Konica Minolta Security White Paper

Security Basic Policies and Technologies

Provided by Konica Minolta

Version 5.6.1

May 2012

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.

Documentation for Konica Minolta Group Company.

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	Oct. 2007	Revised functions and description of applicable models
Version 5.1	Aug. 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

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. 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.
Felica is the registered trademark of Sony Corporation.
Adobe Acrobat is the registered trademark of Adobe Systems Incorporated.

Table of Contents

3. Access control per file

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

Chapter 1 Introduction

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. Basic Security 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 all MFP products (A4/20 or higher PPM) released from March 2004, to objectively prove equipment of security functions.

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 athe certification of FIPS140-2 indispensable.(Model: C754/654/554/454/364/284/224)

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.

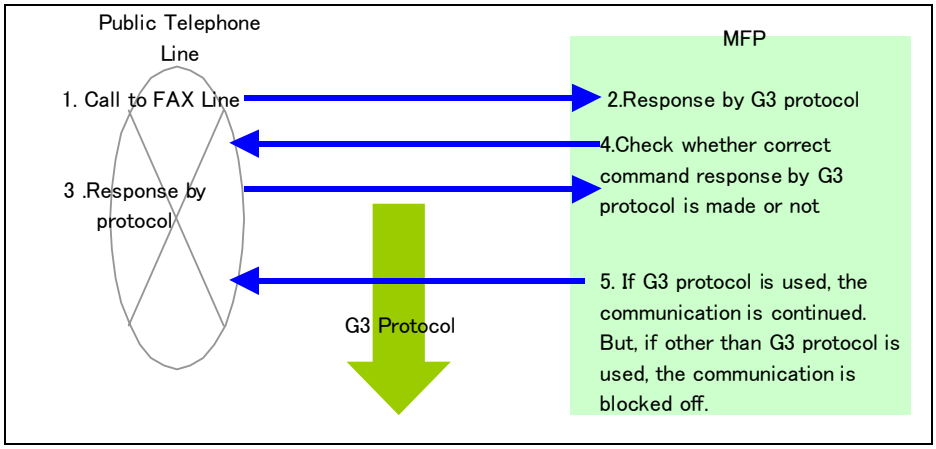


Figure 1

2. Security from line used for remote diagnosis device

The remote diagnosis system uses public line and allows Konica Minolta products to communicate with their service centers. Through this system, Konica Minolta products send the main body data to the service centers and the service centers can change the main body settings remotely. ID is preset on every main body and service center, so they can communicate each other only when the ID is matched.

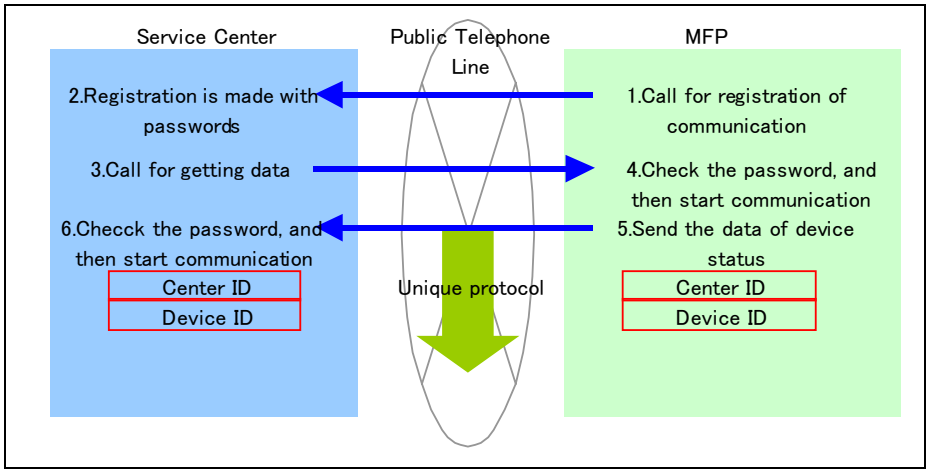


Figure 2

II. Security from LAN connection

1. Security from network protocol

Operation can be enabled/disabled for each port.

Invasion from outside can be prevented by disabling unnecessary ports.

