@Remote™
Intelligent Remote Management System

@ Remote

Intelligent Remote Management System
for the Network Connected Printing Devices

White Paper
(External Appliance Type)

Version 6.00
June.15th,2006

Update History

Version	Release
5.00	July 5th, 2005
4.00	June 10th, 2005
3.00	May 20th, 2005
2.00	February 6th, 2004
1.00	January 30th, 2004

@Remote

White Paper

@Remote Service

Today’s Customer Environment

The way is open

Although potential for growth has never been larger, this is a challenging time for companies everywhere — worldwide opportunities mean global competition, and businesses that want to stay ahead face complex tasks. Not the least of which is how to cut costs while staying abreast with the relentless pace of changing technology.
Business is under ever growing pressure to improve the quality and decrease the turnaround time of their products and services.

Much of the success or failure of a business depends directly on the quality of the equipment and services at its disposal. In big businesses especially, system control and administration is becoming more and more important. Weak maintenance and lack of intelligent system management can negate the advantages of quality equipment and staff.

Start up + Control / Administration + Operation = TCO

Add to this the fact that the IT manager’s workload is increasingly complex, as administration duties and IT development expands. Pressure to get the maximum from a network has never been greater. Control over devices is an elemental factor of network efficiency, since this is key to TCO (Total Cost of Ownership – the sum of three costs: start up, control/administration, and operation).
Also, as competition intensifies, business system costs have grown in significance and are now a major management priority.

The Challenge:

To reduce time lost on equipment maintenance: servicing, supplying, and monitoring.
To overcome human interface issues – relieving dependency on users for reports on device status or malfunctions, reports that unfailingly come after the problem has occurred and, understandably, often lack the technical detail necessary for a prompt assessment and solution.

To counter precisely these obstacles, an ideal remote servicing system would be capable of the following:
Detecting problems before users will become aware of them – to tackle firmware and reboot remotely, with minimal user intervention.
Identifying and pre-diagnosing potential breakdowns or shortages. Technicians could then be dispatched, fully equipped with the necessary parts.
Monitoring device performance, and making whatever modifications necessary to optimize productivity and efficiency.
Watching over supply consumption, and sending out replenishments before they run out.
Providing TCO-relevant data to the administrator.
Establishing an automated, usage-based billing system to streamline running costs.

So what is the end result – the bottom line from the business perspective?

Productivity
Effectiveness of service
Service costs

Ultimately – improved customer satisfaction. Whatever your product or service, the likelihood of delivery problems due to device failings is dramatically reduced.

@Remote is designed to be capable of exactly these functions.
Its purpose is to provide three related enhancements:

*IT equipment maintenance

accident and breakage recovery
toner supply – ordering and delivering

*IT equipment productivity

maximizing device utilization
know how – getting the most from a device, for the least cost

*IT cost reduction

initial outlay for equipment
maintenance and running costs

Solution – @Remote

To limit the downtime of each kind of device (multifunction products, network printers, copiers), it is of growing necessity that we attempt to deploy our systems and tools optimally. @Remote provides for this, allowing users to benefit from improved business productivity, independence from maintenance responsibility and the costs such concerns formerly involved.

@Remote – Advantages for Network Connected Printing Devices

There are four broad features of @Remote that make it particularly advantageous for our users:

1. Remote maintenance avoids time spent on service calls and firmware upgrades – performing such tasks automatically, or as and when problems are detected.

1. Reduced Device Downtime

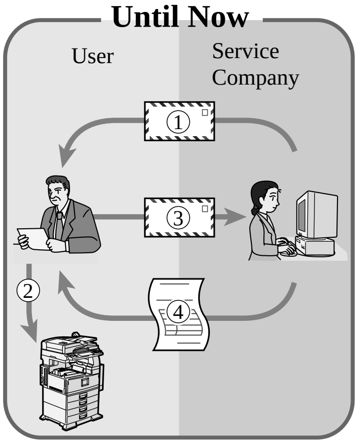
Device downtime is reduced through remote maintenance. Specifically, remote maintenance cuts downtime by sending service calls automatically to our service technician.
Also, these services are only made possible through connection to the Internet. This means users can operate without worrying about incomplete jobs or being tied to maintenance or repairs; companies are freed from time-consuming duties and additional downtime expense.

2. Counter monitoring is fully automatic. This means production efficiency can be measured directly, counter figures confirmed, and TCO-relevant data obtained and acted upon.

2. Automated Counter Checking

Remote counter monitoring means the user no longer has to manually report counter figures.

The traditional counter checking procedure involved:



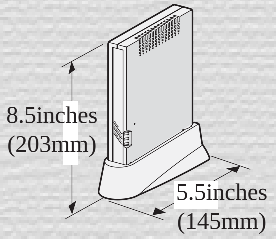
① The service company requests the user to check the counter (s).

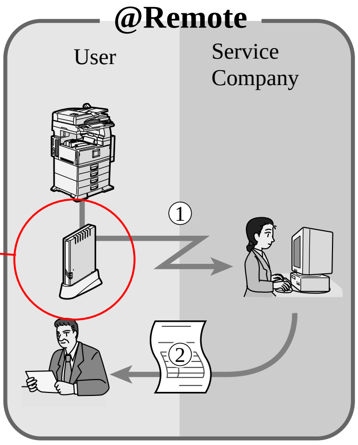
② The user checks the device's counter.

③ The user reports the counter figure by postcard, fax, or telephone.

④ The service company sends the bill.

Remote Communication Gate (External)





① The Remote Communication Gate (a relay unit which connects the user's devices to the @Remote System) sends the counter information to the service company automatically.

② The service company sends a bill back to the user.

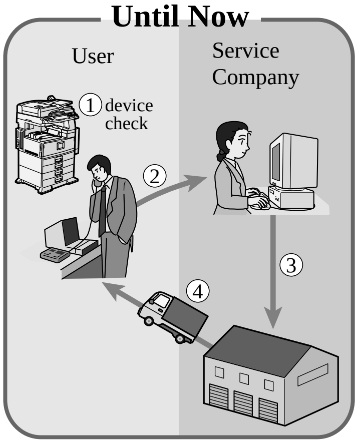
@Remote offers an improvement in the form of remote, automated counter checking.

User workload is reduced.

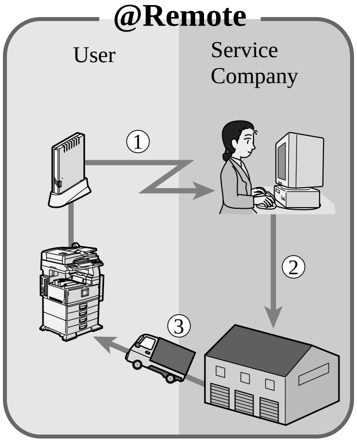
3. Supply level (toner, staples) monitoring is continuous - reporting is automatic when toner reaches 'near end'.

3. Ordering Supplies (toner, etc.)

@Remote reports toner level (near end/end) data to our service company – device downtime is reduced, as the user no longer has to worry about re-order telephone calls, forgotten stock, supply control and so on, now that monitoring and dispatch is fully user-independent.
The ability to automate toner fulfillment is dependent upon the service provider.



① Device runs out of toner. User calls the service company.
② The service company requests toner delivery from the delivery center.
③ The delivery center delivers the toner to the user.



① Device runs out of toner. The Remote Communication Gate detects the “toner end” information and automatically sends this to the service company.
② The service company requests toner delivery from the delivery center.
③ The delivery center delivers the toner to the user.

4. The device’s operational status can be remotely ascertained, production efficiency assessed, and potential problems pre-diagnosed. TCO supervision / administration is provided also.

4. Device Monitoring

This provides information on device operation, making use of it for more effective control.

Summary of Advantages

Advantages	Main Features	Currently	@Remote Advantage
1. Reduce Device Downtime	Auto Service Call	When Service Calls occur, customers contact their sales/service companies for device maintenance or repair.	@Remote can receive device failure calls automatically, carry out remote diagnostics, and perform remote updates in the event of firmware problems.
2. Automated Counter Checking	Auto Counter Reading & Billing	Meter reading is usually by postcard, fax, and telephone – between customer and sales company.	@Remote carries out meter reading periodically, without requiring user intervention.
3. Ordering Supplies (toner, etc)	Auto Supply Replenishment	When supplies run out (reach end), customers contact their sales companies to order or stock supplies.	@Remote can obtain toner level information (near end/end) from devices automatically.
4.Device Monitoring	Device Status Monitoring	IT managers want to manage their devices correctively. However, they have to utilize each vender's management software and it's difficult to find out/manage new network device to be installed individually.	@Remote can monitor not only Ricoh family group devices but also those of other companies, and finds new devices automatically.

ISO/IEC15408(EAL3) Certified Function

What is ISO/IEC15408?

ISO/IEC15408 is the only international standard in the world with respect to IT products and systems which provides the way in which security measures are to be laid out in order to prevent any occurrence of security issue, and how guarantee methods should be put in place. It is a standard to evaluate if security functions of products and systems are implemented “correctly”, “sufficiently” and “compatibly”. Evaluations of products by third party organizations are emphasized in IT security industry. Since it is difficult to visually check if security functions are working correctly in many cases, it is important to “have a third party guarantee that the products are implemented properly according to the specifications”. In Europe and North America, independent criteria for evaluations had been used to conduct such security evaluations since more than a decade ago. In 1998, evaluation criteria called TCSEC in the United States, CTCPEC in Canada and ITSEC in Europe were integrated as CC（Common Criteria. It was later issued as an international standard, ISO/IEC 15408 in 1999.

Certification Report of Remote Communication Gate is available at the following website.

