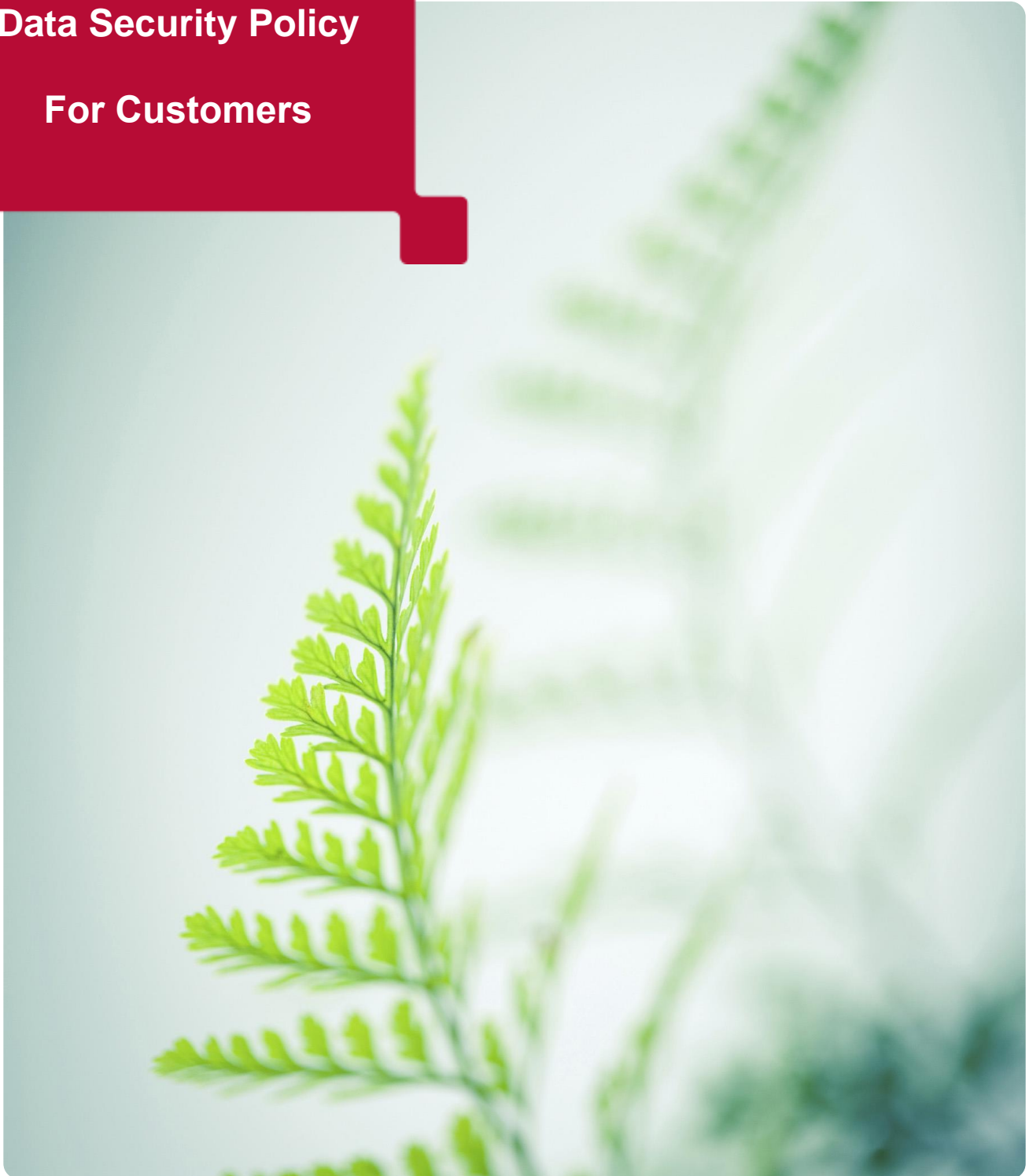


**RICOH @Remote  
Service**

**White Paper  
and  
Data Security Policy**

**For Customers**



### Revision History

Version No.	Release Date
1.00	November 7, 2017
1.01	November 24, 2017
1.1	June 30, 2020

**Copyright © 2020 Ricoh Co., Ltd. All Rights Reserved.**

[www.ricoh.com](http://www.ricoh.com)

Ricoh Co., Ltd.

<b>Table of Contents</b>	<b>Revision History</b>	<b>2</b>
<b>1 Overview</b>		<b>5</b>
1.1 About This White Paper		5
<b>2 What is RICOH @Remote?</b>		<b>6</b>
<b>3 @Remote Service Offerings</b>		<b>7</b>
3.1 @Remote Service Offerings		7
3.1.1 Automated Meter Reading		7
3.1.2 Automated Toner Notification / Order / Delivery		8
3.1.3 Automated Service Maintenance Alerts		9
3.1.4 Remote Firmware Update		10
3.1.5 Fleet Usage Reporting		11
<b>4 @Remote Service Architecture</b>		<b>12</b>
4.1 Operating Principles		12
4.2 @Remote Service System Overview		13
4.3 Remote Service Communication Activities		15
<b>5 @Remote System Security</b>		<b>16</b>
5.1 @Remote Network Communication Security		16
5.2 @Remote Authentication Security		17
5.3 Encryption Levels		17
5.4 RICOH Data Center Security		18
5.4.1 Security Specifications		18
5.4.2 Acquired certifications		19
5.5 RICOH Server Security		19
<b>6 @Remote Communications</b>		<b>20</b>
6.1 Operating Principles		20
6.2 Initiating Communication		20
6.3 Data Contents Sent by Devices		21
6.4 Data Acquisition		21
<b>7 @Remote Appliance Security</b>		<b>22</b>
7.1 Appliance Box		22
<b>8 Data Handling Policy</b>		<b>23</b>
8.1 Use of Device Data		23
8.2 Management of Device Data		23
8.3 Return of Device Information		23
8.4 Non-Disclosure of Device Information		24
<b>9 Appendix</b>		<b>25</b>
9.1 @Remote Protocols and Use of Network Ports		25
9.1.1 Use of Network Ports between Customer's Devices and RICOH Server Communications		25
9.1.2 Use of Network Ports between Customer's Devices and @Remote Appliance Communications		25
9.2 Encrypted Communication and Encryption Keys		25
9.2.1 About Public Key Encryption		25
9.2.2 About Common Key Encryption		27
9.2.3 How TLS Encrypts Communications		28
9.3 Glossary of Terms		29

