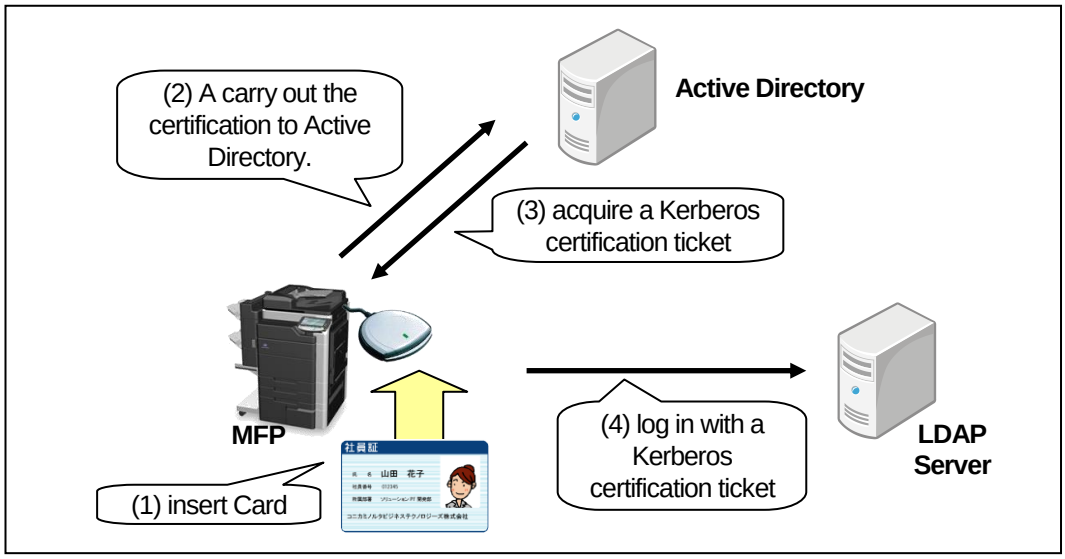


Figure 7-2

3. SMB sender that PKI Card is used

When SMB transmits the data which you scanned, you log in to the computer of the address with the Kerberos certification ticket which you acquired by the Active Directory certification. Because you can access it by one certification, you can build the Single Sign-On environment where the convenience is high. And, you can perform the SMB transmission of a message safely so that the use that does not cancel a password on a network by using a certification ticket is enabled.

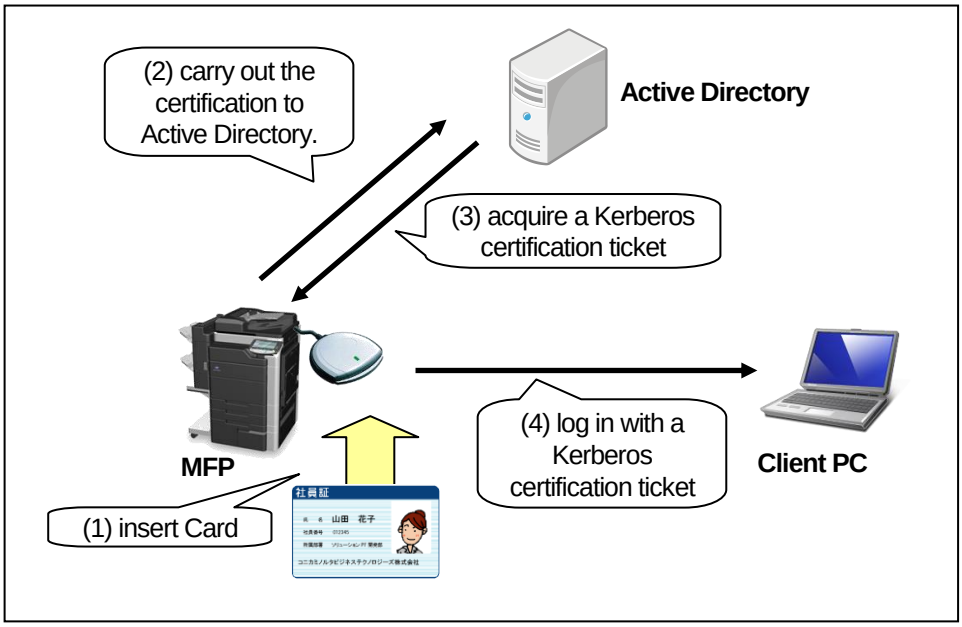


Figure 7-3

4. E-mail sender（S/MIME）that PKI Card is used

You use a PKI card at the time of the E-mail transmission of a message and can carry out a digital signature. You can prove an origin of transmission of a message of E-mail by carrying out a digital signature.

And, If the certificate of the address is registered, you put coding of E-mail together and can transmit a message. You can prevent an information leak to the person on the transmission course of the third by you code E-mail, and transmitting a message.

