RICOH Smart Integration

Security Design Guide

Ver. 1.2.8

Revision History

Version	Date	Change Description
1.1.1	April 24, 2019	First version released
1.2.0	April 6, 2020	Merge DM-PF, ISS
1.2.1	May 22, 2020	Replace Link of RICOH information security policy Replace words “ISS”, “FollowMePrint” 2.1 add Business-PF into Common-PF 2.3.2.1 request parameter fixed
1.2.2	April 8, 2022	1.2 Add scope 2.3 Add the following to the use cases and data flow - General users - Linking External Services - Execution of Workflow Application by Webhook - Execution of Workflow Application Triggered by Email Reception - Execute Workflow Application Triggered by Email Receipt - Automatic synchronization of users with AzureAD - Tenant administrator - Set the destination of the email that notifies the completion of report creation - Set the destination of the email that notifies the completion of report creation - Set the billing code - Set up guest login - Change the settings of the device - Set the billing code - Manage user information 2.4.1 Add static.xxxx, help.xxx, print document upload, and communication destination 2.4.2 Adding New 3.4.9 New addition 4.1 There is a lack of description in the data to be managed in Table 4, so it was added. Job information, external account information, etc. 4.1.1 Added about security measures etc. 4.3.3 Job log data Job log preservation period was

		modified. 5.3.3 Corrected common explanations for receiving mail, etc. 5.5 Added AWS WAF to the network description
1.2.8	Dec. 12 2022	● The same document version number is assigned as the Japanese version because it had been the difference in numbering. ● 2.4.1 Add jp environment ● 2.4.2 Add URLs to communicate ● 4.1.2, 4.2.3, 4.3.4 Review of detailed descriptions ● 4.2.2 Corrected a description error. ● 8. Add about trademark of Microsoft 365

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this guide is to explain the security information concerning the Ricoh Smart Integration solution. The version applicable to this guide is RSI which was released at the end of March 2020. Ricoh implemented additional security measures in later versions to maintain optimal security in the current state.

1.2. Scope

The scope of this guide is the security functions of RSI applications that are used in RSI center servers (authentication, DS-PF, and RS-PF), devices (Multi-functional devices (MFD)), and Client PCs. The security of the APIs on the center server side used is described. As a client of RSI-Cloud, there is RICOHSmartDeviceConnector (development theme: Rimoco) , but this is outside the scope of this document.

The Ricoh Group treats information security management as an integral part of products and services when providing them to customers so that RICOH products and services can be used safely and securely [1]. This information security management system covers most of the organizational and operational measures specified in the guidelines[1]. However, these measures are not covered here because this guide focuses on explaining physical and technological measures.

[1] Information Security at the Ricoh Group (updated where necessary)
https://www.ricoh.com/sustainability/society/information-security-management-system/http://jp.ricoh.com/security/management/

2. System Configuration

2.1. Overall Configuration

The RSI-Cloud system consists of PCs in the customer environment, devices (MFD), and RSI-Cloud on Internet. RSI-Cloud consists mainly of RSI DS-PF (“DS-PF” stands for DocumentService-PF. DS-PF is for system tools, workflow application development tools, workflow apps, and conversion servers), RSI Remote Service-PF (for Device Management, Job Log Collection, and Reporting), RSI Common-PF (for Accounts Management, Authentication, Workplace, and Business-PF(manage contract e.g. contract site)) and a Pull Print (formerly released as FlexRelease CX) server that manages Pull Print jobs. In order to use the workflow application from MFD, MFD has the operation unit browser NX which is installed as the standard. For device authentication, status monitoring, and job log collection of MFD, the applications provided by RSI Integrated Solution (e.g. RSI Control+ in RE) have to be installed. RSI-Cloud system uses a port monitor as a client to upload jobs that will be printed out by Pull Print features provided by RSI Integrated Solution.

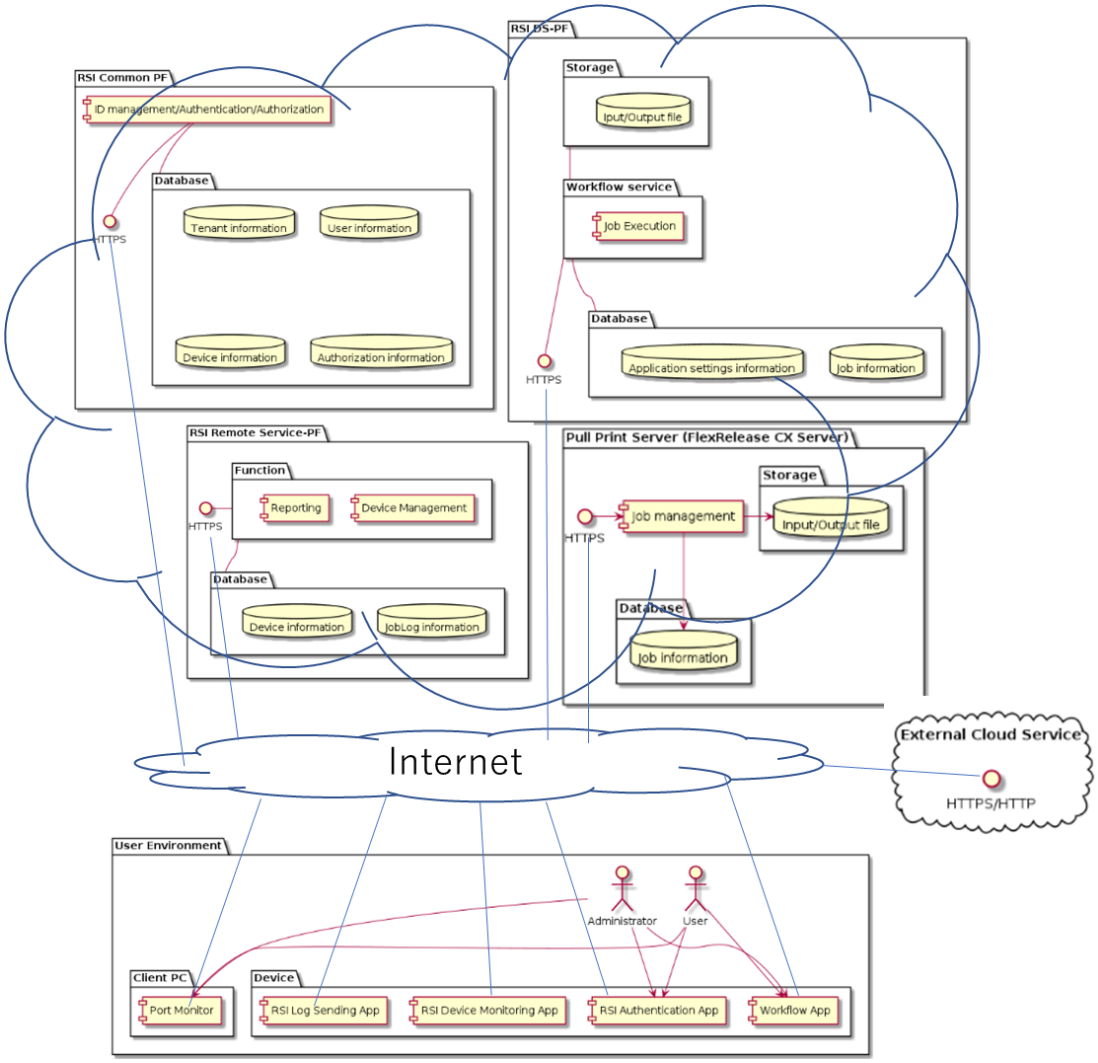

Figure 1 RSI System Configuration

2.2. Use Cases

Refer to this list to understand end user’s and administrator’s secure capabilities.

- General users
  - Perform RSI authentication from a PC or device.
  - RSI authentication with the external cloud service account
  - Configure external service integration
  - Scan paper documents from the device (MFD). The document information is e-mailed to the user who scan it via RSI-Cloud.
  - Scan paper documents from the device (MFD). The document file and information are delivered to the other cloud service via RSI-Cloud.
  - Print the document in the other cloud service by selecting it on the operation panel of the device.
  - Executing a workflow application with webhook
  - <New configuration> Executing workflow application triggered by email receipt
  - <Old configuration> execution of workflow app triggered by email receipt
  - Upload the print data (document) from the PC.
  - Print the document by selecting it on the operation panel of the device (MFD).
  - Access to the workplace via the user’s PC browser to set up user settings, authentication collaboration, and authorization settings.
  - Perform automatic synchronization of users with AzureAD
- Tenant administrators
  - Register devices from the operation panel of devices (MFD)
  - Access to the workplace via the user’s PC browser to check the list of devices.
  - Access to the workplace via the user’s PC browser to create and download reports.
  - From the user’s PC browser, access to the workplace to manage users, manage the tenant information, and set up workflow apps.
  - Setting the Destination of e-mails notifying of device malfunction
  - Receiving e-mail notifications of device malfunctions
  - Set the recipient of an email notifying the completion of report creation
  - Receiving an email notification of report completion
  - Setting a billing code
  - Configuring guest login
  - Changing device settings
  - Receiving email notification of task execution completion
  - Administrators can manage users and tenant information from a PC.
  - Manage the user's information

2.3. Data Flow

2.3.1. General User

This section describes the data flow between devices on RSI when the system is used by a general user. Typical use cases for general users described here are "Authentication on PC", “Authentication on device", “Authentication with the external cloud service account”, “Scanning and e-mailing paper documents to the user”, ” The scan document is delivered to the other cloud service via RSI-Cloud”, “Print File in the other cloud service Selection and Print Execution on Device (MFD)”, “Upload a print document from PC”, “Select print jobs of Pull Print from the device” and "Configure user OAuth setting".

2.3.1.1. RSI authentication on PC

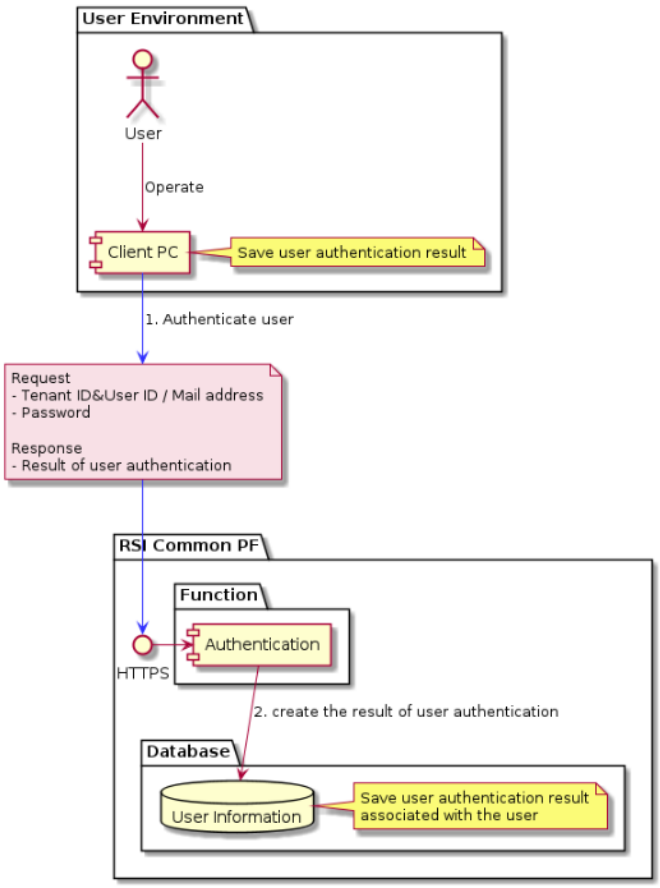

Figure 2 Data flow for RSI authentication on PC

The end user uses workplace or port monitor from the client PC to send the user information and password to RSI common PF for authentication. RSI common PF then verify the user information and password, stores the verification result in the user information database, and replies the result to the end user’s client PC.

2.3.1.2. RSI authentication on device

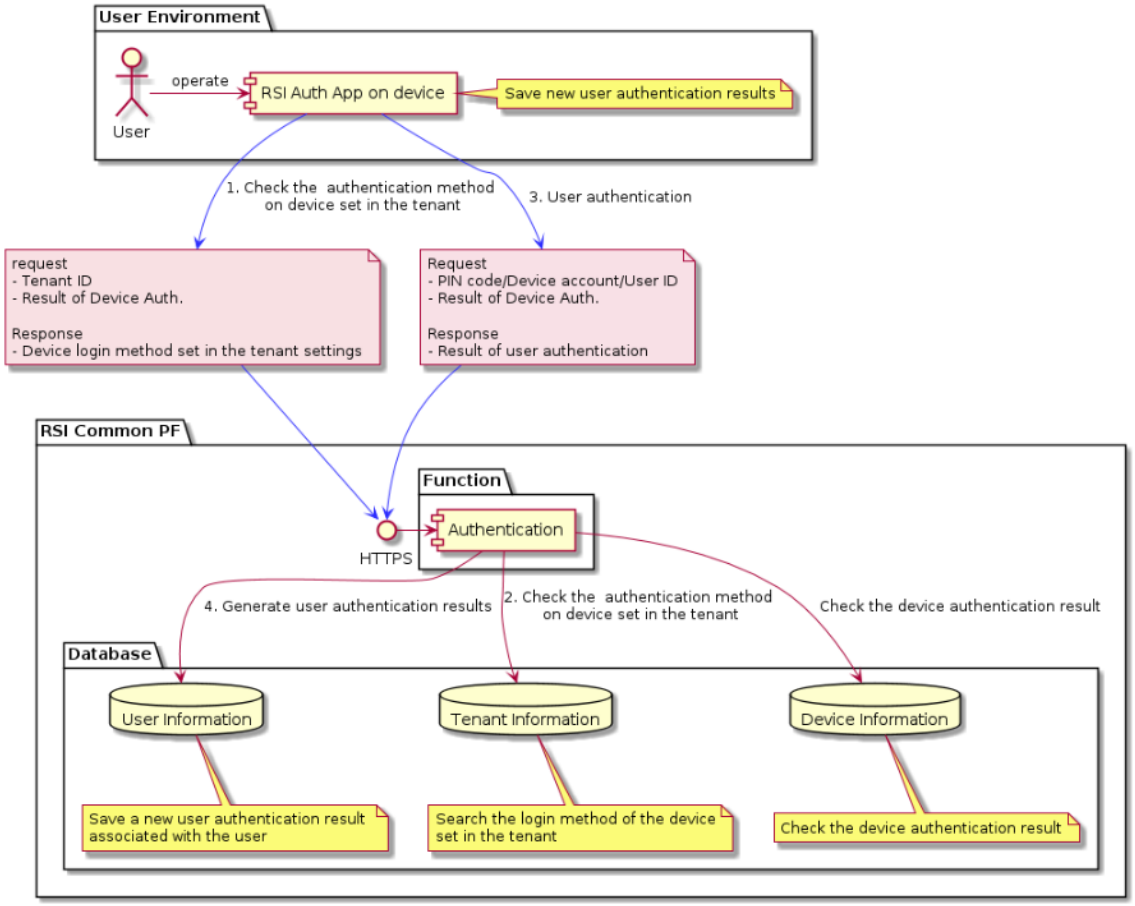

Figure 3 Data flow of RSI authentication from device

The end user starts the RSI authentication app to operate the device. RSI authentication app transmits the device authentication result and tenant ID at the time of device registration (explained later in this section) to RSI common PF in order to request the device login method that is set by this tenant. The common PF verifies the validity of the device authentication result, obtains the device login method from the tenant information, then replies to the RSI authentication app. Then, the RSI authentication app displays the login screen according to the login method so that the end user can enter the user information for the authentication. The RSI authentication app sends this user information and the device authentication result (also used earlier by the RSI common PF) to request for the end user's authentication result. RSI common PF is now requested for authentication, and it checks the validity of the device authentication results, verifies the user information, stores the authentication result in the user information database, and then replies the results to the RSI authentication app.

Providing the authentication result is OK, the RSI authentication app unlocks the device so that the device is available to end users.

In addition to the above, it is also possible to authenticate RSI by e-mail address/password or tenant ID/user ID/password, PIN code, without using the RSI authentication application.

There is also a user-selected login method that allows authentication using only the user ID. This is explained in Section 4.1.1.

2.3.1.3. Scanning and e-mailing paper documents to the user

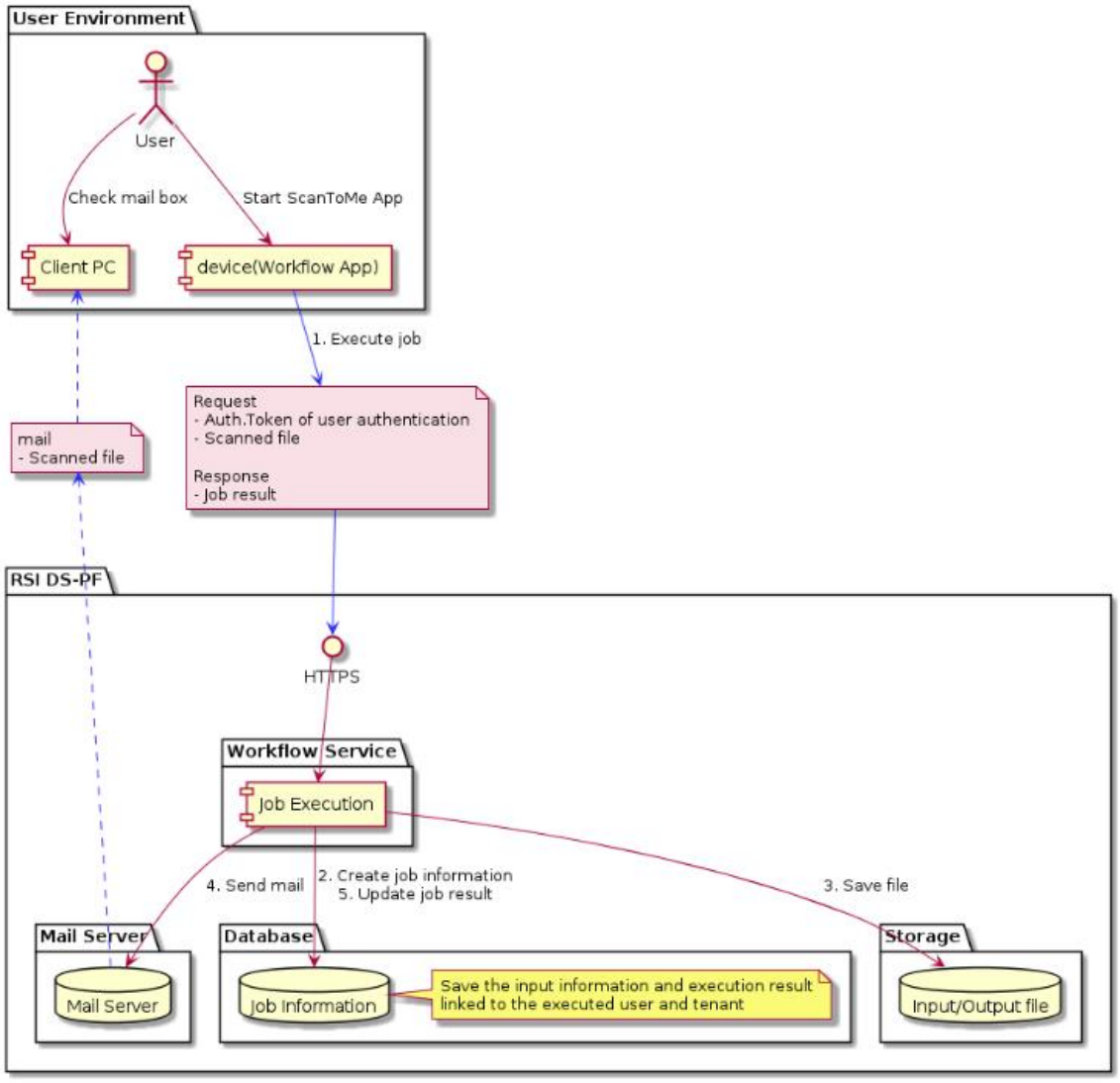

Figure 4 Data flow for mailing a scanned document read to the user

End users must first perform RSI authentication on the device (for the flow, see 2.3.1.2). After this, the end user has to start the ScanToMe workflow app to send the scanned document to the cloud service (1). The workflow app sends DS-PF a job with scanned image as the input file and the user information as the parameter. The DS-PF workflow service generates the job information and stores it in the job information DB (2) and stores the input file in the storage (3). Then to the mail service, the workflow service sends the destination address and the input file, and requests to send the email with the input file as an attachment to the end user (4). Finally, the mailing result is recorded in the job information DB (5) and the input file is deleted from the storage.

