@ Remote

Intelligent Remote Management System
for the Ricoh Family Group Network Connected Printing Devices

White Paper
(Embedded Type)

Version. 1.00

June.15th,2006

Update History

Version	Release

@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.
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 two related enhancements:

*IT equipment maintenance

accident and breakage recovery
toner supply – ordering and delivering

*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 three 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

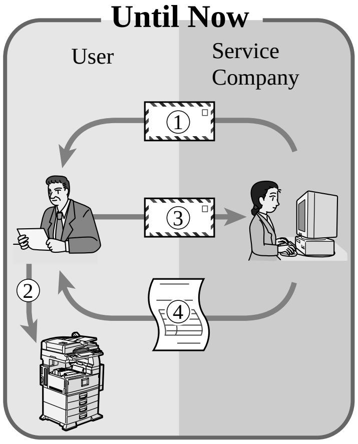
Device downtime is reduced through remote maintenance. Specifically, remote maintenance cuts downtime by sending service calls automatically to our service technician.
Also, these services are only made possible through connection to the Internet. This means users can operate without worrying about incomplete 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:

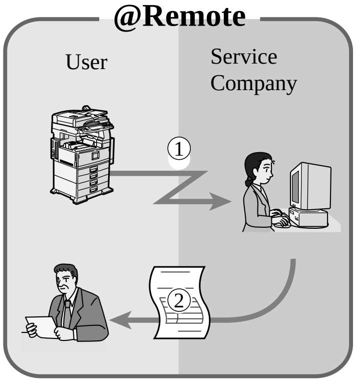


① The service company requests the user to check the counter (s).

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.



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.

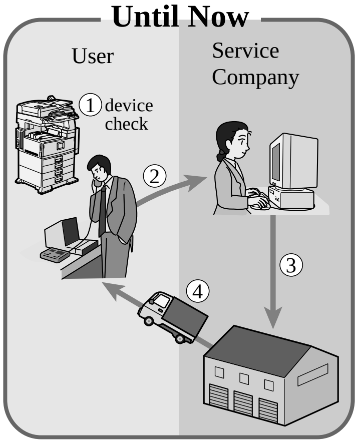
② The service company sends a bill back to the user.

@Remote offers an improvement in the form of remote, automated counter checking.
User workload is reduced.

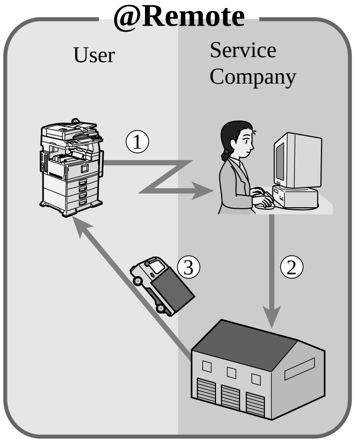
3. Supply level (toner, staples) monitoring is continuous - reporting is automatic when toner reaches 'near end'.

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.

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 Ricoh Family Group devices automatically.

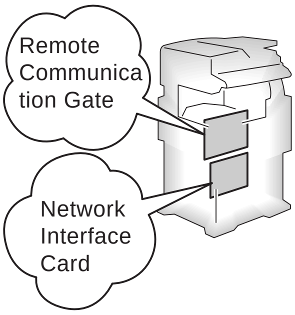
HTTPS is a web server and client (browser) protocol for sending and receiving data: HTTP + SSL (Secure Socket Layer). For privacy and information security, data between browser and server is encrypted - hence widely used in Internet shopping.

Communication Methods and Information Security

1. What Embedded Type is

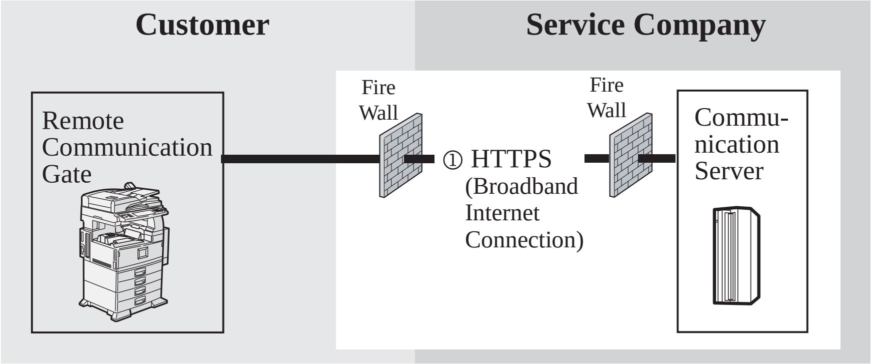
*It houses within itself a module which notifies equipment information to the device.

