Canon

imageWARE

Remote

Technology/Security Whitepaper

IMPORTANT NOTICE

This document was created based on the latest technical information available at the time of its publishing. This information is subject to change without notice.

Table of Contents:

1. Overview

About this Whitepaper

This document is intended for IT administrators who would like to study the security features, system architecture and network impact of Canon L.A.'s imageWARE Remote service.

About imageWARE Remote

imageWARE Remote is a service developed by Canon Inc. that is being made available to Canon L.A.'s dealers and service providers, enabling them to provide better service to their customers.

imageWARE Remote consists of two components: imageWARE Remote Meter Reading (collects meter reads automatically from enabled imageRUNNER devices) and imageWARE Remote Service Monitor (provides information about device status, error notifications and statistics about parts lifetime and consumables). Both services use the same underlying technology - eRDS (**e**mbedded **R**emote **D**iagnostic **S**ystem), to capture device information and transmit such information to a server managed by Canon Inc. via the Internet, where it is accessible by the service provider via a web interface (the Canon Inc. **U**niversal **G**ate**w**ay or "**UGW"**).

The eRDS solution does not require any additional hardware or software since the solution is already embedded within the imageRUNNER device.

Once activated, eRDS will submit both meter readings and service information to the UGW. However, depending on the business model selected by the Service Provider, the UGW will allow for access of meter reading only (imageWARE Remote Meter Reading) or both meter reading and service information will be made available (imageWARE Remote Service Monitor).

Supported Devices

eRDS

All Canon imageRUNNER devices, from the 70 Series and later, are supported. This includes the entire imageRUNNER ADVANCE line. The embedded RDS technology is already available on these devices and needs to be activated in service mode to start working. At the time of imageWARE Remote launch, Canon imageRUNNER 30 Series devices will only support eRDS if they are equipped with a Canon Multi-PDL printer board.

For a list of supported models, please contact our service department via phone or e-mail (latam_oetech@cusa.canon.com) directly to obtain the most current information regarding imageWARE Remote.

2. Embedded RDS Overview

What is eRDS? Canon's imageRUNNER series devices ship equipped with embedded Remote Diagnostic System (eRDS) capability.

eRDS is a technology that allows the imageRUNNER devices to connect directly to the Universal Gateway Server (UGW) for the purpose of collecting counter, jam, error, and alarm data in order to improve the level of customer support and service that Canon service providers can offer to their customers. eRDS provides the following benefits:

Automatic Meter Reading

eRDS captures and provides meter data automatically via the network to the UGW, reducing the need for manual collection of meter readings by the customer and reporting them to the service provider for billing purpose.

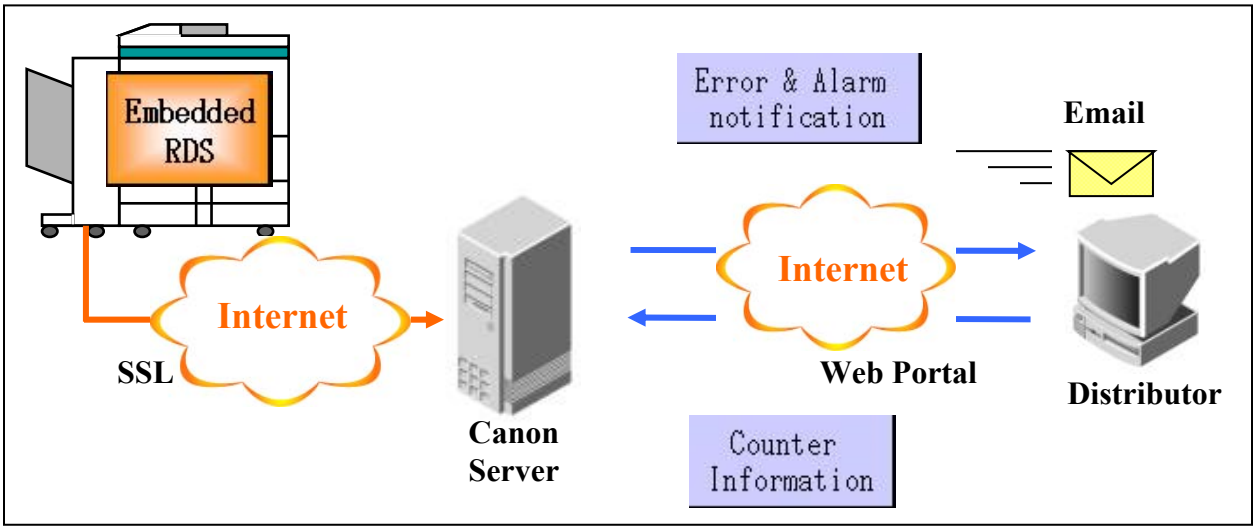
Enhanced Service Offering

Automatic error, jam, and alarm notifications can be used to improve service provider's response time.

Usage Statistics, Parts Lifetime and Consumables Management

As part of the imageWARE Remote Service Monitor feature, service providers have access to information on parts usage of customers' registered imageRUNNER devices. This can be used to offer pre-emptive service to the customer, before consumable and durable parts reach the end of their expected life cycle. In addition, information about toner usage allows the service provider to make suggestions about re-ordering or stock quantities.

eRDS Architecture



This simplified figure shows the architecture of the eRDS system.

The eRDS system on the device pushes the data out via secure SSL connection to the UGW server (push process)

Once the data is on the UGW server:

- Meter readings are available on the UGW server for download by the service provider (pull process).
- Error/jam/alarm notifications can be sent directly to the service provider by e-mail upon occurrence (push process).
- The service provider can also log onto UGW to obtain information on any error/jam/alarm notification (pull process).