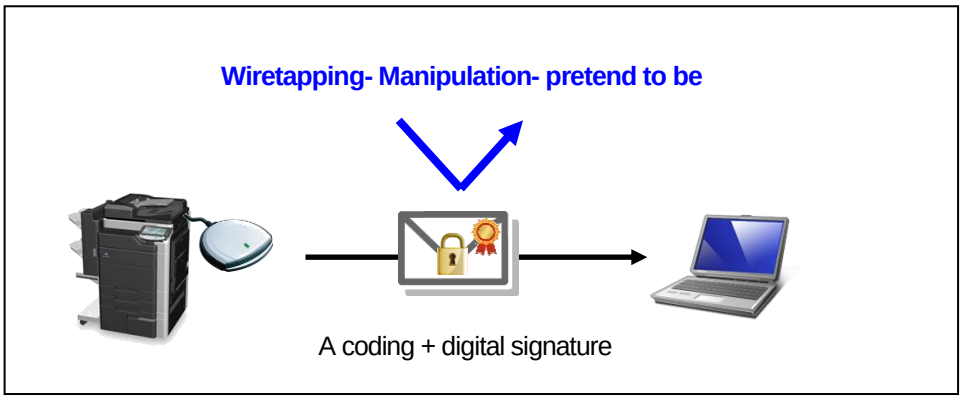


Figure 7-4

5. PKI Card Print

You code print data with a PKI card from printer driver and transmit a message in MFP. The print data are accumulated in the PKI coding box of MFP and because the same user carries out the PKI card certification in MFP, You decode it and can print it.

The print data can maintain the secrecy of data so that a print is enabled only after the certification with the PKI card succeeds in MFP.

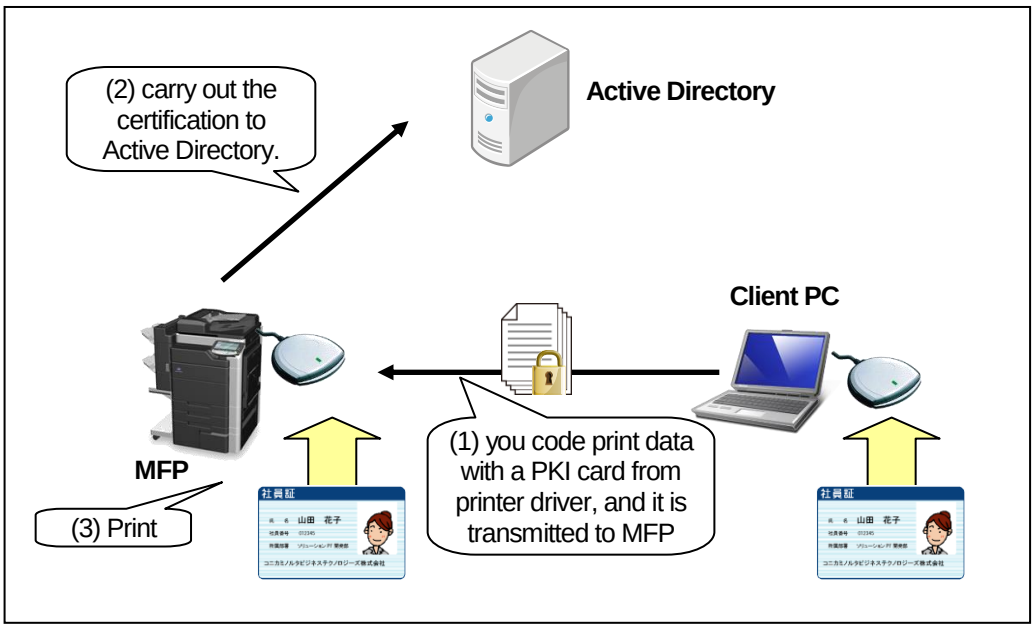


Figure 7-5

6. Scan To Me / Scan To Home

It is a function to transmit the data which you scanned to one's E-mail address and computer. Because you acquire it at the time of the Active Directory certification, one's E-mail address and the pass of the Home folder can easily transmit a message.