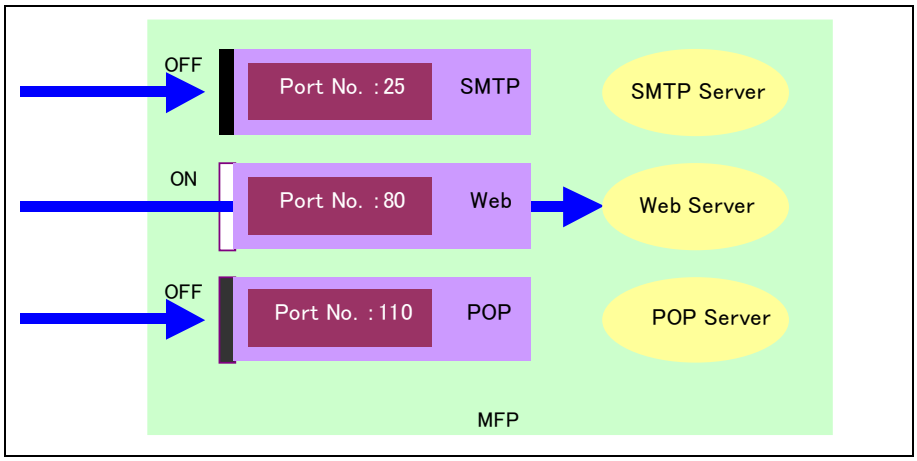


Figure 3

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

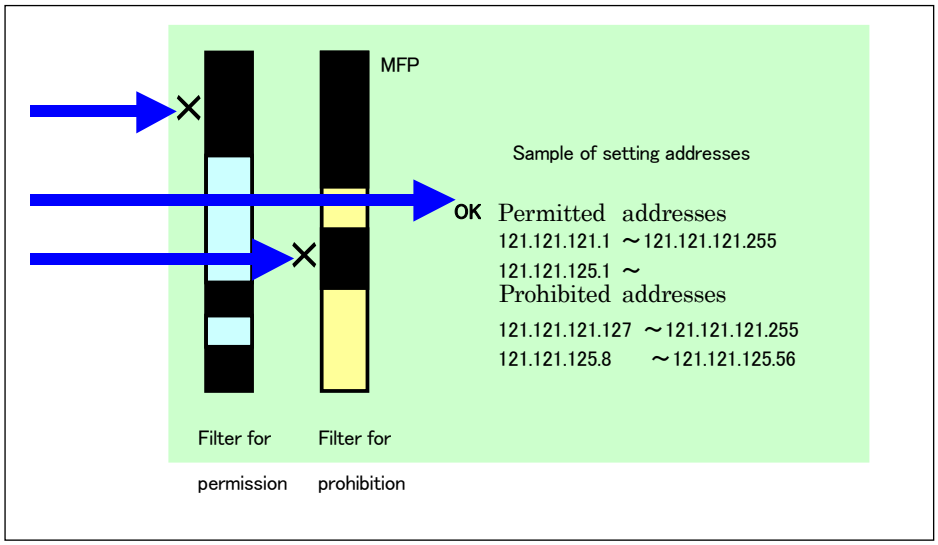


Figure 4

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.

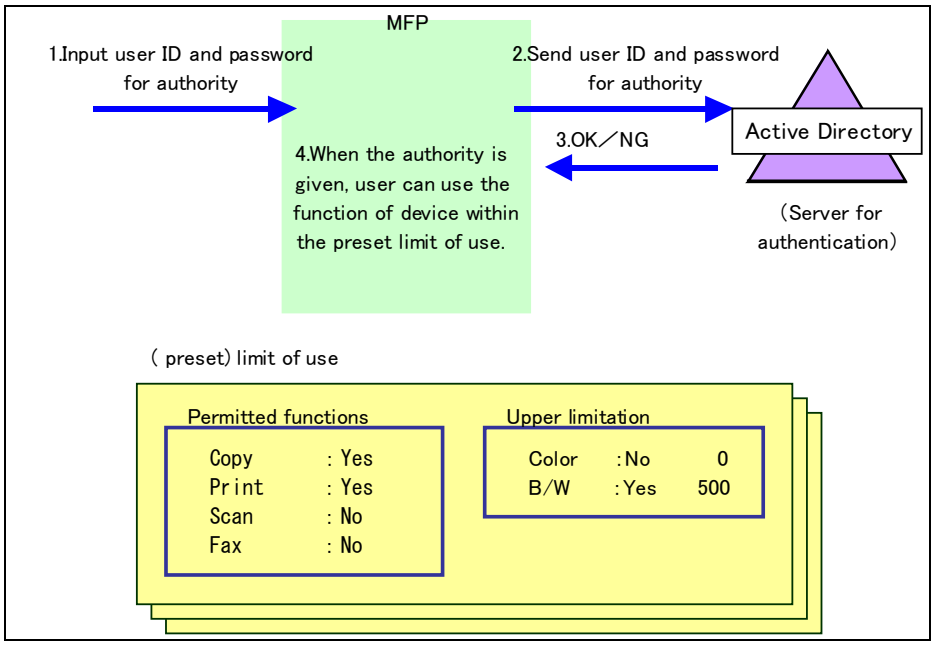


Figure 5

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.

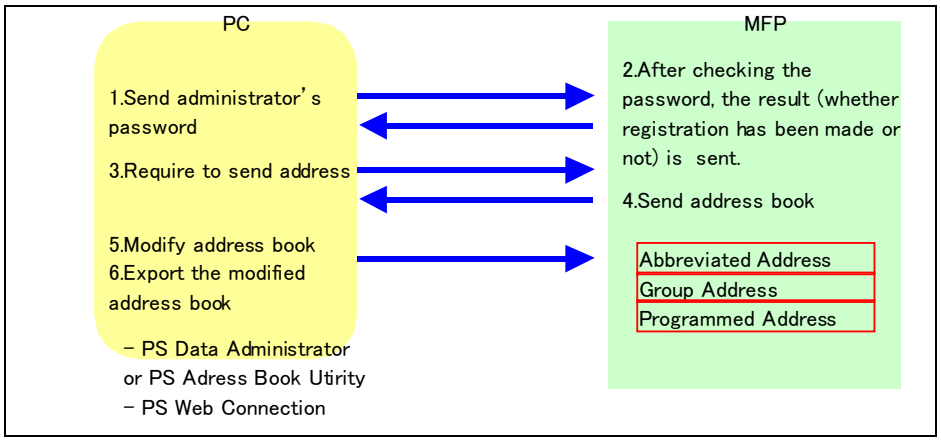


Figure 6

(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), the data is safely protected by bizhub OpenAPI.