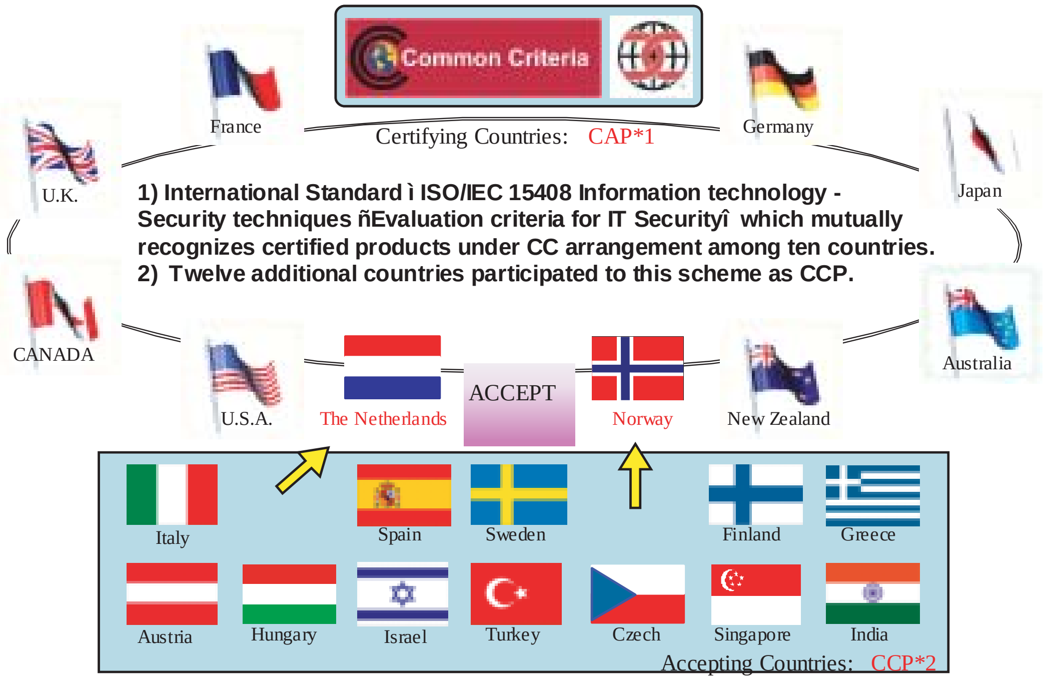
https://www.secure.trusted-site.de/certuvit/pdf/9240BE.pdf

Certificate of Remote Communication Gate is available at the following website.

https://www.secure.trusted-site.de/certuvit/pdf/9240UE.pdf

“Furthermore, Remote Communication Gate (External Appliance Type) is corrently undergoing evaluation with in Japanese Commun Criteria Evaluation and Certification Scheme. When it is acquired, approval by CCRA(Common Criteria Recognition Arrangement) will be obtained.

CCRA (Common Criteria Recognition Arrangement)



1) International Standard ì ISO/IEC 15408 Information technology - Security techniques ñEvaluation criteria for IT Securityî which mutually recognizes certified products under CC arrangement among ten countries.

2) Twelve additional countries participated to this scheme as CCP.

CAP*1: Certificate Authorizing Participants CCP*2: Certificate Consuming Participants

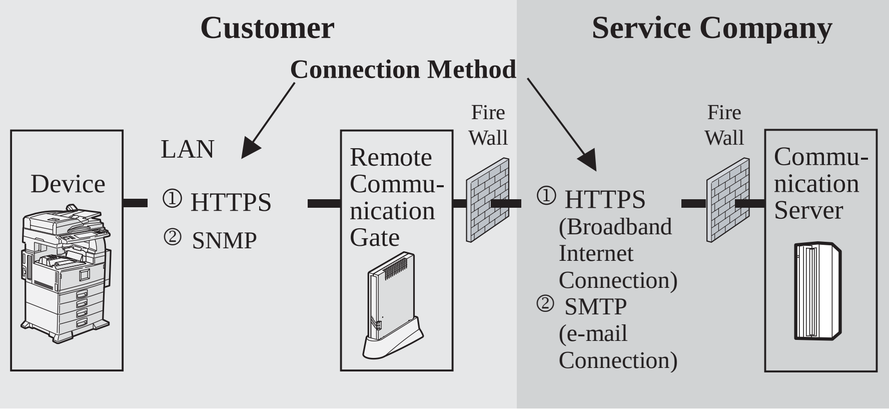
As of Mar 2006

@Remote System Structure

@Remote is an interactive system, allowing data to flow between two main components:

1. The Remote Communication Gate – this appliance acts as a relay unit to which all the Customer's devices (multifunction products, network printers, copiers) are connected.

2. The Communication Server – at the service company end, where the Remote Communication Gate's data is received.

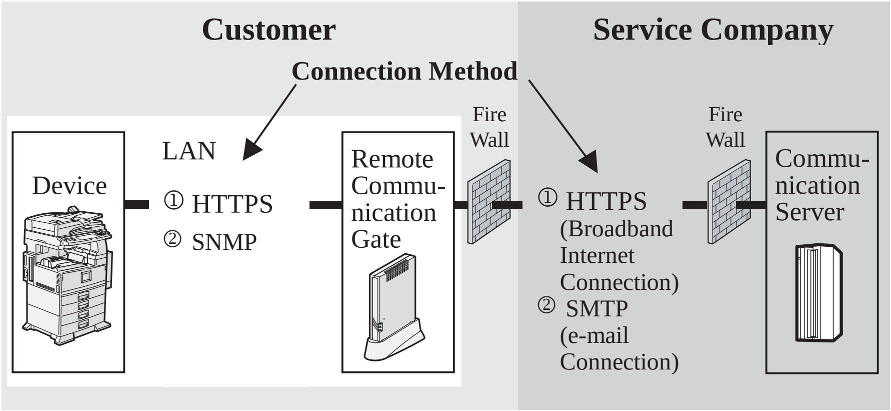


Communication Methods and Information Security

1. How communication between Remote Communication Gate and connected devices works

*There are two types of communication method used between the Remote Communication Gate and connected devices:

1. **HTTPS** (Hyper Text Transfer Protocol Security)
2. **SNMP** (Simple Network Management Protocol)
   MIB (Management Information Base) information is obtained from devices via regular Remote Communication Gate polling.



HTTPS Method

1. Remote Communication Gate to device communication (and vice versa) is in SSL (Secure Socket Layer) format.
2. Data is encrypted Remote Communication Gate (V3.34 or later) supports Triple-DES (Data Encryption Standard) Cipher 168 bits key, However if device supports only DES 56 bits key, encryption level must be reduced to DES 56 bits key, This key is created and changed each and every session
3. Both Remote Communication Gate and devices have RSA 512 bits certificates for @Remote and use security authentication checks.
4. For each communication, a mutual authentication procedure is completed before the data is sent.

Comments

Access to customer server/client computers is not possible, because the Remote Communication Gate recognizes only printer MIB.

HTTPS is a web server and client (browser) protocol for sending and receiving data: HTTP + SSL (Secure Socket Layer). For privacy and information security, data between browser and server is encrypted - hence widely used in Internet shopping.

1-1. HTTPS (Hyper Text Transfer Protocol Security)

HTTPS communication takes two forms:

I. Access from devices to Remote Communication Gate

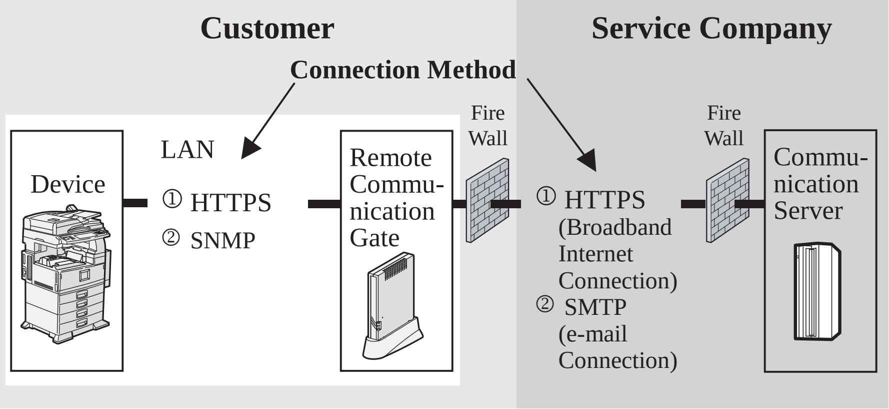
Example:

1. Emergency call (Device failure call or Toner end/near end call)

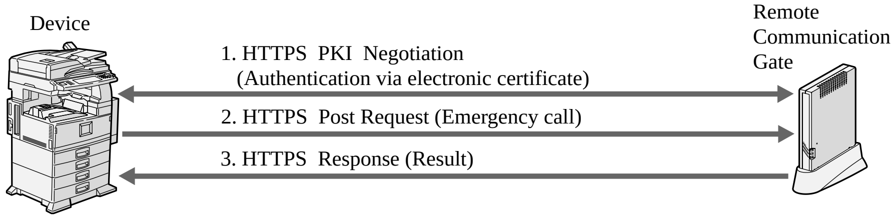
II. Access from Remote Communication Gate to devices

Example:

1. Counter information(number of prints, copies, etc)



I. Access from devices to Remote Communication Gate


Device
Remote Communication Gate
1. HTTPS PKI Negotiation (Authentication via electronic certificate)
2. HTTPS Post Request (Emergency call)
3. HTTPS Response (Result)

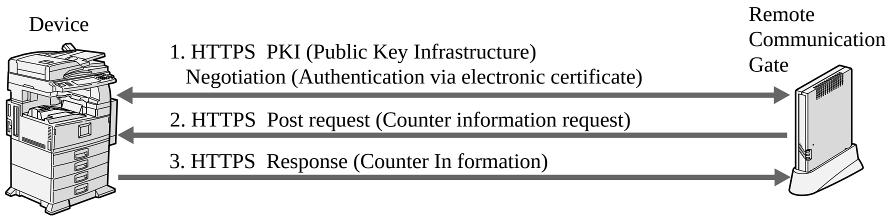
1. When there is a device alarm, the device initiates authentication via electronic certificate with the Remote Communication Gate.
2. Devices send Device failure call information to the Remote Communication Gate by HTTPS POST Request.
3. The Remote Communication Gate confirms receipt of Device failure call information by sending back the RESULT via HTTPS Response.

PKI : Public Key Infrastructure

HTTPS : Hypertext Transfer Protocol Security (HTTP over SSL - Secure Socket Layer)

Post : Refers to sending (Posting) message to the receiver.

II. Access from Remote Communication Gate to devices


Device
Remote
Communication
Gate
1. HTTPS PKI (Public Key Infrastructure)
Negotiation (Authentication via electronic certificate)
2. HTTPS Post request (Counter information request)
3. HTTPS Response (Counter In formation)

1. When the Remote Communication Gate is initiating, authentication via electronic certificate takes place between Remote Communication Gate and the devices.
2. The Remote Communication Gate sends the obtain counter information request to devices using HTTPS POST Request.
3. Devices confirm receipt of the counter information request by sending back the counter information via HTTPS Response.