2.3.1.4. Configure external service integration

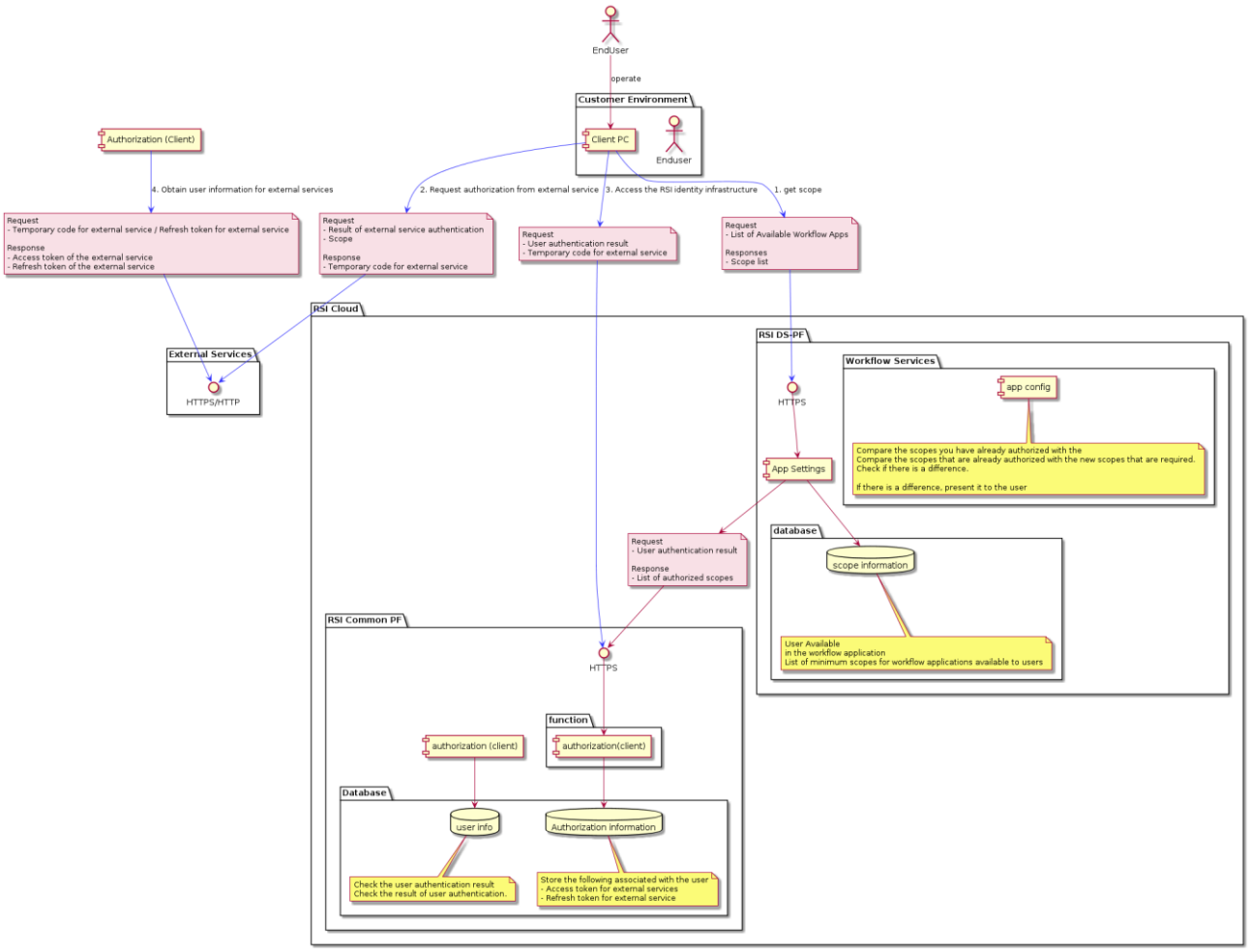

Figure 5 Data flow for configure external service integration

Pass the list of workflow applications from the client PC to the application settings in the DS-PF workflow service, obtain the list of authenticated scopes obtained from the RSI common PF and the minimum list of scopes in the workflow application that the user can use from the scope information in the database. If there is a difference, present the user with additional scope settings (1). Next, the client PC makes an authorization request to the external service, passing the external service authentication result and scope (2). In the response, it obtains the temporary code for the external service, passes the user authentication result and the temporary code for the external service to the RSI common PF (3), checks the user authentication result in the database, and then obtains the user information for the external service (4). The token of the external service obtained in the response is stored in the database.

2.3.1.5. RSI authentication with the external cloud service account

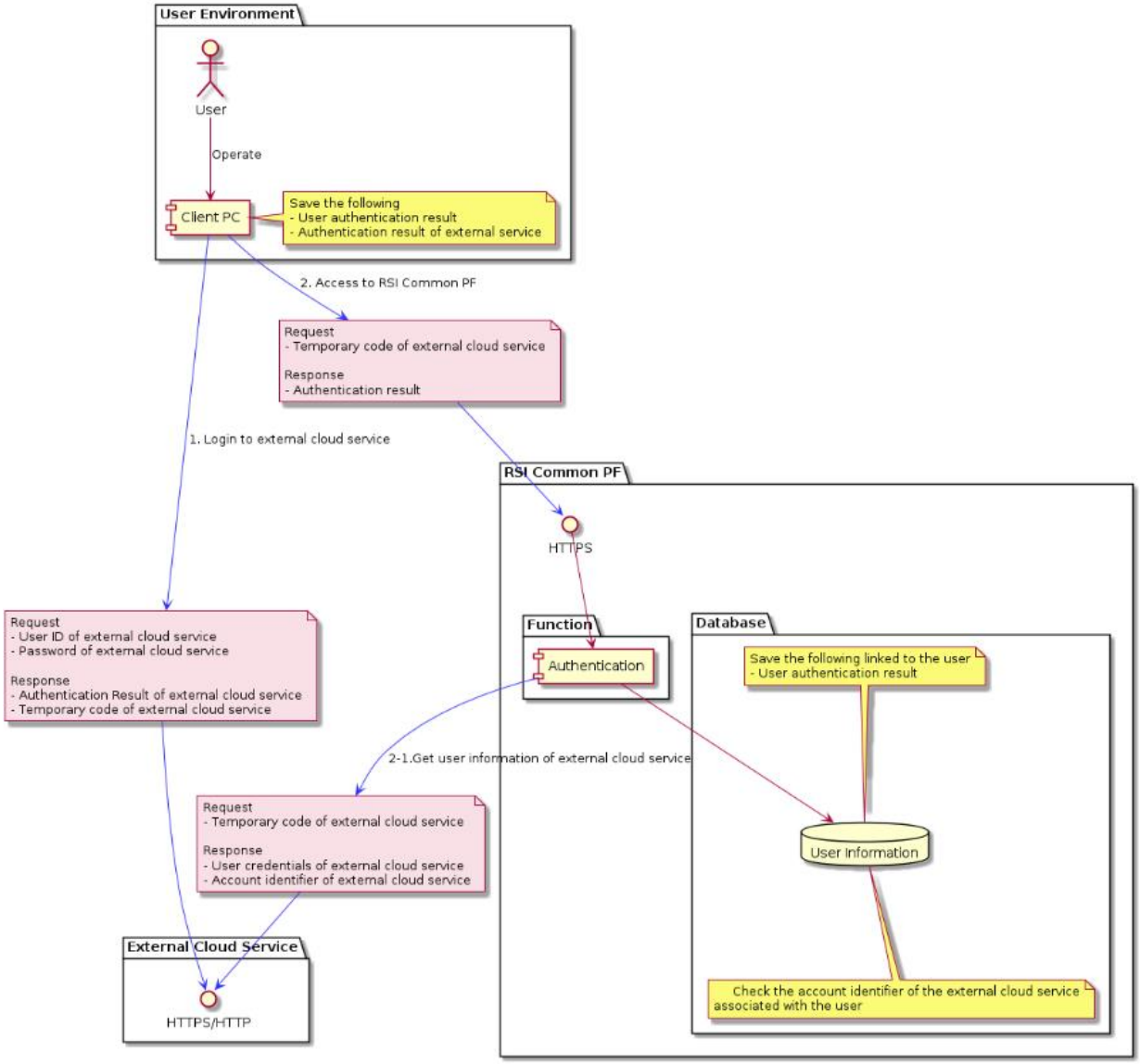

Figure 6 Data flow for RSI authentication with an external service account

To use an external cloud service account (only Office365 is supported as Nov. 2022) to perform RSI authentication on the workplace or port monitor, the user uses the client PC to access to the external service web page. The client PC then sends the user information to the external services that return the authentication results and temporary codes as the reply. Then, the client of RSI-Cloud (on the client PC that received this reply) forwards the temporary code for the external service to RSI common PF requesting to authenticate for the user to use RSI. RSI common PF receives the request, forwards this temporary code to the external service, and requests the user certificate and the account identifier related to this temporary code. This account identifier of the external service is received by RSI common PF that verifies if there is a registered user who has an account identifier. If there is such a user, RSI common PF replies that the user can be authenticated. The authentication result is stored in the user information database.

2.3.1.6. The scanned document is delivered to the other cloud service via RSI-Cloud.

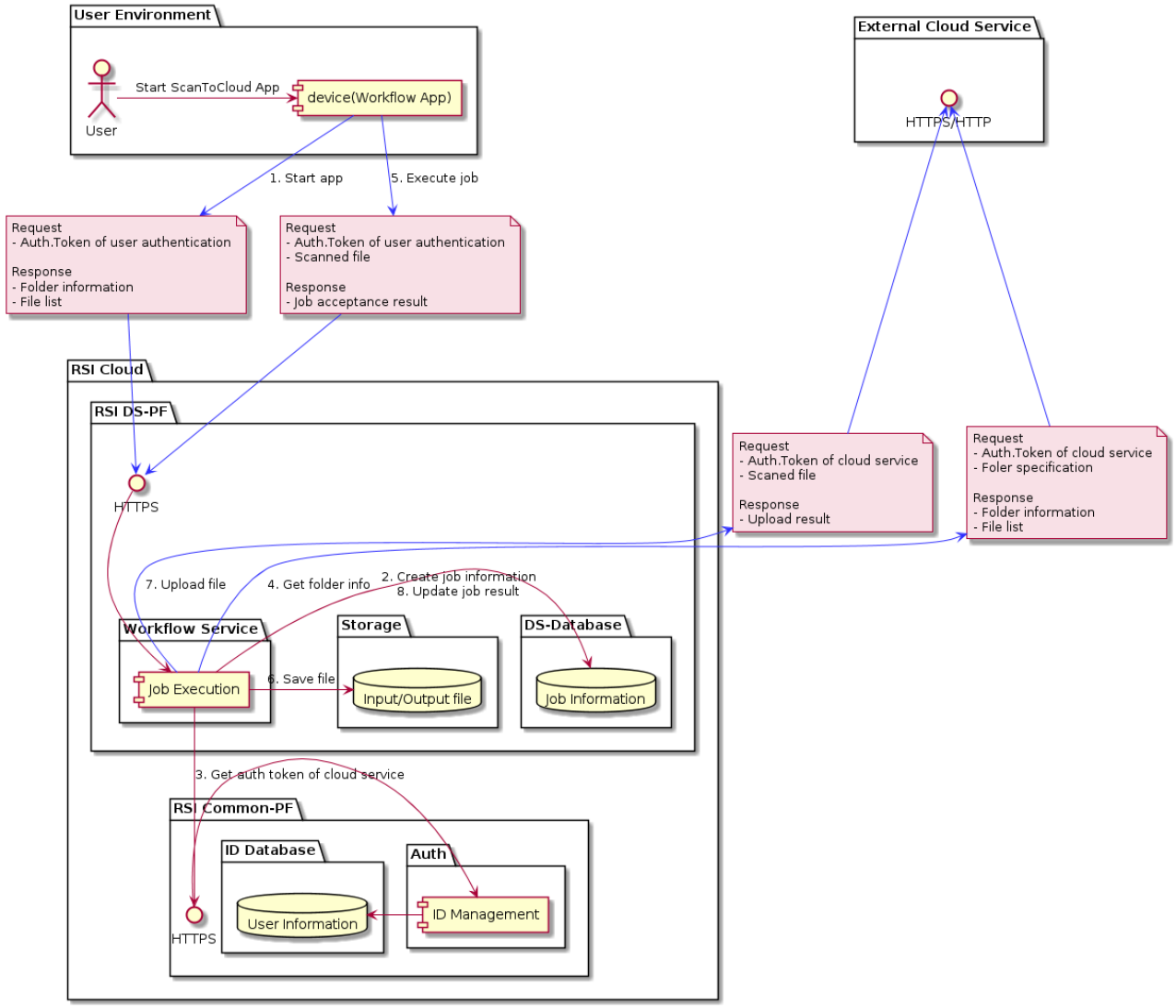

Figure 7 Data flow for the scanned document is delivered to the other cloud service via RSI-Cloud.

The end users must first perform RSI authentication on the device (for the flow, see 2.3.1.2). After this, the end user has to start the ScanToCloudService workflow app to send the scanned document to the cloud service. The workflow app sends auth token in order to get the folder information and file list (1). The DS-PF workflow service generates the job information and stores it in the job information DB (2) and get the auth token of external cloud service from RSI Common-PF (3). Then the DS-PF get folder information from the external cloud service sending auth token of the external cloud service and folder specification (4), then workflow app shows the folder information to end users.

Then the end users execute workflow app, workflow app sends scanned file with auth token (5). The DS-PF stores the input file in the storage temporary (6), then uploads it to the external cloud service with

auth token of the external cloud service (7) and receives the upload result. The DS-PF updates the job information by the upload result (8) and delete the input file.

2.3.1.7. Print file in the other cloud service selection and print execution on device (MF)

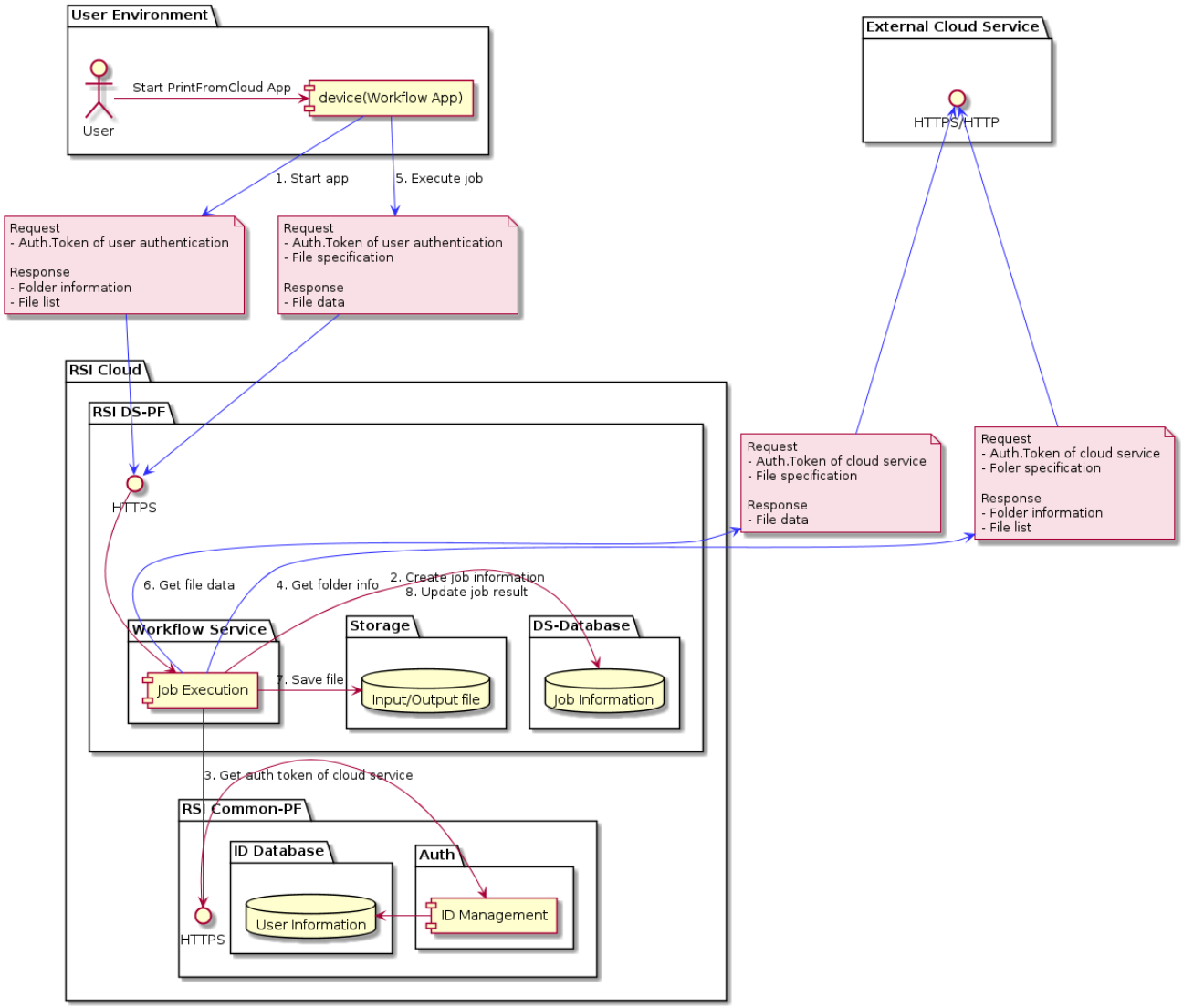

Figure 8 Data flow for print file in the other cloud service selection and print execution on device (MFD)

The end users must first perform RSI authentication on the device (for the flow, see 2.3.1.2). After this, the end user has to start the PrintFromCloudService workflow app to print the document from the cloud service. The workflow app sends auth token in order to get the folder information and file list (1). The DS-PF workflow service generates the job information and stores it in the job information DB (2) and get the auth token of external cloud service from RSI Common-PF (3). Then the DS-PF get folder information and file list from the external cloud service sending auth token of the external cloud service and folder

specification (4), then workflow app shows the folder information and file list to the end users.
Then the end users execute workflow app specified print document, workflow app sends file specification with auth token (5). The DS-PF downloads the specified file from the storage with auth token of the external cloud service (6), then stores it in the storage temporary (7). The workflow app downloads the specified file. The DS-PF updates the job information if the file is downloaded successfully (8) and delete the temporary stored file.