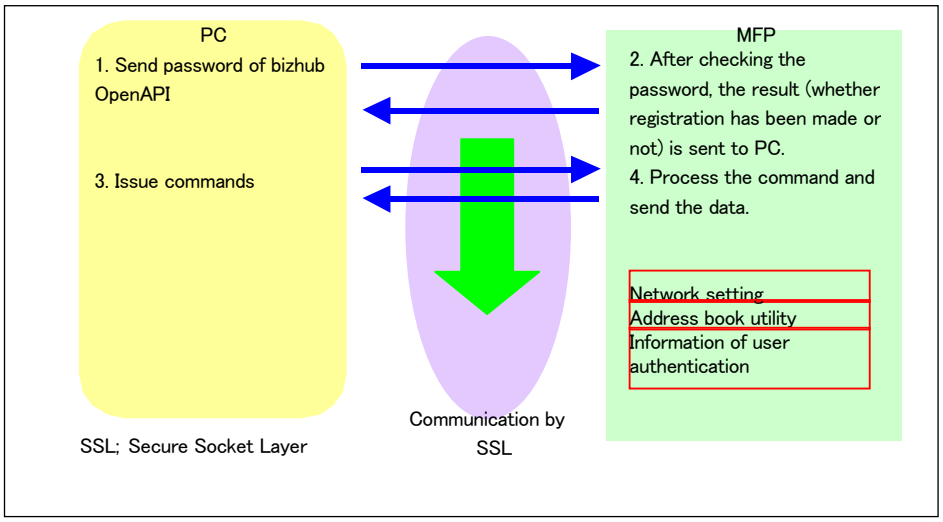


Figure 7

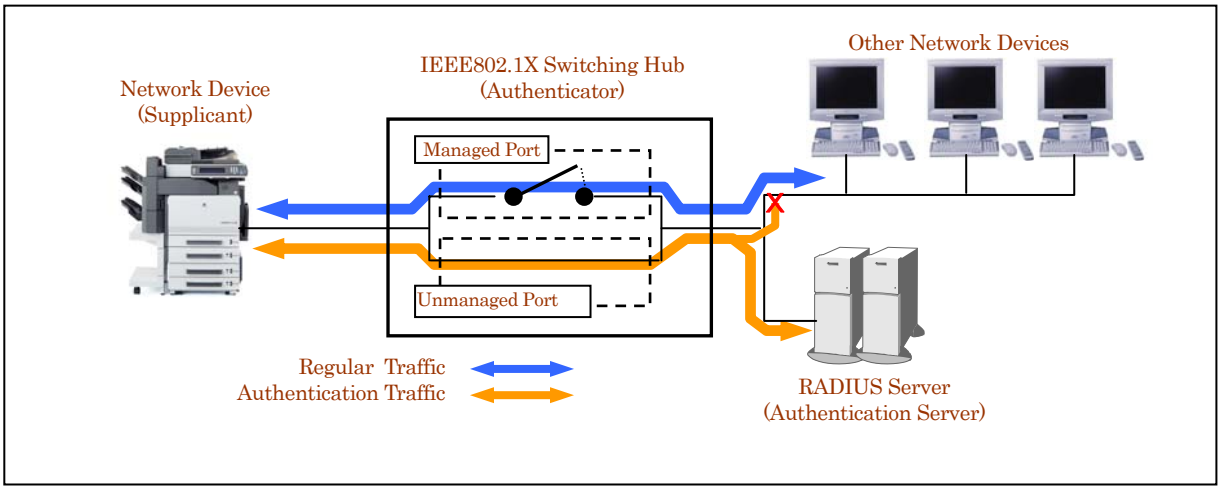
4. Encryption of data communication

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.

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. These networks will only allow devices into the network if the RADIUS server approves the authentication



6. 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.

7. 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.

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, reoutput 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, reoutput or retransfer of the data by 3rd person is prevented.

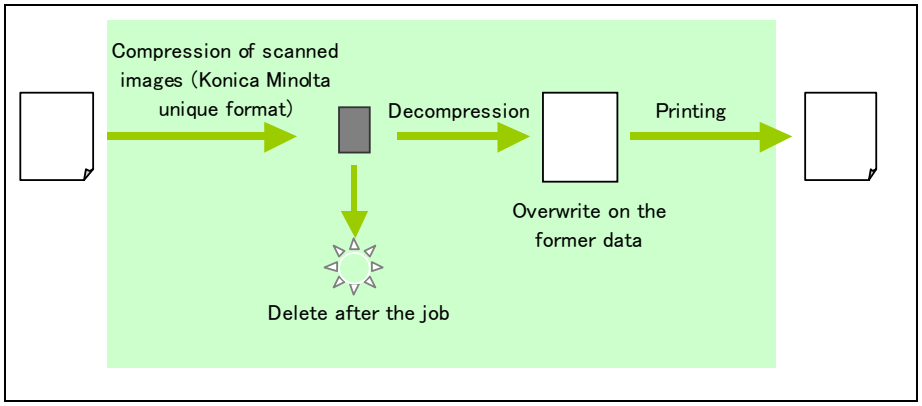


Figure 8

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.

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.

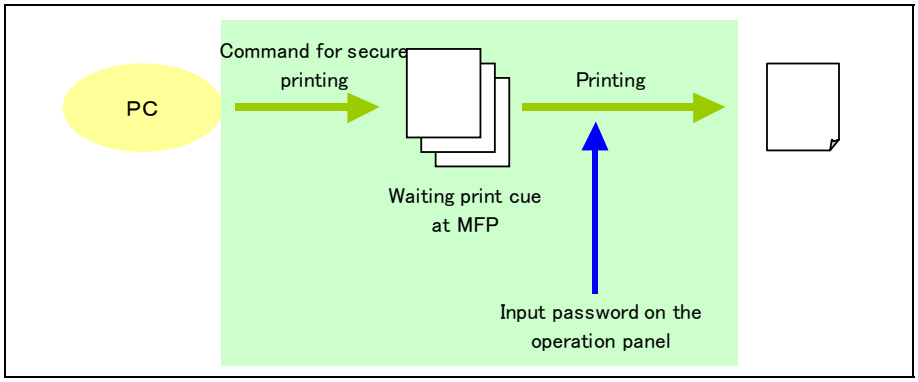


Figure 9

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.

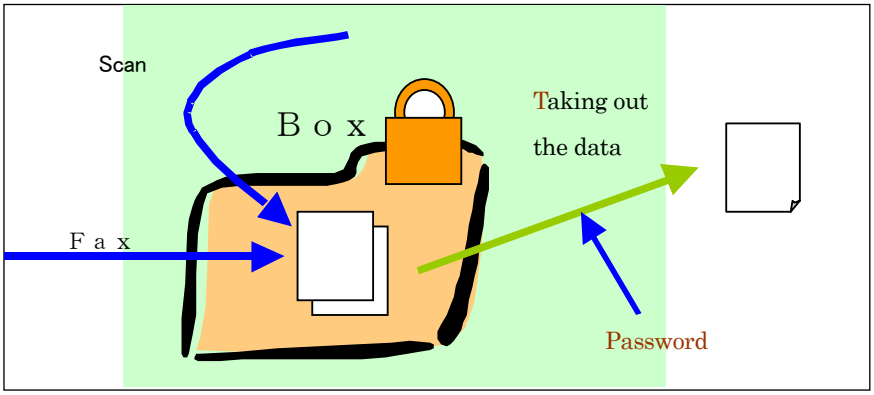


Figure 10

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.