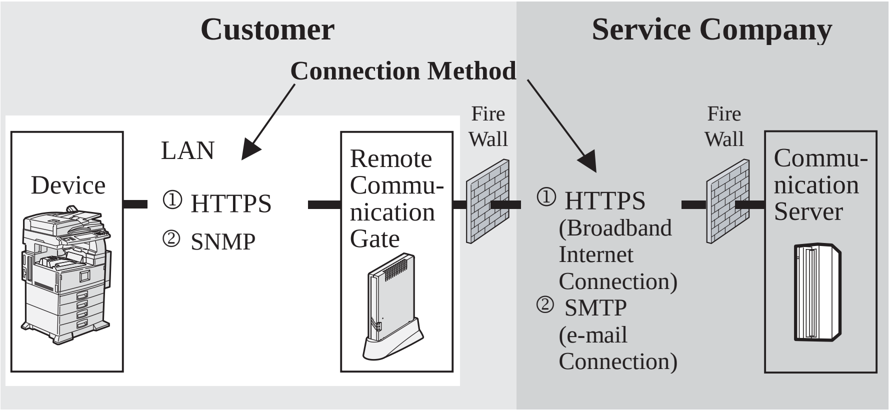
1-2. SNMP (Simple Network Management Protocol)

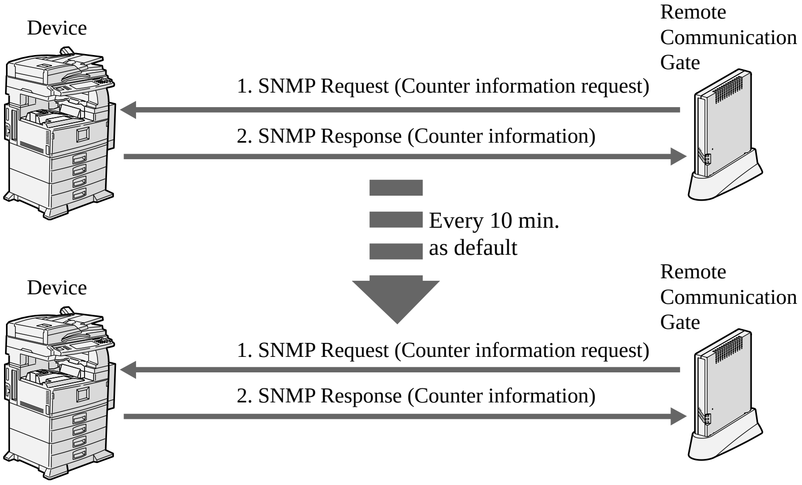
Device MIB information is obtained from periodic (default: 10 minutes) Remote Communication Gate to device polling.

Example:

1. Counter information
2. Emergency call (Device failure call or Toner end/near end call)

* Device-to-Remote Communication Gate access is not possible.




Device
Remote Communication Gate
1. SNMP Request (Counter information request)
2. SNMP Response (Counter information)
Every 10 min. as default
Device
Remote Communication Gate
1. SNMP Request (Counter information request)
2. SNMP Response (Counter information)

Procedure

1. Devices obtain counter information request OIDs from the Remote Communication Gate via SNMP Request.
2. Devices send back their counter information via SNMP response.

SNMP: Simple Network Management Protocol

OID: Object Identifier

MIB: Management Information Base

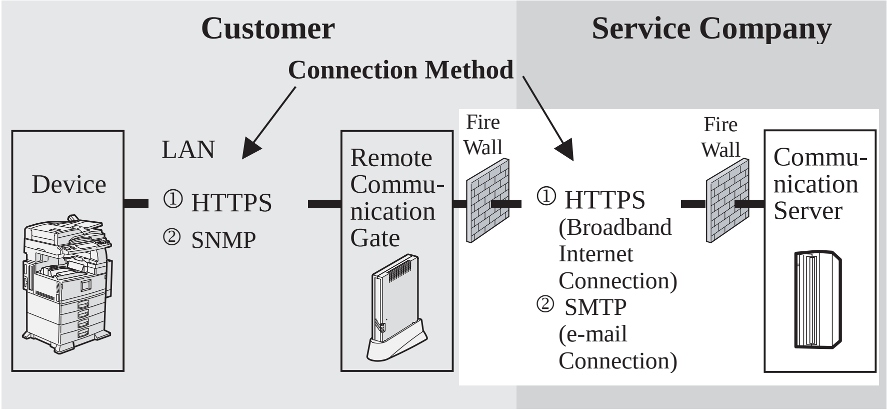
EOT: End Of Text

HTTPS is a web server and client (browser) protocol for sending and receiving data: HTTP + SSL (Secure Socket Layer). For privacy and information security, data between browser and server is encrypted - hence widely used in Internet shopping.

2. How communication between Remote Communication Gate and Communication Server works

*Two types of communication method are used between the Remote Communication Gate and Communication Server:

1. HTTPS (Hyper Text Transfer Protocol Security) -Broodband Internet Connection.
2. SMTP (Simple Mail Transfer Protocol) – e-mail Connection.



About HTTPS

1. Remote Communication Gate to device communication (and vice versa) is in SSL (Secure Socket Layer) format.
2. Data is encrypted (Refer to Page 12).
3. Both Remote Communication Gate and Communication Server use security authentication checks.
4. For each communication, a mutual verification procedure is completed before the data is sent.

About SMTP

1. Remote Communication Gate includes a digital signature.
2. Data is encrypted using Triple-DES Cipher 168 bits (Remote Communication Gate (V3.34 or later).
3. The Triple-DES Cipher key is encrypted by Communication Server's public key.
4. Remote Communication Gate sends it with S/MIME format (Base64) as E-mail.

2-1. HTTPS(Broadband Internet Connection)

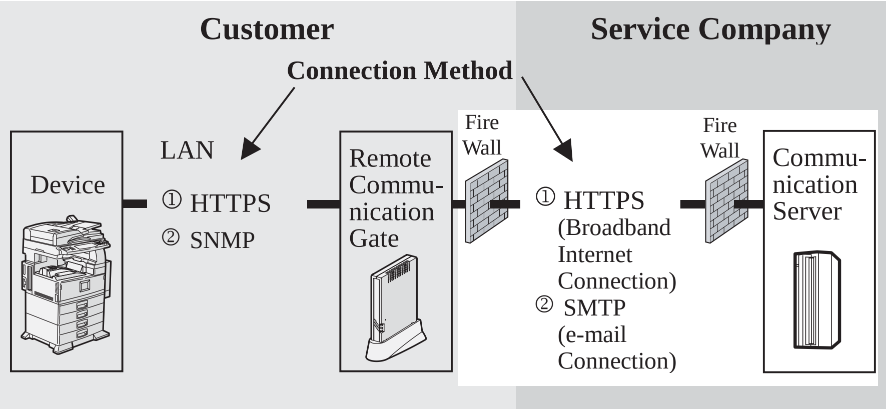
Listed below are the two reasons for HTTPS communication initiation.

I. Emergency call (Device failure call or Toner end/near end call)

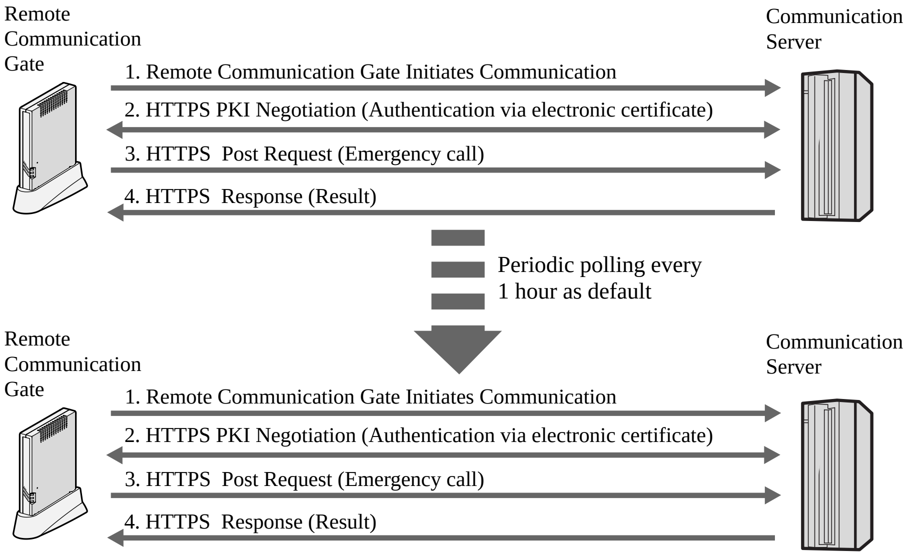
-Sending from the Remote Communication Gate

II. Counter Information(number of prints, copies, etc)

- Handling Communication Server requests by initiation from Remote Communication Gate



I. Emergency Call


Remote Communication Gate
Communication Server
1. Remote Communication Gate Initiates Communication
2. HTTPS PKI Negotiation (Authentication via electronic certificate)
3. HTTPS Post Request (Emergency call)
4. HTTPS Response (Result)
Periodic polling every 1 hour as default
Remote Communication Gate
Communication Server
1. Remote Communication Gate Initiates Communication
2. HTTPS PKI Negotiation (Authentication via electronic certificate)
3. HTTPS Post Request (Emergency call)
4. HTTPS Response (Result)

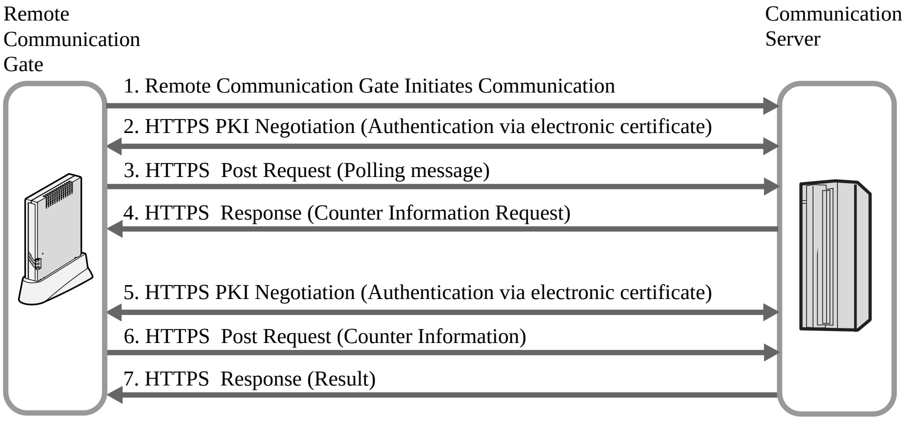
Procedure

1. Remote Communication Gate Initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends Device failure call information to the Communication Server, via HTTPS POST Request.
4. The Communication Server confirms receipt of Device failure call information by sending back the RESULT via HTTPS Response.