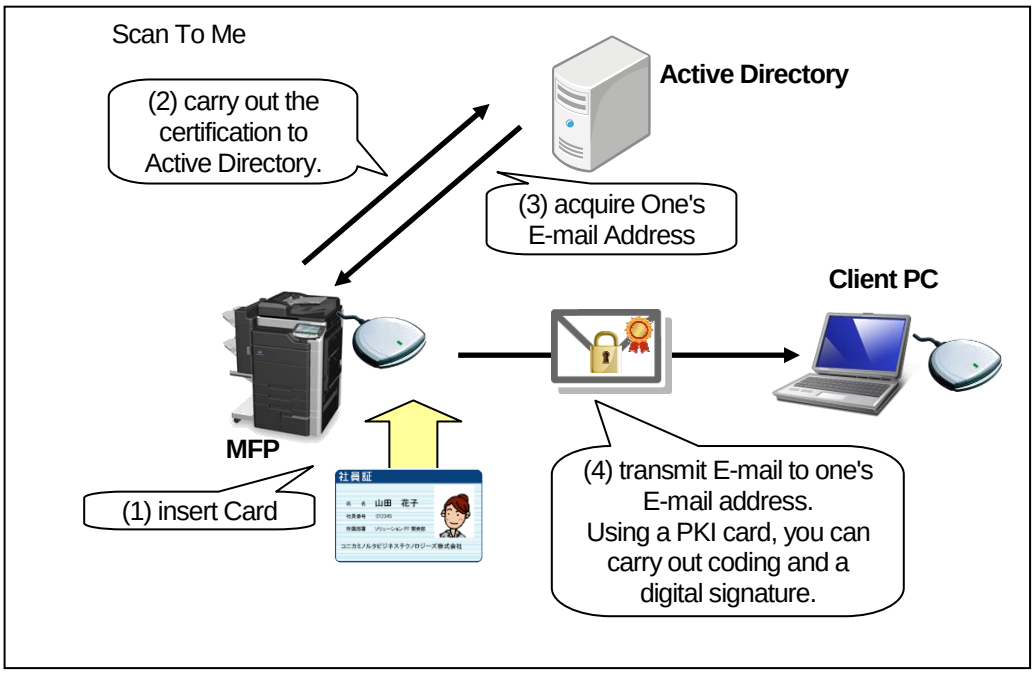


Figure 7-6

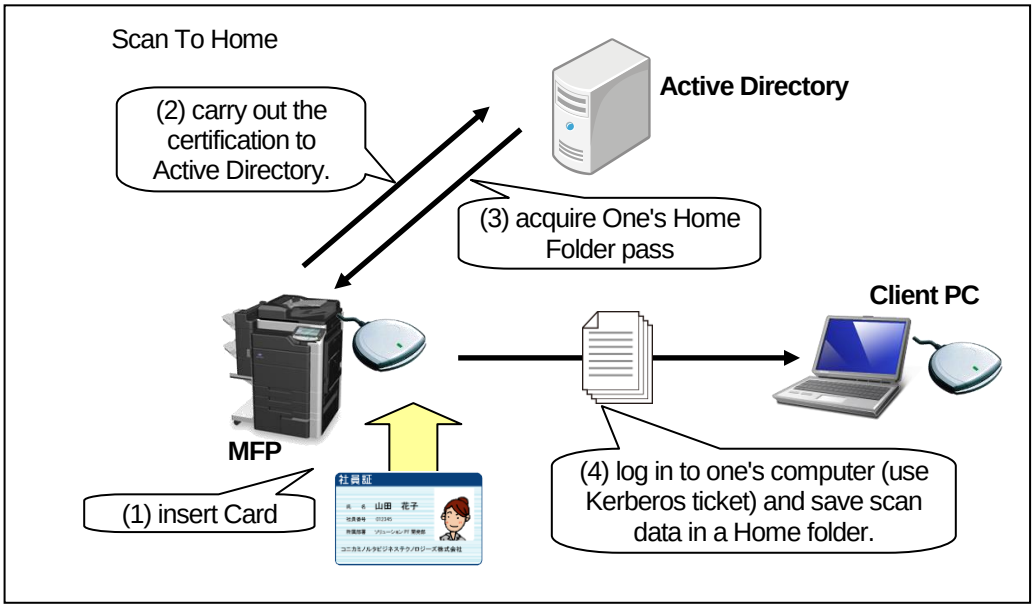


Figure 7-7

VIII. Security about MFP self-protection

1. Verify Function for Firmware

   When MFP Firmware rewriting is performed, hash value is confirmed whether Firmware data is altered. When hash value is not in agreement, Warning is taken out and Firmware rewriting is not performed.

   And, when the setting of Enhanced Security Mode is enabled, hash value is confirmed also at the time of the main power supply ON. When hash value is not in agreement, Starting of MFP is forbidden.

IX. Security about CS Remote Care

1. Security when public lines (modem, FAX) are used.

   In the remote diagnosis system using a public line, the communication between the main body and the CS Remote Care (hereinafter called CSRC) host is established to send the main body data and change the setting of the main body.

   To communicate in the remote diagnosis system, establish a connection communication using the ID that was registered in both the CSRC host and the device in advance. This communication confirms whether the registered content of the CSRC host corresponds with the sent content of the device, and after the communication finishes normally, it's ready for the remote diagnosis communication.

   The remote diagnosis communication confirms the ID per communication. If the ID doesn't coincide, the communication is not established.

   The data CSRC collects is service information including counter values and does not include the details of FAX addresses and personal information.