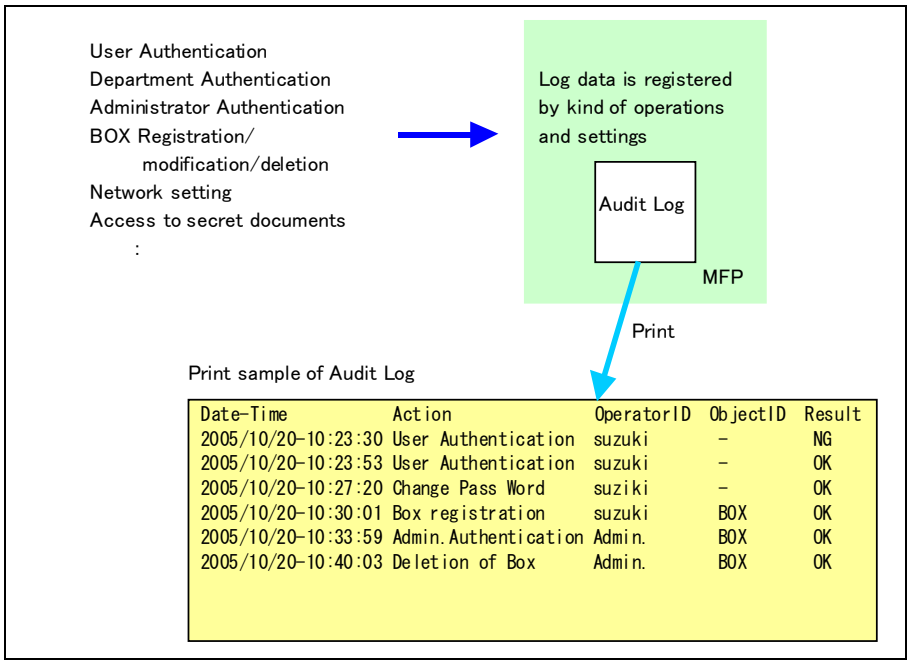


Figure 11

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.

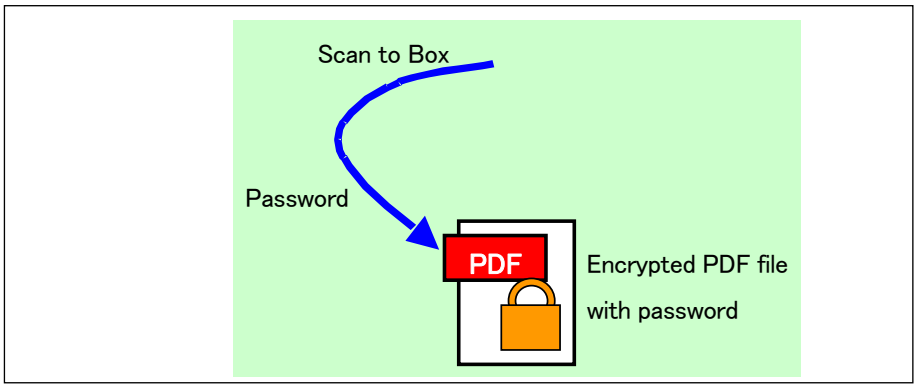


Figure 12

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 can not 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.

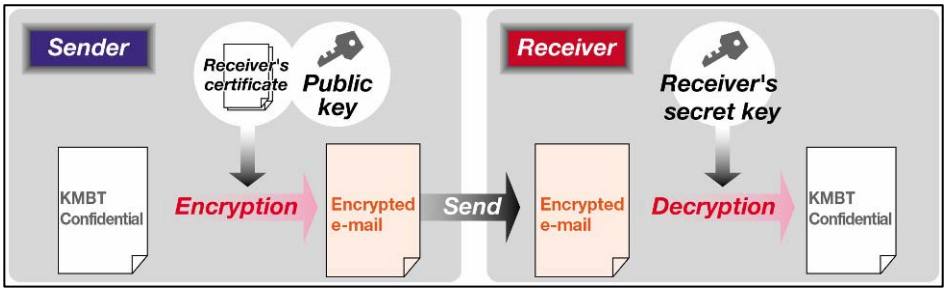


Figure 13

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.

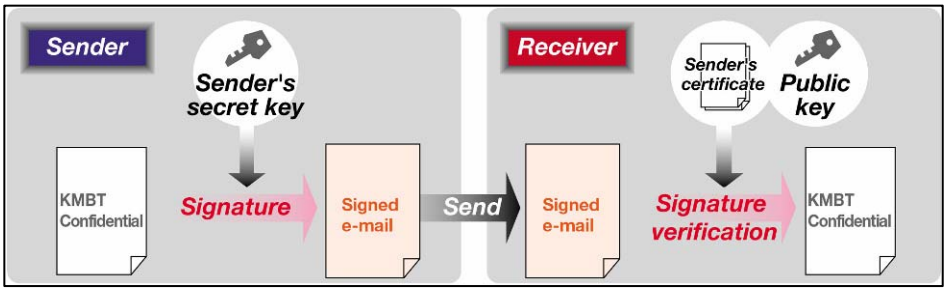


Figure 14

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 20

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

When the setting of Overwrite to delete the temporary data (HDD data) is "On", MFP overwite to deteta 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 is 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

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.

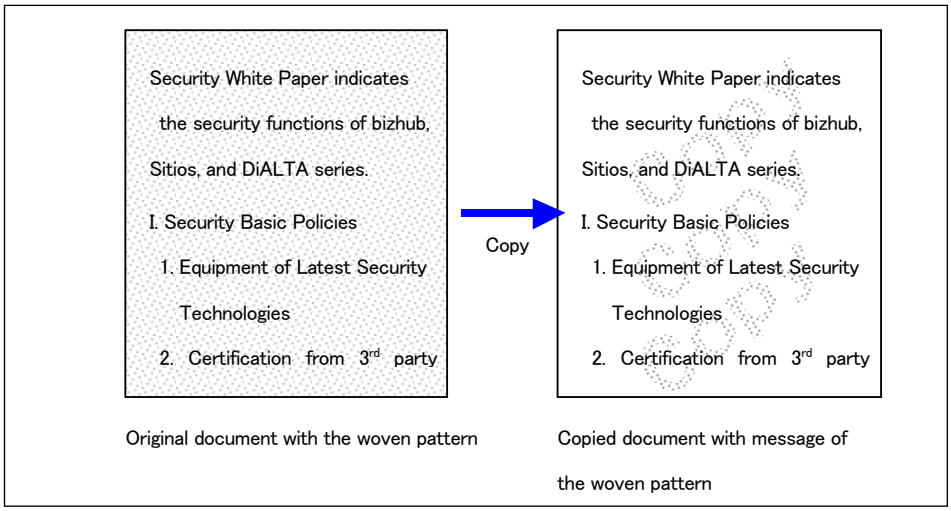


Figure 15

(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.