2.3.1.8. Executing a workflow application with Webhook

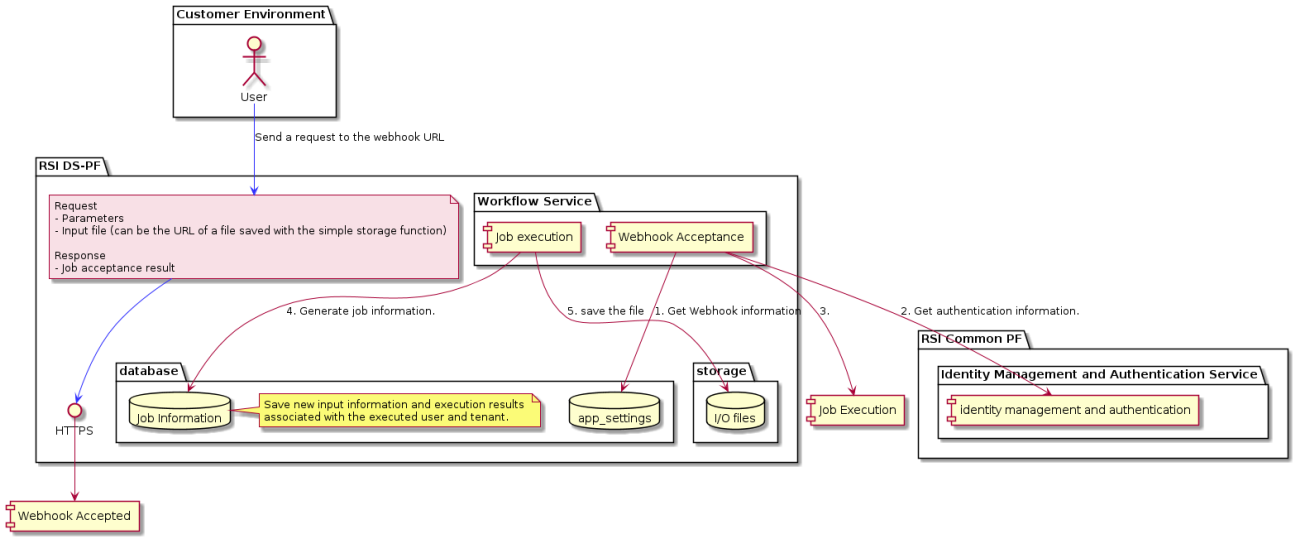

Figure 9 Data flow for executing a workflow application with webhook

The end user makes a request to the Webhook URL provided by DS-PF by specifying the input file and parameters (1), and when the workflow service accepts the request, it obtains the Webhook information from the application configuration information based on the URL information (2). The user is managed by linking the user to an unguessable random string contained in the URL, and the authentication information is obtained from the ID management and authentication service of RSI Common PF using that linking information (3). The requested job execution is started (4), the input information and execution results are newly saved in the database linked to the user and tenant who executed the job (5), and the file is saved in the storage (6). Thereafter, the system operates in the normal workflow flow, and the temporarily stored files are deleted.

Supplemental: The following security measures have been implemented.
Webhook URLs can be requested without authentication information, but Webhook URLs with signatures that are difficult to guess are issued.
Webhook URLs are issued with signatures that are difficult to guess.
Disable a Webhook URL when the number of jobs executed by the Webhook exceeds the upper limit available in a certain period of time (the upper limit can be specified for each Workflow application)

2.3.1.9. <New configuration> Execution of workflow application triggered by email receipt

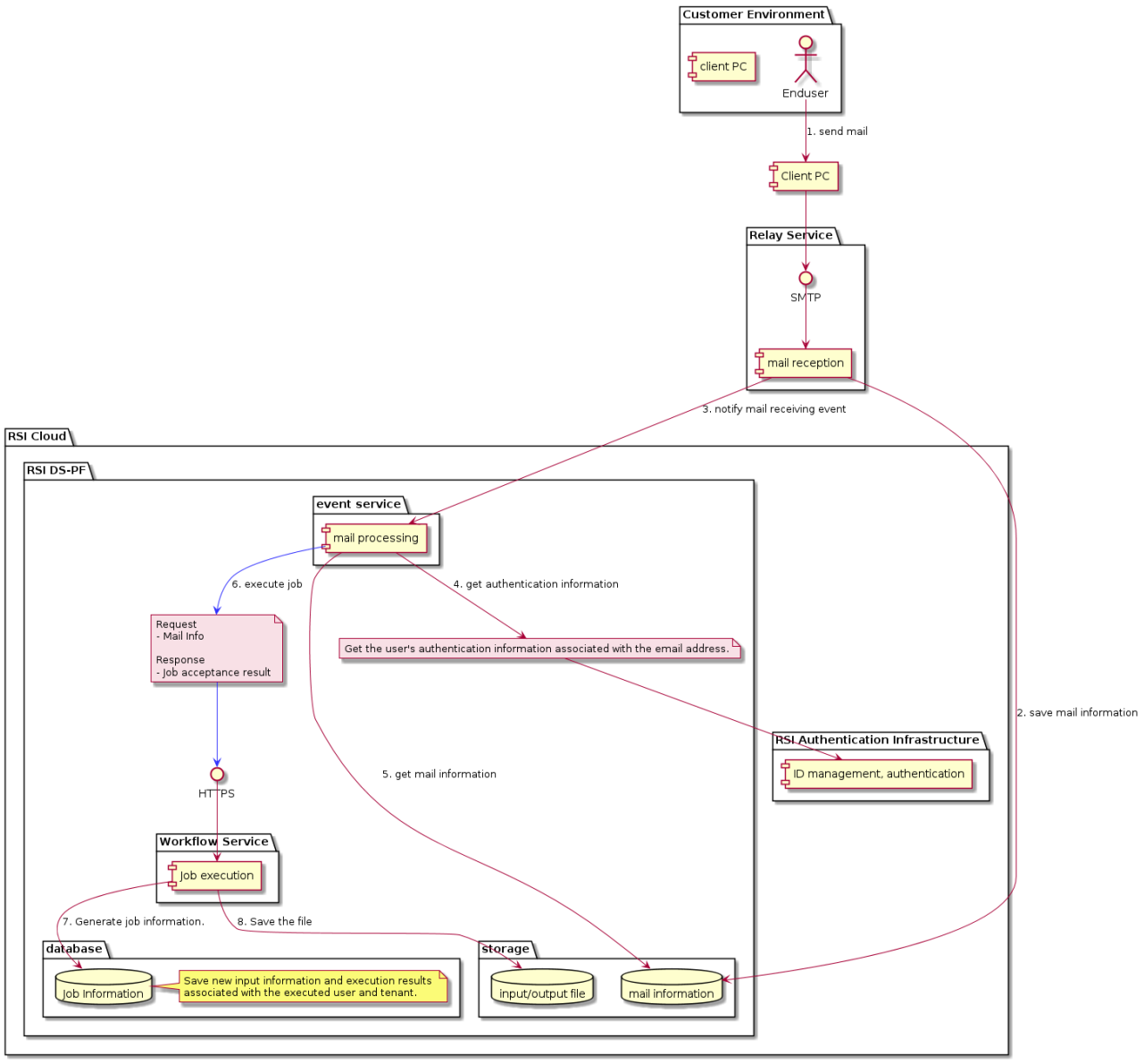

Figure 10 Data flow for <new configuration> execution of workflow application triggered by email receipt

The end user sends an e-mail from the client PC to the relay service using the e-mail address provided by DS-PF (1). First, the mail information is stored in the mail information of the storage (2), the event service receives a notification of receipt (3), and the authentication information associated with the mail address is obtained from the RSI authentication infrastructure (4). Next, the mail information is retrieved from the storage (5), and the job execution is requested to the workflow service (6). The input information and execution results are newly saved in the database (7), linked to the user and tenant who executed the job, and the file is saved in the storage (8). From then on, the system operates in the normal

workflow flow, and the temporarily stored files are deleted.

See 5.3 for details of the security contents.

2.3.1.10. <Old Configuration> Execution of workflow application triggered by email receipt

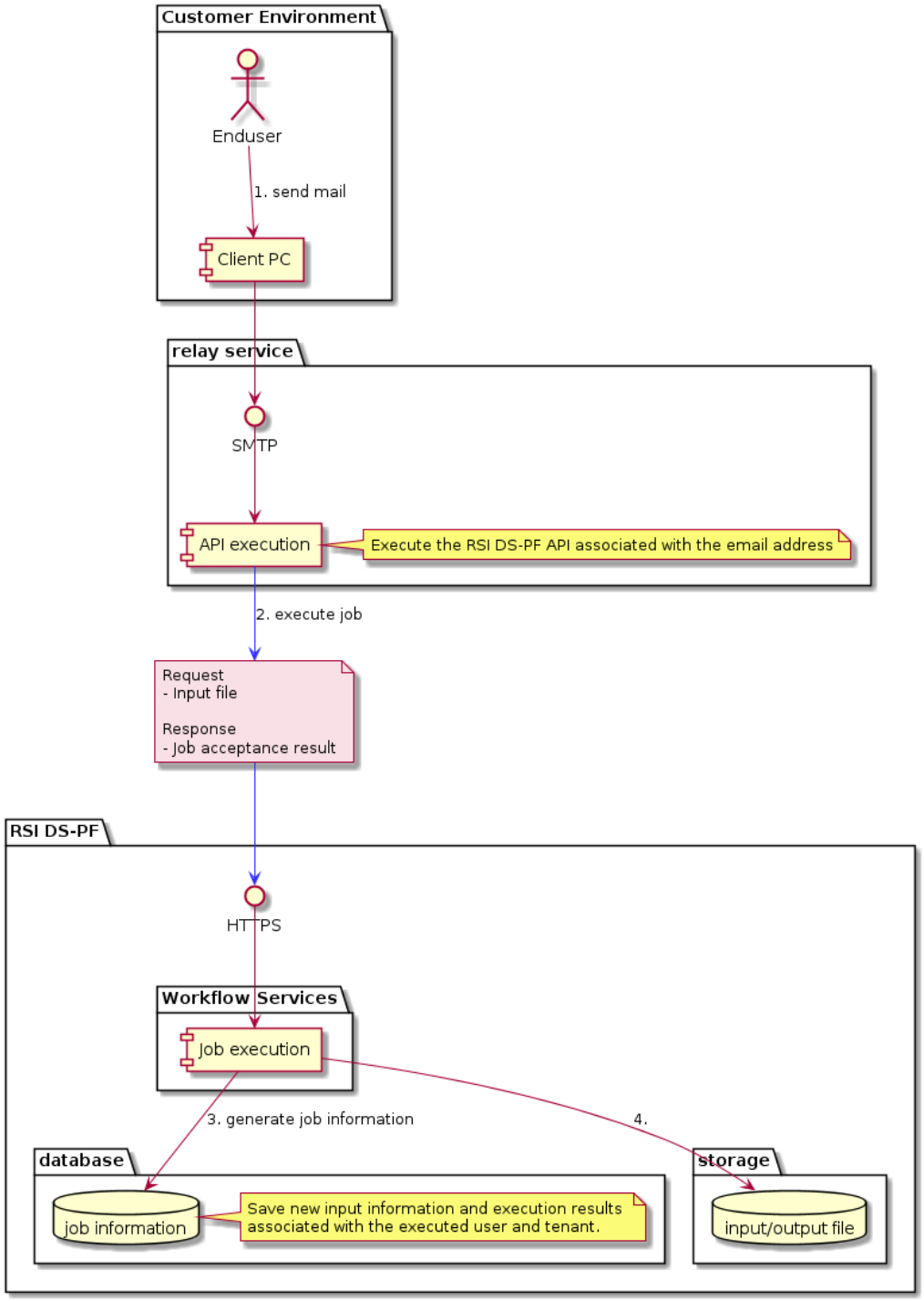

Figure 11 Data flow for <old configuration> execution of workflow application triggered by email receipt

The old configuration is the configuration until November 2020. Some applications developed before then that have not been updated to the new configuration after November 2020 are executing jobs in the old configuration.

The end user sends e-mail from the client PC to the relay service using the e-mail address provided by DS-PF (1). The relay service executes the DS-PF API associated with the email address and requests the workflow service to execute the job (2). The input information and execution results are newly saved in the database (3), linked to the user and tenant who executed the job, and the file is saved in storage (4). (3) The file is saved in the storage (4). Thereafter, the workflow works as usual, and the temporarily saved file is deleted.

2.3.1.11. Upload a print document from PC (via port monitor)

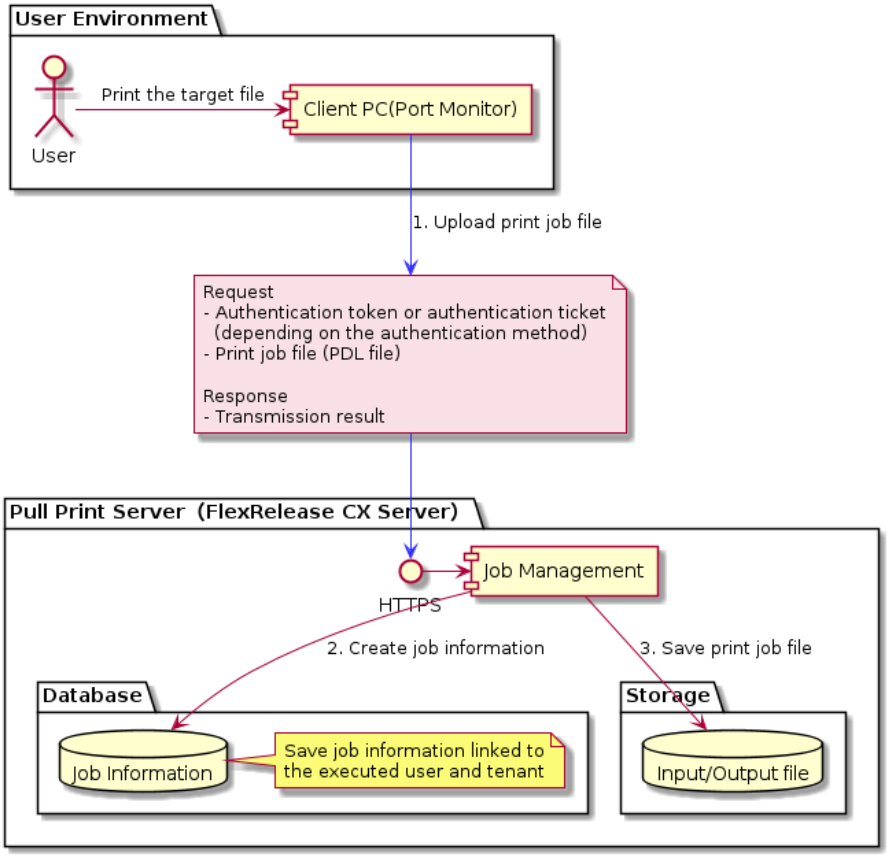

Figure 12 Data flow for uploading a print document from PC

End users obtain RSI certification results (for the data flow, see 2.3.1 or 2.3.3). Then, via the port monitor, the client PC sends the authentication result and the PDL data to the Pull Print server. The Pull Print server generates the job information by linking the authenticated user information and PDL data that were received via the port monitor. PDL data is stored in a storage in the Pull Print server, then the job information is updated by adding the URL information.

2.3.1.12. Select print jobs of pull print from the device

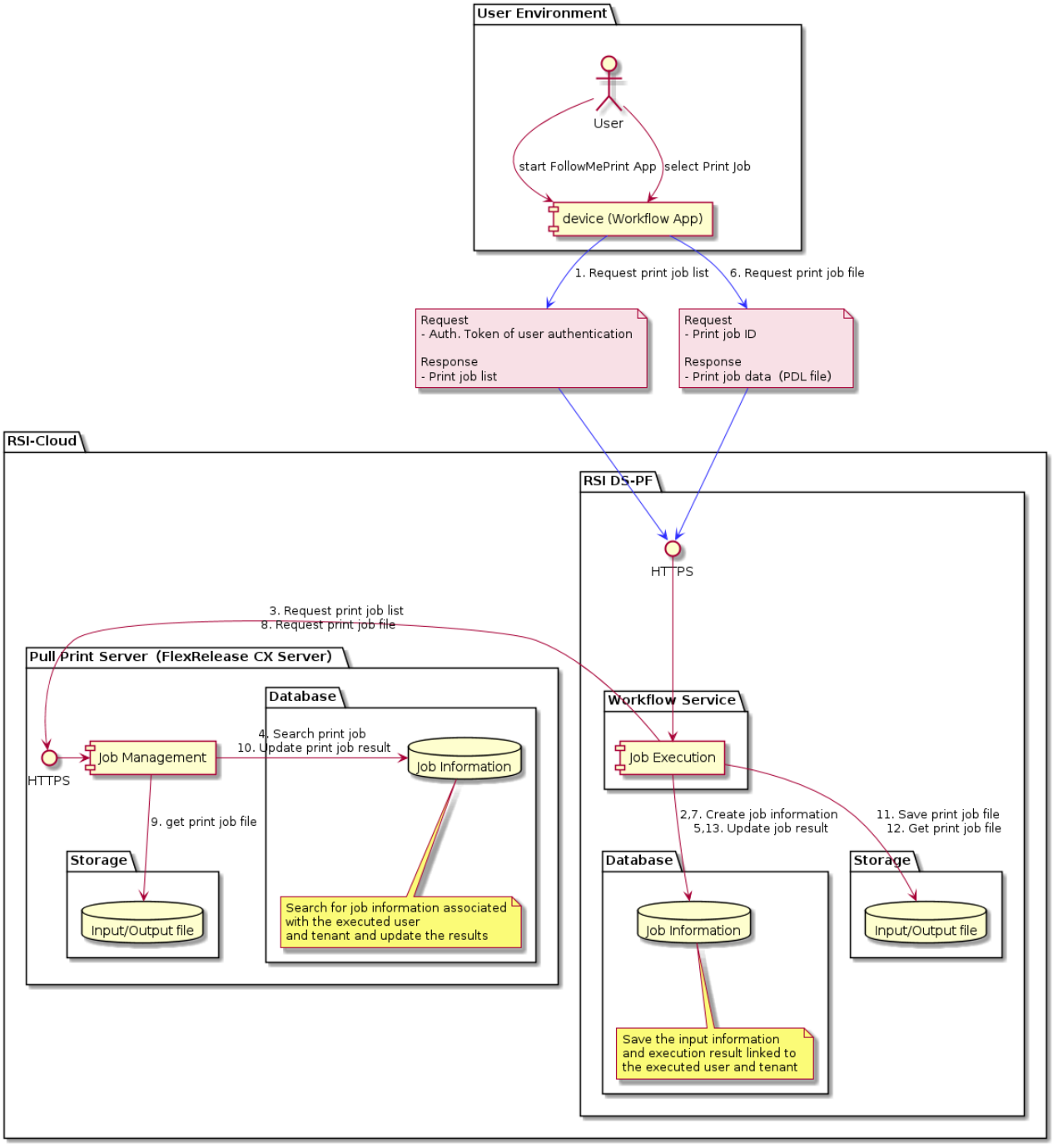

Figure 13 Data flow for printing by selecting a print job on the device

End users first perform RSI authentication on the device (for the data flow, see 2.3.2). Upon the authentication success, the device's workflow app requests DS-PF for the end-user's print job list. The DS-PF workflow service generates the job information, then requests the Pull Print server for the print job list. The Pull Print server replies to the workflow service with the end user's print job list from its own Job Information Database. The workflow service adds the DS-PF job information about whether the user's job list was obtained or not, then replies to the workflow app. The workflow app then displays the print job list screen to the end user.

The end user selects jobs from the print job list on screen and executes printing. The workflow app receives the print instruction then requests DS-PF for the print file data. The DS-PF workflow service that received the request generates the job information to requests the Pull Print server for the print job file data. The Pull Print server then finds the print job file from its file storage, reply to the workflow service, and the communication results are recorded in the job information database. The workflow service temporary stores the data in DS-PF storage, retrieves the file from this temporal storage, replies the print job file to the workflow app, and records the communication result in the job information database. After receiving the print job file, the user can send the print job file to the print app on the device to print out the data.