*Communication between Remote Communication Gate and Communication Server is initiated only by the Remote Communication Gate.

*Normally periodic polling between Remote Communication Gate and Communication Server is performed once an hour. However when the Communication Server receives specific call information such as Service Call of devices, the polling interval is temporally changed to every one minute. After Communication Server receives SC (Service Call) Reset Call, the polling interval is restored to every one hour.

II. Counter information


Remote Communication Gate
Communication Server
1. Remote Communication Gate Initiates Communication
2. HTTPS PKI Negotiation (Authentication via electronic certificate)
3. HTTPS Post Request (Polling message)
4. HTTPS Response (Counter Information Request)
5. HTTPS PKI Negotiation (Authentication via electronic certificate)
6. HTTPS Post Request (Counter Information)
7. HTTPS Response (Result)

Procedure

1. Remote Communication Gate initiates communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends polling information to the Communication Server, via HTTPS POST Request.
4. The Communication Server confirms receipt of polling information by sending back the RESULT to the Remote Communication Gate, via HTTPS Response, and adds to this further Counter information request commands.
5. The Remote Communication Gate, when the Counter information request commands in the HTTPS Response are processed, responds to the Communication Server, after initializing mutual electronic certificate authentication.
6. The Remote Communication Gate sends its response to Counter information back to the Communication Server, via HTTPS POST Request.
7. The Communication Server confirms receipt of response by sending back the RESULT, via HTTPS Response.

Since sending is not from the Communication Server through the customer firewall, it is not necessary to open a port for HTTPS reception from outside the customer firewall.

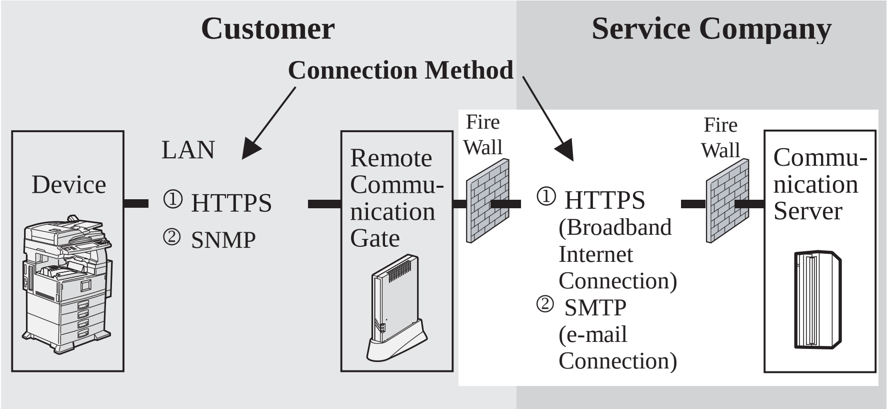
PKI: Public Key Infrastructure

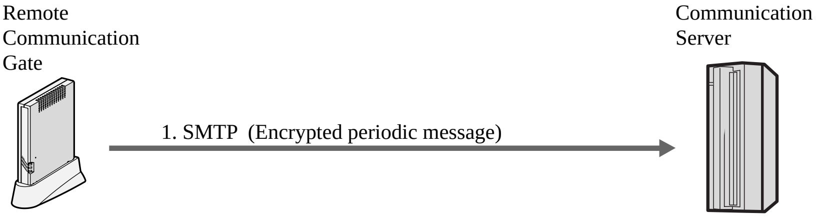
2-2. SMTP (e-mail connection)

*Only send functions, like normal e-mail, can be performed from Remote Communication Gate to Communication Server.

Example:

1. Counter information




Remote Communication Gate
Communication Server
1. SMTP (Encrypted periodic message)

Procedure

1. The Remote Communication Gate sends device information to the Communication Server as an encrypted(S/MIME) E-mail attachment.

The Remote Communication Gate sends E-mail in only one direction; E-mail from outside does not have Remote Communication Gate reception functions.

The Remote Communication Gate supports two type of SMTP authentication:

1. SMTP authentication
2. POP before SMTP authentication

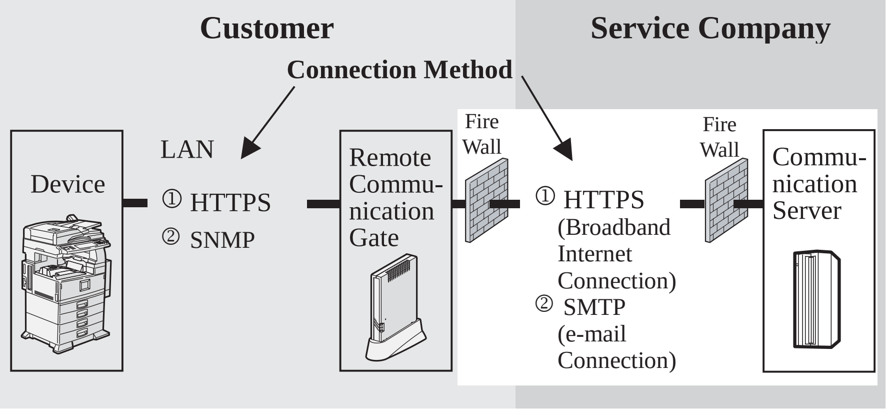
SMTP: Simple Mail Transfer Protocol

Remote Communication Gate checks the connection of target devices for control connected by the network and RS485 at specified time intervals.

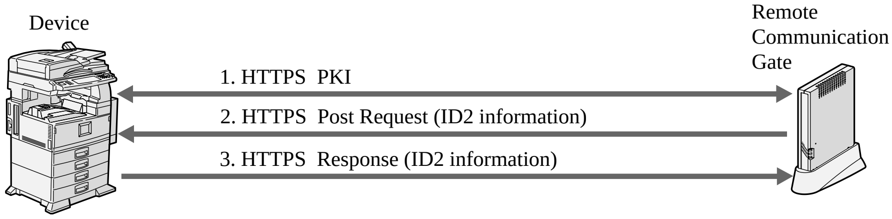
The check includes if communication exists or not, and if the serial number stored in Remote Communication Gate is identical with the serial number of the target devices for control.

3-1. HTTPS (Hyper Text Transfer Protocol Security)

I. When connected via HTTPS



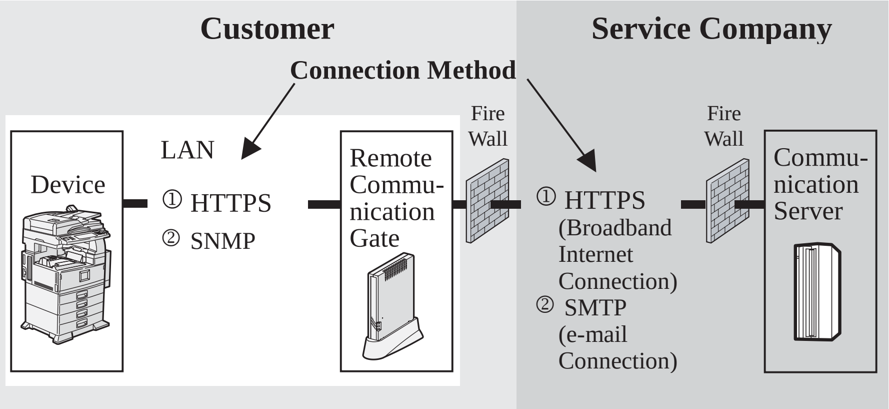
I. Access from Remote Communication Gate to devices


Device
Remote Communication Gate
1. HTTPS PKI
2. HTTPS Post Request (ID2 information)
3. HTTPS Response (ID2 information)

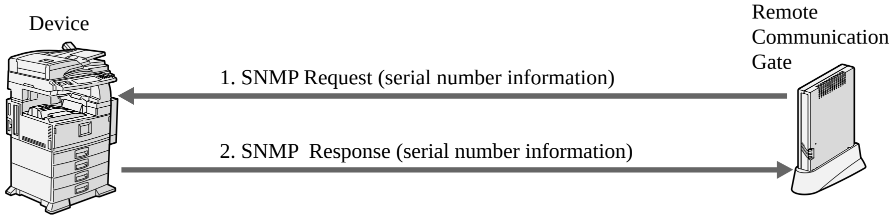
1. Mutual authentication.
2. ID2 request from Remote Communication Gate via HTTPS POST Request.
3. Devices send back ID2 via HTTPS Response.

3-2. SNMP

I. When connected via SNMP



I. Access from Remote Communication Gate to devices

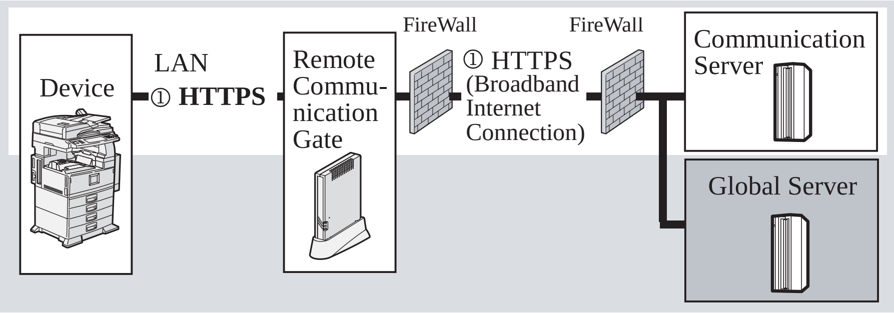

Device
Remote Communication Gate
1. SNMP Request (serial number information)
2. SNMP Response (serial number information)

Procedure

1. Serial number information request OIDs from the Remote Communication Gate via SNMP Request.(Ricoh machines acquire serial number, other companies' machines acquire MAC address.)
2. Devices send back serial number information via SNMP response.