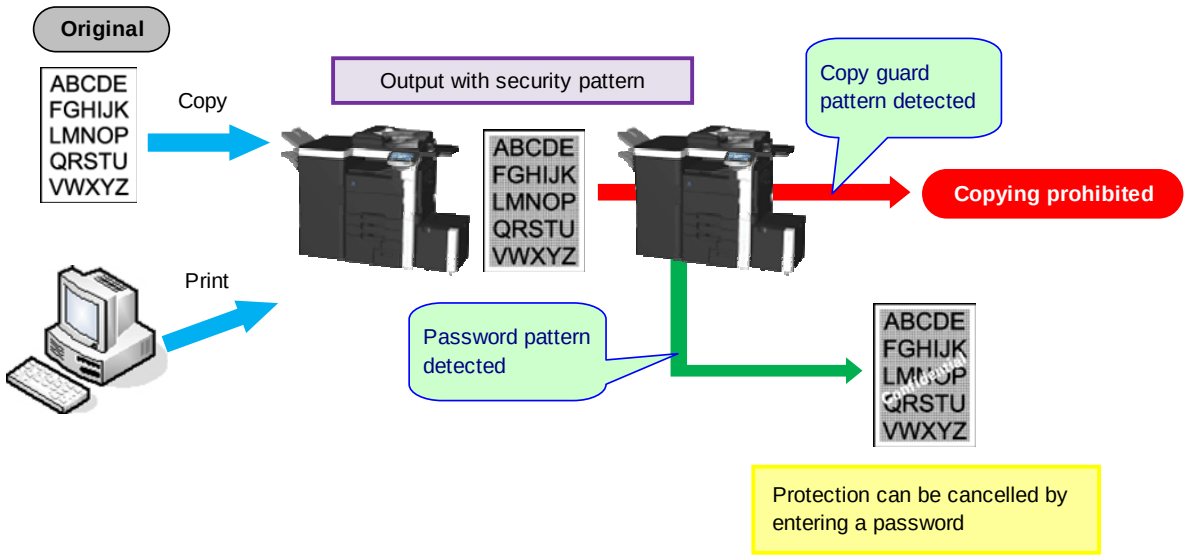


Figure 21

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 can not be used illegally.

The Vein on the finger as the biometric data

The vein is located in the body and it can not be scanned/read without notice

unlike finger print. 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.

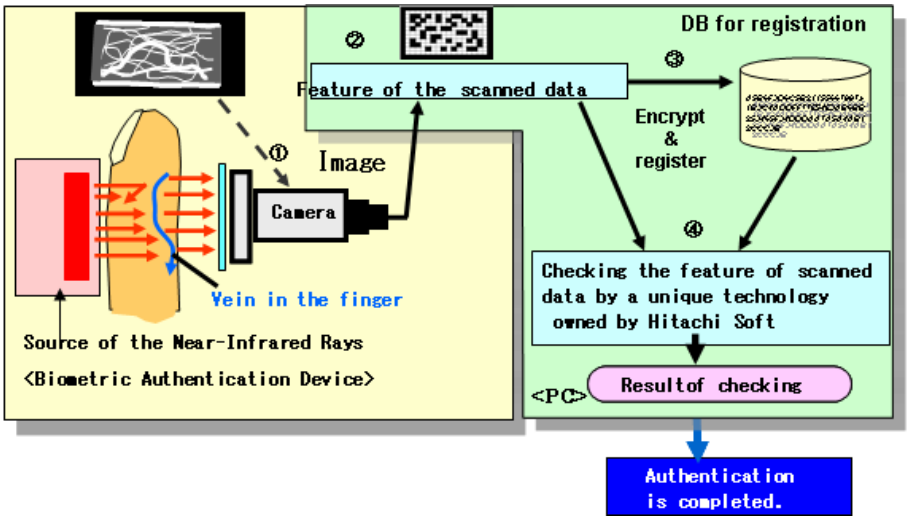


Figure 16

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 17

Ⅵ. Extended functions in cooperation with PageACSES

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

1. Scan with authentication
   (1) Authorized user can log-in with IC card (FeliCa) instead of password.
   (2) The scanned data is encrypted by PageACSES and transmitted to PC securely.
   (3) Scan (and received Fax) log data (incl. image) can be transferred to the server and traced by the administrator.

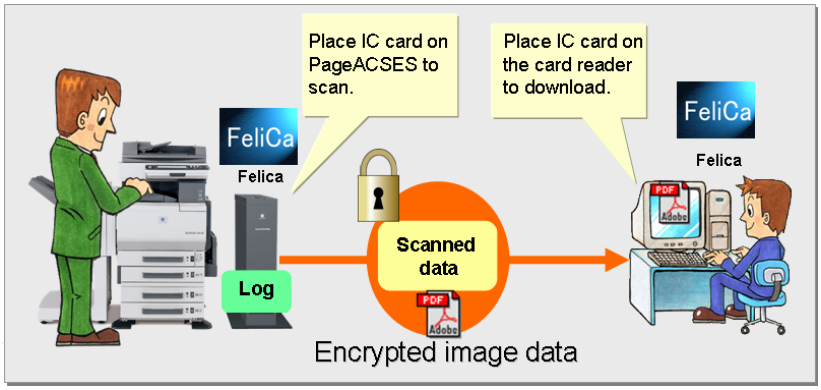


Figure 18

2. Print with authentication
   (1) Authorized user can log-in with IC card (FeliCa) instead of password.
   (2) The print data is encrypted by PageACSES and printed out securely.
   (3) Print log data can be stored in PageACSES and traced with its file name.