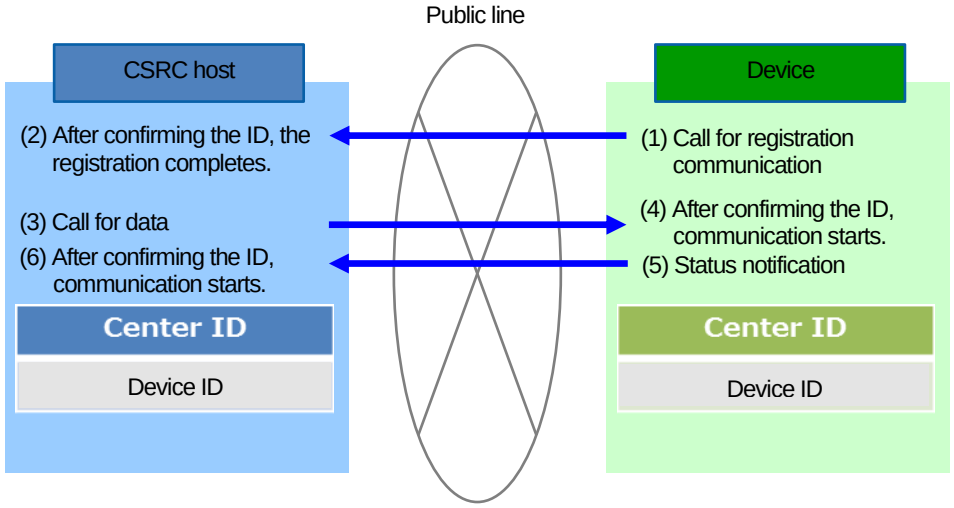


Figure 9-1

2. E-mail security

- Encryption of transmitted data

Data is encrypted using an encryption key (common key) in the main body and the CSRC host.

* The main body and the center can set the possibility of encryption.

In a common key encryption system, a same key is used for encryption and decryption in the main body and the center. This allows safety sending/receiving of e-mails without interception by others.

- Confirmation of IDs, etc.

Sent/received e-mails contain information (CenterID or serial No.) that the source and the destination can confirm.

The consistency of this information is checked to confirm if the source and the destination are correct.

Also, e-mails sent from the center have e-mail IDs.

Response e-mails from MFP utilize e-mail IDs of response source e-mails.

Check if it corresponds with the e-mail ID sent by the center to confirm the ID.

- Elimination of false e-mails

If the information (CenterID or serial No.) that the source and the destination can confirm or the e-mail ID doesn't coincide, the sent/received e-mail is considered as a false e-mail and eliminated without data registration.

3. Security on HTTP communication

- Encryption of transmitted data

Like original e-mails, data is encrypted using an encryption key (common key) in the main body and the CSRC host.

* The main body and CSRC host can set the possibility of encryption.

By means of a common key encryption system, a same key is used for encryption and decryption in the device and the CSRC host.

In addition, in HTTP communication, SSL can be set. (HTTPS)

Via SSL, encryption is performed in the communication data between "device and WebDAV server" and "WebDAV server and CSRC host".

- Many secure functions the HTTP protocol has can be diverted.

The HTTP protocol doesn't rely on the environment, and can use a lot of secure functions such as authentication, Proxy and SSL.

In SSL, the combination of security technologies such as public-key cryptography, private-key cryptography, digital certificate, and hash function can prevent wiretapping or manipulation of data and spoofing.

At the center as well, security measures suited for the customer's environment can be taken using these secure functions.

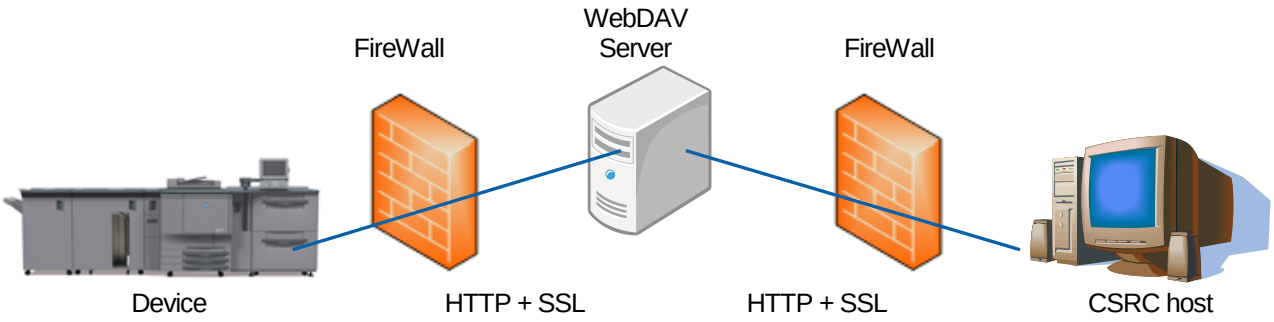


Figure 9-2

4. Product authentication

- End-to-End data security

In HTTP communication, reading and writing are carried out for the WebDAV server on the Internet.

Therefore, there is a little security vulnerability such as information leakage.

In product authentication, in order to make more robust the security, client authentication of SSL is conducted to secure the validity of the communication between the device and the WebDAV server, and the WebDAV server and the CSRC host.

In product authentication, the license administrative server issues a unique license code to the user first.

Registration of the issued code in the certificate-issuing server allows the issue of a client certificate and a server certificate to the certificate-issuing server.