## Table of Figures

<i>Figure 1: Overview of @Remote Network Monitoring Output Devices .....</i>	<i>6</i>
<i>Figure 2: @Remote Automated Meter Reading Submissions Supporting Billing.....</i>	<i>7</i>
<i>Figure 3: @Remote Automated Notifications and Alerts Supporting Continuous Operations .....</i>	<i>8</i>
<i>Figure 4: @Remote Automated Maintenance Alert Submissions Support Continuous Operations.....</i>	<i>9</i>
<i>Figure 5: @Remote Automatically Downloads and Applies Firmware Updates .....</i>	<i>10</i>
<i>Figure 6: @Remote Fleet Usage Reporting Data Flow.....</i>	<i>11</i>
<i>Figure 7: @Remote Service System Communications General Overview .....</i>	<i>13</i>
<i>Figure 8: Sample of Customer Communication Network Configuration with RICOH Server.....</i>	<i>16</i>
<i>Figure 9: @ Remote Device Authentication Security Operations.....</i>	<i>17</i>
<i>Figure 10: @ Remote System Communication Initiation Steps Operations .....</i>	<i>20</i>
<i>Figure 11: Public and Private Keys Used for Encryption and Decryption .....</i>	<i>26</i>
<i>Figure 12: Common Key Used for Encryption and Decryption .....</i>	<i>27</i>
<i>Figure 13: Encrypted Data Exchange using Public and Common Key .....</i>	<i>28</i>

# 1 Overview

This section describes the white paper's purpose and structure.

## *1.1 About This White Paper*

RICOH is pleased to provide this technical and security white paper to Customers. This document describes RICOH's @Remote security policy so users can understand the technology structure behind the service offerings and use the remote monitoring system with confidence that their enterprise fleet data is securely managed and stored.

White paper contents are organized as follows:

1. RICOH @Remote Overview
2. What is RICOH @Remote?
3. @Remote Service Offerings
4. @Remote Service Architecture
5. @Remote System Security
6. @Remote Communications
7. @Remote Appliance Security
8. Data Handling Policy
9. Appendix: Additional Information

## 2 What is RICOH @Remote?

RICOH @Remote is a set of remote services that support LAN/Broadband environments, enabling customers to use their multifunctional devices with convenience and reassurance that their data are safe. RICOH @Remote provides reliable and timely services by obtaining accurate device status and usage information in real time. Ricoh can provide additional value for customers by analyzing and reporting fleet and asset information obtained from devices.

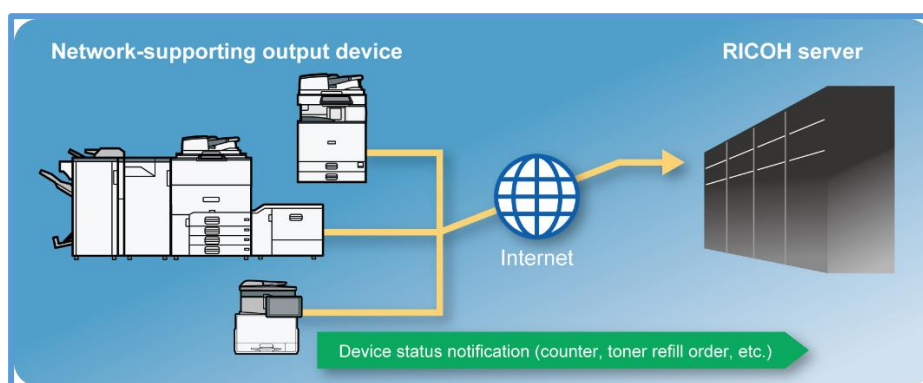


Figure 1: Overview of @Remote Network Monitoring Output Devices

### RICOH @Remote Benefits for Customers

Here are some Customer benefits of using RICOH @Remote services:

1. Eliminating the need for customers to manage devices.
2. Supporting stable device operations, keeping customer's business running without costly interruptions, for example, through automated system alerts for consumables and service notifications.
3. Keeping current with automated, remotely managed firmware updates.
4. Helping visualize device usage through reporting to control costs, efficiently manage the fleet, and make informed decisions.

### 3 @Remote Service Offerings

RICOH @Remote service consists of five main offerings. Through the service, RICOH makes every possible effort to reduce the burden of device management for customers with:

1. Automated Meter Readings
2. Automated Toner Notifications / Ordering / Delivery
3. Automated Service Maintenance Alerts
4. Remote Firmware Updates
5. Fleet Usage Reporting

#### 3.1 @Remote Service Offerings

This section provides an outline of @Remote Service offerings. RICOH's @Remote services are available based on countries/regions in focus, the customer's technical infrastructure, device's version, and the type of @Remote module being used.

##### 3.1.1 Automated Meter Reading

With the Automated Meter Reading service, @Remote automatically transmits device meter information to the RICOH Server on a regularly scheduled basis through a secure communication channel. This eliminates the need for customers to manually collect and report meter readings and helps improve usage data for more accurate billing.