When a smart device associated with an RSI account is held at the control panel and logged into the MFD, the RSI Auto Print application can be designated in advance by the end user to automatically output the print job uploaded via the port monitor.

2.3.1.13. Configuring user OAuth settings on client PC

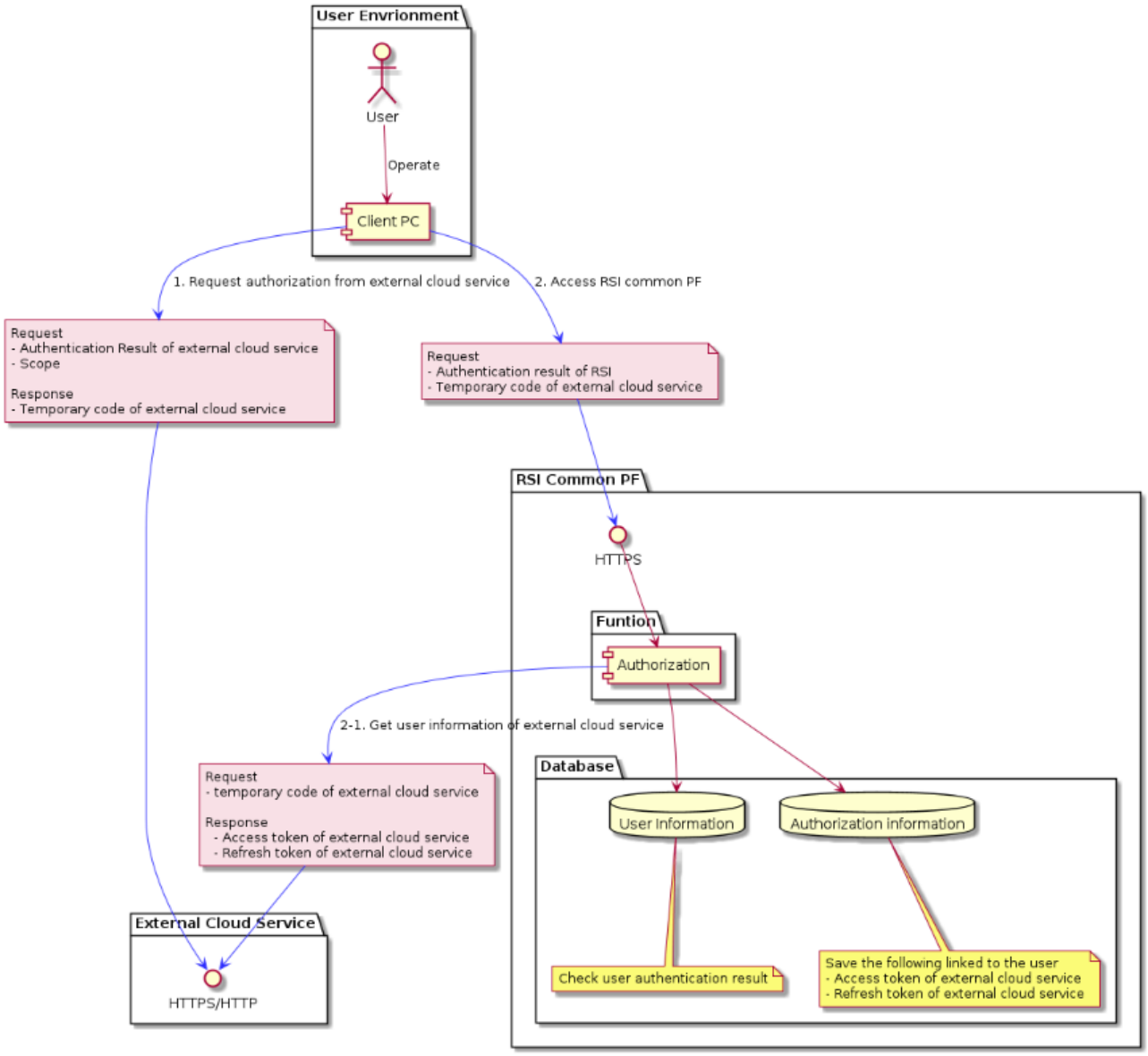

Figure 14 Data flow for OAuth settings on PC

Oath setting is required before an end user can log in to the system by using the ID of an external service (as seen in 2.3.3). By the end user accessing the Workplace via the client PC and starting to configure OAuth, the web page of the external service is displayed. After the user enters the authentication information for the external service that is sent to the external service together with the scope of the OAuth configuration, the external service validates the authentication information and replies the temporary code to the Workplace if the result is OK (1). The Workplace then sends the user authentication result by RSI and the temporary code for the external service to RSI common PF. The common PF now sends the temporary code to the external service and requests for the access and refresh Tokens for the external service. The tokens received through this process are stored in the authorization information DB.

2.3.1.14. Perform automatic synchronization of users with AzureAD

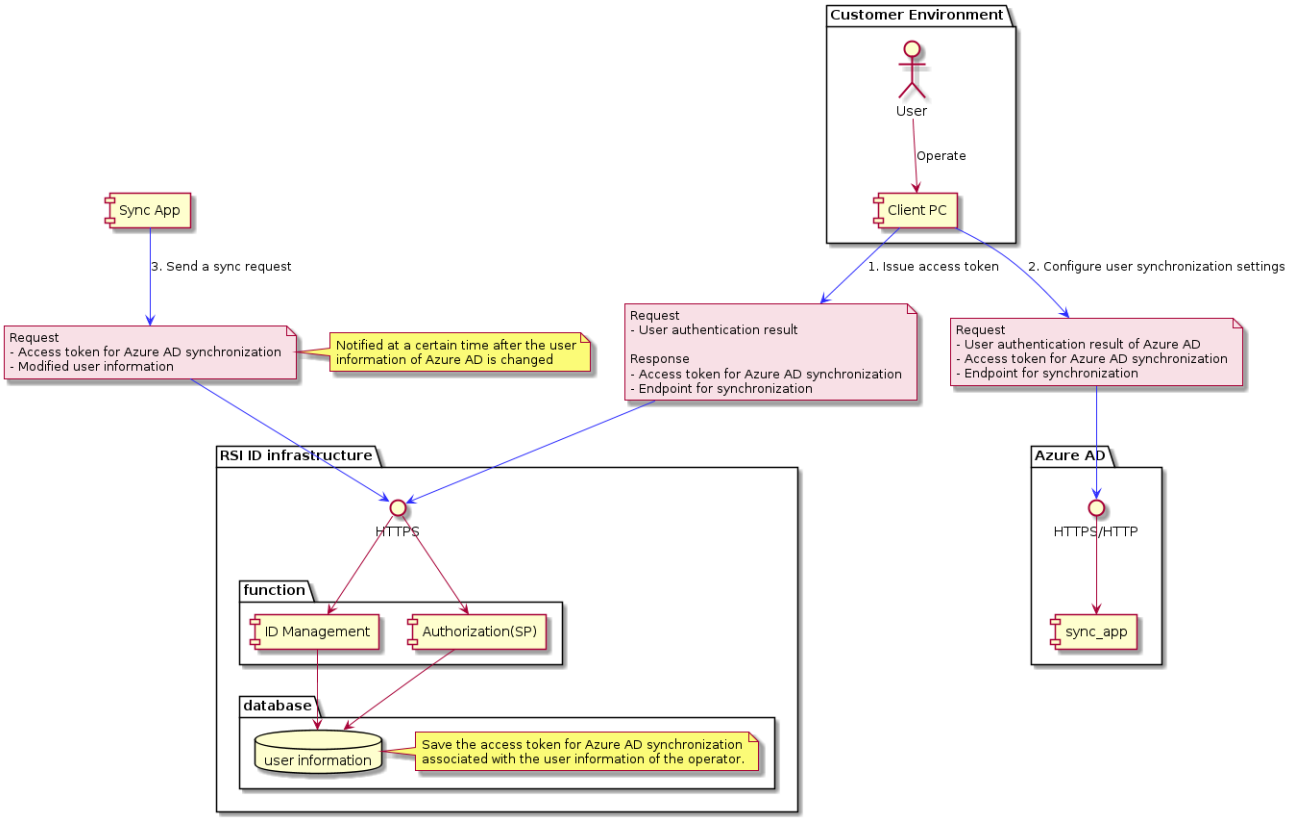

Figure 15 Data flow for perform automatic synchronization of users with AzureAD

・As a preliminary condition, the following must be met

・You must have RSI user authentication.

・Log in to the Azure AD portal.

To issue an access token, the end user operates the PC and passes the RSI authentication result to the RSI identity management authentication service to obtain an access token for Azure AD synchronization and an endpoint for synchronization (1). Next, pass the AzureAD user authentication result, the AzureAD synchronization access token, and the synchronization endpoint to AzureAD to set up user synchronization (2). The synchronization application in AzureAD sends a synchronization request and passes the access token and the changed user information to RSI's identity management authentication service to save the user information (3). This process will be notified at a certain timing after the user information in AzureAD is changed.

User automatic synchronization with Azure AD is handled securely in accordance with the standard protocol called SCIM2.0 (RFC7642, RFC7643, 7644).

Supplemental: Security measures

The RSI endpoint that accepts synchronization requests is different for each tenant.

In order to accept synchronization requests, an access token issued by the RSI tenant administrator is required.

The access token cannot be used by other tenants.

2.3.2 Tenant administrator

This section describes the data flow between devices on RSI when the system is used by a tenant administrator. Typical use cases for tenant administrator described here are "Registering a device", "Checking the list of devices via client PC", “Creating and downloading reports via/from PC” and "User management".

2.3.2.1 Registering a device

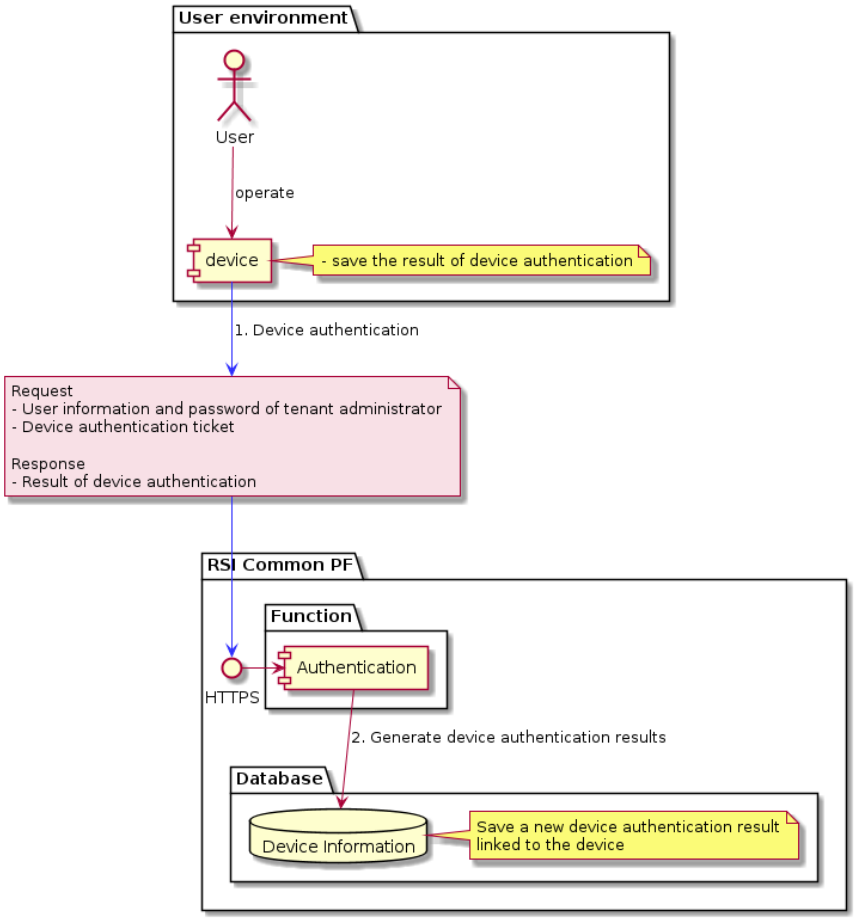

Figure 16 Data flow for device registration

The end user starts the device's cloud setting app to enter the tenant administrator's information. The

cloud setting app sends the entered information and the device authentication ticket to the RSI common PF to request for the device registration. RSI common PF then verifies the device's serial ID. When it is correctly verified, RSI common PF saves the verification result in the device information DB as a tenant's device which information is obtained from the tenant administrator information, and send the communication result to the cloud setting app.

2.3.2.2 Checking the list of devices via client PC

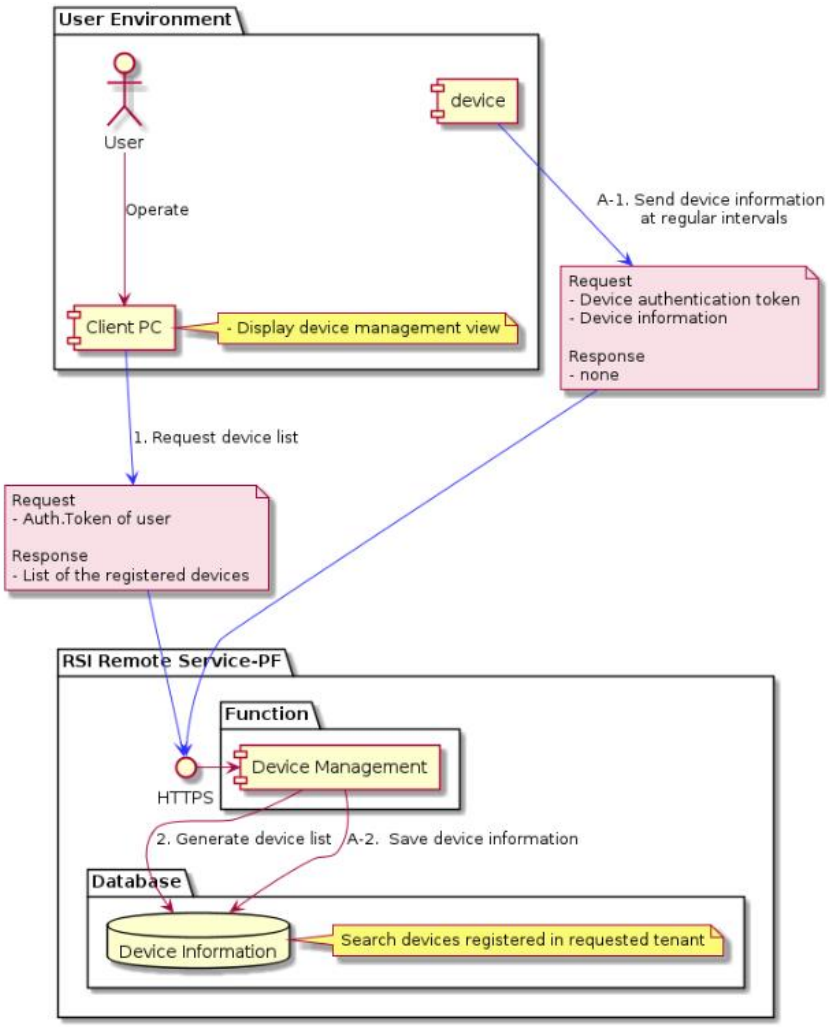

Figure 17 Data flow for viewing the device list

Once the device is registered (for its procedure, see 2.3.2.1), the RSI device monitoring app periodically sends the device information (for details, see Table 5 "Data managed by Remote Services-PF") to RSI Remote Service-PF (A-1). The device information that Remote service-PF received is stored in the device information DB (A-2).

End users can check the device list by accessing the Workplace via the client PC, performing RSI authentication (for the steps, see 2.3.1.1 or 2.3.1.3), then opening the device management device list screen (1). Remote service -PF receives the device list display request so it searches for the tenant device information that is requested by the device information DB in order to create the device list (2).

The Workplace's device list screen displays the results.

2.3.2.3 Creating and downloading reports via/from PC

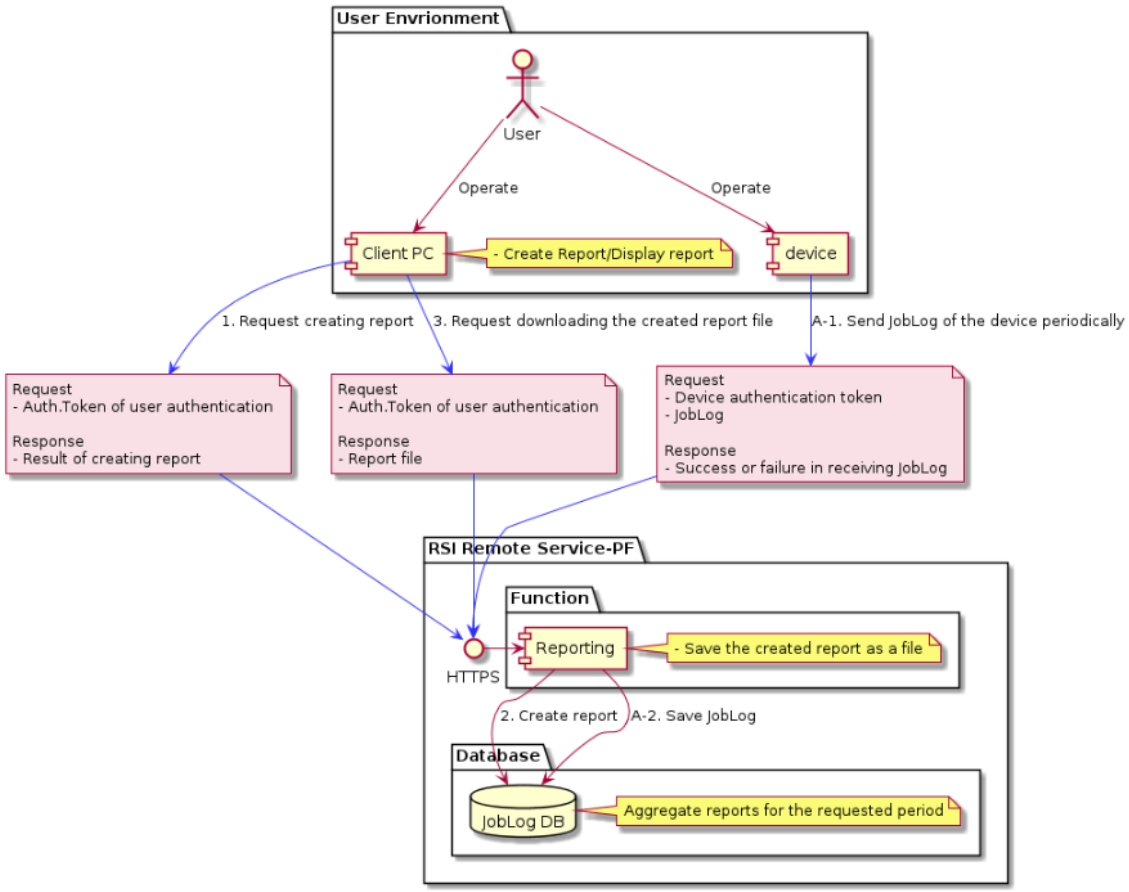

Figure 18 Data flow for creating and downloading reports via/from PC

When an end user uses a device, a job log is generated. This job log and the Instrument Authentication Token are sent to RSI Remote Service-PF by the RSI Log Send App (A-1). The RSI Remote Service-PF identifies the tenant based on the device authentication Token. If the tenant holds a valid license for reporting, the RSI Remote Service-PF receives the job log and stores the data in the job log DB, then return the communication result to the RSI log submission app (A-2).