When the client certificate is used in MFP and the center, and the server certificate is sent to the e-mail address of the user to be set to WebDAV, the data security of the communication between the device and the WebDAV server, and the WebDAV server and the CSRC host is enhanced.

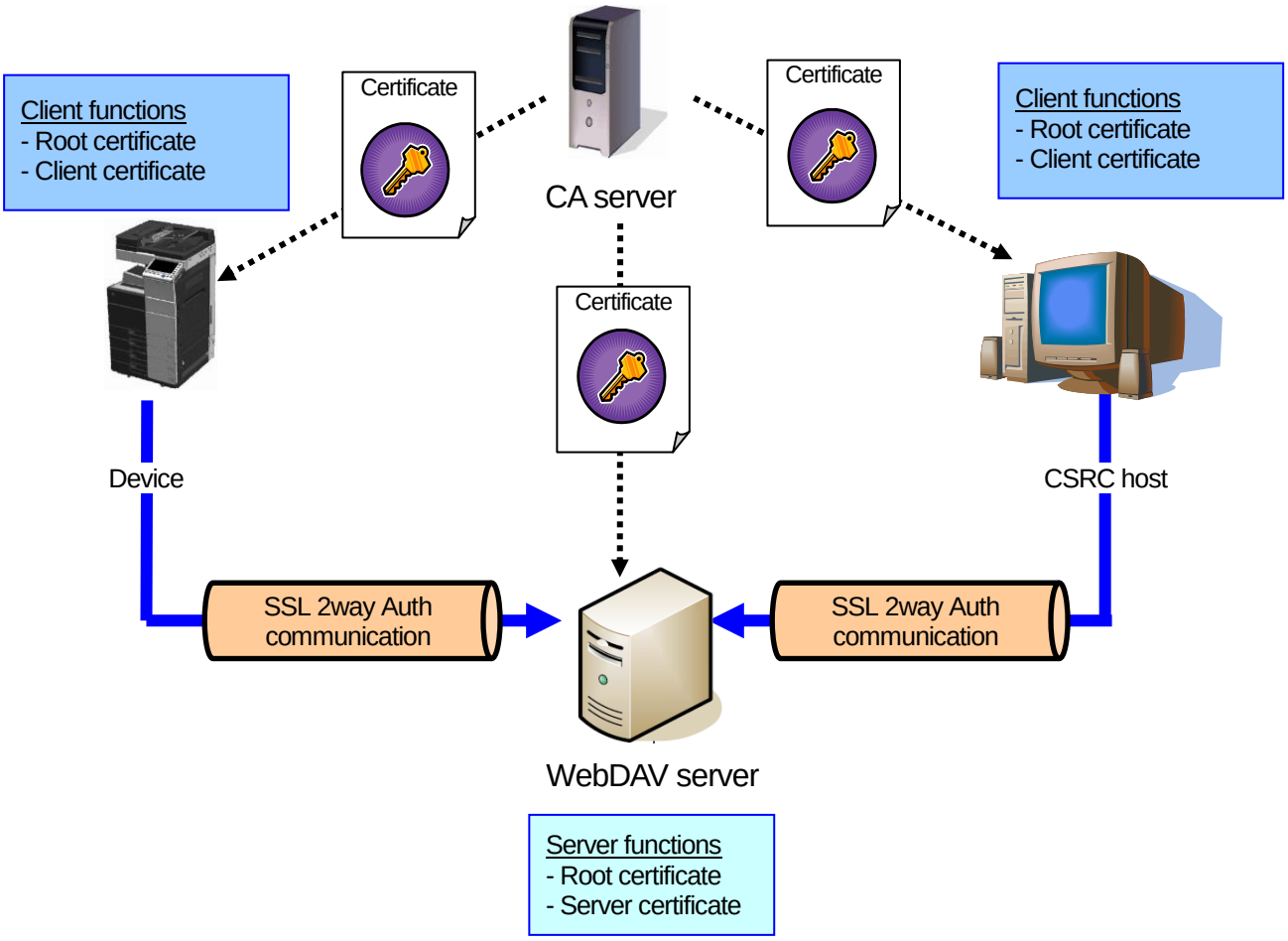


Figure 9-3

5. Security at DCA

- SNMPv3 communication between DCA and device

DCA (Device Collection Agent) supports SNMPv1 and SNMPv3 communications as a communication method with a device.

In SNMPv1 communication, plain text flows on the network route, therefore if the environment has a risk of packets being captured from the outside, the data during transmission may be sniffed.

Because the “community name” which is the only authentication in SNMPv1 communication is also leaked at the same time, all of the data stored in MIB of the device managed by the leaked “community name” can be accessed fraudulently.

In SNMPv3 communication, in addition to “user name” corresponding to “community name” of SNMPv1 communication, a mechanism for authentication has been added to enhance the robustness of access to a device. Also, all of the data flowing the communication pathway are encrypted; therefore, it is difficult to sniff the data except when the same encryption system/encryption key is known.