4. Updating firmware

HTTPS only



Device
LAN
① HTTPS
Remote Commu-nication Gate
FireWall
① HTTPS (Broadband Internet Connection)
FireWall
Communication Server
Global Server

Above is an outline of behaviors when updating the firmware of devices

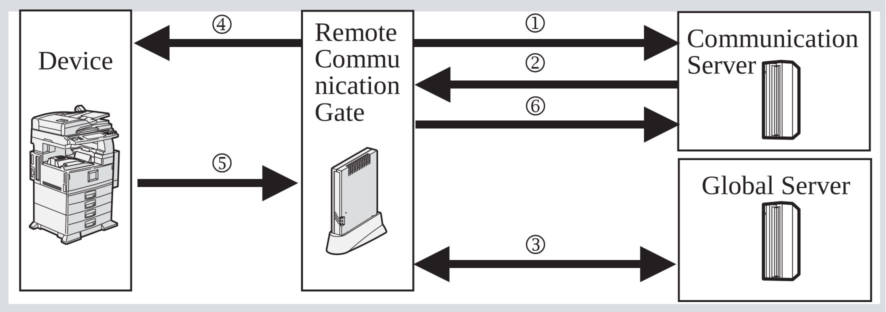
To update firmware of devices, the following equipment is used.

Communication server ； Equipment to specify the firmware version and the implementation date※to be updated.

Remote Communication Gate ； In response to the request from Communication server, it acquires firmware data from Global Server, and transfers the firmware to the Target device.

Global server ； Equipment to Store the firmware.

Device ； Target device for the firmware update.



※Time cannot be set for Firmware update of Remote Communication Gate.

※Device (e-g-MFP)firmware updates can be implemented at specified time (such as, out of working hours).

The firmware of devices is updated through communication from ① to ⑥ indicated in the diagram in the above. Individual communication is explained in the following.

① Remote Communication Gate initiates communication.

② Communication server requests Remote Communication Gate for the firmware update of target devices via HTTPS communication. (Target devices, date of update)

③ When the date of update is reached, Remote Communication Gate acquires the firmware data from Global Server via HTTPS.

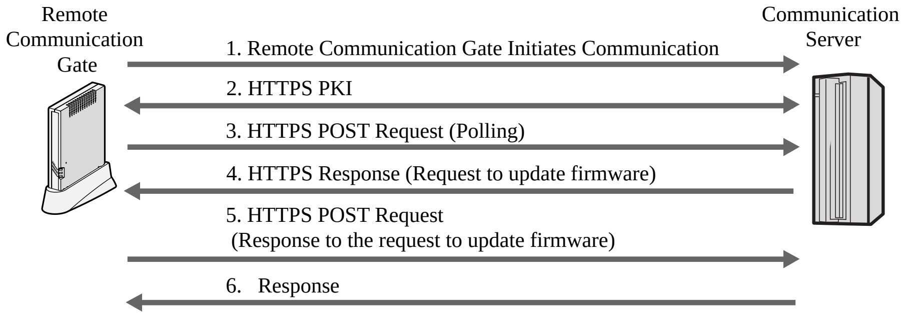
④ First, Remote Communication Gate sets up the Device ID and Password for FTP communication via HTTPS communication. Subsequently, the firmware date is sent to the Device via FTP communication.

⑤ The Device sends Remote Communication Gate a boot notification to automatically reboot after updating the firmware.

⑥ Remote Communication Gate notifies the result of the firmware update to the Communication server via HTTPS communication.

Details of the procedure ①②

Request to update the firmware of devices


Remote Communication Gate
Communication Server
1. Remote Communication Gate Initiates Communication
2. HTTPS PKI
3. HTTPS POST Request (Polling)
4. HTTPS Response (Request to update firmware)
5. HTTPS POST Request (Response to the request to update firmware)
6. Response

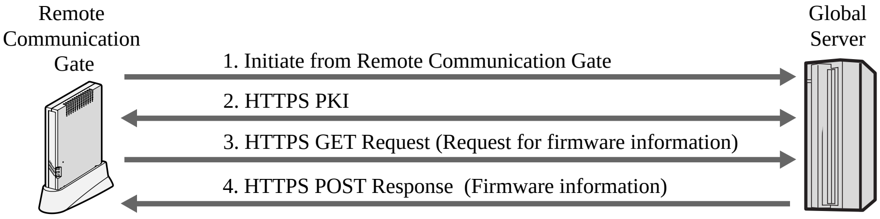
Procedure

1. Remote Communication Gate Initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends Polling to the Communication Server, via HTTPS POST Request.
4. The Communication Server confirms receipt of Polling by sending back the request to update firmware information via HTTPS Response.
5. The Remote Communication Gate sends response to the request to update firmware to the Communication Server, via HTTPS POST Request.
6. The Communication Server sends HTTPS Response.

*Communication between Remote Communication Gate and Communication Server is initiated only by the Remote Communication Gate.

Procedure of ③

Remote Communication Gate acquires the firmware date from Global server


Remote Communication Gate
Global Server
1. Initiate from Remote Communication Gate
2. HTTPS PKI
3. HTTPS GET Request (Request for firmware information)
4. HTTPS POST Response (Firmware information)

Procedure

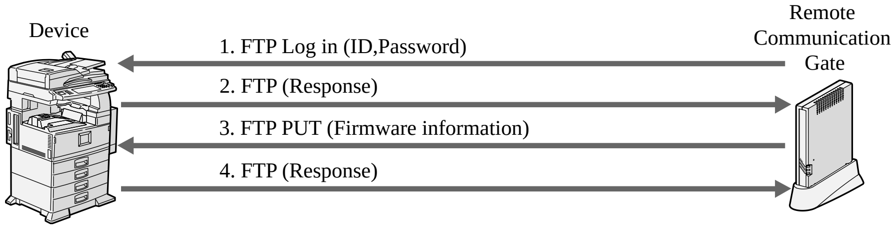
1. Remote Communication Gate initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends request for firmware information to the Global server, via HTTPS GET Request.
4. The Global server confirms receipt of request for firmware data by sending back the RESULT to the Remote Communication Gate, via HTTPS Response, and adds to this further firmware data request commands.

Since sending is not from the Communication Server through the customer firewall, it is not necessary to open a port for HTTPS reception from outside the customer firewall.

PKI: Public Key Infrastructure

Procedure of ④

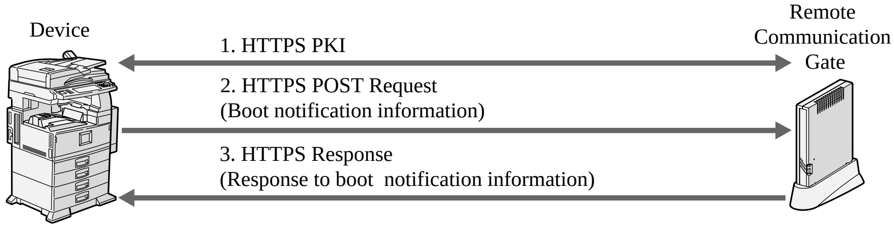
Access from Remote Communication Gate to devices


Device
Remote Communication Gate
1. FTP Log in (ID,Password)
2. FTP (Response)
3. FTP PUT (Firmware information)
4. FTP (Response)

1. Send ID and Password via FTP login.
2. Connection is made when ID and Password are correct.
3. Send firmware data to the Device via FTP.
4. Receive response if firmware data was received via FTP.

After receiving the firmware data, Device updates the firmware, and then automatically reboot.

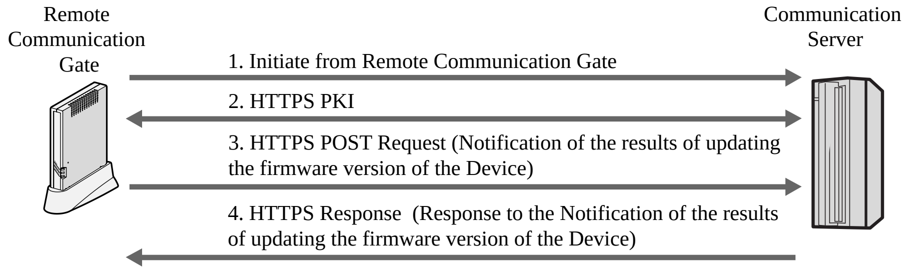
Procedure of ⑤


Device
Remote Communication Gate
1. HTTPS PKI
2. HTTPS POST Request
(Boot notification information)
3. HTTPS Response
(Response to boot notification information)

1. When there is a device alarm, the device initiates authentication via electronic certificate with the Remote Communication Gate.
2. Devices send boot notification information to the Remote Communication Gate by HTTPS POST Request.
3. The Remote Communication Gate confirms receipt of boot notification information by sending back the RESULT via HTTPS Response.

Procedure of ⑥

Remote Communication Gate notifies the result of the firmware update to communication Server.


Remote Communication Gate
Communication Server
1. Initiate from Remote Communication Gate
2. HTTPS PKI
3. HTTPS POST Request (Notification of the results of updating the firmware version of the Device)
4. HTTPS Response (Response to the Notification of the results of updating the firmware version of the Device)

Procedure

1. Remote Communication Gate initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends Notification of the results of updating the firmware version of the Device information to the Communication Server, via HTTPS POST Request.
4. The Communication Server confirms receipt of Response to the Notification of the results of updating the firmware version of the Device information by sending back the RESULT to the Remote Communication Gate, via HTTPS Response.

PKI: Public Key Infrastructure

5. AutoDiscovery

AutoDiscovery has the functions to automatically discover devices on customer’s network with which Remote Communication Gate is connected, and sends the discovered information of devices to Communication Server.

The notification is sent from Remote Communication Gate to Communication Server by selecting either via HTTPS system or E-mail.

Devices selected for auto discovery are specified by identifying selected network segments.

The following conditions can be set at Remote Communication Gate.

Execution interval	Set value	Note
Once per day	・Time : (0:00～23:59)	Example : 13:00
Once per week	・Day : (Sun～Sat.) ・Time : (0:00～23:59)	Example : 12:00, Sun.
Once per month	・Day of month : 1～28th ・Time : (0:00～23:59)	Example : 9:00, the 20th

The optimum method is set as the factory default which is once per day at 12 noon

* If the electrical power source is turned off or the device is not connected to the network at the meter reading time, no meter data will be obtained. As such, the factory default setting provides the greatest likelihood to obtain meter data for your devices each month.