End users can create a report by accessing the Workplace via the client PC, performing RSI authentication (for steps, see 2.3.1.1 or 2.3.1.3), then requesting for the report via the reporting screen (1). Remote service-PF that receives a report creation request creates a report and replies the results (2). End users can download the report file via the Workplace reporting screen (3). The download request is received by Remote Service -PF that replies with the file created in step 2 (4).

2.3.2.4 Set the destination of the email notifying of device failure

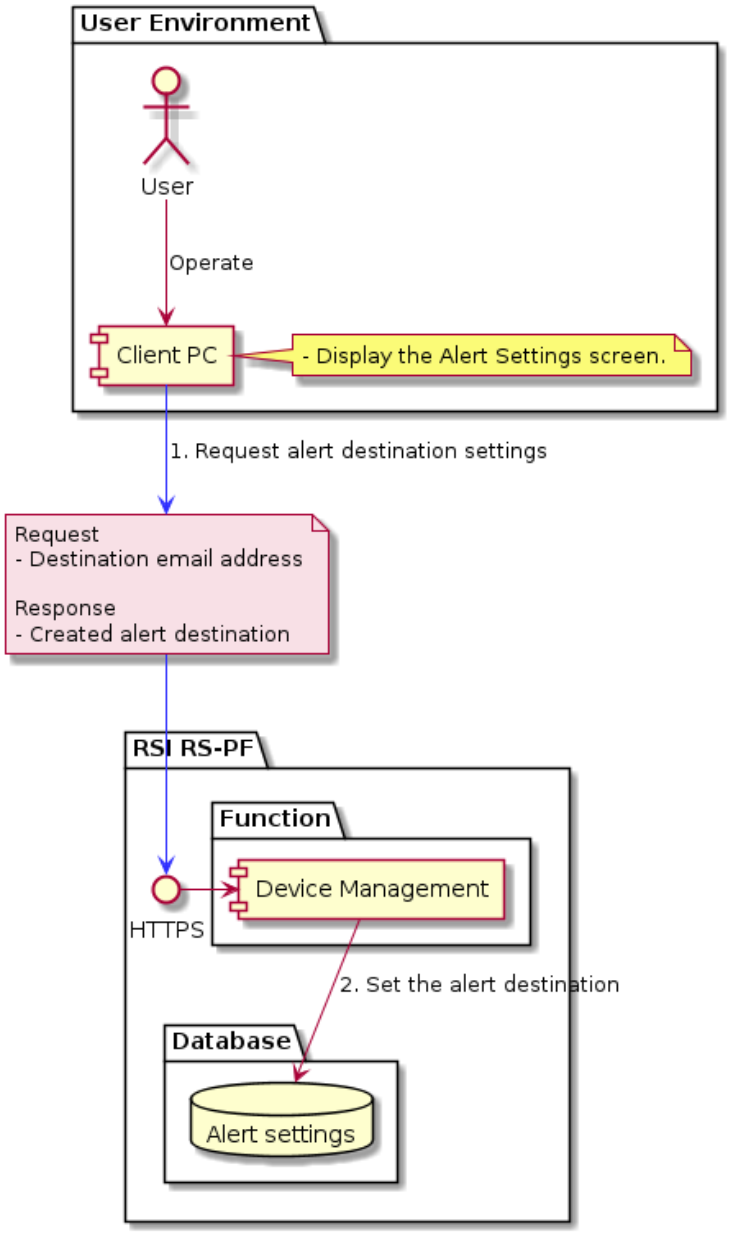

Figure 19 Data flow of set the destination of the email notifying of device failure

The end user accesses the common setting site with the client PC, and after performing RSI authentication according to the procedure described in 2.3.1.1 or 2.3.1.3, opens the mail notification destination setting screen of the device management and requests the destination setting (1). RSI Remote Service-PF saves the received destination settings in the database (2).

2.3.2.5 Receiving e-mail notifications of device malfunctions

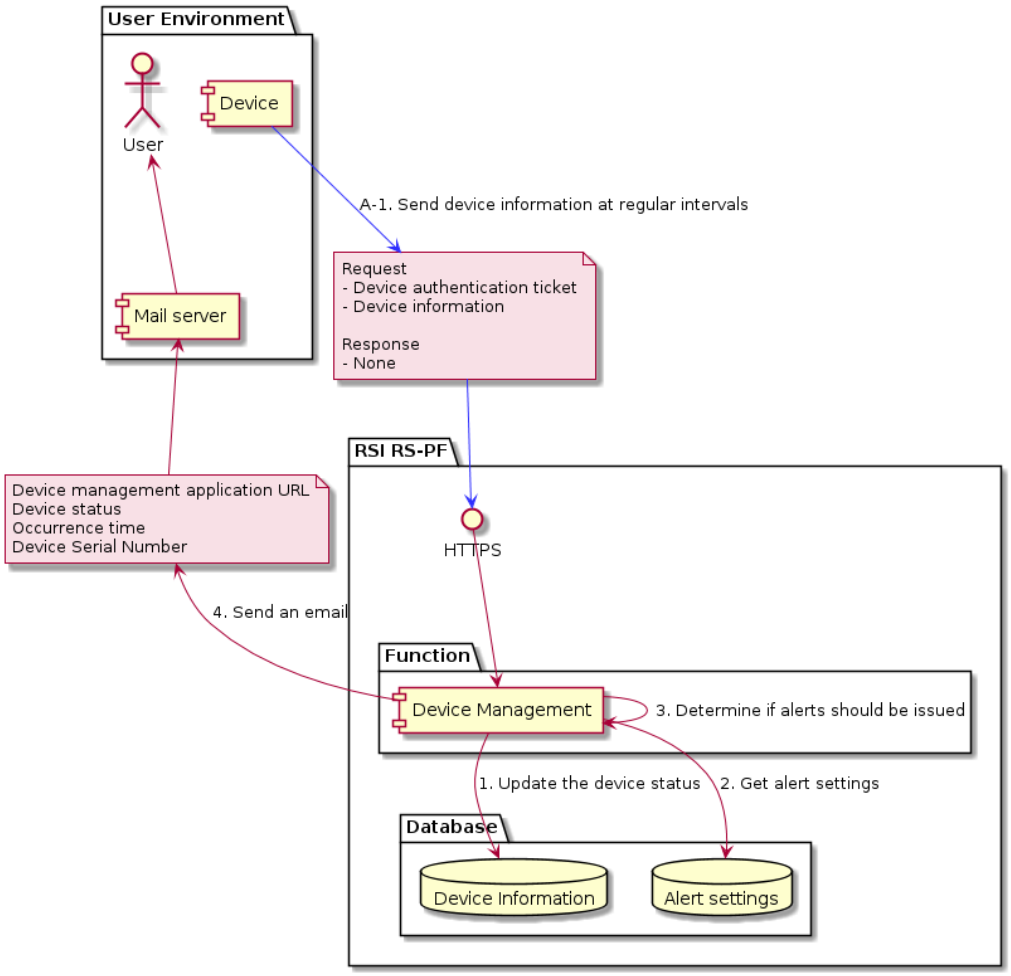

Figure 20 Data flow of receiving e-mail notifications of device malfunctions

After the device is registered in the procedure described in 2.3.2.1 the RSI device monitoring application sends the device information (see device information in Table 5) to the RSI Remote Service-PF periodically (A-1).

Upon receiving the device information, Remote Service-PF will store the device information in the device information DB (1). It checks the device status, alert settings (ON/OFF, destination), and current alert status to determine whether an alert mail should be sent out (2, 3). If it is determined that an alert mail should be sent, an alert mail is sent to the end user via a mail server (4).

2.3.2.6 Set the email address to be notified when the report has been created.

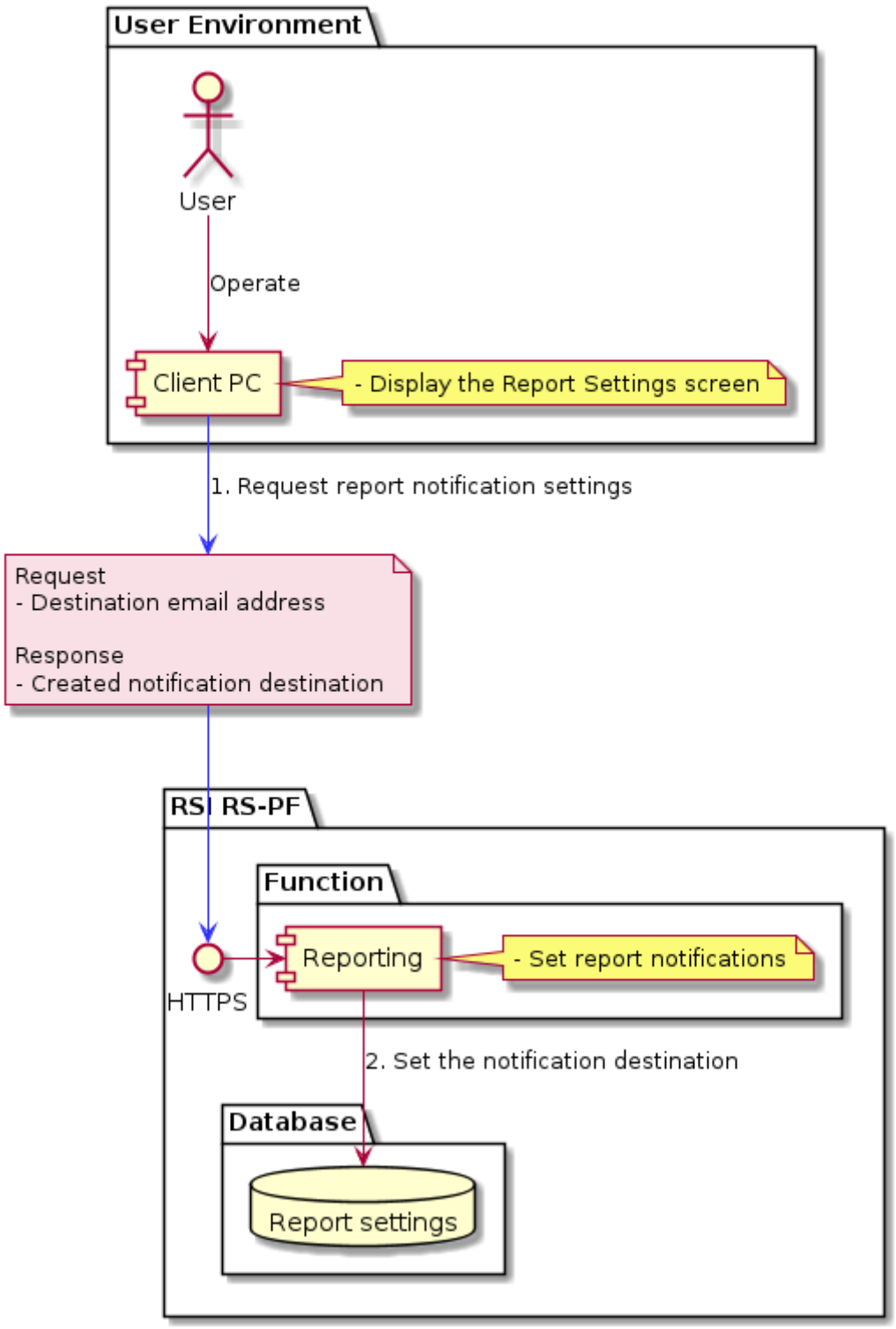

Figure 21 Data flow of set the email address to be notified when the report has been created.

The end user accesses the common setting site with the client PC, and after performing RSI authentication

according to the procedure described in 2.3.1.1 or 2.3.1.5, opens the E-mail Notification Destination Setting screen of the device management and requests the destination setting (1). RSI Remote Service-PF saves the received destination settings in the database (2).

2.3.2.7 Receive an email notifying the report creation is complete

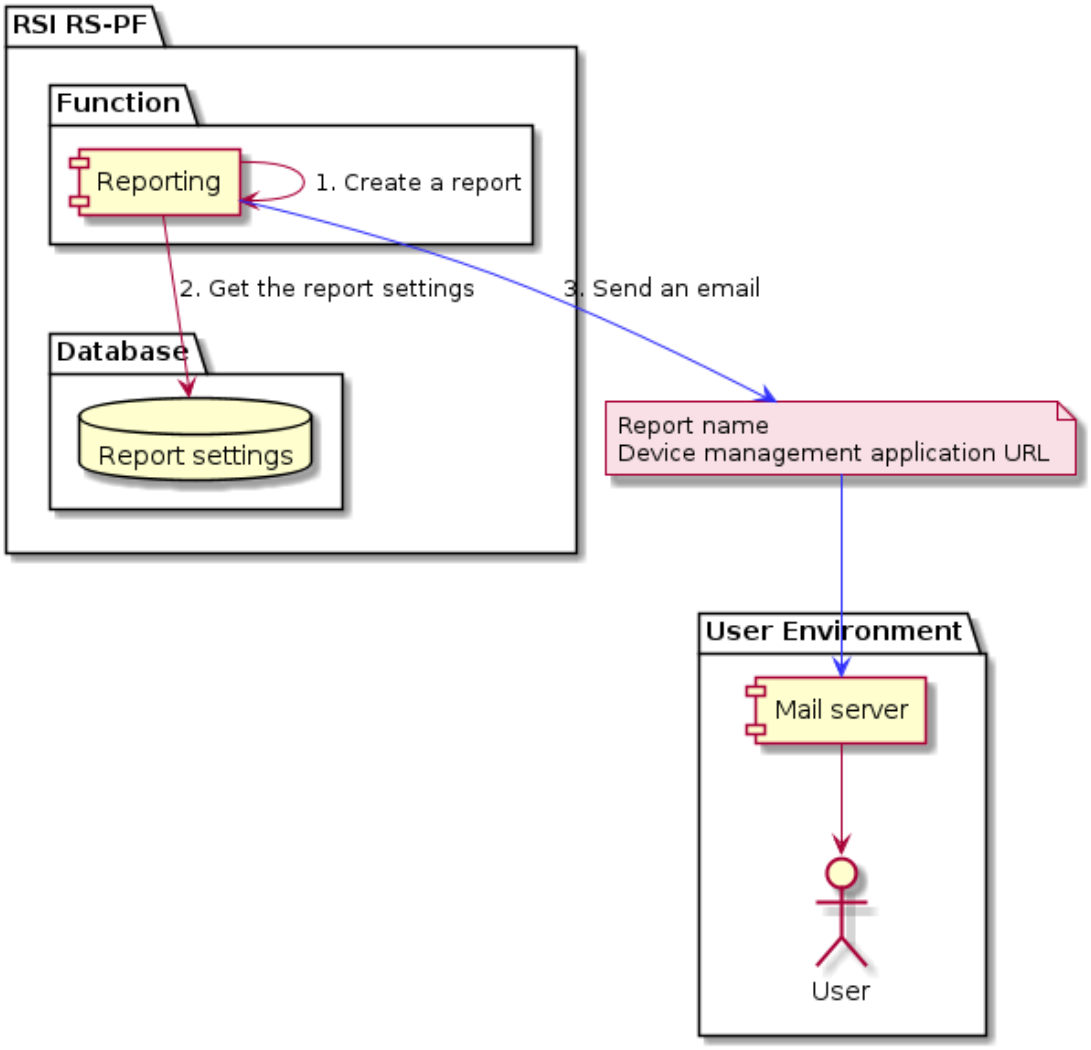

Figure 22 Data flow of receive an email notifying the report creation is complete

Upon detecting the completion of report creation, Remote Service-PF will check the report settings and determine whether a notification mail should be sent out (2). If it is determined that a notification mail should be sent out, the mail will be sent to the end user via the mail server (3).

2.3.2.8 Set the billing code

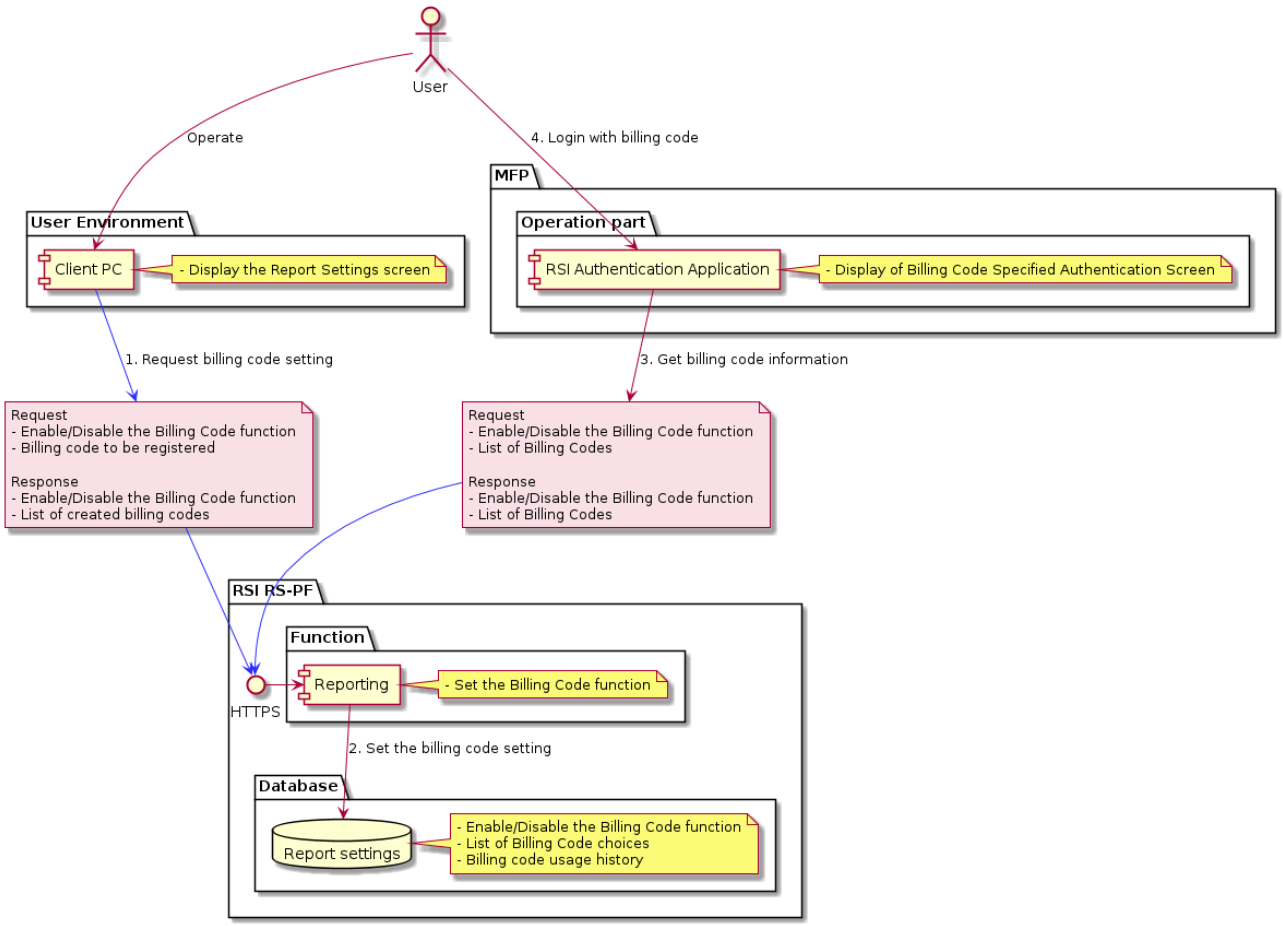

Figure 23 Data flow of set the billing code

The end user accesses the common configuration site with a client PC, and after performing RSI authentication according to the procedure in 2.3.1.1 or 2.3.1.5, opens the report configuration screen of the device management and requests the billing code setting (1). RSI Remote Service-PF stores the received billing code setting in the database (2).