- Communication between DCA and CSRC host

The communication between DCA and the CSRC host is encrypted using SSL on the HTTP protocol.

Also, a unique ID is assigned to DCA; data transfer is made after checking the ID per communication.

If this ID doesn't coincide during communication, any data will not be transferred.

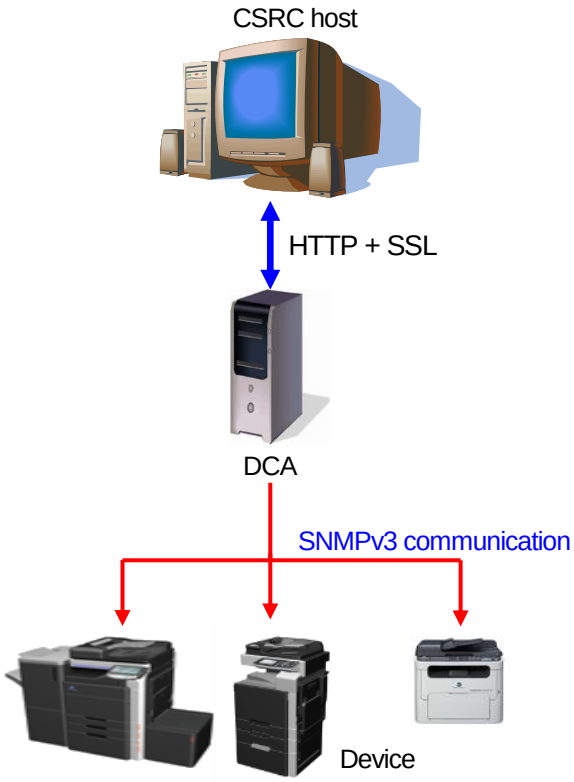


Figure 9-4

X. Security about bizhub Remote Panel

1. Communication, Connection trigger

bizhub Remote Panel cannot perform HTTP communication without cipher. Every communication is enciphered with SSL and performed on HTTPS.

In addition, connection from the bizhub Remote Panel Server side to devices is disabled. Since connection is enabled only from devices, the customer's security is ensured.

2. Authentication

Further highly secure communication is available by setting the certificate issued by the trusted third party CA (Certificate Authority) to devices and bizhub Remote Panel Server

3. Access Code

Multiple devices and multiple users (clients) can use bizhub Remote Panel Server. A user selects a device to connect from the list of multiple devices and input a 4-digit Access Code to connect. The authenticated 4-digit Access Codes displayed on the

device panel are informed to the client who is authorized by the customer (service person and operator) in advance.

4. Audit log

When a device is connected to bizhub Remote Panel Server, the log that a client (user) operates the device remotely and logs out is recorded. The administrator can monitor the access to the bizhub Remote Panel user by tracing the log.