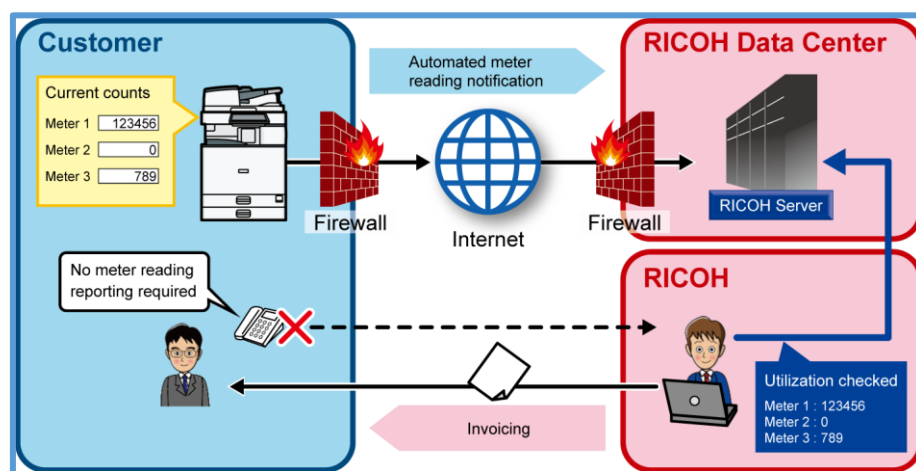


Figure 2: @Remote Automated Meter Reading Submissions Supporting Billing

### 3.1.2 Automated Toner Notification / Order / Delivery

With the Automated Toner Notification/Order/Delivery service, @Remote sends toner-end or replacement information at the time of the event. Additionally, @Remote periodically sends information on the level of remaining toner through a secure communication channel. Using these notifications, the system can automatically order additional toner for delivery to the customer as appropriate.

@Remote automated notifications reduces a customer's labor for toner inventory management and ordering and device downtime.

**Note:** This service offering may not be available in some countries or regions and depends on the customer's technical environment.

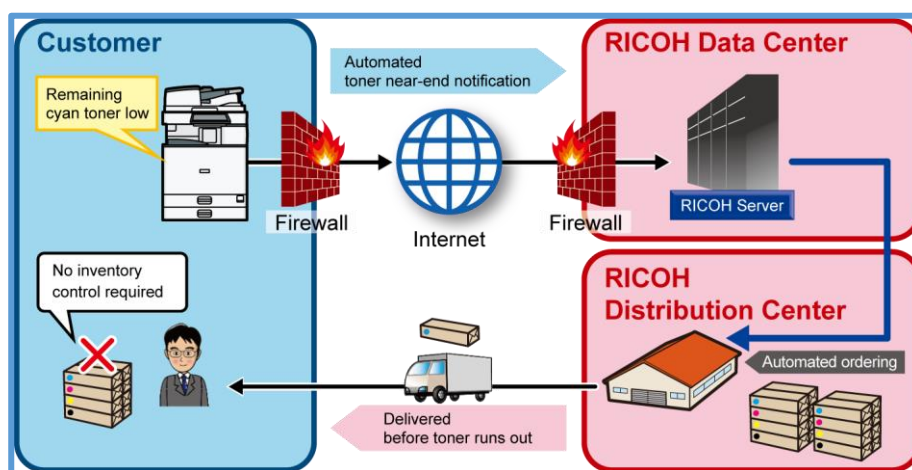


Figure 3: @Remote Automated Notifications and Alerts Supporting Continuous Operations





### 3.1.4 Remote Firmware Update

With the Remote Firmware Update service, the customer's devices automatically check the RICOH Server for firmware update operation commands. If operation commands are available, @Remote-connected devices download the firmware over a secure connection and automatically apply it. As a result, field service technicians do not need to visit and interrupt the customer's business workflow for firmware updates. Customers can keep devices up-to-date with the latest software, improving device output quality over time.

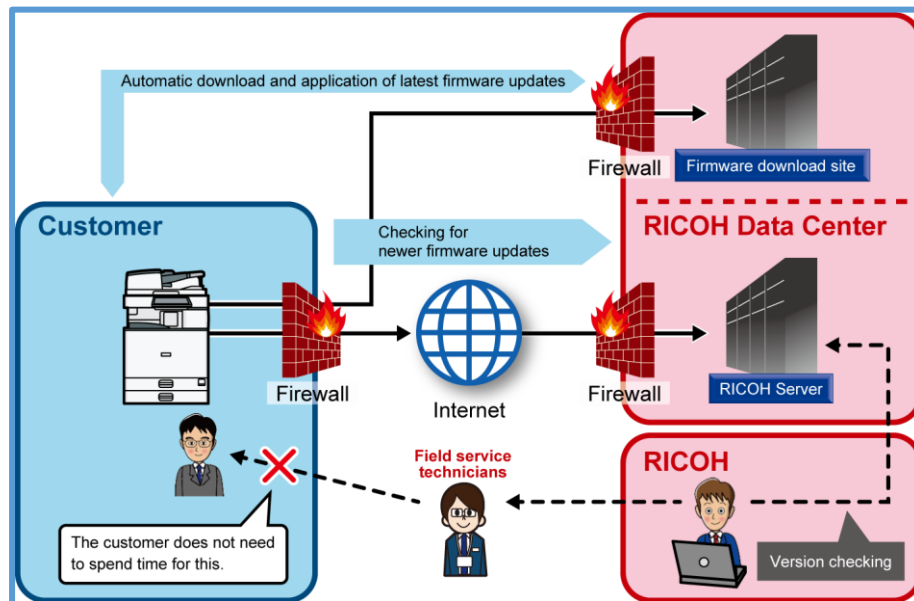


Figure 5: @Remote Automatically Downloads and Applies Firmware Updates

### 3.1.5 Fleet Usage Reporting

With the Fleet Usage Reporting service, RICOH generates usage reports from the device information submitted to the RICOH Server and delivers reports through the @Remote Web portal. Information on how devices are being used can be visualized in report charts, helping customers make the right decisions about fleet size and requirements.

**Note:** Reports may not be available in some countries or regions and some report content may not be accessible depending on the customer's technical environment.