When the end user logs in the mainframe at the MFD, the RSI authentication application obtains the above billing code setting (3) and displays the authentication screen for specifying the billing code, so the end user specifies the billing code and logs in the mainframe (4).

2.3.2.9 Configure guest login

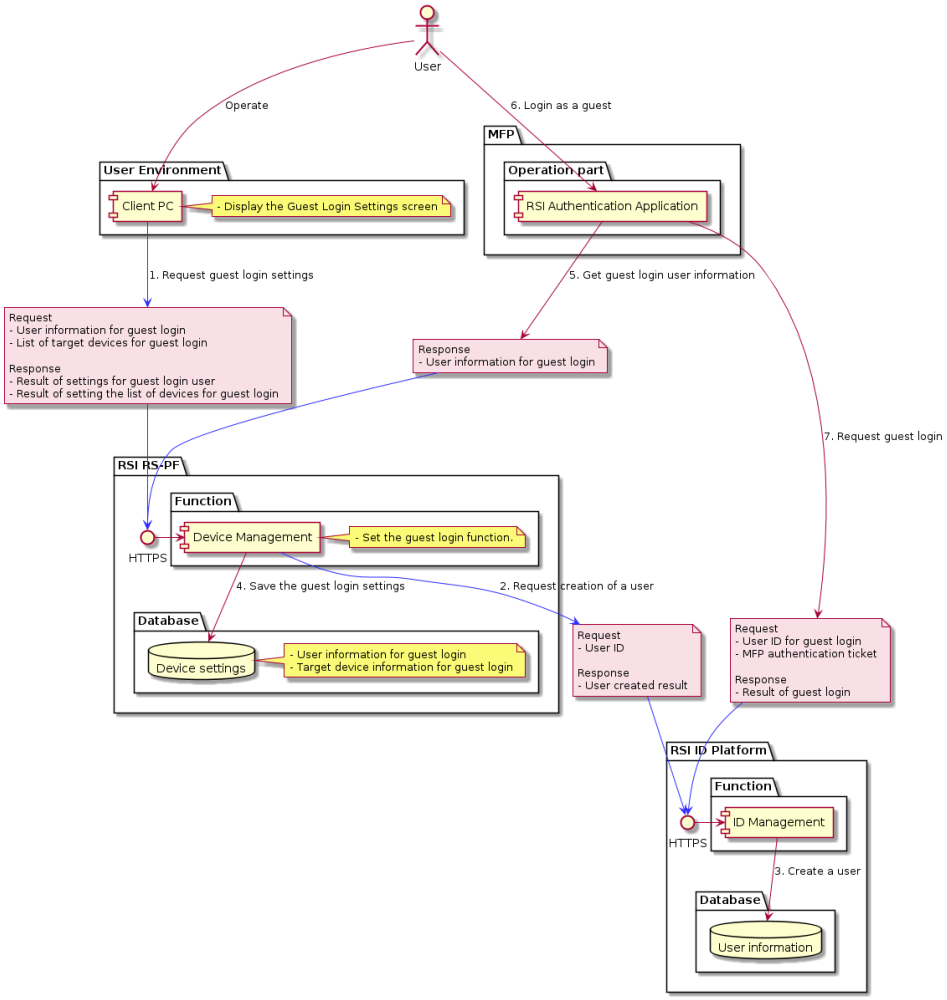

Figure 24 Data flow of configure guest login

The end user accesses the common setting site with a client PC, and after performing RSI authentication according to the procedure described in 2.3.1.1 or 2.3.1.5, opens the guest login setting screen of the device management and requests the guest login setting (1). RSI Remote Service-PF requests user creation against RSI common PF ID management (2), and save the created user name and the device information for guest login in the database (3).

When the end user logs in the mainframe with the MFD, the RSI authentication application obtains the above Guest Login setting information (5) and displays the authentication screen, so the end user logs in the mainframe as a guest (6, 7).

(Note) Guest login is not possible in tenants other than those in which the MFD is registered.

2.3.2.10 Change the settings of the device

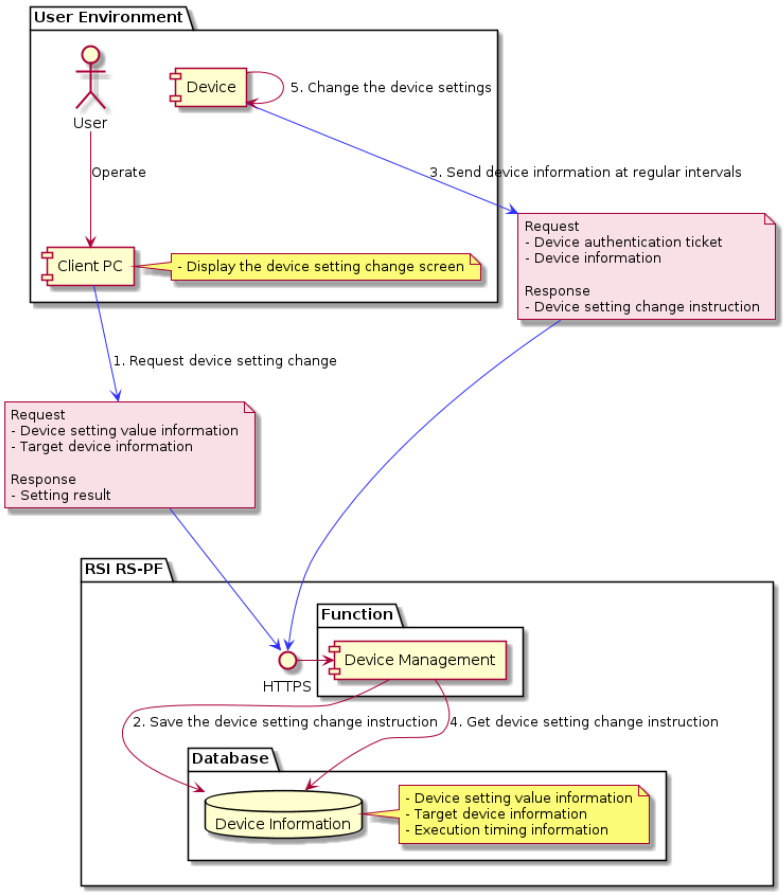

Figure 25 Data flow of change the settings of the device

The end user accesses the common setting site with a client PC, and after performing RSI authentication according to the procedure described in 2.3.1.1 or 2.3.1.5, opens the device setting change screen of the device management and requests a device setting change (1). RSI Remote Service-PF saves the received device setting change information in the database (2).

After the device is registered according to the procedure described in 2.3.2.1, the RSI device monitoring application will periodically send the device information (see device information in Table 5) to RSI Remote Service - PF (3). The Remote Service-PF that receives the device information will acquire the device setting change instruction information from the database (4). The device that receives the device setting change instruction will change the device settings (5).

2.3.2.11 Receive an email notifying of the completion of a task

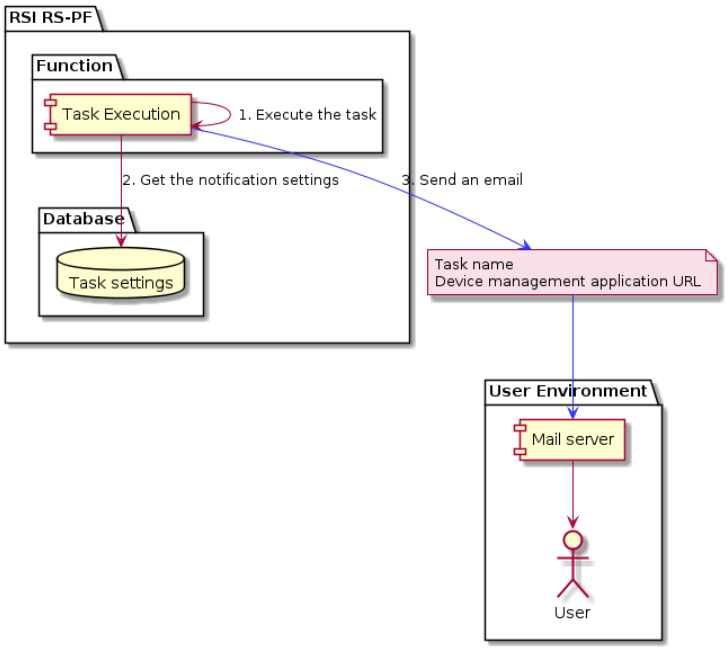

Figure 26 Data flow of receive an email notifying of the completion of a task

Upon detecting the completion of a task, Remote Service-PF will check the task information and determine whether a notification e-mail should be sent out (2). If it is determined that a notification mail should be sent out, it will send the mail to the end user via the mail server (3).

2.3.2.12 Administrators manage users and tenant information from PC

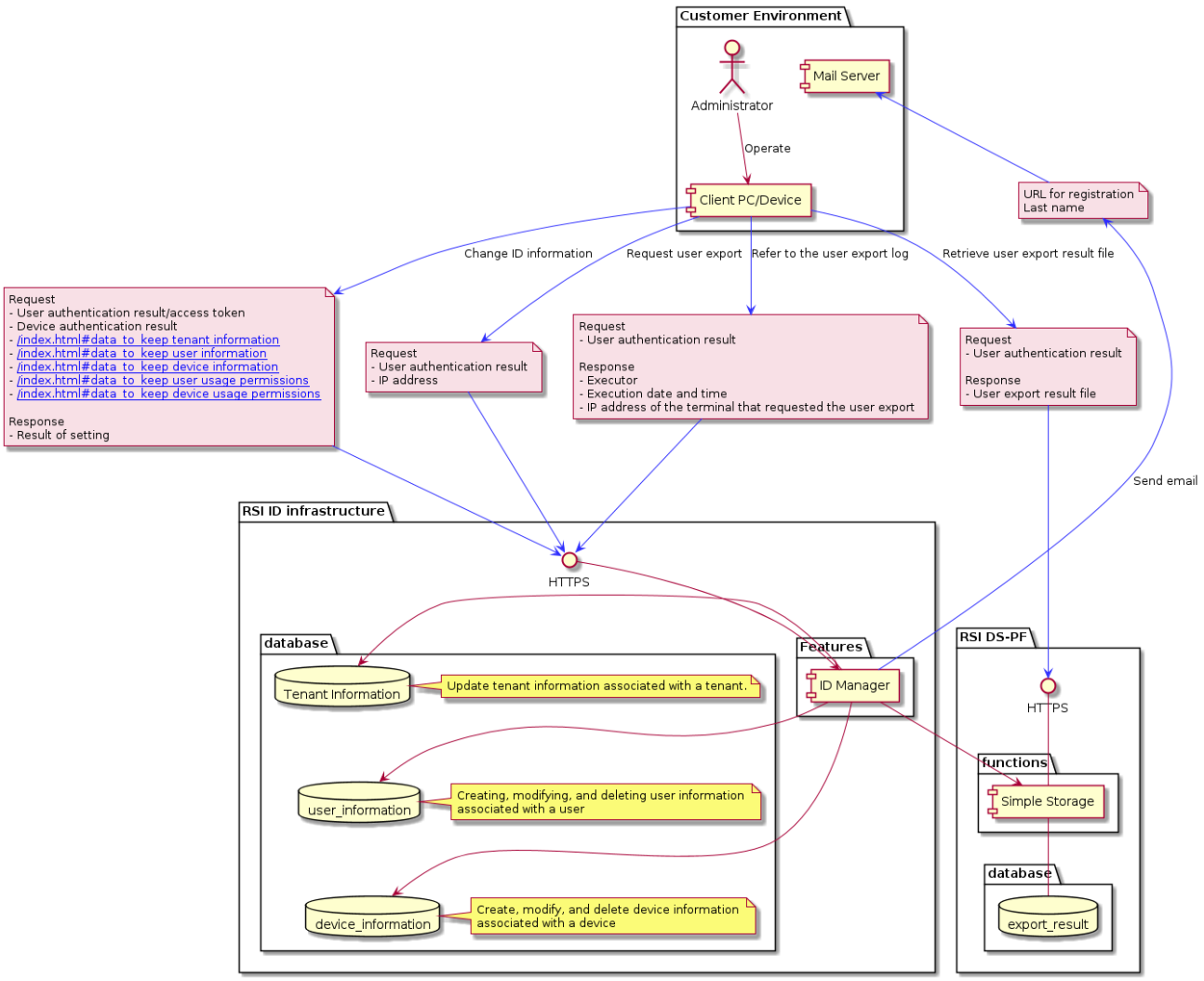

Figure 27 Data flow of administrators manage users and tenant information from PC

Administrator can manage ID information in tenant

The ID information is as follows.

- Tenant information
- User information
- Device information

When changing the ID information, the administrator operates the client PC / device to request the ID information to be changed. (1)

Update the information of the corresponding database on the ID base of the requested RSI.(2)

Based on the information entered by the administrator and the information obtained from the device, ID

information and usage authority are set in the RSI ID base.

In addition, when an administrator registers a user or changes an e-mail address, an e-mail is sent to the e-mail address of the registered user.(3)

The user who receives the email needs to complete the process by accessing the URL in the email body and entering the necessary information.

Since the URL of the email body has the following specifications, it is unlikely to be abused even if the URL is leaked.

For the URL in the body of the mail, refer to 5.4Sending Mail.

When exporting the user information, the administrator operates the client PC/device, passes the authentication result and the IP address information of the requesting terminal, and requests the export, and saves the export result in the DS-PF simple storage from the ID management. To retrieve the exported result file, pass the authentication result and retrieve it from the DS-PF simple storage. When referring to the log of the export, it is possible to retrieve it from the ID management and refer to the executor, execution date and time, and IP address of the terminal that requested it stored in the database.

2.3.2.13 Manage personal information

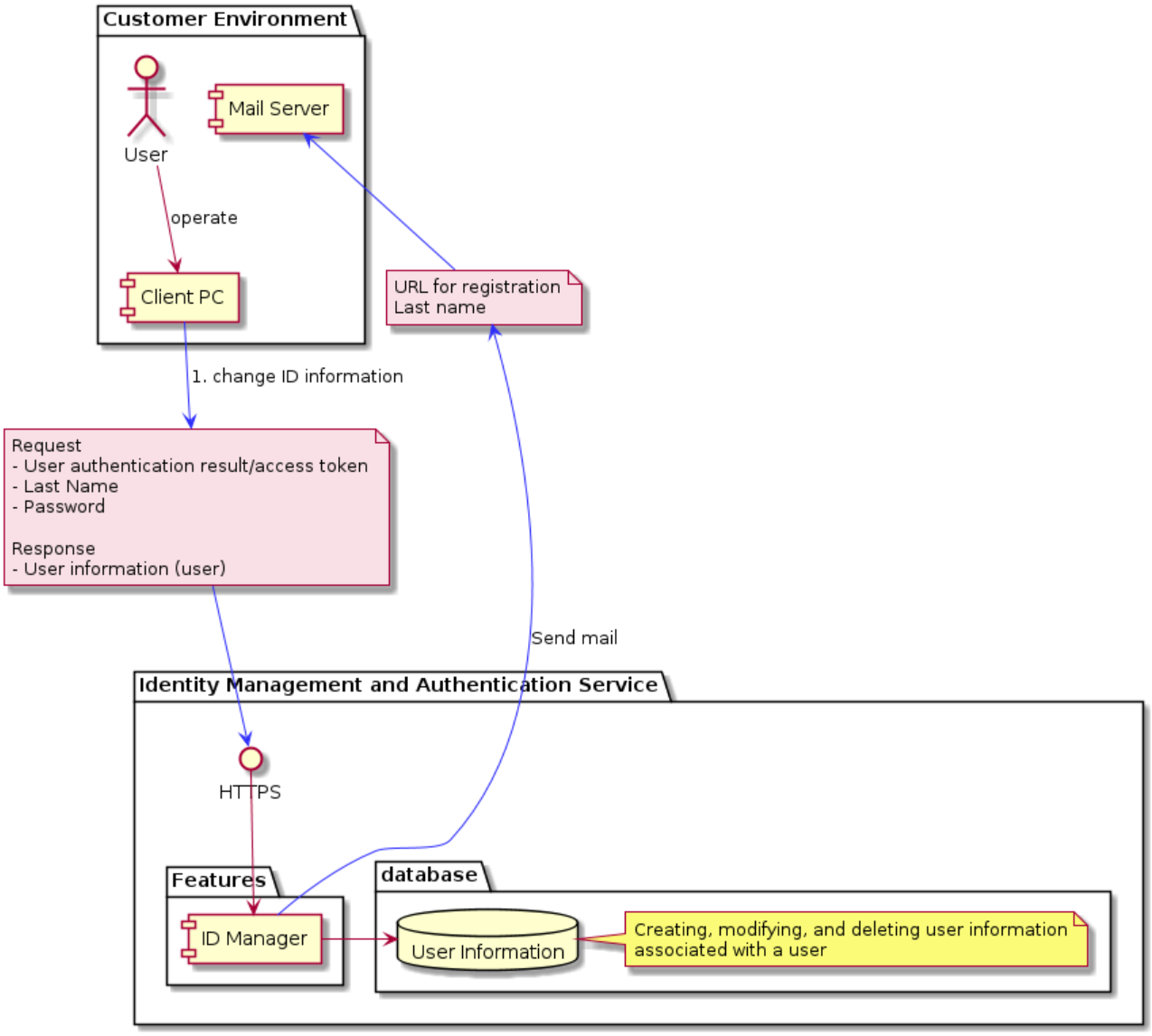

Figure 28 Data flow of manage personal information

General users can change their own information or reset their password. When a change in ID information is requested from a client PC, ID management will return the user information in the database as a response. Also, when a password reset is performed, the ID Manager will send an e-mail with a URL for registration.
For more information about sending e-mails, please refer to 5.4 Sending e-mails.

2.4. Communication Protocols

This section describes the various secure communication methods across the Integrated Solution Strategy platform.