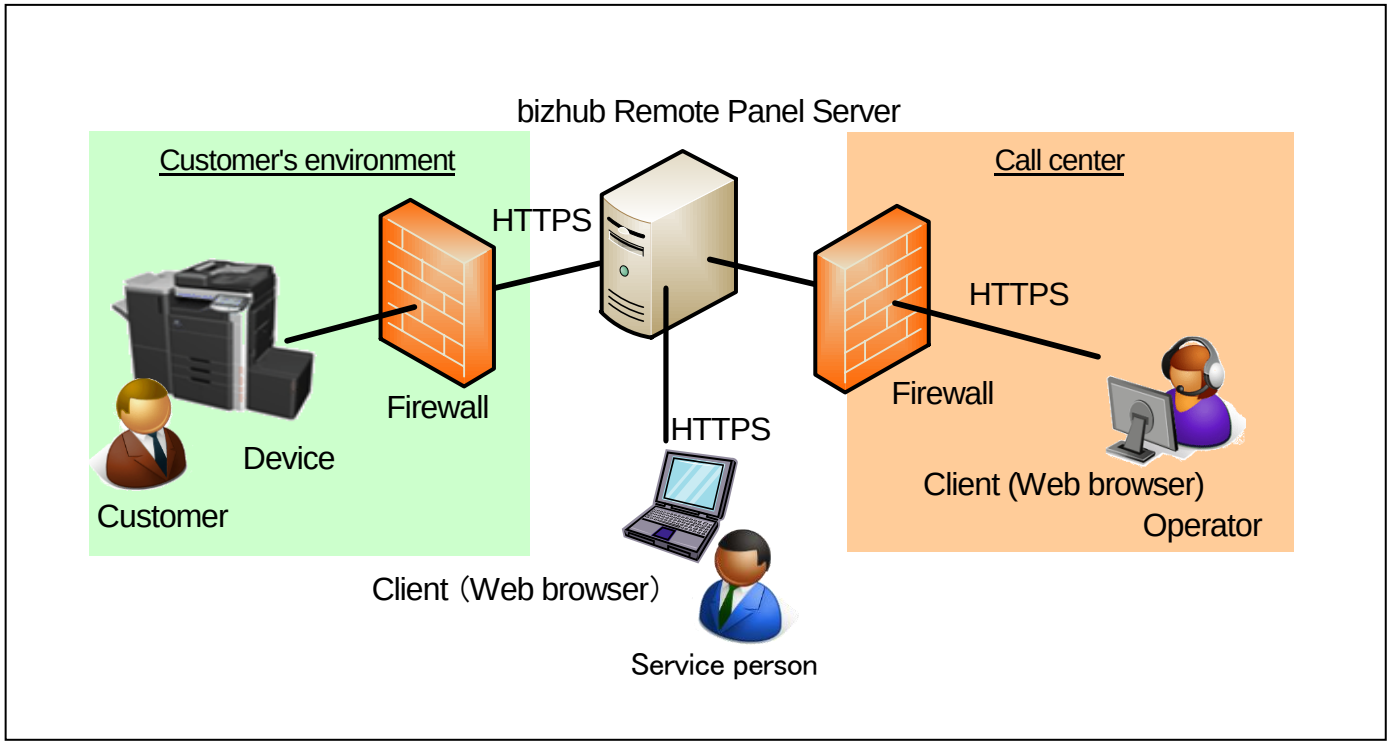


Figure 10-1

XI. Security about bizhub Remote Access

<Outline>

Installing bizhub Remote Access on a smart phone or tablet terminal using GooglePlay or AppStore enables the panel screen of an MFP connected via network to be remotely displayed on the screen of the smart phone or tablet terminal. By touching the screen displayed on the MFP panel, the MFP can be controlled remotely.

1. Communication, Connection trigger

The MFP rejects remote connection from bizhub Remote Access unless the bizhub Remote Access function is enabled. Thus it is possible to prevent the prohibited MFP from being accessed remotely.

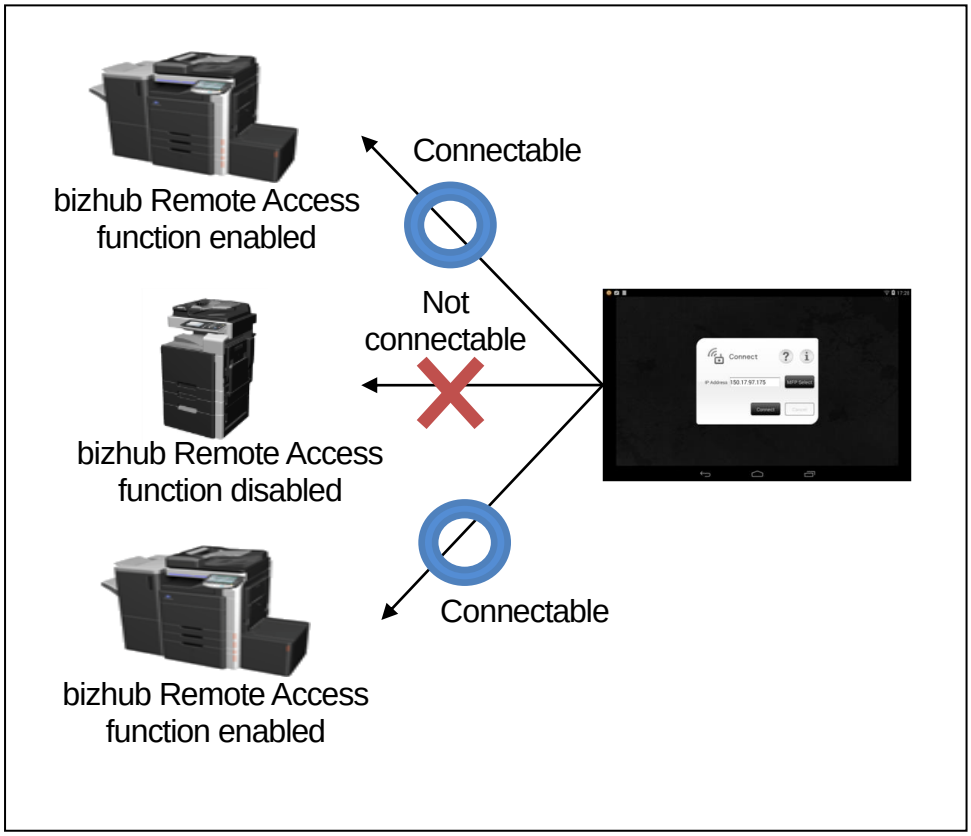


Figure 11-1

2. Auto cut-off due to timeout

When the remote connection from bizhub Remote Access has been left for a long time, the MFP automatically cuts off the connection with bizhub Remote Access. This function ensures security even for users who left the terminal during remote operation.

3. Security on administrator mode

On administration mode, the MFP rejects a remote connection from bizhub Remote Access, so that security can be ensured on administrator mode.

4. Security when cut off during remote operation

When connection with bizhub Remote Access is cut off during remote operation, the MFP resets the screen, so that security can be ensured even when accessing a user box with password, or entering the password.