Negligible Impact to Network Traffic

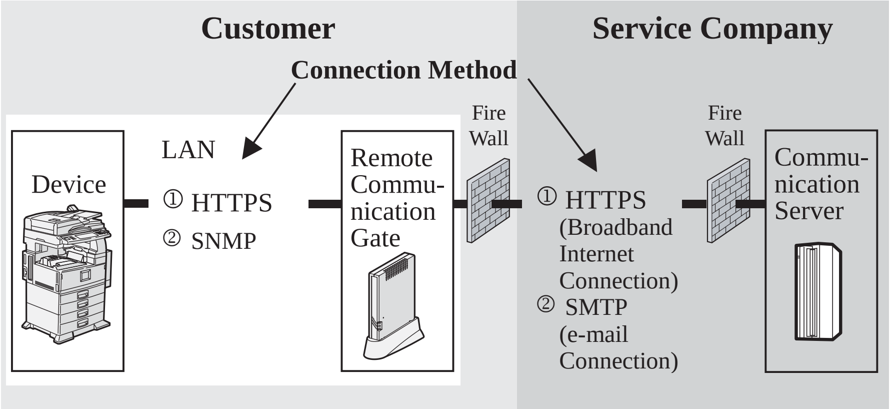
Traffic Size & Communication Timing (By Device Type & Purpose)			Between Device & RemoteCommunication Gate	Between Remote Communication Gate & Communication Server
SNMP Communication Device	Meter Data	Traffic Size	Approx. 4KB or less/ per Device	*Approx. 40KB or less/per Message
		Communication Timing	Daily/12:00 Noon Polling as default	Right after the device data is captured

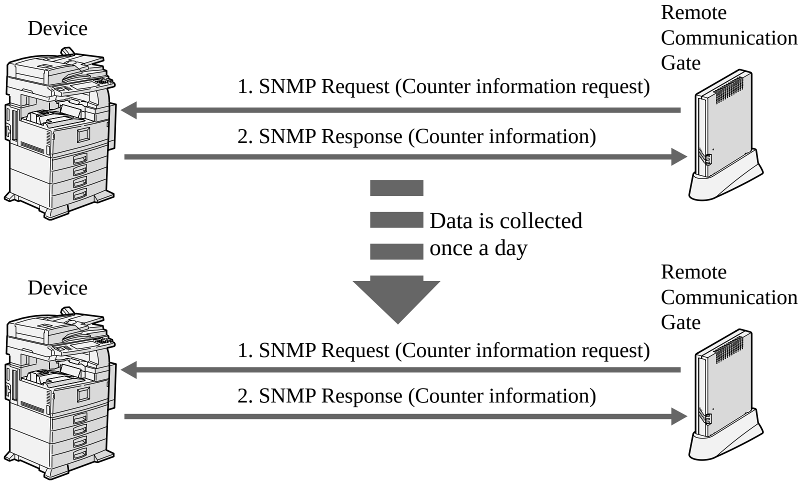
* The volume of 5 devices is sent together at once when sending it to Communication Gate.

Since the transmission is via SSL communication, the data size will be doubled.

5-1. SNMP

Device MIB information is obtained from periodic Remote Communication Gate to device polling.




Device
Remote Communication Gate
1. SNMP Request (Counter information request)
2. SNMP Response (Counter information)
Data is collected once a day
Device
Remote Communication Gate
1. SNMP Request (Counter information request)
2. SNMP Response (Counter information)

Procedure

1. Devices obtain counter information request OIDs from the Remote Communication Gate via SNMP Request.
2. Devices send back their counter and machine information via SNMP response.

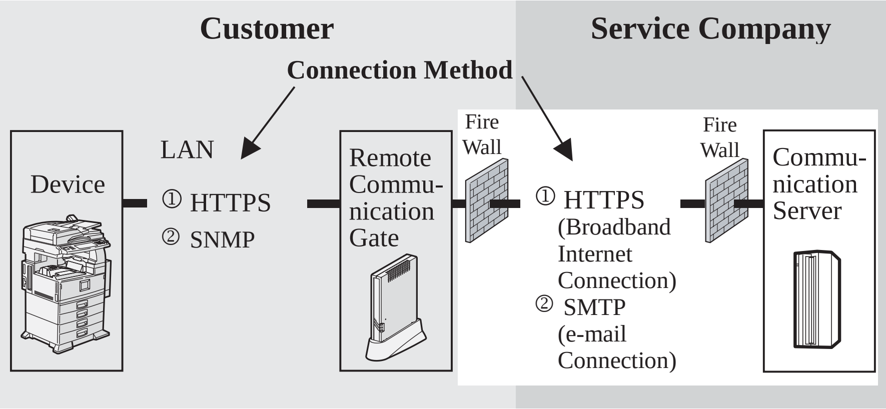
SNMP : Simple Network Management Protocol
OID : Object Identifier
MIB : Management Information Base

5-2. HTTPS (Brodband Internet Connection)

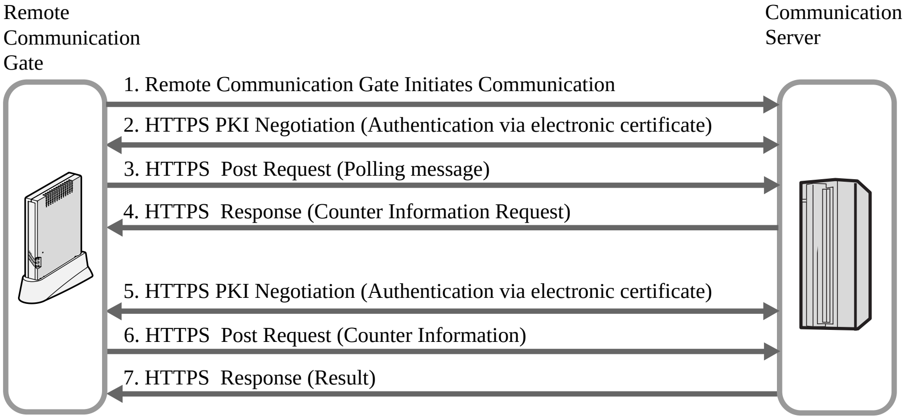
HTTPS has two methods of communication, explained here.

Autodiscovery

The information of devices acquired via SNMP is stored at Remote Communication Gate(RAM) temporarily, and then notified collectively by the following procedures for every 5 devices.



Autodiscovery



1. Remote Communication Gate Initiates Communication
2. HTTPS PKI Negotiation (Authentication via electronic certificate)
3. HTTPS Post Request (Polling message)
4. HTTPS Response (Counter Information Request)
5. HTTPS PKI Negotiation (Authentication via electronic certificate)
6. HTTPS Post Request (Counter Information)
7. HTTPS Response (Result)

Procedure

1. Remote Communication Gate initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends polling information to the Communication Server, via HTTPS POST Request.
4. The Communication Server confirms receipt of polling information by sending back the RESULT to the Remote Communication Gate, via HTTPS Response, and adds to this further Counter information request commands.
5. The Remote Communication Gate, when the Counter information request commands in the HTTPS Response are processed, responds to the Communication Server, after initializing mutual electronic certificate authentication.
6. The Remote Communication Gate sends its response to Counter information back to the Communication Server, via HTTPS POST Request.
7. The Communication Server confirms receipt of response by sending back the RESULT, via HTTPS Response.

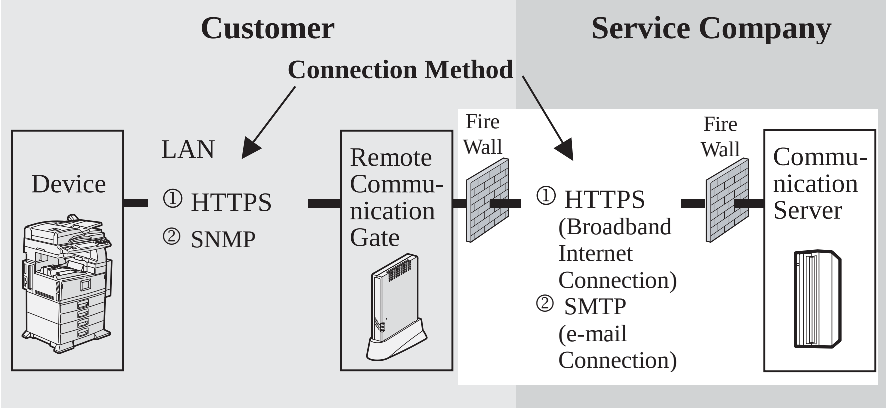
Since sending is not from the Communication Server through the customer firewall, it is not necessary to open a port for HTTPS reception from outside the customer firewall.

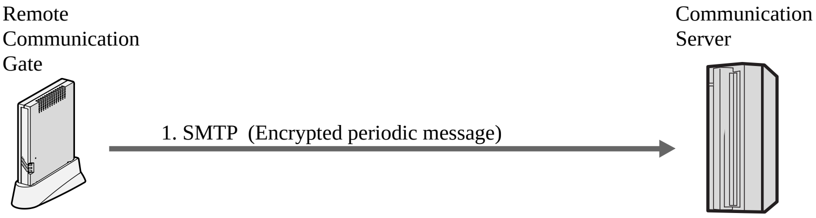
PKI: Public Key Infrastructure

5-3. SMTP (e-mail connection)

Autodiscovery

The information of devices acquired via SNMP is stored at Remote Communication Gate temporarily, and then sent when either maximum of 100 units or 1MB is reached according to the following procedure.




Remote Communication Gate
Communication Server
1. SMTP (Encrypted periodic message)

Procedure

1. The Remote Communication Gate sends device information to the Communication Server as an encrypted(S/MIME) E-mail attachment.

The Remote Communication Gate sends E-mail in only one direction;
E-mail from outside does not have Remote Communication Gate reception functions.

The Remote Communication Gate supports two type of SMTP authentication:

1. SMTP authentication
2. POP before SMTP authentication

SMTP: Simple Mail Transfer Protocol

Security Levels: Comparison Chart

	HTTPS		SMTP	
	Possible?	Because	Possible?	Because
Security Concern				
Attack from outside of customer network	NO	No HTTPS server.	NO	No SMTP server.
Customer data security- Unauthorized access Malicious data interference Illicit network monitoring	NO	All data is encrypted, and also sent to the specified address by mutual authentication.	NO	Only outbound E-mail is encrypted.