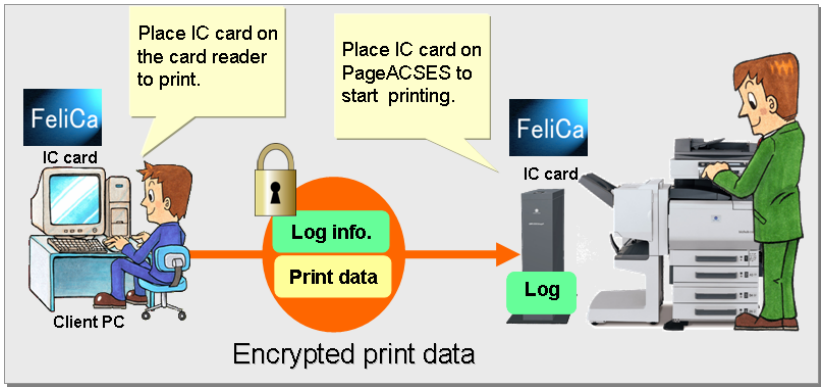


Figure 19

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 can not be read.

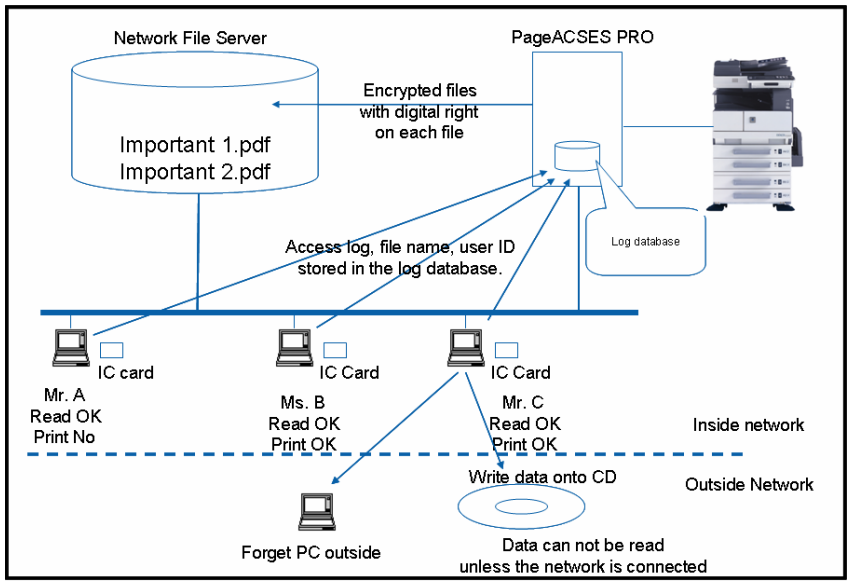


Figure 20

Ⅶ PKI Card authentication System

＜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 carry out the certification to Active Directory. Then, the digital certificate which has been sent to MFP from Active Directory can be inspected in MFP.

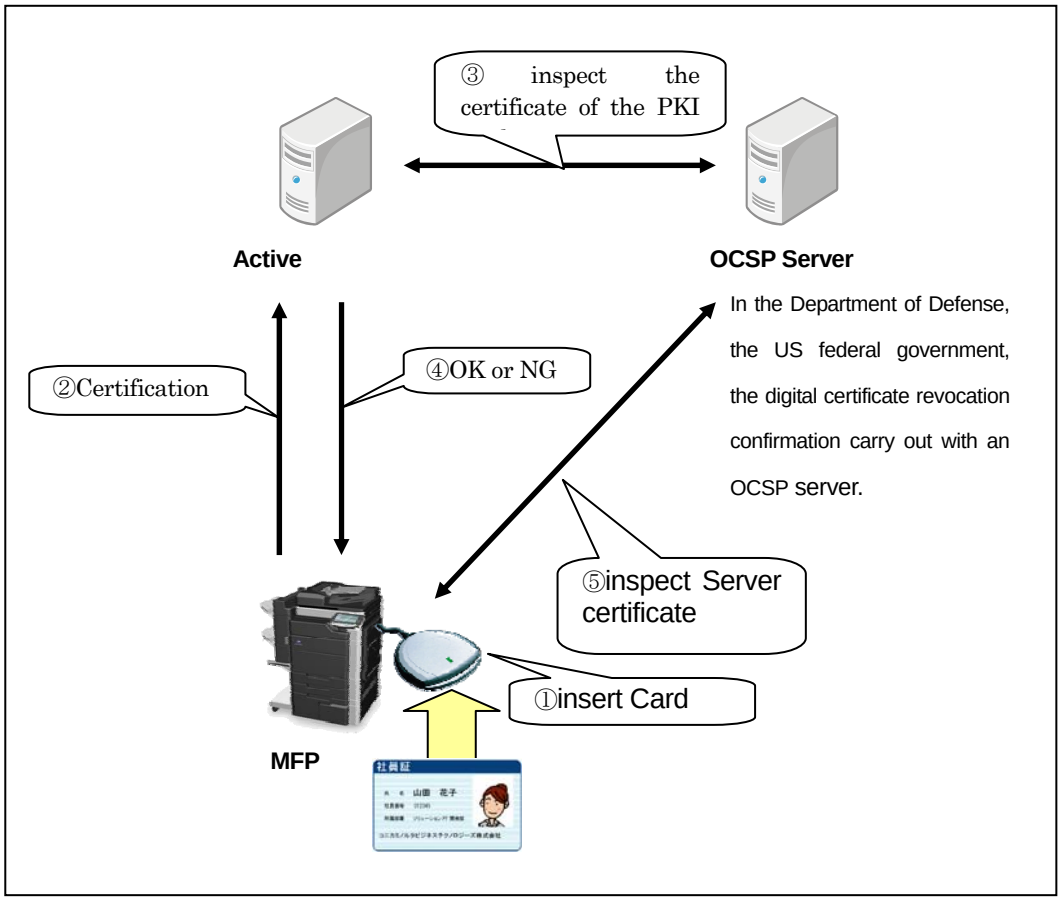


Figure 21

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.