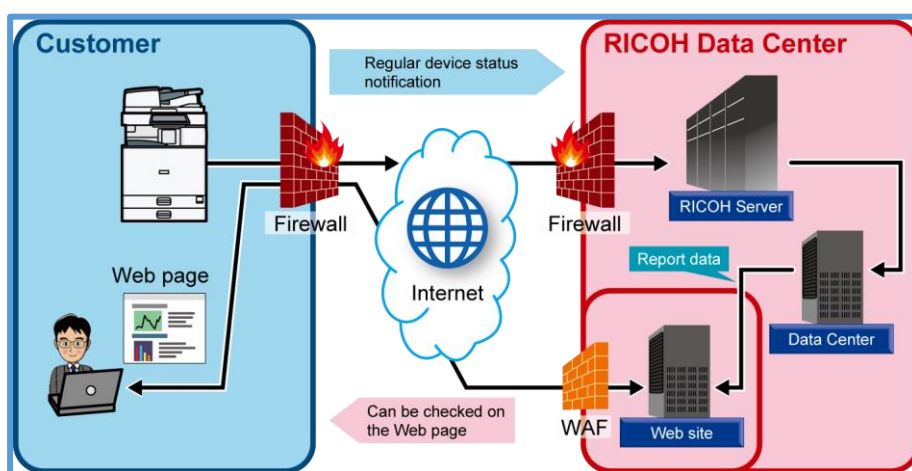


Figure 6: @Remote Fleet Usage Reporting Data Flow

## 4 @Remote Service Architecture

This section describes the system's service principles and technical architecture.

### *4.1 Operating Principles*

Following are the system's operating principles.

1. @Remote services involve network communication initiated only from the customer's devices to the RICOH Server. RICOH never initiates communication to any of the customer's devices.
2. @Remote service and its components can be activated or disabled from the customer's devices and is within the customer's control.
3. All device data is always transferred via a secure, encrypted Internet connection.
4. The customer's devices communicate only with the RICOH Server or an @Remote appliance.
5. The customer's devices only access the RICOH Server or an @Remote appliance after successful authentication with an electronic certificate.
6. @Remote service does not enable access to any personal information such as the customer's print data or address book.

## 4.2 @Remote Service System Overview

The following diagram provides a general overview of networked communications between the remote service components, i.e., firmware download site, certification authority, server, data center, web site, and the RICOH @Remote service system, i.e., connected devices, appliances, and customer's access to the portal.

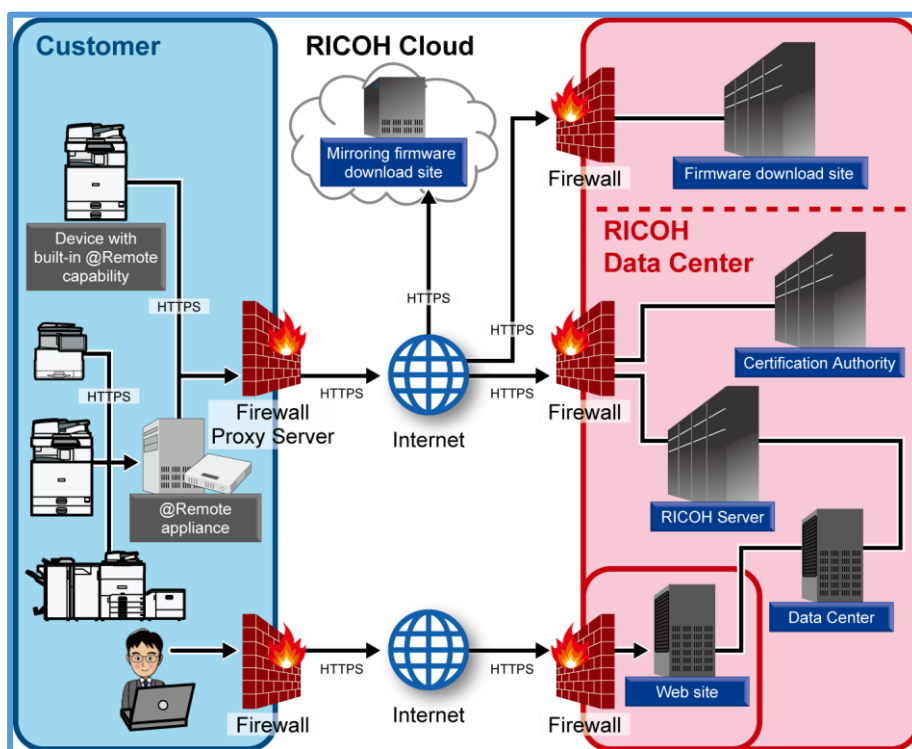


Figure 7: @Remote Service System Communications General Overview

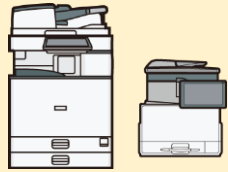


### Communication Requirements

- ✓ **External communication over the internet:** The remote service plugins use Transport Layer Security (TLS) to communicate over the Internet. The service also establishes connections using AES 256 bit session encryption.
- ✓ **Service plugins:** To use RICOH @Remote Service, one of the following modules must be installed in order to connect and communicate to the @Remote system. The supported communication methods differ between these module plugins.

**Note:** When creating customer's firewall exception is needed, please confirm to RICOH personnel to have the IP Address or URL of @Remote system.

## @Remote Module Types

This chart contains module types, communication method, and general remarks.

Module Type		Communication Method	Remarks
	@Remote embedded devices	Ethernet	Built-in type.
	Software, running on a server	Ethernet	A separate server is required to run the software.
	Appliance box	Ethernet	End of shipment

**Note:** These modules may not be available in some countries or regions and options and implementation depend on the customer's technical environment.

### *4.3 Remote Service Communication Activities*

The RICOH @Remote device, appliance box, or @Remove Service plugin module (software) performs the following communication activities. RICOH enables @Remote appliance box or @Remote Service plugin (software) to communicate with third party devices for collecting limited device information.

Standard, regularly scheduled communication activities follow.

- The device sends the following information to the RICOH Server:
  1. Meter information
  2. Supply requests
  3. Additional device details:
    - Static information such as the device's equipment ID, model name, IP address and settings
  4. Device status information:
    - Dynamic information such as remaining toner level and power consumption
- The device or @Remote appliance checks for commands from the RICOH Server for:
  1. Firmware update commands
  2. Device setting commands
  3. Gathering information related to device failures

System-driven communication activities follow.