Appendix 1. Device Information (examples)

Any other counter than Device failure call, Controller/NICversion, Total counter cannot be acquired in the case of Auto Discovery.

Advantages	Information	Details
Reduces downtime	Alert	Device failure call (jam, cover open, etc.)
	Firmware	Controller/NIC version
Automated counter checking	Counter	Total/copier, fax, printer/black & white, color counter
Toner delivery	Supply	Toner end/near end
Device Monitoring	Device	Model name, vendor name, IP address, etc.

Appendix 2. Remote Communication Gate Basic Specifications

1. Hardware

No.	Hardware item	Specification	Comments
1	CPU	TX4925 XB-200	
2	ROM	4 MB (Flash ROM)	
3	RAM	64 MB (DRAM)	
4	SD Card	2 slot	Occupied with 32MB SD card in rear slot
5	NIC	10Base-T/100Base-TX 2 channel	
6	RS-485	Half-duplex serial port	
7	Battery	Lithium coin (attached to PCB）	Used by real-time clock
8	Indicators	Power indicator LED (green) Status indicators (2) LED（red, yellow）	
9	Expansion	PCMCIA card	
10	Power	AC (single phase), 50/60 Hz, 100-240 V	Depending on AC adapter
11	Maximum power consumption	20 W	
12	Dimensions & Weight	W 203 x D 145 x H 31.5 mm, 0.7 kg AC adapter: 0.6 k g	

2. Software

No.	Software item	Specification	Comments
1	Operating system	MontaVista Linux 2.1/MIPS (kernel 2.4.17)	
2	OpenSSL (Secure Socket Layer)	Open SSL (0.9.6 M)	
3	Web server	Apache (1.3.33)	

Appendix 3. @Remote Protocols and Open Ports.

1. Remote Communication Gate Port Usage and Communication Methodologies.

No	Occasion	Communication Direction	Port.No.	Protocol	Type
1	Remote Communication Gate is connecting to Device by FTP.	Remote Communication Gate => Device	20	FTP	TCP
2	Remote Communication Gate is sending firmware information.	Remote Communication Gate => Device	21	FTP	TCP
3	Remote Communication Gate is sending information by E-mail.	Remote Communication Gate => Communication Server	25	SMTP	TCP
4	Remote Communication Gate is capturing MIB information of device.	Remote Communication Gate => Device	161	SNMP	*UDP
5	Remote Communication Gate is authenticating in POP before SMTP.	Remote Communication Gate => POP Server	110	POP	TCP
6	Remote Communication Gate is sending notification to Communication Server via HTTPS.	Remote Communication Gate => Communication Server	443	HTTPS	TCP
	Device is sending notification such as Emergency Call.	Device => Remote Communication Gate			
	CE/Service Technician is operating Remote Communication Gate via laptop.	CE's Laptop => Remote Communication Gate			
	Remote Communication Gate is requesting firmware information.	Remote Communication Gate => Communication Server			
7	Remote Communication Gate is capturing device information.	Remote Communication Gate => Device	7443	HTTPS	TCP
8	Remote Communication Gate tries to communicate with device at the first time.	Remote Communication Gate => Device	7444	HTTPS	TCP

*UDP： User Datagram Protocol

2. Open Ports and Communication Methodologies

No	Communication type	Communication Direction	Port.No.	Protocol	Type
1	Device is sending notification such as Emergency Call.	Device => Remote Communication Gate	443	HTTPS	TCP
	CE/Service Technician is operating Remote Communication Gate via laptop.	CE's Laptop => Remote Communication Gate			

Appendix 4. Cryptographic algorithms of HTTPS

Figure 1 shows SSL negotiation with mutual authentication: client authentication and server authentication.

(1) The first step in the process is for the client to send the server “Client Hello” message. This hello message contains the SSL version and the cipher suites the client can talk and seed of random number. The client sends its maximum key length details at this time.
(2) The server returns the hello message with one of its own in which it nominates the version of SSL and the ciphers and key lengths to be used in the conversation, chosen from the choice offered in the client hello.
(3) The server sends its digital certificate to the client for inspection.
(4) The server sends client certificate request after sending its own certificate.
(5) The client verifies server certificate.
(6) The client sends its certificate.
(7) The client generates a pre master secret and encrypts it using the server's public key.
(8) The client sends pre master secret to the server.
(9) The client signs to data using client secret key.
(10) The client sends a Certificate verify message in which it encrypts a known piece of plaintext using its private key. The server uses the client certificate to decrypt; therefore ascertaining the client has the private key.
(11) The client generates session key with two seeds and pre master secret.
(12) The server verifies client certificate. The server decrypts pre master secret using server private key, and generates session key.
(13) The client now sends a “Finished” message using the new key to determine if the server is able to decrypt the message and the negotiation was successful.
(14) The server sends its own “Finished” message encrypted using the key. If the client can read this message then the negotiation is successfully completed.

Remote Communication Gate and Communication Server have 512 bits certificate; therefore RSA 512 bits cipher suite is used. Triple-DES Cipher (CBC mode) with 168 bits key is used for encryption (Remote Communication Gate (V3.34 or later)). When HTTPS method is selected, session key, i.e. encryption key for HTTPS, is created each and every time.

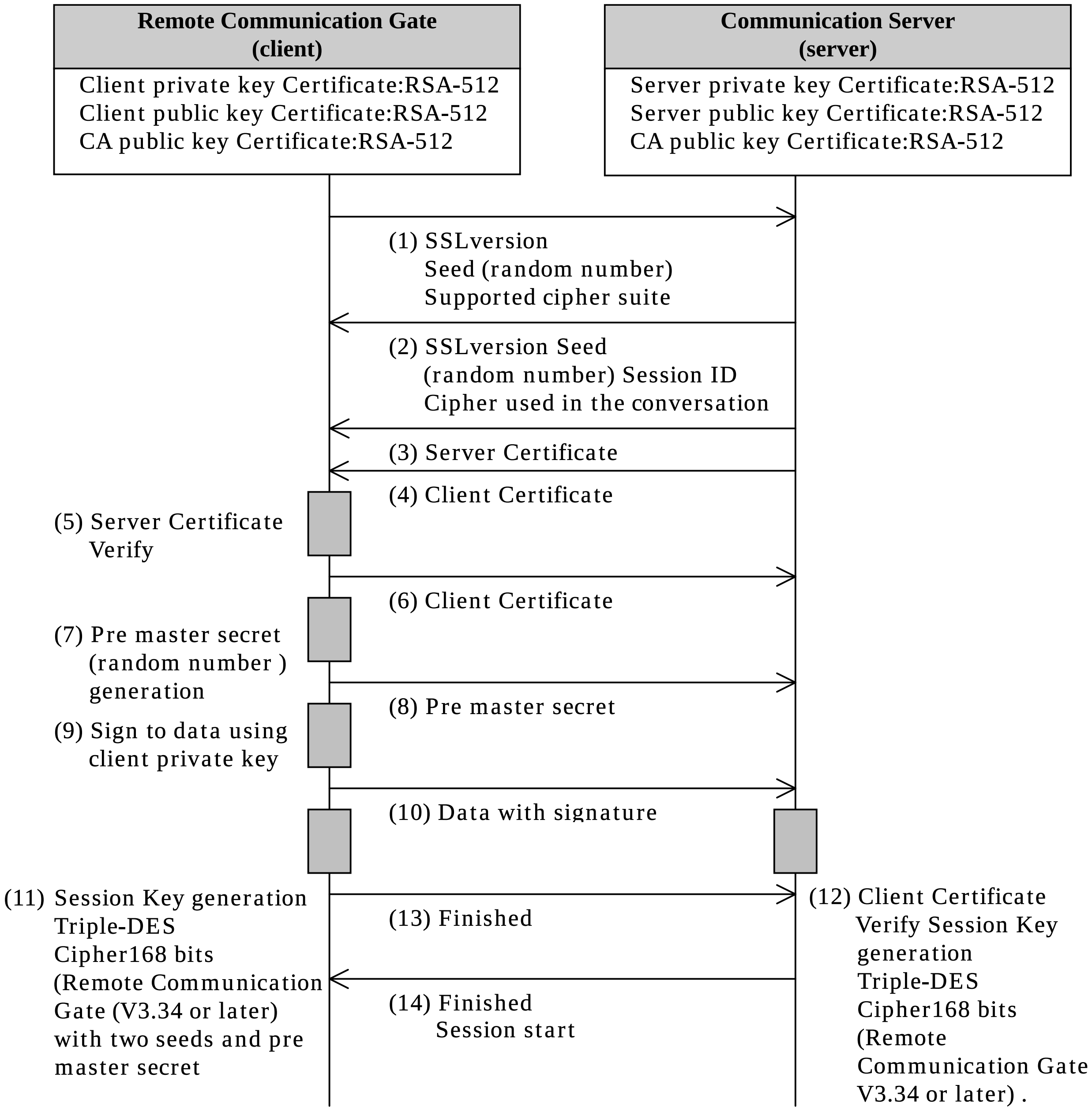

Remote Communication Gate (client)
Client private key Certificate:RSA-512
Client public key Certificate:RSA-512
CA public key Certificate:RSA-512
Communication Server (server)
Server private key Certificate:RSA-512
Server public key Certificate:RSA-512
CA public key Certificate:RSA-512
(1) SSLversion Seed (random number) Supported cipher suite
(2) SSLversion Seed (random number) Session ID Cipher used in the conversation
(3) Server Certificate
(4) Client Certificate
(5) Server Certificate Verify
(6) Client Certificate
(7) Pre master secret (random number) generation
(8) Pre master secret
(9) Sign to data using client private key
(10) Data with signature
(11) Session Key generation Triple-DES Cipher168 bits (Remote Communication Gate (V3.34 or later) with two seeds and pre master secret
(12) Client Certificate Verify Session Key generation Triple-DES Cipher168 bits (Remote Communication Gate V3.34 or later) .
(13) Finished
(14) Finished Session start

Figure 1: SSL Handshake Change Cipher Protocol

Appendix 5. Cryptographic algorithms of S/MIME

Figure 2 shows S/MIME formatted e-mail creation and transmission

(1) The client signs the original data with own private key (signature).
(2) The client creates master key using Triple-DES Cipher algorithm and encrypts it using the server's public key (pkcs7-data),
(3) The client sends it with S/MIME format (Base64) as E-mail.
(4) The mail is sent via Internet.
(5) The server received it as E-mail from SMTP server.
(6) The server decrypts it using the server private key.
(7) The server verifies it using the client public key.