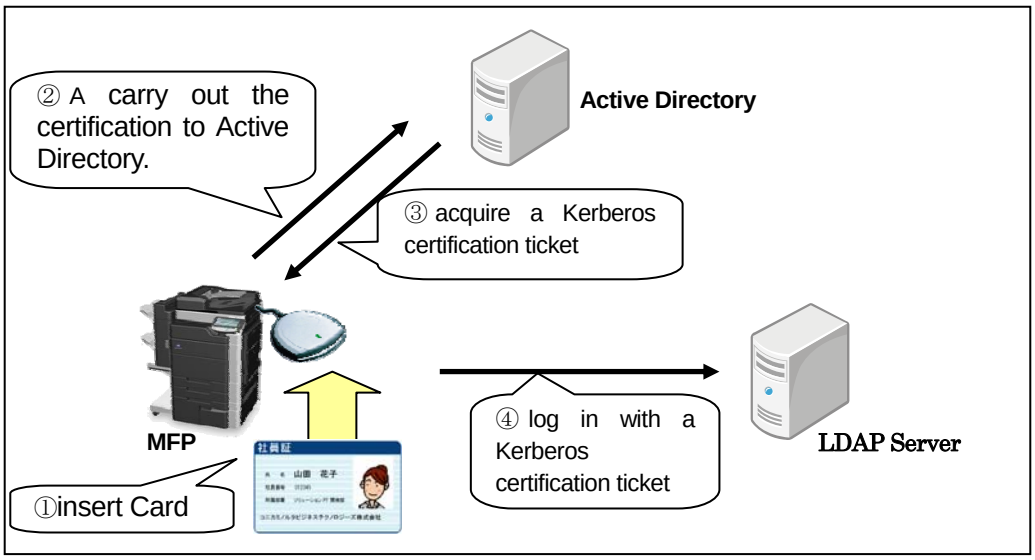


Figure 22

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.

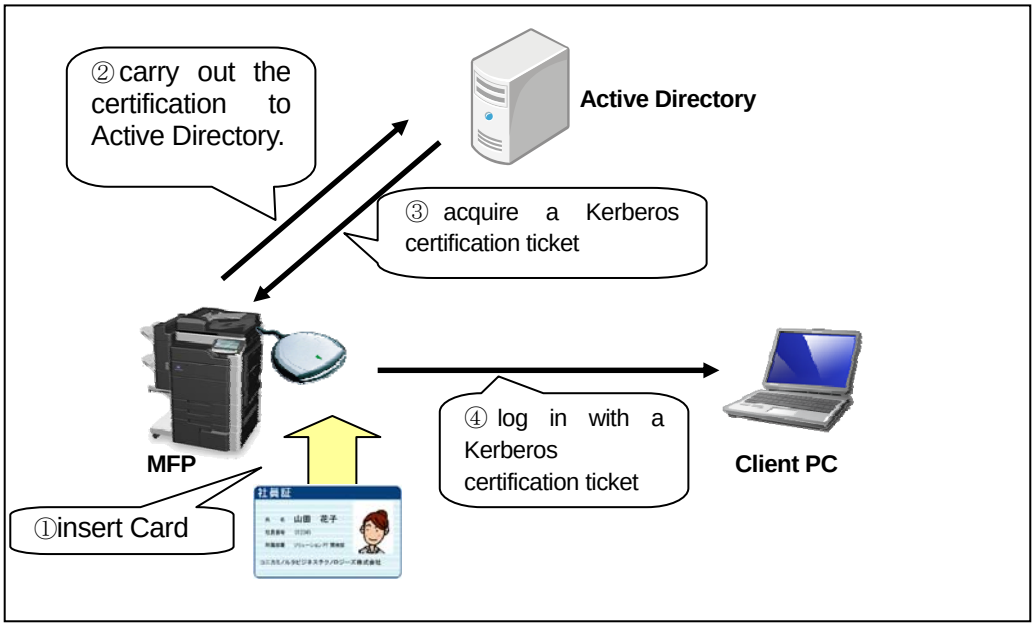


Figure 23

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.

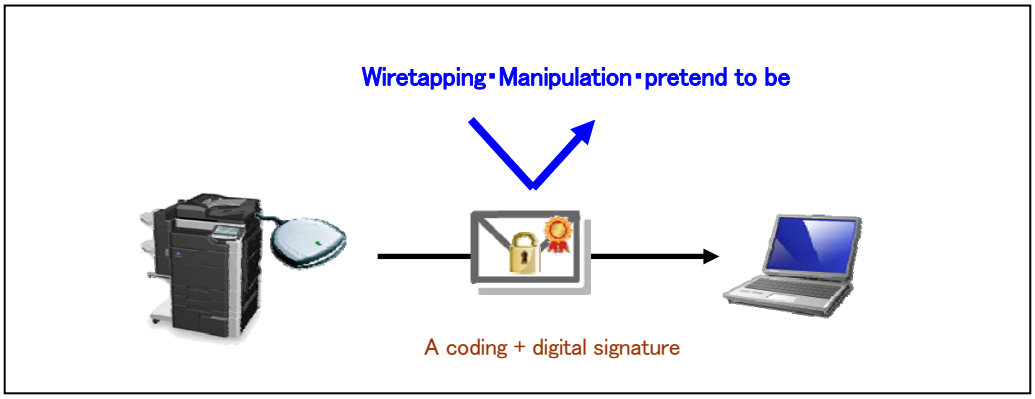


Figure 24

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.