- The device sends the following information to the RICOH Server as necessary:
  1. Supply calls
  2. Service alerts
  3. Device startup notifications
  4. Alarm notifications
  5. Failure recovery notifications
  6. Manual service calls
  7. Failure analysis

**Note:**

1. Some communication activities may not be supported in a specific country depending on the device or @Remote module type.
2. The accuracy of the third party device information cannot be guaranteed.

## 5 @Remote System Security

This chapter presents the @Remote system's communications security structure.

### 5.1 @Remote Network Communication Security

The following diagram shows an example of the network security protocols used for wired communications between the remote service components in the customer's environment and the RICOH data center. When collecting device information, these components communicate with a RICOH Server through the network built by the customer.

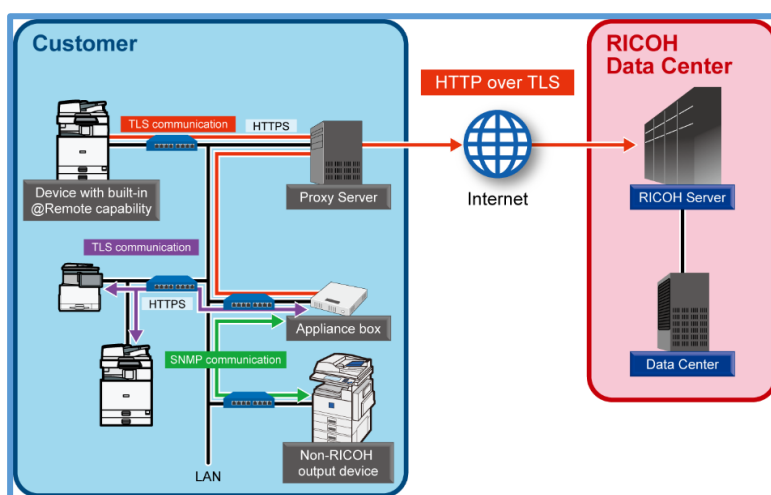


Figure 8: Sample of Customer Communication Network Configuration with RICOH Server

The @Remote system mainly uses TLS (Transport Layer Security) for communications between RICOH devices and RICOH Servers. This includes communications between RICOH devices and the @Remote appliance, or between remote service components and the RICOH data center. For communication between non-RICOH devices and the @Remote appliance, the system mainly uses Simple Network Management Protocol (SNMP). Please refer to 9.1.2 to be more precise.

Following are the communication standards Ricoh supports:

1. The preferred encryption method used for communication is the strongest encryption method available in the customer's environment. However, customers can change the encryption method used according to their environment.
2. TLS is a protocol used for communication requiring security over computer networks such as the Internet. Its major features include communication target authentication, communication encryption, and alteration detection.
3. \*SNMP (Simple Network Management Protocol) is a protocol used for network monitoring and management.  
\* As of January 2020, Ricoh supports TLS 1.2 and SNMPv3 or below. Available versions depend on the device or @Remote appliance.



## 5.2 @Remote Authentication Security

RICOH devices, @Remote appliances, and RICOH systems, such as the RICOH Server, each have electronic security authentication certificates. In every communication, they always exchange authentication certificates to identify each other, before initiating common key encryption-based communication. Thus, communication is protected against unauthorized data acquisition, including spoofing attempts.

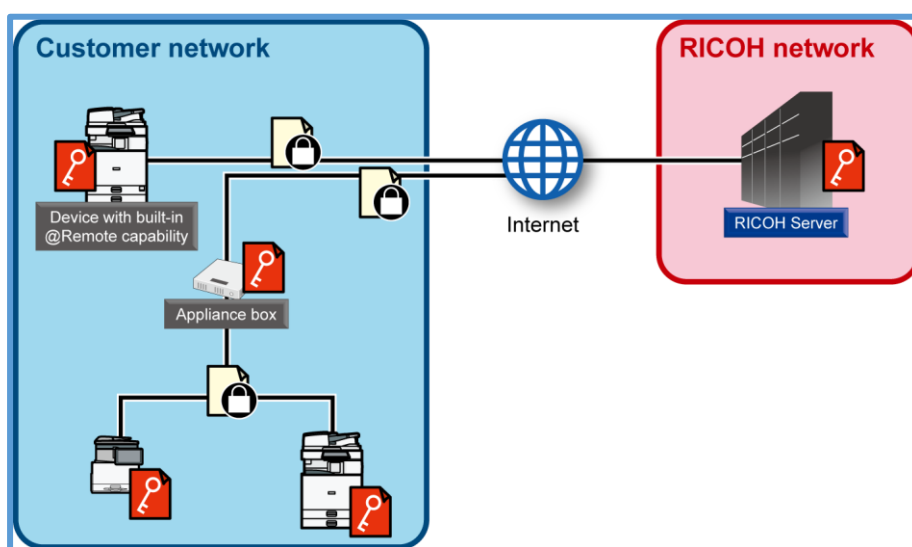


Figure 9: @ Remote Device Authentication Security Operations

## 5.3 Encryption Levels

RICOH devices, @Remote appliances, and the RICOH Server support the following levels of encryption in TLS communications:

Strength		Where used
Hashing	SHA-256	Message Authentication Code
Common key	AES 256	Session connection establishment, electronic certificate, etc.
Public key	RSA 2048	

### Notes:

1. Depending on the devices or @Remote appliance type, only prior encryption standards may be supported. Refer to the appropriate product manual or similar documentation to check which encryption standards are supported.
2. Some RICOH devices may be shipped with a default authenticate key length of 512 bits. If higher security is required, Ricoh will change the key length to 2048 bits on the devices.

## 5.4 RICOH Data Center Security

RICOH @Remote ensures security levels not only for communications, but also for the data center. Customers can rely on Ricoh's safety management systems at the data center. The following table lists the safety measures implemented and certifications acquired for the data center.

### 5.4.1 Security Specifications

This table contains RICOH data center's established security measures for four categories: disaster, security, business continuity, and environmental.