Remote Communication Gate and Communication Server have 512 bits certificate; therefore RSA 512 bits cipher suite is used. Triple-DES Cipher (CBC mode) with 168 bits key is used for encryption (Remote Communication Gate (V3.34 or later)). When SMTP method of Remote Communication Gate is selected, master key, i.e. encryption key for S/MIME, is created each and every time too.

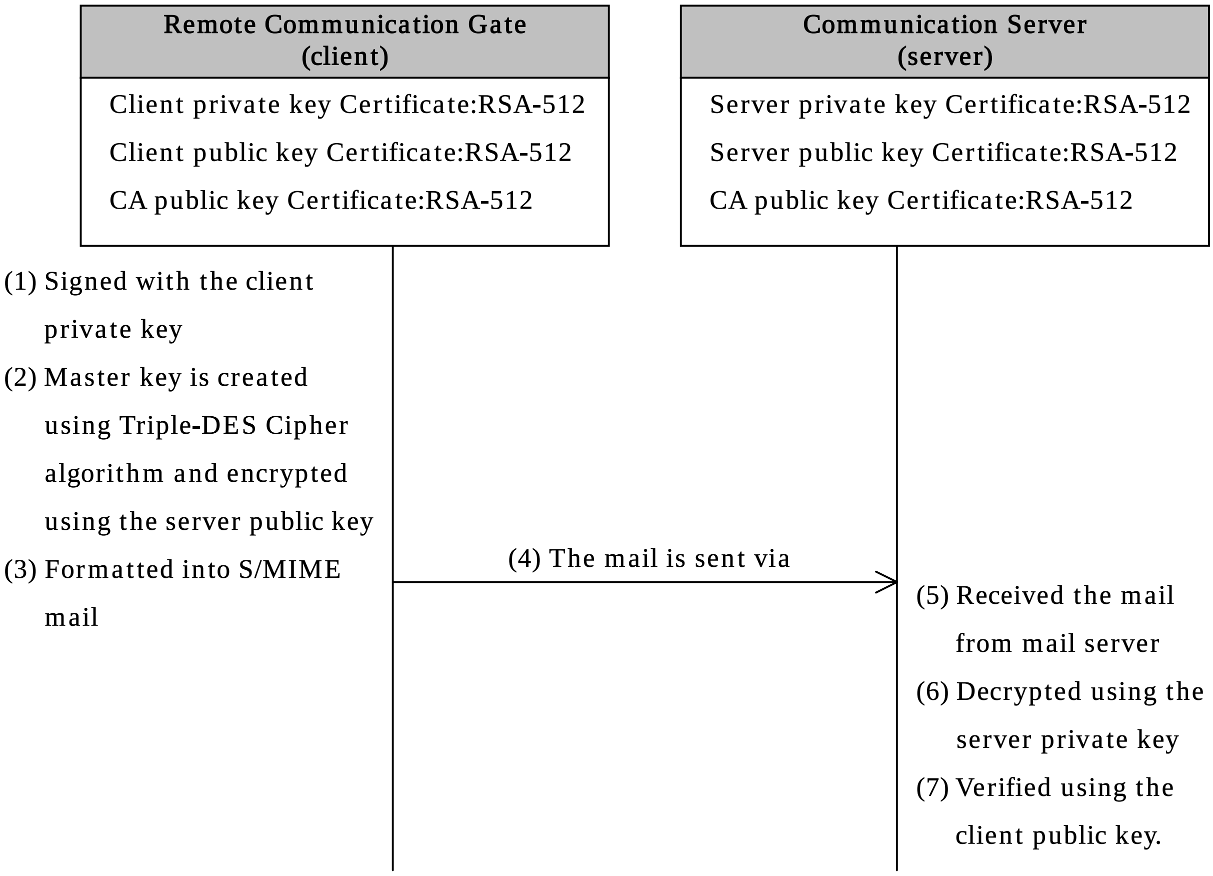

Remote Communication Gate (client)
Client private key Certificate:RSA-512
Client public key Certificate:RSA-512
CA public key Certificate:RSA-512
Communication Server (server)
Server private key Certificate:RSA-512
Server public key Certificate:RSA-512
CA public key Certificate:RSA-512
(1) Signed with the client private key
(2) Master key is created using Triple-DES Cipher algorithm and encrypted using the server public key
(3) Formatted into S/MIME mail
(4) The mail is sent via
(5) Received the mail from mail server
(6) Decrypted using the server private key
(7) Verified using the client public key.

Figure 2: S/MIME sending and receiving sequence

Appendix 6. Network Traffic & Communication Timing

Traffic Size & Communication Timing (By Device Type & Purpose)			Between Device & Remote Communication Gate	Between Remote Communication Gate & communication Server
SNMP Communication Device	Meter Data	Traffic Size	Approx. 4KB or less/per Device	Approx. 80KB or less/per Message (depending on the # of Devices)
		Communication Timing	Every 12 Hours Polling as default	Monthly (on the Meter Reading Due Date)/13:00-15:00 Local Time
	Failure/ Supply Call	Traffic Size	Approx. 4KB/per Device	Approx. 8KB/per Device
		Communication Timing	Every 10 minutes Polling as default	Real Time (Right After Failure Call / Supply Call is captured)
	Device Connection Check when Disconnected	Traffic Size	Approx. 1KB/per Disconnected Device	
		Communication Timing	Search for the Disconnected Device Every 6 Hours	
HTTPS Communication Device	Meter Data	Traffic Size	Approx. 160KB/per Device	Approx. 1.5MB or less/per Message (depending on the # of Devices)
		Communication Timing	Every 12 Hours Polling as default	Daily at Random Timing
	Serive Call/ Supply Call	Traffic Size	Approx. 100KB/per Device	Approx. 100KB/per Device
		Communication Timing	Real Time	Real Time
	Firmware Upgrade	Traffic Size	Ave. 6MB (Max. 16MB)/per Firmware	Ave. 6MB (Max. 16MB)/per Firmware
		Communication Timing	Specified Date & Time	Specified Date & Time
	Device Connection Check when Disconnected	Traffic Size	Approx. 1KB/per Disconnected Device	
		Communication Timing	Search for the Disconnected Device Every 6 Hours	

Questions and Answers

Q1. Should the Remote Communication Gate be installed in a special location?

A. The Remote Communication Gate does not require any specific location. Install it where you would normal office equipment.

Q2. Does the Remote Communication Gate emit noise or odor?

A. There is no internal fan so no noise is emitted. No chemicals are used inside the Remote Communication Gate so no odor is produced

Q3. The Remote Communication Gate has three sockets (apart from the power socket), what are these and how are they different?

A. One is for serial connection, and the other two are for the network. The network sockets are the same, but one is for service technician use only, the other is for connecting to the user network (LAN).*

* There are two types of Remote Communication Gate: network and modem. The above applies to the network type.

Q4. How are Remote Communication Gate settings protected?

A. Access is user name and password protected.

Q5. Should power to the Remote Communication Gate normally be left on? What about power to devices?

A. Leave the power supply on, so the Remote Communication Gate can collect device data at the times specified during setup. Also, because it should remain connected, the Remote Communication Gate has no power switch.
Make sure main power switches on devices are on (a device's status cannot be read if its main power is switched to off).

Q6. What action is to be taken in the event of a power outage?

A. Keep the Remote Communication Gate plugged in（it will recover itself automatically）.

Q7. **How can I turn off the Remote Communication Gate?**

A. First, press the “Shut Down “ button on the Remote Communication Gate UI, and then pull the Plug out.

Q8. **What happens to data in the Remote Communication Gate if there is a power outage?**

A. When Remote Communication Gate power is lost during device to Remote Communication Gate / Remote Communication Gate to Communication Server communication:

Data in communication is lost. However, the Remote Communication Gate’s SD card backs up data once an hour – backed up data remains stored.

When the power is back on, incompletely sent data, due to power outage (including that not stored on the SD card), is automatically resent

Q9. **Does the Remote Communication Gate require any supplies or additional replacement parts over time?**

A. No.

Q10. Is data that is sent out over the Internet secure?

A. Yes – because it is transmitted in SSL protocol, after both ends verify each other’s identity, and only to the address specified at setup. Also, for further security, the data itself is encrypted (encryption level is at Triple DES 168bits. Remote Communication Gate (V3.34 or later). between device and Remote Communication Gate/Remote Communication Gate and the Communication Server).

Communication between Remote Communication Gate and the Communication Server uses the form initiated by the Remote Communication Gate.

* Communication is never initiated from the Communication Server.

Q11. What kind of data is received from the Communication Server?

A. When the Communication Server requires device information it sends a request (status sense) for it.

Also, if a device encounters problems, the Communication Gate sends the latest firmware to help it recover.

Q12. How is the firewall passed from the Communication Server?

A. Initiation is from the Remote Communication Gate:

To go through the firewall, the Communication Server must send necessary information in reply to the signals sent regularly from the Remote Communication Gate (frequency specified at setup).

* Communication does not come from the Communication Server.

Q13. Can viruses enter the user network when communicating over the Internet?

A. No - because communication occurs only within the limits of Remote Communication Gate and the Communication Server.

Also, the data (virus checks are carried out before sending) is sent in SSL protocol after mutual authentication.

Q14. How many devices can the Remote Communication Gate Manage?

A.

*Internet encryption communication (HTTPS) Method
Managed devices registered to the Communication Server
100 devices (including a maximum of 5 devices connected to the RS-485 interface)

Auto Discovery
500 devices (including those registered to the Communication Server on the Network)

*E-mail (SMTP) Method
Auto Discovery
500 devices

Q15. What about traffic size on the user network and its communication timing?

A. Traffic size and its communication timing will differ depending on the installation mode, or communication data type. Please refer to Appendix 6 for the detailed traffic size and its communication timing.

Q16. Is there any chance to obtain customer's server or client PC's information via Remote Communication Gate?

A. No. Information of customer's server or client PC is never obtained via Remote Communication Gate.

Q17. Does it support TokenRing environment?

A. No, it doesn’t.