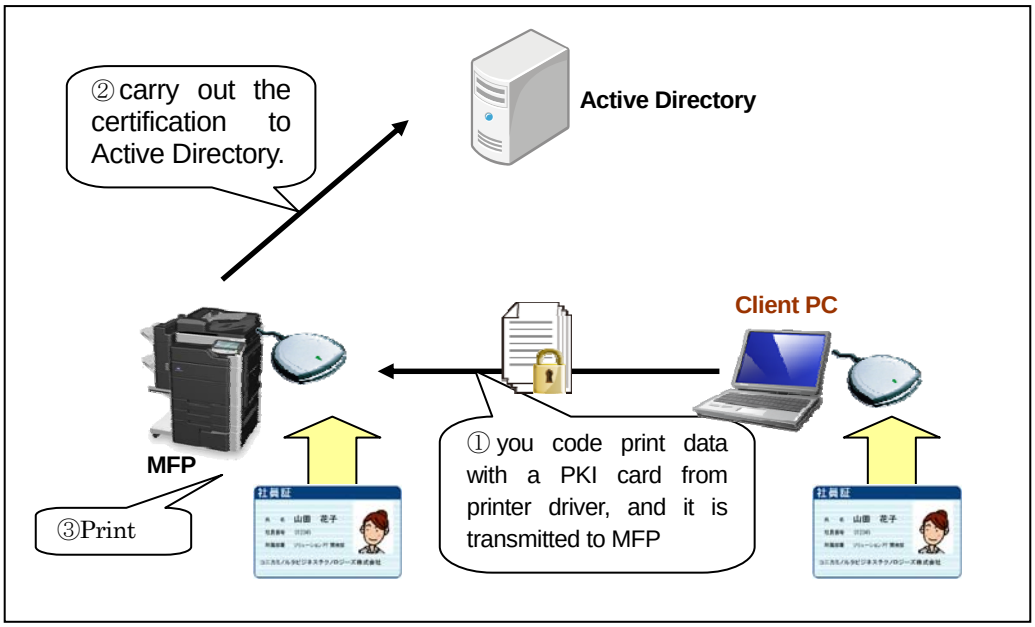


Figure 25

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.

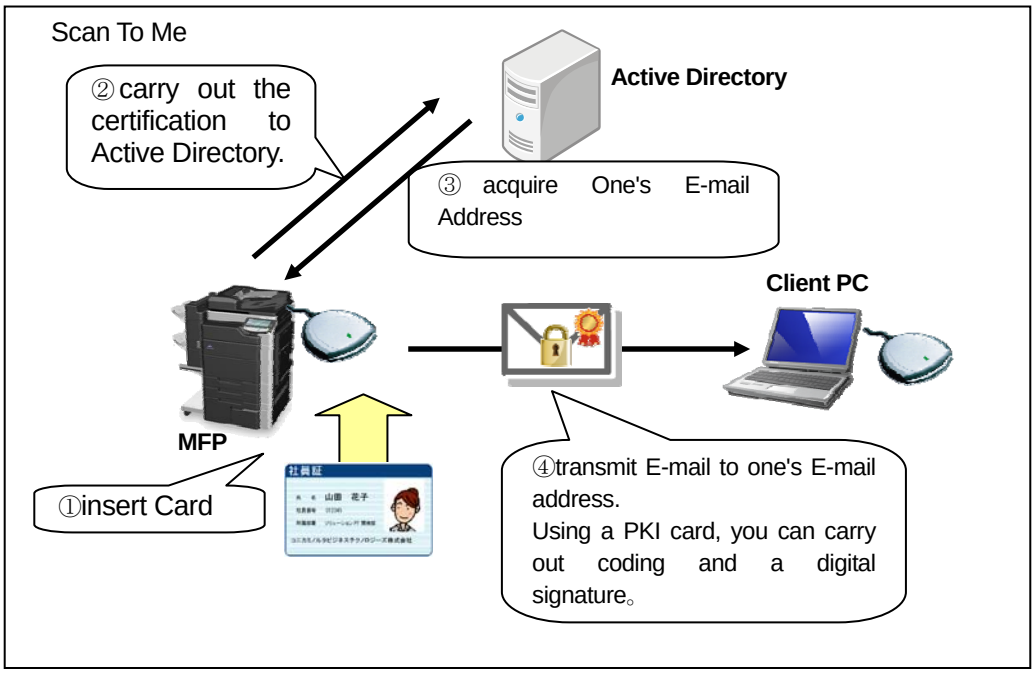


Figure 26

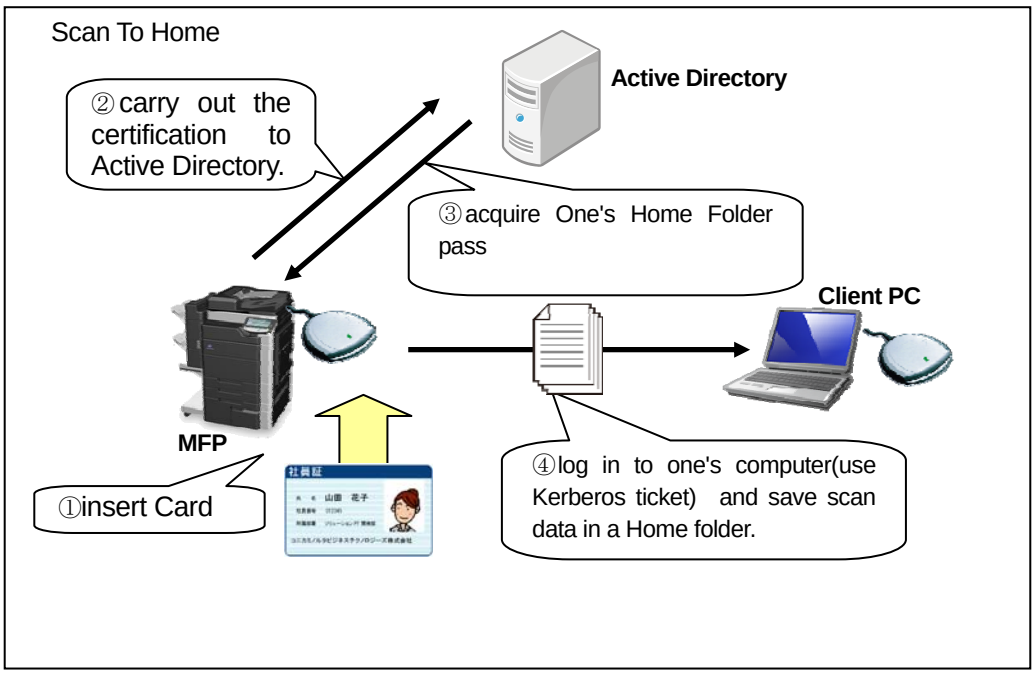


Figure 27

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, Wnen the setting of Enhanced Security Mode is enable, 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.