<b>Disaster measures</b>	Earthquake measures	Seismic base isolation, solid ground, non-liquefaction danger zone
	Power failure measures	Dual power, UPS and PDU redundancy, UPS for air conditioning, private power generation (72 hours' worth of fuel stockpiled, contract-based prioritized power resupply in case of disaster)
	Fire measures	Nitrogen gas fire extinguishing equipment, ultra-high sensitivity smoke sensors
<b>Security measures</b>	Intrusion prevention	External Infrared sensor-based monitoring, 24-hour manned monitoring, monitoring cameras (no blind spots)
	Entrance/exit control	ID card and palm vein authentication-based entrance/exit control, accompaniment prevention, personnel location management system
	Unauthorized carry-in/-out prevention	Metal detector, biometric-based server rack open/close control, security-tag based media management
<b>Business continuity measures</b>	Disaster-related	Safety confirmation and calling system, emergency earthquake alert system
	Novel flu	Masks, protective clothing, and thermographic fever checks with antiseptic stockpile
<b>Environmental measures</b>	Electric power system	High-voltage power distribution, highly efficient UPS, highly efficient transformer, solar power, rack-level temperature and electric current monitoring, LED lighting
	Air conditioning system	Thermal fluid simulation analysis, free cooling + fresh air cooling, hot and cold temperature control, highly efficient air-cooled chiller with dry coil, localized air conditioning, waste heat energy recycling

### *5.4.2 Acquired certifications*

This list contains RICOH data center's acquired security certifications from global organizations for the @Remote service:

1. Japan Quality Assurance Organization
  - a. ISO/IEC20000 certification
  - b. ISO/IEC27001 certification
  - c. ISO9001 certification
2. Assurance Report
  - a. Standard: ISAE3402/SSAE16 (former SAS70)
3. Japan Audit and Certification Organization for Environment and Quality (JACO)
  - a. ISO14001 certification
4. JIPDEC
  - a. Privacy mark certification
5. Information Security Rating by I. S. Rating Co., Ltd.
  - a. Information security rating "AAA1s"

### *5.5 RICOH Server Security*

The RICOH Server is checked based on the vulnerability information from JPCERT, and if a high-risk vulnerability is found, software upgrades and other plans will be made and addressed them.

## 6 @Remote Communications

This chapter contains @Remote communications details.

### 6.1 Operating Principles

Following are the @Remote system's operating principles.

1. RICOH @Remote Service never sends or obtains sensitive information or data (such as personal information).
2. RICOH @Remote Service does not access any sensitive information such as the customer's print data, address book, or files contained in the device's local storage disk.

### 6.2 Initiating Communication

Communication is always initiated by a RICOH @Remote-supporting device, appliance box, or @Remote Service plugin module (software). The RICOH Server never initiates any communication with these @Remote-supporting devices. Therefore, only outbound communication should be opened on the customer's firewall, and can be opened only to connect to @Remote server specific address.

When it is necessary for the RICOH Server to obtain device information, for example, for remote diagnostics, the RICOH system sends a secure instruction back in response to regular polling by the @Remote Service plugin module.

For example, when it is necessary for the RICOH Server to obtain device information, the RICOH system performs steps 1 to 6 in the following diagram, in this order.

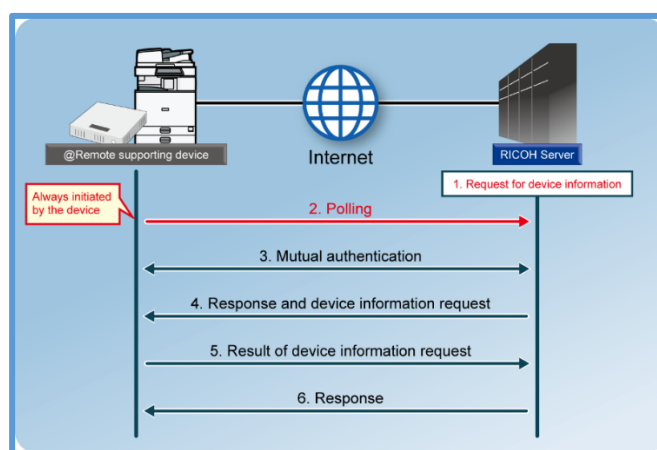


Figure 10: @ Remote System Communication Initiation Steps Operations

**Note:** The @Remote-supporting devices regular polling of the RICOH system in order to [1] notify operating status and [2] check for any commands from the RICOH Server.

### *6.3 Data Contents Sent by Devices*

The following list contains the core data set that the customer's devices send to the RICOH data center. Please note that, in addition to these data elements, the data sent includes RICOH-specific information required to connect to the RICOH Server.

- ✓ Core data set elements:
  1. Device name
  2. Model name
  3. IP host name
  4. IP address
  5. Various meter readings: total output, total color output
  6. Various status information: paper end, door open, etc.
  7. History information: jam count, operating time, service call count
  8. Alert information: service calls, etc.
  9. Last communication date and time
  10. Device information for failure analysis: sensor data, etc.

**Notes:**

1. The data that can be sent varies depending on the device, device configurations, or the service plugin module type.
2. Ricoh can configure devices to withhold some of the above-listed data elements.

### *6.4 Data Acquisition*

In addition to push communications, the @Remote system also uses pull communication methods to ascertain what data are needed for a device. For example, when it is necessary to perform a remote firmware update on the customer's devices or remotely change or modify an incorrect value, the device checks by polling and then tries to obtain the necessary firmware or device settings, as described in the previous section "Initiating Communication." This ensures preventing the plugin module from receiving unintended files that may be sent by an unauthorized server through a push communication.

## 7 @Remote Appliance Security

This chapter describes the @Remote appliance box's security details.

### *7.1 Appliance Box*

The box type appliance stores data from devices in its internal database. This internal data is protected with an authentication feature. The appliance-box type relay is certified to the international information security standard, ISO/IEC 15408 (CC) (evaluation assurance level 2).

**Note:** ISO/IEC 15408 is an international information security evaluation standard for products and systems. This standard defines a set of evaluation criteria for determining the integrity of a product or system's security design, and the implementation of the product or system is exactly as per the design. Mainly designed for military information systems, these criteria were standardized across countries and brought under the ISO standard.