HTTPS (Broadband Internet Connection)



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

1. HTTPS (Hyper Text Transfer Protocol Security)
 -Broadband Internet Connection.


Customer
Service Company
Remote Communication Gate
Fire Wall
① HTTPS (Broadband Internet Connection)
Fire Wall
Commu-nication Server

About HTTPS

1. Data is encrypted AES (Advanced Encryption Standard) 256bits.
2. Both Remote Communication Gate and Communication Server use security authentication checks.
3. For each communication, a mutual verification procedure is completed before the data is sent.

3. HTTPS (Broadband Internet Connection)

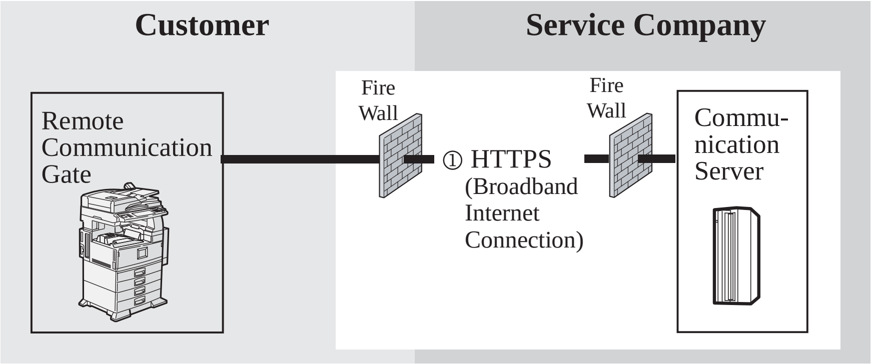
Listed below are the two reasons for HTTPS communication initiation.

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

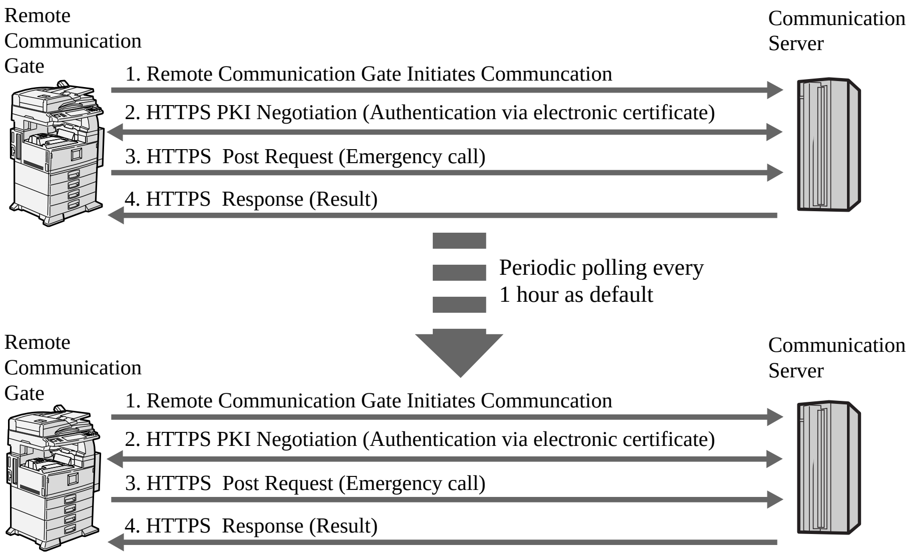
- Sending from the Remote Communication Gate

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

- Handling Communication Server requests by initiation from Remote Communication Gate


Customer
Service Company
Remote Communication Gate
Fire Wall
① HTTPS (Broadband Internet Connection)
Fire Wall
Commu-nication Server

I. Emergency Call


Remote Communication Gate
Communication Server
1. Remote Communication Gate Initiates Communcation
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 Communcation
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.