2.4.1. Communication from customer environment to RSI

Table 1 Communication from the customer environment to RSI-Cloud

Function	Destination Host	Port	Protocol
Connection/Authentication from PC to RSI-Cloud	www.na.smart-integration.ricoh.com api.na.smart-integration.ricoh.com www.eu.smart-integration.ricoh.com api.eu.smart-integration.ricoh.com www.jp.smart-integration.ricoh.com api.jp.smart-integration.ricoh.com na.accounts.ricoh.com eu.accounts.ricoh.com jp.accounts.ricoh.com na.smart-integration.status.ricoh.com eu.smart-integration.status.ricoh.com jp.smart-integration.status.ricoh.com asset.dm.na.smart-integration.ricoh.com asset.dm.eu.smart-integration.ricoh.com asset.dm.jp.smart-integration.ricoh.com	443/TCP	HTTPS TLS1.2
(same as above)	static.na.smart-integration.ricoh.com static.eu.smart-integration.ricoh.com static.jp.smart-integration.ricoh.com help-eu.eu.smart-integration.ricoh.com help-us.na.smart-integration.ricoh.com help-ra.na.smart-integration.ricoh.com help-rkr.na.smart-integration.ricoh.com	443/TCP	HTTPS TLS1.2 TLS1.3
Device registration	www.na.smart-integration.ricoh.com api.na.smart-integration.ricoh.com www.eu.smart-integration.ricoh.com api.eu.smart-integration.ricoh.com www.jp.smart-integration.ricoh.com api.jp.smart-integration.ricoh.com na.accounts.ricoh.com eu.accounts.ricoh.com jp.accounts.ricoh.com na.smart-integration.status.ricoh.com eu.smart-integration.status.ricoh.com jp.smart-integration.status.ricoh.com	443/TCP	HTTPS

Document upload onto Pull Print	www.start.ricoh.com eu.start.ricoh.com jp.start.ricoh.com	443/TCP	HTTPS
Document download to print	www.na.smart-integration.ricoh.com api.na.smart-integration.ricoh.com www.eu.smart-integration.ricoh.com api.eu.smart-integration.ricoh.com www.jp.smart-integration.ricoh.com api.jp.smart-integration.ricoh.com	443/TCP	HTTPS
Scanned document upload	www.na.smart-integration.ricoh.com api.na.smart-integration.ricoh.com www.eu.smart-integration.ricoh.com api.eu.smart-integration.ricoh.com www.jp.smart-integration.ricoh.com api.jp.smart-integration.ricoh.com	443/TCP	HTTPS
Uploading printed documents (location-free printing)	www.start.ricoh.com eu.start.ricoh.com jp.start.ricoh.com	443/TCP	HTTPS
Connection to RSI-Cloud (MFD)	www.na.smart-integration.ricoh.com api.na.smart-integration.ricoh.com www.eu.smart-integration.ricoh.com api.eu.smart-integration.ricoh.com www.jp.smart-integration.ricoh.com api.jp.smart-integration.ricoh.com custom-ui.na.smart-integration.ricoh.com custom-ui.eu.smart-integration.ricoh.com custom-ui.jp.smart-integration.ricoh.com edge-api.dm.na.smart-integration.ricoh.com edge-api.dm.eu.smart-integration.ricoh.com edge-api.dm.jp.smart-integration.ricoh.com	443/TCP	HTTPS

*EMEA uses ”eu” site, and Americas, Asia Pacific, Japan use “na” site.

2.4.2 Communication from customer environment to non-RSI

Table 2 Communication from the customer environment to non-RSI-Cloud

Purpose	Destination Host	Port	Protocol
Storing data on NewRelic to improve the user experience	bam.nr-data.net js-agent.newrelic.com	443/TCP	HTTPS TLS1.2, TLS1.1,TLS1.0(1.1,1.0

			To be decommissioned)
Data storage in Google Analytics to improve user experience	www.googletagmanager.com www.google-analytics.com	443/TCP	Undocumented on official website - How Google Analytics secures your web traffic * https://support.google.com/analytics/answer/6385009
Help function of MFD (support settings)	sa.gateway.ricoh.jp	443/TCP	TLS 1.0, TLS 1.1, TLS 1.2
Microsoft365 login usage	login.microsoftonline.com	443/TCP 80/TCP	HTTP, HTTPS (Based on following Microsoft specifications - Technical reference details about encryption, * https://learn.microsoft.com/en-us/microsoft-365/compliance/technical-reference-details-about-encryption?view=o365-worldwide#tls-cipher-suites-supported-by-office-365 - Preparing for TLS 1.2 in Office 365 and Office 365 GCC * https://learn.microsoft.com/en-us/microsoft-365/compliance/prepare-tls-1.2-in-office-
Get preview data for workflow applications integrated with OneDrive for Business / SharePoint Online	*.sharepoint.com 13.107.136.0/22 40.108.128.0/17 52.104.0.0/14 104.146.128.0/17 150.171.40.0/22 2603:1061:1300::/40 2620:1ec:8f8::/46 2620:1ec:908::/46 2a01:111:f402::/48 ssw.live.com, storage.live.com *.search.production.apac.trafficmanager.net *.search.production.emea.trafficmanager.net *.search.production.us.trafficmanager.net *.wns.windows.com admin.onedrive.com officeclient.microsoft.com g.live.com, oneclient.sfx.ms *.sharepointonline.com spoprod-a.akamaihd.net	443/TCP 80/TCP	

	*.svc.ms Note: For the latest information, please refer to the Microsoft web page. - SharePoint Online and OneDrive for Business *https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?redirectSourcePath=%252fja-jp%252farticle%252f-8548a211-3fe7-47cb-abb1-355ea5aa88a2&view=o365-worldwide#sharepoint-online-and-onedrive-for-business		365?view=o365-worldwide) Note: Whether or not HTTP (80/TCP) is used depends on the URL specified by the Microsoft services.
Get preview data for workflow applications integrated with OneDrive	onedrive.com *.onedrive.com onedrive.live.com login.live.com g.live.com spoprod-a.akamaihd.net *.mesh.com p.sfx.ms oneclient.sfx.ms *.microsoft.com fabric.io *.crashlytics.com vortex.data.microsoft.com posarprodcssservice.accesscontrol.windows.net redemptionservices.accesscontrol.windows.net token.cp.microsoft.com/ tokensit.cp.microsoft-tst.com/ *.office.com *.officeapps.live.com *.aria.microsoft.com	443/TCP 80/TCP	

	*.mobileengagement.windows.net *.branch.io *.adjust.com *.servicebus.windows.net vas.samsungapps.com odc.officeapps.live.com login.windows.net login.microsoftonline.com *.files.1drv.com *.onedrive.live.com *.*.onedrive.live.com storage.live.com *.storage.live.com *.*.storage.live.com *.groups.office.live.com *.groups.photos.live.com *.groups.skydrive.live.com favorites.live.com oauth.live.com photos.live.com skydrive.live.com api.live.net apis.live.net docs.live.net *.docs.live.net policies.live.net *.policies.live.net settings.live.net *.settings.live.net skyapi.live.net snapi.live.net *.livefilestore.com *.*.livefilestore.com storage.msn.com *.storage.msn.com *.*.storage.msn.com Note: For the latest information,		

	please refer to the Microsoft web page. - Supported hosts and ports for OneDrive. *https://learn.microsoft.com/EN-US/sharepoint/required-urls-and-ports#supported-hosts-and-ports-for-onedrive		
Executing on-premise workflow using SMB	Host specified by end user	137/UDP, 138/UDP, 139/TCP, 445/TCP	SMB 1.0, SMB 2.02, SMB 2.10, SMB 3.00, SMB 3.1.1
Executing on-premise workflow using SFTP	Host specified by end user	Ports specified by end user	SFTP
Executing on-premise workflow using FTP	Host specified by end user	Ports specified by end user	FTP

Note: The descriptions in this document refer only communications performed by components provided by Ricoh. Communications performed provided by regions and partners are not shown in this document.
Note: Communications performed by Smart Operation Panel and Application site for Smart Operation Panel are not described in this document. For more derails refer to respective security design guide.

2.4.3 Communication from RSI to an internet environment

Specifications of external service linkage follows the external service's specifications. Generally, HTTPS is used for communication. If the destination service does not support HTTPS, HTTP (80/TCP) is used instead.
NTP (123/UDP), DNS (53/TCP, 53/UDP) and SMTP (25/TCP) are also used for communication.

2.5 Multi-Tenant Support

RSI provides services for various companies and organizations. The term "tenants"[1] is used for companies and organizations to which services are provided, and one hardware manages the information for multiple tenants. The data on the system is logically separated among tenants to maintain independence from each other[2]. See Section 4.1 for the details about data accesses.

The tenant types are customer tenants and region tenants.
In the case of a customer tenant, the end users use applications on RSI but cannot reference the information of other tenants.
In the case of a region tenant, operations such as WF application development, package creation and opening new customer tenants are performed. The tenant information and license information can be referenced, and new licenses can be issued for opened customer tenants.

[1] The term "tenant" is used instead of "company" because, in some cases, a “tenant” may be licensed to multiple companies.
[2] This type of system architecture is called a "multi-tenant architecture".

3 General System Security Measures

Use this chapter as a reference for monitoring platform operations, vulnerability information and assessments, patch applications, and logs.

3.1 Operation Monitoring, Error Monitoring and Performance Monitoring

The status and performance of network, servers, applications, and other operations are monitored for 24 hours a day, 365 days a year that makes it possible to handle errors quickly if they occur. Capacity is also managed[3] to ensure sufficient system availability.

3.2 Periodic collection of vulnerability information and patch applications

Collection and handling of vulnerability information are operated by following the Ricoh's process rules. Security patches for OS and middleware, etc. are planned and applied to the production environment after examining their importance and impact on the system and also after testing them in the development environment.

Vuls is also used to automatically detect vulnerabilities in packages running on each server. In addition, JVNDB is used to confirm the vulnerability information about the running package. In this way, the influence on the service and the need of improvement are investigated and managed for each package

[3] Sufficient storage resources are allocated by calculating the expected total volume of tenants, users, devices, licenses, and jobs. The actual usage is also monitored.

3.3 Vulnerability Assessment

Using IBM's AppScan as a vulnerability scanner to assess web applications, following items are checked once every three months to ensure that every known vulnerability is detected.

Table 2 List of vulnerability diagnostics by AppScan

Test Category	Test Items
Authentication	・Brute force attack ・Improper authentication
Authorization	・Indexing/session guessing ・Session fixation ・Insufficient session expiration ・Improper permission
Applications	・Privacy test ・Quality test
Client-side attacks	・Cross-site scripting ・Content spoofing
Command execution	・LDAP injection ・OS command ・SQL injection ・SSL injection ・XPath injection ・Buffer overflow ・Format string attack
Information disclosure	・Directory indexing ・Path traversal ・Information omission ・Disclosure of inferable resources
Logical attacks	・Denial of service attack ・Abuse of functionality

Furthermore, Ricoh (IT/S department) runs rapid7's InsightVM once every one month as a vulnerability scanner to assess web applications, confirming that no known vulnerabilities left in the product.

Examples of the items InsightVM assesses are as follows.

Table 3 List of vulnerability diagnostics by InsightVM

Test Category	Test Items
General vulnerabilities in external services	・Search for SSL server information ・Information of SSL session caching ・Consistency of SSL Certificate Common Name ・Allowance of unauthorized SSL/TLS protocol versions ・Support for TLS_FALLBACK_SCSV of SSL/TLS servers ・Support information for safe renegotiation extension of TLS ・Block size in TLS encryption
Web server vulnerabilities	・Web server/SSL Web server versions ・SSL certificate information ・Web directory list ・Support for HTTP request pipelining by Web server ・HTTP protocol version of Web server ・Vulnerabilities of internal IP address/internal network name disclosure ・Presence of autocomplete attributes in form-based authentication
TCP/IP vulnerabilities	・List of public TCP services (port scan) ・Randomness of TCP initial sequence number ・Randomness of IP header ID value ・Estimated uptime based on TCP Timestamp option ・Availability of ICMP Timestamp request
Vulnerabilities of programs running on Web server	・Display of standard Web pages ・Presence of HTTP security header
Email service vulnerabilities	・SMTP banners ・Detection of SMTP services
Firewall	・Presence of firewall

3.4 Logs

Use this chapter as a reference for system, server, and application log security details.

3.4.1. General Matters/Common

The application logs from RSI DS-PF and RSI Cloud Core servers are collected together so that unauthorized access and system failures can be analyzed at the same time. RSI RS-PF server also collects application logs for unauthorized access and system failure analysis. Together with system logs in each server, these logs are backed up regularly. The time setting of every server is synchronized with NTP. The log retention period shall be five years. The output information does not output passwords or other confidential information.

3.4.2. Workflow app (in BrowserNX on operation panel)

Workflow app sends print/scan job settings and execution results to the app server.

Workflow app that works in the operation unit BrowserNX. If an error occurs during events like initialization or during printing/scanning, Workflow app sends the error log to the device (MFD) as the log of BrowserNX.

3.4.3. Workflow app (in server application)

The app server stores the application logs and all job logs for the jobs it has run in the server (such as the folder acquisition of the print, delivery, and storage services). These logs contain the following information: date and time of job execution, tenant ID, user ID, app name, job status, communication results with external services, and result of intermediate processing. For the jobs with printing and delivery applications, document names and print/scan settings are also included. Print/scan settings also includes Folder ID and email address to be used for failure analysis.

This log information can be used for appropriate server access restrictions in order to prevent unauthorized accesses from inside and outside of the company (see Section 4.1.2).

3.4.4. Port Monitor for Pull Print

The Pull Print port monitor stores the installation log and print logs in the PC in which Pull Print is installed. These logs include the following information: PC login user name, PC name, date and time of print execution, and print file name. These logs are only sent to the PC's installation folder and they are not automatically sent to RSI-Cloud.

3.4.5. RSI authentication app

The RSI authentication app outputs application logs to the device (MFD) so that these logs can be used for problem analyses. These application logs contain: operation record (i.e. screen names displayed during the operation), login type, results of communications with other services and RSI cloud (used API name, success/failure, reason of failure), and results of intermediate processes. No information about the customer or password is included in these logs. Note that the application logs are stored only in the device and not automatically sent to RSI cloud.

3.4.6. RSI Device Monitoring App

The RSI device monitoring app outputs application logs to the device (MFD) so that these logs can be used for problem analyses. These application logs contain: results of processes in the app while collecting the device information (collection start, collection end, collected names of device information items) and results of processes in app while sending the device information to the RSI cloud. The result of the transmission (success/failure, failure reason in case of failure) are stored. Stored logs do not contain the information about customer. Note that these logs are stored only in the device and they are not automatically sent to RSI cloud.

3.4.7. RSI Log Transfer App

The RSI log transmission app outputs the application logs to the device (MFD) so that these logs can be used for problem analyses. These application logs contain: log generation notification information (log ID) from MFD, results of log transmissions to RSI cloud (log ID, success/failure, and error code if transmission fails), and the results of intermediate processes in the app. Stored logs do not contain information about customers including password.

3.4.8. Remote Service Platform (RS-PF) Servers

It stores application logs and the information sent from the device (via RSI device monitoring app and RSI log transmission app). The application logs include: tenant ID, user ID, date and time of execution, results of communications with devices and other services in RSI cloud, and the results of intermediate processes. For the information that the device sends, see the chapters about the RSI device monitoring app and RSI log transmission app. For failure analysis, the application logs also include IP address and serial number of the device. The password of the RSI user and the device administrator account information are not included.
This log information can be used for appropriate server access restriction settings in order to prevent unauthorized accesses from inside and outside of the company (see Section 4.1.2).

3.4.9. RSI Automatic printing application

When a smart device associated with an RSI account is held at the control panel to log in to the MFD, the RSI Auto Print application can be designated in advance by the end user to automatically output print jobs uploaded via the port monitor. The RSI automatic printing application outputs the application log to the device (MFD) itself so that it can be analyzed in case of failure. The above application logs include the results of communication with the printing service (success/failure, reason for failure in case of failure) and the execution results of intermediate processes, and all logs do not output passwords or other customer information. The output logs are stored only in the device itself and are not automatically sent to the RSI cloud.

4 Data Security Measures

Refer to this chapter to review data security measures for Ricoh's integrated solution.

4.1 Data Access Control

Table 4 shows the data that RSI-Cloud app server and RSI cloud core server manage. These data are managed either on the user or tenant basis, and an authentication ticket issued through user authentication is required in order to access each data type. Which data type is available for the user is controlled by the authentication ticket so users will not have access to different user's print data or the user information that belongs to different companies.

The data managed by RSI-Cloud DS-PF, RSI Common PF, and Pull Print servers are stored in either Amazon RDS or Amazon S3. The direct access to the stored data from the Internet is not possible and accessing the data must be done via an endpoint in RSI-Cloud.

AWS IAM also sets permissions for accounts that can access to AWS so that it can prevent the data accesses even from inside AWS if the data is not related to the user's business needs.

Table 4 Data managed by RSI Common PF, DS-PF, and Pull Print

Personal Data Type	Data Acquisition Method	Storage Location	Accessible by *1
Name	The user or the administrator inputs the data	Data layer in Figure 29. Logs on S3	Developers
Email address	The user or the administrator inputs the data	Data layer in Figure 29. Logs on S3	Developers
Password	The user inputs the data	Data layer in Figure 29.	Hashing.
PIN code	The system automatically generates the data or the user inputs it.	Data layer in Figure 29. Logs on S3	Developers
Web browser type, version, OS	Acquired automatically when the user uses the system.	Logs on S3	Developers and S&S
IP address	Acquired automatically when the user uses the system.	Logs on S3	Developers
Date and time of use	Acquired automatically when the user accesses the system.	Data layer in Figure 29. Logs on S3	Developers and S&S
MFD serial number	The administrator or CE inputs the data.	Data layer in Figure 29.	Developers and S&S

		Logs on S3	
Scanned image file	Acquired automatically when the user uses the system.	S3	Developers *2*3
Print file	Acquired automatically when the user uses the system.	S3	Developers *3
Scan settings	Acquired automatically when the user uses the system.	Data layer Logs on S3	Developers and S&S *3
Print settings	Acquired automatically when the user uses the system.	Data layer Logs on S3	Developers and S&S *3
Job information: input parameters received during job execution.	Automatically acquired during end-user use	Data layer in Figure 29.	Developers *3
Job information: Text data output as a result of job execution	Workflow execution results	Data layer in Figure 29.	Developers *3
Access token of external service (Office 365, Box, Google, Dropbox, DocuWare)	External service issues the token.	Data layer in Figure 29.	Developers *3
Refresh token of external service (same as above)	Issued by external service	Data layer in Figure 29.	Developers *3 The data itself is also encrypted.
Account information (user ID, password, etc.) required to log in to external services	Input by end users themselves, input by administrators	Data layer in Figure 29.	Developers *3 Each external service is encrypted and stored with a different key.
License Information	The administrator or CE inputs the data.	Data layer in Figure 29. Logs on S3	Developers

*1 Ricoh checks the data only when it is inevitable, for example, to analyze a problem or to respond to an inquiry.

*2 Data may not be stored on the server, depending on the WF application settings

*3 It is technically possible to decrypt the data, however, accessing to the data is virtually impossible due to strict access restrictions.

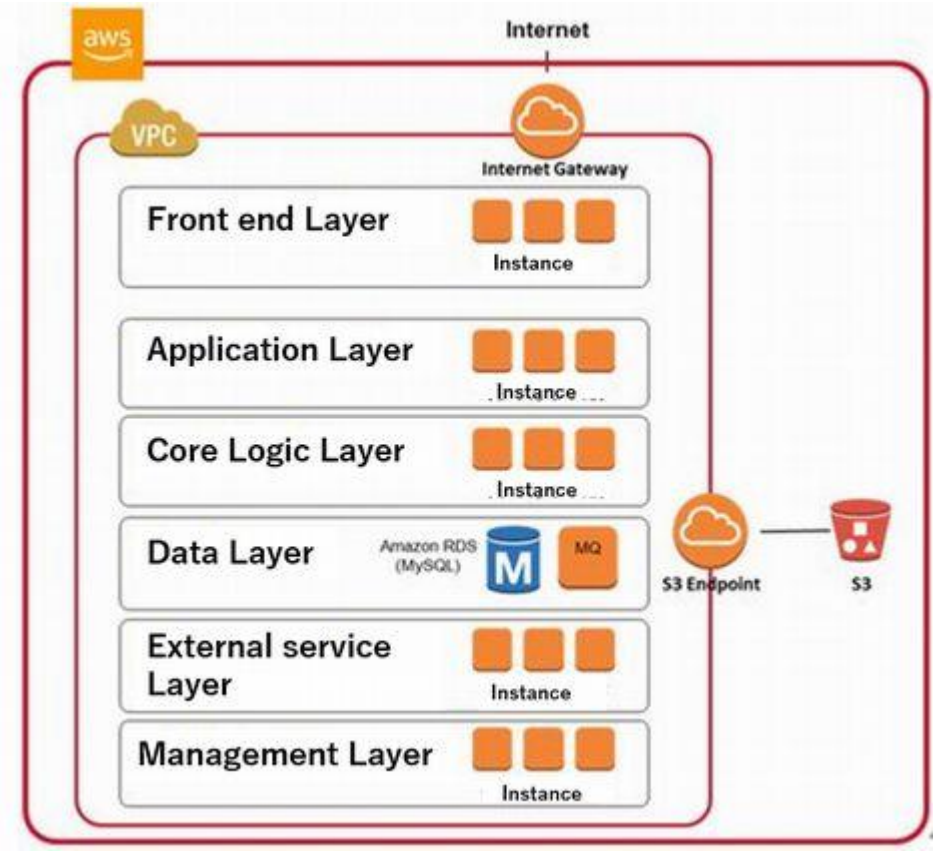

Figure 29 RSI-Cloud Infrastructure Configuration

In contrast, the data managed by the RSI-Cloud remote service server is shown in Table 5. These data are managed per tenant, and accessing each data is controlled by an authentication ticket issued during user authentication.
Because authentication ticket method is used to control which data is available to the user, the user will not have any access to the device information or reports that belong to different companies.