## 8 Data Handling Policy

This chapter describes Ricoh's secure data management policy.

### *8.1 Use of Device Data*

Based on our enforced policy, RICOH always appropriately handles device information obtained from the customer to provide to the @Remote Service. Use of @Remote Service indicates that the customer accepts its use conditions as specified by RICOH. RICOH will use device information from the customer to provide the following services:

1. Automated Meter Reading
2. Automated Toner Order/Delivery
3. Fleet Usage Reporting
4. Device Management or Failure Monitoring and Analysis
5. RICOH Marketing Status Analysis
6. RICOH Product Development-related Information Analysis
7. Proposals and Recommendations of Additional Services
8. Responses to Various Inquiries

### *8.2 Management of Device Data*

RICOH uses customer device information only for the purposes defined by this policy and manages it appropriately in compliance with RICOH's basic information protection policy (including RICOH company regulations and related laws and legal regulations) to prevent leakage, loss, illegal use of, and illegal access to such information. RICOH also uses and manages customer information appropriately in compliance with the information protection-related laws and legal regulations of each country where @Remote Service is used.

### *8.3 Return of Device Information*

RICOH will not return device information obtained through our @Remote system. RICOH assumes the responsibility of securely deleting, destroying, and disposing of such device information.

### *8.4 Non-Disclosure of Device Information*

RICOH will not disclose device information obtained from customer devices to any third party without explicit customer approval; provided, however, that this shall not apply to the following conditions:

1. RICOH's related subsidiary companies should not be considered as third party in this section.
  - a. Disclosure is requested by law or provision is based on the law.
  - b. The customer is explicitly notified of the information that may be disclosed, and consents to such disclosure.
  - c. To fulfill the use of data for provision of @Remote services, RICOH needs to provide device information to a business partner such as subcontractors or business agents, whom RICOH will manage appropriately.
  - d. To protect the interests of a person or legal entity, such as life, physical body, or property, yet it is difficult to obtain explicit customer approval.
  - e. Device information needs to be taken over and disclosed for merger or business succession based on legal reasons, in which case it will be handled within the scope of the use of data.
  - f. RICOH is required to submit device information without the customer's consent in order to cooperate to the duties of the central or local government institutions or their subcontractors set by law, in which case obtaining explicit customer approval may obstruct the concerned duties.



## 9 Appendix

This appendix contains information about @Remote security protocols, ports, and encryption.

### 9.1 @Remote Protocols and Use of Network Ports

This section presents communications security details.

#### 9.1.1 Use of Network Ports between Customer's Devices and RICOH Server Communications

This table identifies two communication scenarios between the customer's devices and the RICOH Server and the port number.

No.	Scenario	Communications Direction	Port Number	Protocol
1	Sending notification to the RICOH Server	Device TO RICOH Server	443	HTTPS
2	Requesting operation command to the RICOH Server			

#### 9.1.2 Use of Network Ports between Customer's Devices and @Remote Appliance Communications

Please refer to each @Remote appliance white paper because ports and communications depend on appliance specifications.

1. RC-Gate A2: RICOH Remote Communication Gate A2 White Paper
2. RICOH @Remote Connector NX: RICOH @Remote Connector NX White Paper (Appliance Type: Server Type Solution)
3. RICOH Streamline NX @Remote Connector: Security White Paper for RICOH Streamline NX v3.2.0

### 9.2 Encrypted Communication and Encryption Keys

To prevent a malicious third party from reading or altering communications, most communications use an encryption key to encrypt authentication or communications. RICOH @Remote uses TLS encryption for communications, and TLS uses public key encryption and common key encryption for communication.

#### 9.2.1 About Public Key Encryption

Public key encryption uses a pair of encryption keys, [1] a public key and [2] a private key, for encryption and decryption. Data encrypted with one key of the pair can only be decrypted with the other key of the pair.

There are a number of different public key encryption methods. Among these methods, RSA cryptography is a typical public key encryption method. NIST\*<sup>1</sup> has publicly announced in computer security report, SP800-57, that RSA using the 2048-bit key length will be available until year 2030\*<sup>2</sup>.

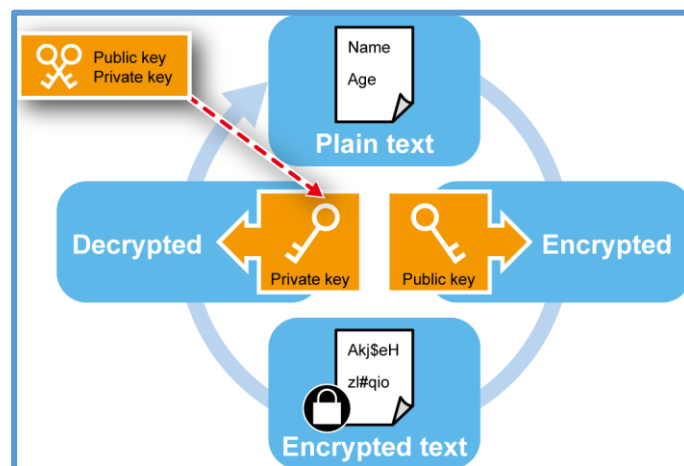


Figure 11: Public and Private Keys Used for Encryption and Decryption

**Notes:**

1. \*National Institute of Standards and Technology (NIST) is a governmental institution within the U.S. Department of Commerce. NIST studies and researches instrumentation and standards in scientific technologies.
2. \*As of January 2016.

### 9.2.2 About Common Key Encryption

Common key encryption uses the same common key for encryption and decryption. Data encrypted with a common key can only be decrypted with the common key.