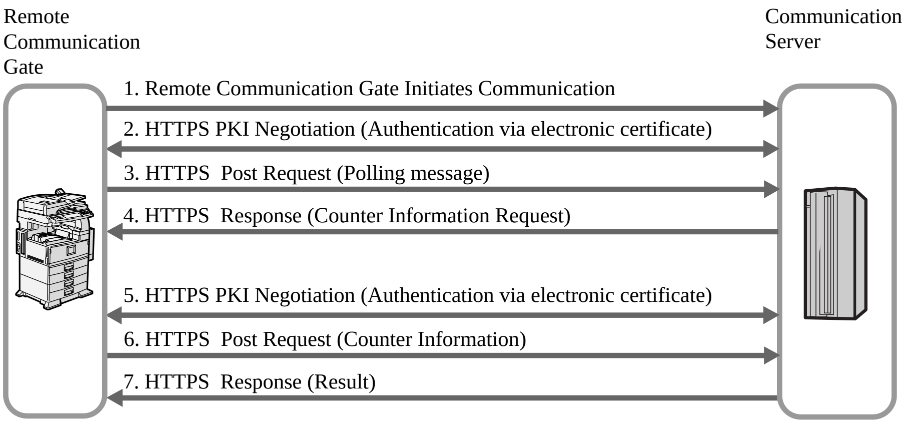
*Communication between Remote Communication Gate and Communication Server is initiated only by the Remote Communication Gate.

*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.

PKI: Public Key Infrastructure

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

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

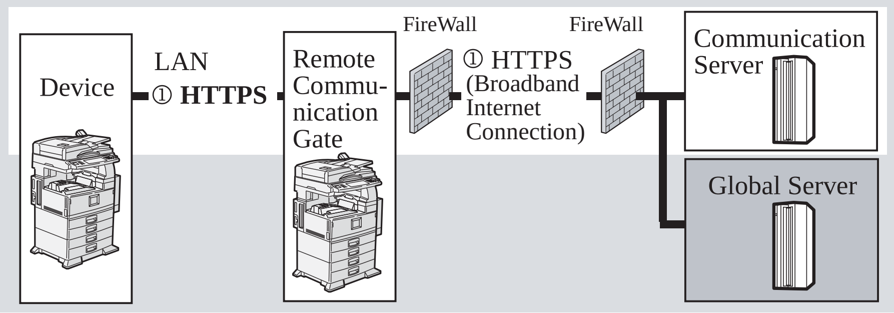
1. Remote Communication Gate Initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Communication Server.
3. The Remote Communication Gate sends polling information to the Communication Server, via HTTPS POST Request.
4. The Communication 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.

Firmware update

1. Updating firmware

HTTPS only


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

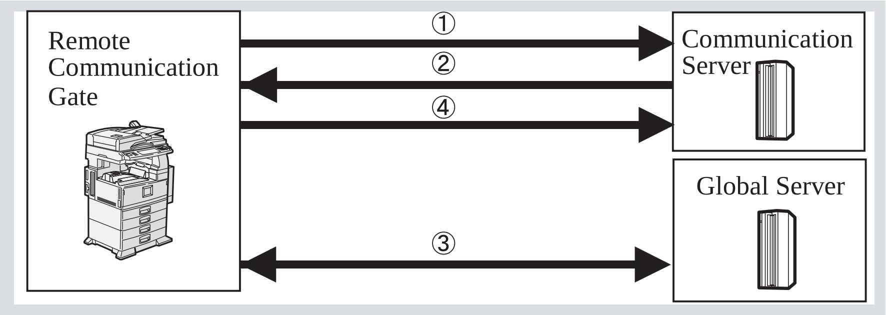
Above is an outline of behaviors when updating the firmware of devices

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..



※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 ④ indicated in the diagram in the above. Individual communication is explained in the following.

① Remote Communication Gate initiates communication.

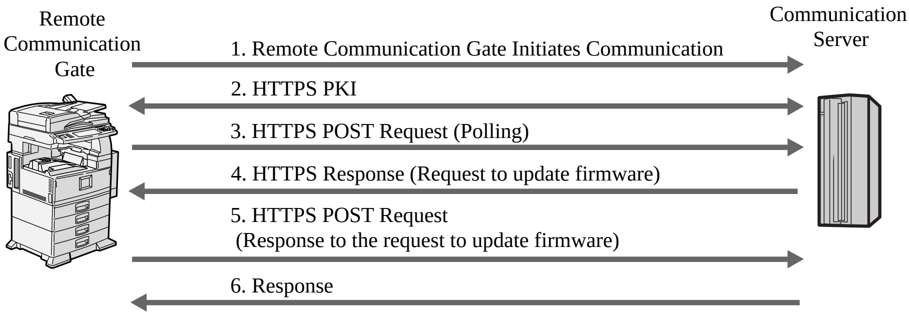
② Communication server requests Remote Communication Gate for the firmware update of target devices via HTTPS communication. (Target devices, date of update)