The data managed by the Remote Service Server is stored both in RSI-Cloud and in Amazon S3. The data in them cannot be accessed directly via Internet and the access has to be done via an endpoint in RSI-Cloud.
Further, AWS IAM gives accounts access rights for accessing AWS so that it can prevent the data accesses even from inside AWS if the data does not concern the RCL operator’s business needs.

Table 3　Data managed by Remote Services-PF

Data type	Data Acquisition Method	Accessible by
Device Info: Device Display Name	The user inputs the data. The system automatically generates the default value.	Developers *1
Device Info: Address (This means IP address)	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Manufacturer	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Product Name (MFP/LP or IWB)	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Model Name	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Serial Number	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Location	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Device version (This means ~~Farmwear~~ IWB version, this info is blank if the device is MFD)	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Agent version (This means RSI monitoring App version)	RSI device monitoring app acquires the data automatically.	Developers *1
Device Info: Device Registration Date	The system automatically generates the data.	Developers *1
Device Info: Final Update Date	The system automatically generates the default value.	Developers *1
JobLog of device (For details, please refer to the MFD JobLog specification.)	RSI log send app acquires logs automatically.	Developers *1
Schedule of Creation report	The user inputs the data.	Developers *1

Report	The system generates the data on a user request	Developers *1

4.1.1 User Authentication

Common specifications for login

To access RSI, the user must first login to the system (by user authentication) either with the tenant ID, user name, and password or with the email address and password. The subsequent operations are not allowed without succeeding the authentication.Available is a single sign-on function that uses accounts of external services.

Security measures (passwords)

Policies can be set on a tenant-by-tenant basis

- Number of characters
    - o Minimum number of characters: Can be set in the range of 6 to 128 characters
    - o Maximum number of characters: 128 characters fixed
- Character type
    - o Symbols: not required / required (minimum number of characters can be set between 1 and 3)
    - o Numbers: not required / required (minimum number of characters can be set between 1 and 3)
    - o Capital letters: Not required / Required (minimum length is fixed at 1 character)
- Reuse of used passwords
    - o Disable / Disable (The range of disabling can be set from 1 to 10 times before)
- Expiration date
    - o Do not set expiration date / Set expiration date (expiration date can be set in the range of 14 to 730 days)

Note that access restrictions can be applied for hash values and user information to prevent unauthorized access from inside and outside of the company (see section 5.1).

Other Security Issues

- Users can only change their own passwords, so they cannot be changed by others, including tenant administrators.
- Since only the hash value is stored at the center, Ricoh cannot obtain the customer's password and the password string cannot be leaked from the center.

Security measures (others)

- Resistance against brute force and dictionary attacks
    - o Sufficient resistance because the login information has a sufficient number of characters and an account lock mechanism as follows

        Tenant ID is a string of at least 10 digits

        User IDs are alphanumeric characters, hyphens (-), periods (.), and underscores (_).

    User ID is a string of at least 1 character and up to 128 characters consisting of alphanumeric

characters, hyphens (-), periods (.), and underscores (_).

E-mail address is a string of up to 128 characters.

Password is a string of characters with a set complexity according to the security measures (password).

If the password is wrong for a certain number of times in a row when logging in, the account will be locked. If the account is locked, the tenant administrator must either activate it from the user management screen, reset the password himself/herself, or wait for the system to automatically unlock it after 24 hours.

The number of times a password can be incorrectly entered before it is locked can be set by each tenant in the range of 5 to 10 times.

- Resistance to reverse brute force attacks

o Account information such as registered tenant IDs, user IDs, and email addresses are resistant to reverse brute force attacks because the access rights of the center are properly managed according to the infrastructure version, and the information is not leaked.

Login from device (MFD)

In addition to the login methods explained above, it is also possible to login with a PIN code or selecting username (with entering password). The PIN code is issued during user registration and it consists 4 to 16 digits. These login methods can only be performed on the devices registered to RSI-Cloud Core server (MFD) and are not available via client devices such as a computer. It is also possible to use IC cards or smart device logins.

To use a device, the application must be logged in as an administrator when starting the application for the first time and register the device to the center server. During user authentication, the device registered to the server checks the tenant to which the login user belongs, and the device cannot be used by a user who belongs to a different tenant. When the administrator configures the device settings, only the common tenant information can be used. In this case, functions that do not process personal information can be used without the user logging in.

Additionally, even if RSI authentication is not available like in the case where RSI-Cloud cannot be connected, for example, device functions such as copy can still be available. However, it is not possible to identify users in this case.

RSI device authentication is a mechanism for verifying that RSI is being used by Ricoh devices. RSI device authentication can be performed by combining the functions of Ricoh devices and the ID management and authentication infrastructure. The fact that the device is a Ricoh device is checked by combining the API on the device and the API of the ID management and authentication infrastructure. Only applications running on the Ricoh device can use the APIs on the device, so there is no brute force attack from PCs or servers.

Single Sign-on

RSI has a single sign-on function that is linked to an external service. Single sign-on setting can be enabled by configuring the linkage during registration or via the personal settings on the user site.

When configuring the linkage setting for the first time, RSI displays the authorization request screen to acquire the basic profile information of the account in the external service.
After authorization, single sign-on by using the account of the external service becomes available.

Single sign-on is securely processed by following the OpenID Connect standard protocol.
Furthermore, RSI management system is processed by linking the external service account and the RSI account so spoofing by other accounts can be prevented.

In OpenID Connect, the information that the customer authorized in an external service is used as the RSI login information, there is no risk of the external service password being sent to RSI.

User Selection Login

This can be used only when the setting is enabled by the tenant administrator. When this function is enabled, the users displayed in the user list can select themselves from the list. The Login screen is displayed with the user name already entered, which lessens the work when logging in. When the workflow application to be used is a scan application, user selection can also be used to skip entering the password from the next login. In the case of print applications, password entry cannot be skipped. The password must be entered every time.

4.1.2 Access Control Between Roles and Tenants

Every RSI-Cloud user belongs to one tenant only, and there is no privileged user who can access to more than one tenant.

There two types of roles regarding the users that belong to a customer tenant: administrator role and user role. Each tenant must have at least one user with the administrator role (the administrator).
The administrator can add, change or delete users in the tenant as well as having the right to configure applications and to view the job logs (Workflow Job Transaction) of all users.

The five roles for users available for region tenants are the administrator role, user role, developer role, product designer role and setup user role.
The developer role can develop WF applications by using the WF application development tools.
The product designer role can create product packages from the WF applications developed by the developer.
The setup user role can open new customer tenants and assign package licenses to customer tenants.

4.1.3 Use of Devices

Before registering a device or using a WF application, the system checks if the device is a Ricoh product. Therefore, registering devices or using WF applications is not possible with devices of another company (i.e. non-Ricoh machines).

4.1.4 Storage Service Coordination

To use an external storage service, user ID has to be linked with the external storage service before operation because the methods to manage user ID are different between RSI and external services. The user can set the linkage to the service from the personal settings screen on the user site. The service linkage settings are managed based on the user unit, so these settings cannot be viewed by other users. Moreover, there is no interface that allows to extract the authentication information required for the linkage so the information is used only within the system.

4.1.5 Workflow App

- Using Workflow App
  - WF applications can only be accessed by the users who belong to the tenants the application is installed to.
- Using Workflow
  - For the parameters that can be customized per tenant in the workflow, the access permission for each tenant is checked therefore the information cannot be viewed by users of other tenants.
  - When an external cloud service is used in the workflow, credentials such as OAuth[7] tokens are not managed in the workflow but are managed by the authentication service in the same method as the Ricoh's standard applications are managed. Additionally, access credentials are not granted for users who do not have permission.
  - The detailed information about the result of executing a workflow (such as output files) can only be viewed by the user who executed the workflow.
  - All the results of workflow's intermediate processes are deleted when the workflow is completed unless otherwise it is specified. The final process results are also deleted automatically after the storage period specified when executing the workflow has been passed. (The maximum storage period is 72 hours.)
- Editing workflows
  - The editable workflows are limited to the flows that were developed by the corresponding tenant. Workflows developed by other tenants cannot be accessed.

4.2 Data Management

Refer to this chapter to review data security measures for Ricoh’s integrated solution.

4.2.1 Device (MFD)

To register a device in the center server, the tenant ID that was issued when closing the contract, the administrator’s user name and password registered to the tenant ID have to be entered. The tenant ID information is stored in the device, but the administrator's user name and password are not stored in the device.

4.2.2 Delivered Data

Document data scanned on the device (MFD) are stored temporarily in the center server. The data is encrypted and stored inside the AWS firewall, and the access to the storage is allowed only from the inside of the system or from the Ricoh internal LAN. For these reasons, no data can be leaked because there is no means to access the data from external systems.
Temporary file storage is also encrypted, and the encryption key is managed on a separate server to restrict access so that the contents cannot be referred.

4.2.3 Storage Service Linkage

With the storage service that supports the authorization function via OAuth 2.0, this authentication method is basically used to link the services (the proxy authentication method is not used). Tokens stored in the RSI center server do not include password information, therefore security risk is low. Additionally, even if the password in the storage service is changed, there is no need to update the password in RSI.

Due to constraints of the API provided by the storage service or on-premise server (SMB/FTP/SFTP, etc.), the ID and password of the external service are encrypted and stored on the RSI center server, and when service coordination is performed for the storage of documents scanned by the device (MFP), sometimes a method is used where the system logs in by proxy (called a proxy authentication method). If the password in the storage service is changed, the password stored in RSI must also be changed.

4.2.4 Job Log data

Job log data sent from the device (MFD) is stored in the RSI-Cloud remote service server, and the data will not be leaked because there are two reasons why the user does not have means to access from outside of the system: 1) the storage is inside the AWS firewall, and 2) the access to the storage is limited to from the inside of the system or from RICOH internal LAN. Although the database that stores job log data is not encrypted, unauthorized access from inside and outside the company are prevented by appropriate access restrictions on data access (see Section 4.1).

4.3 Data Deletion

Refer to this section to review security measures for RSI data deletions for services and job logs.

4.3.1 Print Data

Uploaded document data for print are deleted as follows: after the device downloads the data when the setting is to delete it after printing, or 72 hours after uploading the data when the setting is not to delete the data.
The same applies to files generated in the format conversion process.

4.3.2 Delivered Data

Document data scanned by the device (MFD) are deleted from the center server after they are sent to the storage service. The same applies to intermediate files generated during OCR processes.

4.3.3 JobLog Data

Job log data sent from the device (MFD) is stored in RSI-Cloud remote service if the data is from a license-enabled device, and the data is immediately discarded if it is received from an invalid device. ~~Once saved, job log data is basically not deleted.~~
Job logs will be automatically deleted after 375 days (365 days plus 10 days) of receiving the job log on the cloud side.[4]

Additionally, job log data from the device (MFD) is deleted after being successfully uploaded to the RSI-Cloud remote service. The log data remains in the device if the upload fails. The failed data is uploaded again with the next job log data and is deleted if the upload is a success and stays in the device if it fails again.

Note that logs remained in the device are deleted by uninstalling the log sending app.

[4] Tenant information other than system logs and other logs will be deleted in response to an explicit deletion request from the customer. Although system logs and other log information will remain, this log information does not contain confidential information such as personal information, and there are no safety issues.

4.3.4 Service or Tenant Cancellation

No data is deleted only by canceling services included in tenants.
When a tenant is cancelled, the following data are deleted from the center server.

- Tenant information
- User information linked to the tenant
- Device information linked to the tenant

The following information are not deleted even when a tenant is canceled[5].

- Workflow App setting information
- Job log information
  - Job log data of Workflow App (Workflow Job Transaction)
  - Job log data sent from device
- Reports created from job log data sent from device
- License information
- Logs such as other related system logs

4.4 Antivirus Measures

Refer to this section to review security measures for RSI antivirus software.

The periodic collection of vulnerability information and patch applications explained in 4.2 are performed and antivirus software (TrendMicro Server Protect 5) is permanently installed in every Windows server. Virus infection is prevented by performing virus checks with the latest patterns on data files in RSI. If a virus is detected, the document data is not used.

4.5 Backup

To prepare for problems such as device troubles or operation mistakes, the setting information and log data in the server are backed up periodically and the restore procedures are checked. Print data, document data scanned on the device, and converted document data that are stored in the server temporarily are deleted after the specified period of time (see 4.3 Data Deletion).

[5] Tenant information during the period of a tenant license or after canceling a tenant will be deleted when an explicit deletion request is received from the customer. Log information will remain, but this will not impair security because the log information does not contain confidential information such as personal information.

5 Network Security Measures

Refer to this section to review security measures for RSI antivirus software.

5.1 Access Control

Refer to this section to review security measures for RSI antivirus software.

5.1.1 Network Access Control

Confidential information such as passwords and document data uploaded by customers are not stored in servers that can be directly accessed via the internet. Instead, as explained in section 5.1, files are stored in Amazon S3 and other data are stored in Amazon RDS, and the storages are in locations to where only RSI AWS accounts can access. Web server is accessed from the internet via AWS Application Load Balancer so packets are filtered and direct login to the server is prevented. Additionally, a port number is set for the communication via the AWS security group (virtual firewall) to prevent unauthorized access from outside the system.

Maintenance are operated by the connection from the Ricoh internal LAN to the center server via internet line. By setting an IP address and port number in the AWS security group (virtual firewall), the access to the center server is allowed only from the Ricoh internal LAN and the communication is further restricted to the encrypted communication with a specified protocol. Maintenance cannot be operated via internet connection. Instead of password, SSH private key is used for the communication with the center server and persons who connect from Ricoh are limited to those who created the public key only. This protects customer information from leaking and being attacked during maintenance operations.

5.1.2 Server (OS) Access Control

To prevent unauthorized access from persons without permission, the accounts registered in the server are restricted to minimum, permissions are maintained every time any of the related persons is transferred, moreover, the registered member list is also reviewed every six months. A password policy has also been established to prevent using easy-to-guess account passwords.

For the data stored in the server, an appropriate access range is determined depending on the data type. Access permission is set per account or server via AWS IAM so that accessing the data outside the permitted range is not allowed. Procedures to access to the data have been established as a rule. In this rule, the data can be accessed only after obtaining the approval by following the procedures. The server administrators are trained about security in advance, and the data handling procedures are regularly informed to the administrators.

5.2 Encryption of Communication Paths

Communications between PCs (web browsers), iOS applications for RSI, devices (MFD), and the center server are all conducted over communication paths with HTTPS encryption, with the exception of email. The server certificate of the center server uses an RSA 2048-bit public key and SHA-2 thumbprint algorithm, which are issued by a third-party certificate authority. The following protocols and protocol versions are supported to be used with HTTPS.

- TLS 1.2

The above are supported based on the compatibilities with web browsers.

5.3 Receiving Emails

5.3.1 Common

Security measures for mail relay services
- Checking for viruses using the latest definition files when receiving e-mail.
- Spam filters are applied, and jobs are not executed if they are judged to be spam.
- Encrypted e-mail is not supported.

5.3.2 Executing a Workflow Application Triggered by Email Receipt

Issuing an email address with a signature that is difficult to guess
Allow users to disable existing email addresses at any time.
Disable the email address when the number of jobs executed by email exceeds the limit available in a certain time (the limit can be specified for each Workflow application)

In the case of the old configuration
Emails can be sent only from the email address of the user who belongs to the tenant where the email address for job execution was issued (only if the email address is the from address).
HTTPS is used to communicate from the relay service to RSI DS-PF, and mail information (including attachments) is safely received.

5.4 Sending Email

5.4.1 Common

Every email sent from the system uses SMTP, and the communication between the mail servers is encrypted by TLS if the receiving server can receive. SPF (Sender Policy Framework) is applied to prevent spoofing email addresses, and DKIM (Domain Keys Identified Mail) is applied as the domain authentication technology. All DNS records used for SPF and DKIM are managed in the highly secure AWS Route 53.

Product Contract Email

Sent to the user when a product is contracted. It contains the contract number, contract details, and login URL.

User Registration Email

Sent to the user when the user is registered from the Common Settings site.
Contains the tenant name, tenant ID, user ID, URL to register login information, and login URL.
The validity period is 7 days.
The URL will become invalid after the process is completed.

Email address confirmation email

Sent to the relevant user when the email address has changed. Contains the URL for email address confirmation.
Valid for 7 days.

Password reset email

Sent to the relevant user when the password is changed. Contains the URL for changing the password setting.
The validity period is 12 hours or until the password is set once.
The URL will be invalidated after the process is completed.

Notification emails for reissuing the PIN

When reissuing a PIN is requested, the system sends an email with a new PIN.

Email delivery of scanned document data

Even when the email delivery destination is inside the company, the email is always sent via the RSI center server. When delivering emails to which scanned documents are attached, a send error email may be returned to the system for reasons such as the destination email address not existing. These error emails are not stored in the system.

Sending error notification emails when delivering scanned document data

When a scanned document data is delivered to an external storage or emailed to a specified address, and if the delivery fails due to an error notification from the external storage, a timeout or exceeding the capacity for email, an error notification is emailed to the specified address.
If it fails to deliver the email for a reason that, for example, the destination email address does not exist. In such cases, the error notification is returned to the system therefore not stored.

Sending e-mails to notify device (MFD) of abnormalities

When the device status received from the device (MFD) is abnormal or warning, an email notifying the device of the abnormality is sent to the specified email notification destination. The notification e-mail contains the URL of the device management application, the device status, the time of occurrence, and the serial number of the device.

Sending an email to notify the completion of report creation

When the creation of a report by scheduled execution is completed, an email notifying the completion of report creation is sent to the specified email notification destination. The URL of the device management application and the report name are included in the notification email.

Sending an email notifying the results of task execution

When a task to change device settings or check for configuration consistency is completed by scheduled execution, an email notifying the specified email recipient of the task execution completion will be sent. The URL of the device management application and the task name will be included in the notification email.

5.5 AWS WAF

AWS WAF has been implemented as a security measure in RSI's common infrastructure and DS-PF.
The details of the WAF specifications will not be disclosed for security reasons.

6 Data Center Security Measures

The RSI server groups are built on AWS. The data center security measures comply with AWS.[6]

[6] Overview of AWS security processes: https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

7 Measures for business continuity against the failures in data center

RSI-Cloud servers are built with multiple Availability Zones on AWS. This reduces the risk of stopping services for users even if problems occur in AWS.

8 Trademarks

- Google® is a trademarks or registered trademarks of Google Inc. in the U.S. and other countries.
- iOS® is a trademark or registered trademark of Cisco in the U.S. and other countries.
- Amazon Web Services, the "Powered by Amazon Web Services" logo and other AWS trademarks used in related documents are trademarks of Amazon.com, Inc. or affiliated companies in the U.S. and other countries.
- Microsoft365® is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.