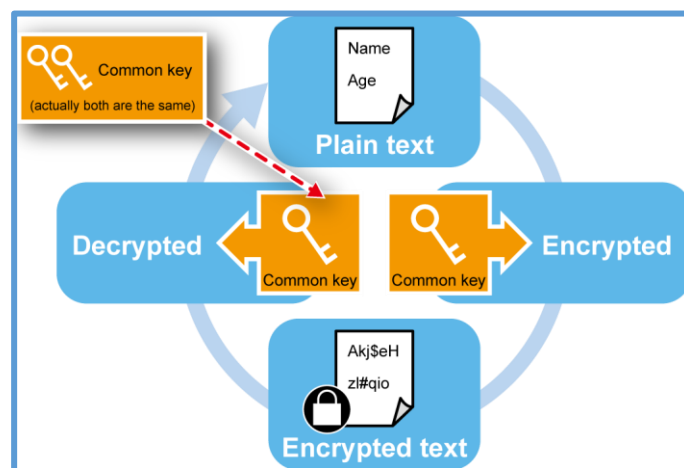


Figure 12: Common Key Used for Encryption and Decryption

The main common key encryption method used is AES cryptography. In this method, three different key lengths are available: 128-bit, 192-bit, and 256-bit. NIST\*<sup>1</sup> has publicly announced in a computer security report that AES using the 256-bit key length will be available until year 2030\*<sup>2</sup>.

#### Notes:

1. \*National Institute of Standards and Technology (NIST) is a governmental institution within the U.S. Department of Commerce. NIST studies and researches instrumentation and standards in scientific technologies.
2. \*As of January 2016.

### 9.2.3 How TLS Encrypts Communications

TLS encrypts communication by using public key encryption to establish a secure communication session and common key encryption to exchange the actual data.

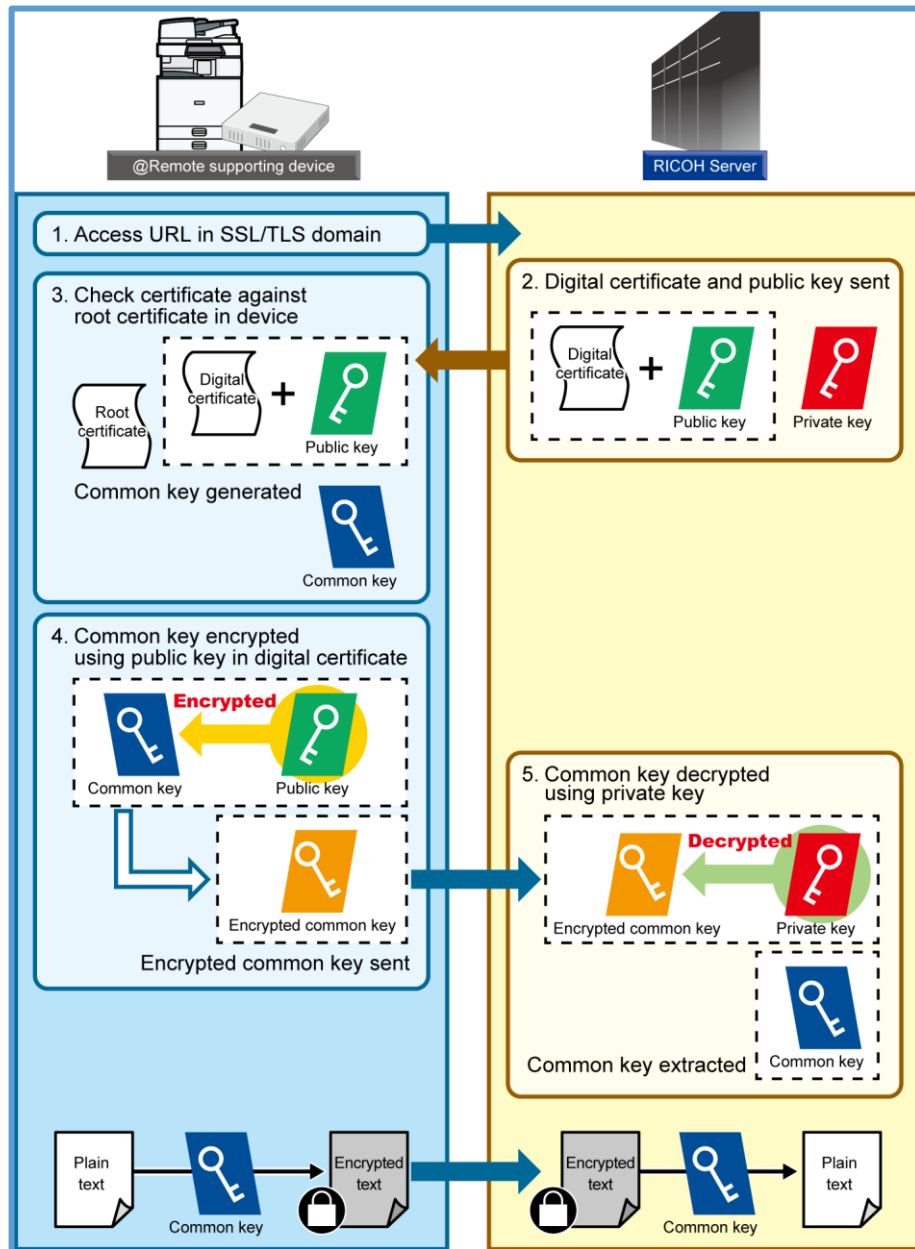


Figure 13: Encrypted Data Exchange using Public and Common Key

### 9.3 Glossary of Terms

Acronym or Term	Meaning
AES	Advanced Encryption Standard
HTTP over TLS	Hypertext Transfer Protocol over Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISAE	International Standard on Assurance Engagements
ISO	International Standards Organization
JACO	Japan Audit and Certification Organization
JIPDEC	Japan Institute for Promotion of Digital Economy and Community
LAN	Local Area Network
LED	Light emitting diode
NIST	National Institute of Standards and Technology
PDU	Power Distribution Unit
RSA 2048	Rivest – Shamir – Adleman (2048-bit key)
SAS 70	Statement on Auditing Standards (No. 70)
SHA 256	Secure Hash Algorithms (256-bit)
SNMP	Simple Network Management Protocol
SSAE	SSAE 16 replaces SAS 70 as reporting standard
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
WAF	Web Application Firewall

Document End