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

④ 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

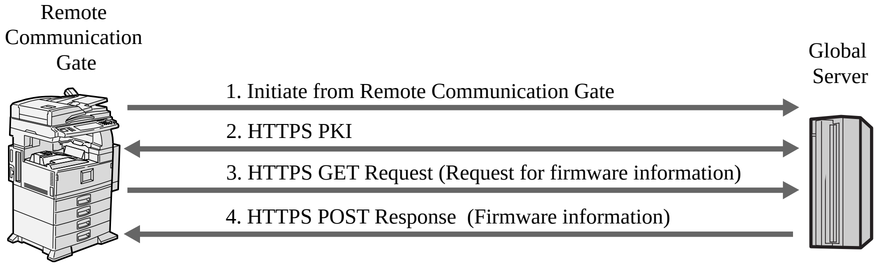
Procedure

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

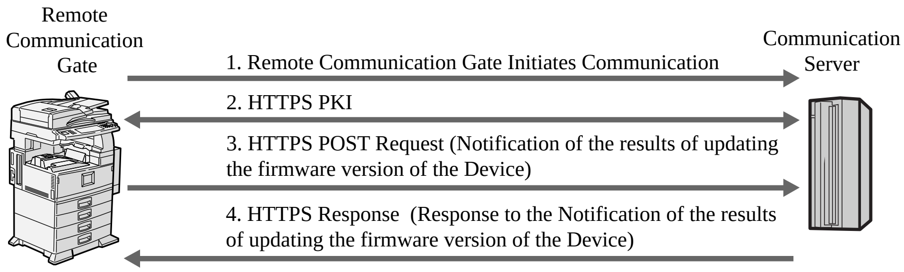
1. Remote Communication Gate initiates Communication.
2. Mutual authentication via electronic certificate takes place between Remote Communication Gate and Global Server.
3. The Remote Communication Gate sends request for firmware information to the Global server, via HTTPS GET Request.
4. The Global 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

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


Remote Communication Gate
Communication Server
1. Remote Communication Gate Initiates Communication
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

Appendix 1. Device Information (examples)

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

Appendix 2. Remote Communication Gate(Embedded Type)Encryption Library

1. Software

No.	Software item	Specification	Comments
1	Open SSL (Secure Socket Layer)	Open SSL (0.9.7D)	

Appendix 3. @Remote Protocols and Open Ports.

Remote Communication Gate Use Ports and Occasion

No	Occasion	Communication Direction	Port No	Protocol	Type
1	Remote Communication Gate (Embedded Type) is sending information by E-mail.	Remote Communication Gate (Embedded Type) =>IT Administrator	25	SMTP	TCP
2	Remote Communication Gate (Embedded Type) is authenticating in POP before SMTP.	Remote Communication Gate (Embedded Type) => POP Server	110	POP	TCP
3	Remote Communication Gate (Embedded Type) is sending notification to Communication Server via HTTPS.	Remote Communication Gate (Embedded Type) => Communication Server	443	HTTPS	TCP
	Remote Communication Gate (Embedded Type) is requesting firmware information.	Remote Communication Gate (Embedded Type) => Communication Server			

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. AES (Advanced Encryption Standard) with 256 bits key is used for encryption. When HTTPS method is selected, session key, i.e. encryption key for HTTPS, is created each and every time.