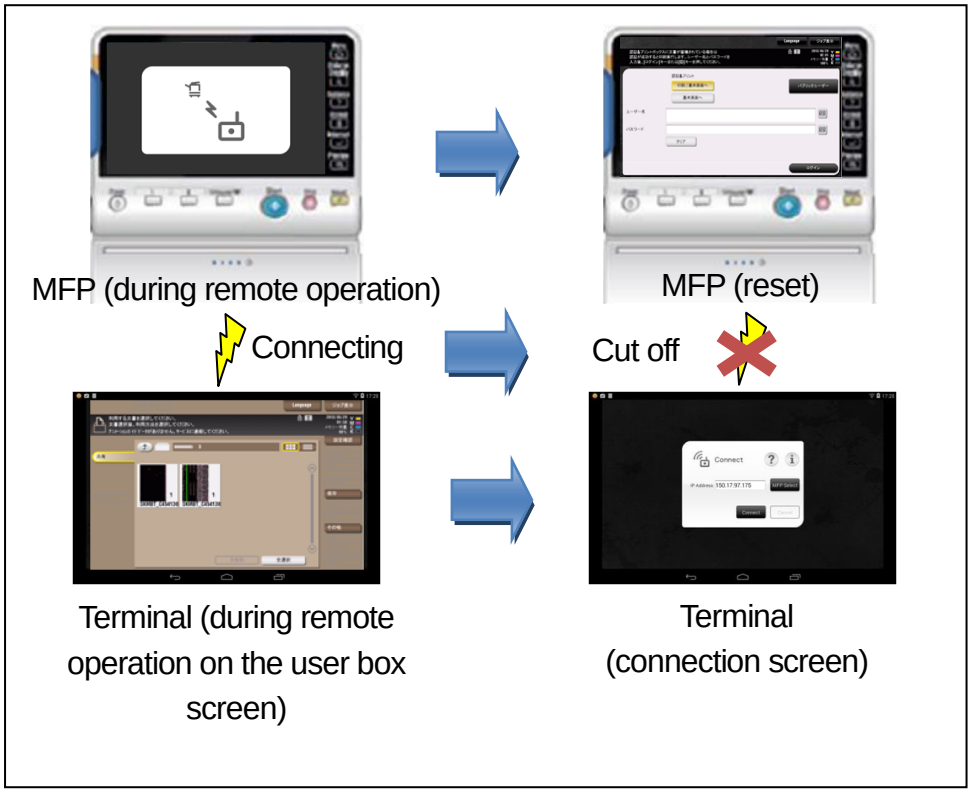


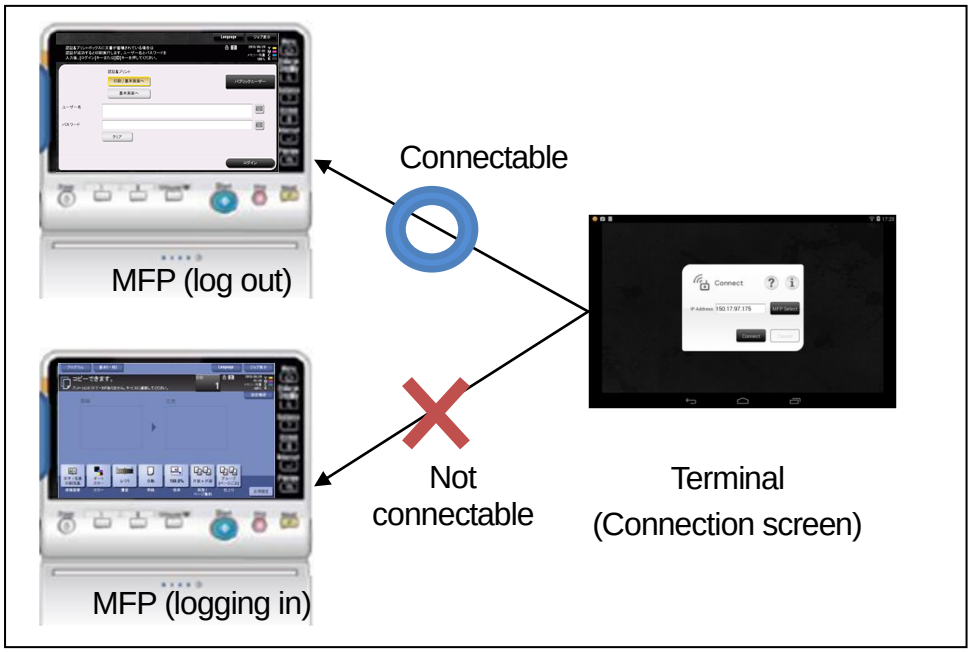
Figure 11-2

5. Security when used in both user authentication and account authentication

When the MFP is under user authentication or account authentication, connection from bizihub Remote Access will be rejected.

Furthermore, when connection between the MFP and bizhub Remote Access is cut off during authentication, the MFP will log out automatically.

Above functions ensure security for authentication user or account.



Figurer 11-3