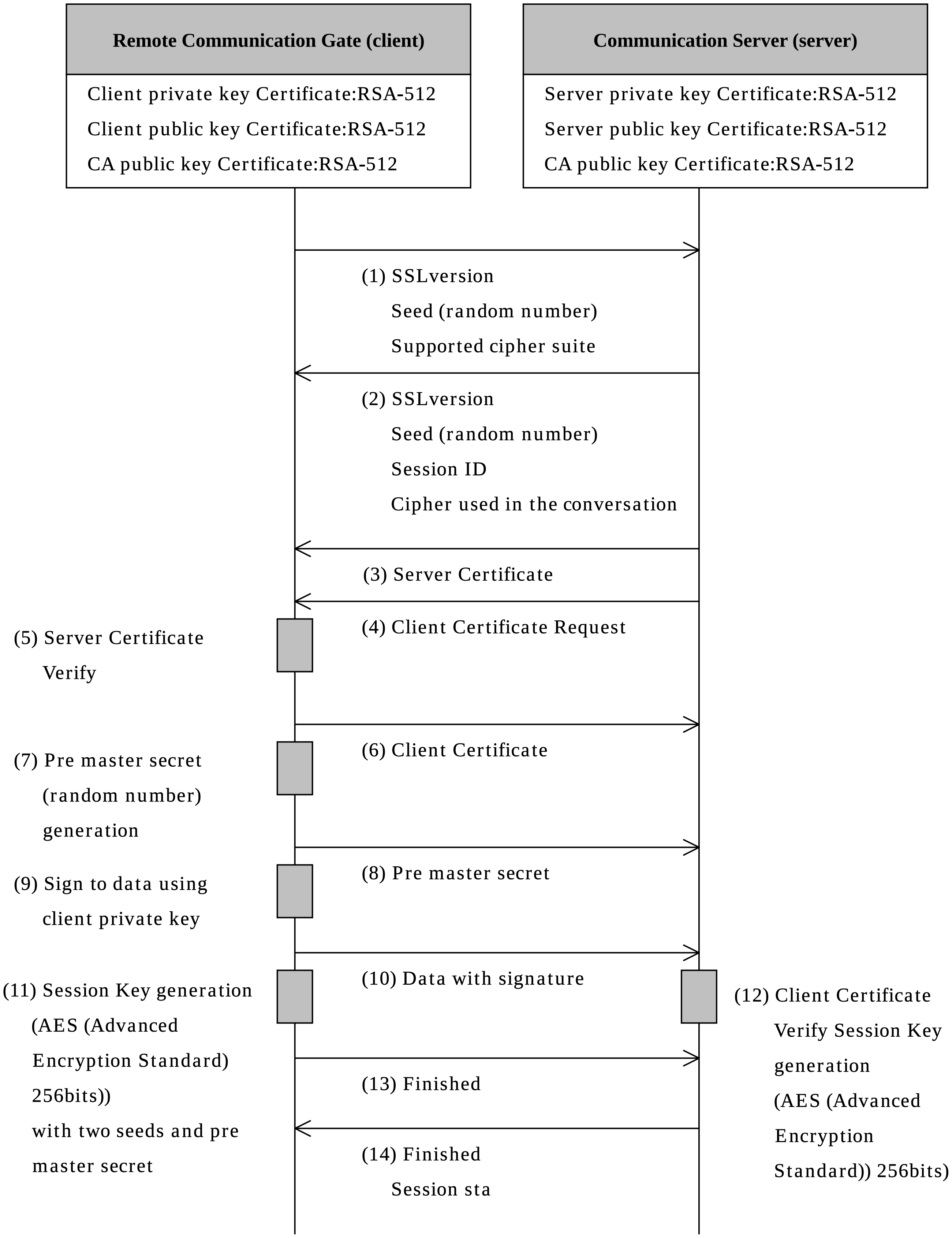


Figure 1: SSL Handshake Change Cipher Protocol

Appendix 5. Network Traffic & Communication Timing

Traffic Size & Communication Timing (By Purpose)		**Remote Communication Gate & Communication Server**
Meter Data	Traffic Size	Approx. 160KB
	Communication Timing	Daily at Random Timing
Serive Call / Supply Call	Traffic Size	Approx. 100KB
	Communication Timing	Real Time
Firmware Upgrade	Traffic Size	Ave. 6MB (Max. 16MB)/per Firmware
	Communication Timing	Specified Date & Time

* When the power of device is off at the timing of communication on the Meter Data, its Data will be sent to Communication Server as soon as the power is turn on

Questions and Answers

Q1. 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 (AES (Advanced Encryption Standard)256bits).

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.

Q2. 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.

Q3. 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.

Q4. 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.

Q5. What about traffic on the user network and its communication timing?

A. Traffic size and its communication timing will differ depending on the communication data type.

Please refer to Appendix 5 for the detailed traffic size and its communication timing.

Q6. Does it support TokenRing environment?

A. No, it doesn't.