3. eRDS Network Security

LAN

Communication Target and Protocol

The eRDS communicates only with the UGW and is unable to communicate with other devices that are connected to a customer's Local Area Network.

Communication between UGW Server and eRDS Devices

Communication Target

The eRDS enabled imageRUNNER communicates only with the UGW when sending device information. The authentication method is described later.

Communication Protocol

The eRDS enabled imageRUNNER communicates with the UGW by using the HTTPS protocol. The eRDS enabled imageRUNNER acts as the "Client", and will never become a HTTP server for the purposes of eRDS communication. Please note that some imageRUNNERs may act as a HTTP server for other non-eRDS related features.

Data to be collected and forwarded

The data to be collected by eRDS and forwarded to UGW is shown in Table 1. The eRDS enabled imageRUNNER sends the data shown in Table 1 to the UGW at the specified timing.

In the "regular counter transmission", the maximum size of the transmitted data package is about 250 KB. This transmission occurs only once every 16 hours.

Table 1

Data to be sent	Description	Timing to send	Amount of data
Error data	Includes the error code, error subcode, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	When an error occurs	4 KB
Jam data	Includes the jam code, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	When a jam occurs	4 KB
Alarm data	Includes the alarm level, alarm code, alarm subcode, date of occurrence, and total counter at	When an alarm occurs	4 KB

	occurrence.		
Status data	The data when a status change occurs.	When status change occurs	4 KB
Billing counter data	The counter data typically used for billing, such as Total, Copy, Print, B/W, and Color.	Every 16 hours	Approx. 250 KB (Billing counter: 62 KB, Detailed counter: 42 KB, Parts counter: 33 KB, Mode counter: 111 KB)
Detailed Counter data	The detailed counter data for each paper size such as Total, B/W, and Color.		
Parts counter data	The counter data indicating the amount of usage by part. The number of parts varies by model.		
Mode Counter data	The counter data by operation mode. The number of modes varies by model.	Every 7 days	
ROM version data	The ROM version data of Main, Scan, Print, Feeder, Finisher, Fax, PDL, and Tray.	Every 7 days	Approx. 5 KB
Debug log data	The log data output by an application for analyzing a malfunction.	When the size of the debug log reaches a specified size.(512KB)	13.5 KB
Environment log data	Environment log data of the device (e.g. temperature, humidity)	The data is sent once every twelve hours.	Approx. 6 KB

The transmission start time is determined by UGW based on the return value of the communication test.

Data Encryption

From eRDS to the UGW server, data is encrypted at the transport layer though a SSL connection, which is typically used to secure connections over the Internet. Therefore the data does not need to be encrypted at the application layer.
The key length used in the HTTPS communications are as follows:

Public Key length : 1024bit
Symmetric Key length : 128bit

eRDS activation

eRDS is integrated in the main unit firmware of the imageRUNNER device. In order to enable eRDS, the setting must be activated from service mode, therefore a user cannot accidentally activate the option.

Authentication Procedures

Server Authentication

The UGW uses SSL Authentication together with application authentication. The eRDS function will not transmit information to servers other than the UGW using these methods.

1) SSL Authentication
SSL Authentication is performed according to the following procedures. Please note the following steps describe the SSL protocol and are not specific to Canon's eRDS technology.

- "Root Certificates" published by Verisign are installed in an imageRUNNER when it ships from the factory.
- When the eRDS enabled imageRUNNER starts communicating, eRDS will receive the "Server Certificate" published by Verisign from the UGW by HTTPS.
- The eRDS device compares the "Server Certificates" with the "Root Certificates".
- If these certificates match, the eRDS device successfully authenticates the other communicating party as the UGW server.
- The encryption method is negotiated using HTTPS, afterwards, HTTPS communications begin and the data is encrypted

2) Application level authentication
Application-level authentication further secures the eRDS communication between the imageRUNNER and the UGW.
The URL of the UGW Server is pre-populated into the firmware of the imageRUNNER.
Service personnel can change this URL. However, the firmware will only attempt a transmission if the domain name of the URL is in the UGW's DNS domain.

In the event that a user changes the URL to something outside of the UGW DNS domain, the imageRUNNER will not transmit any data.

Client Authentication

This section describes the client authentication used by the UGW.

1) Client authentication by SSL (OSI Layer 4 to 5)
Client authentication by SSL is not performed.

2) Client authentication by application (OSI Layer 7)
The UGW will receive information only from devices whose serial numbers have been registered on the UGW by the service provider. Prior to registration on the Universal Gateway, a communication test needs to be performed on the imageRUNNER, establishing communication between the UGW and the device.
Reverse engineering is impossible because of SSL encryption and the use of the Canon proprietary Simple Object Access Protocol ("SOAP") schema communication protocol. Therefore, a rogue client cannot be developed.

4. General Considerations

Customer Requirements

Network Connection

In order for the eRDS to work effectively, a continuous network connection is necessary. If the network connection is lost temporarily or permanently, the functions of imageWARE Remote (Meter Reading and Service Monitor) will not be available, resulting in the delayed reporting of meter reads. Additionally, service notifications will not be transmitted in a timely manner, jeopardizing the benefits of the Service Monitor feature.

Network Traffic

Although the data packages sent from the eRDS enabled imageRUNNER are very small, IT administrators will most likely note increased network traffic due to the communications between the eRDS unit and the UGW.

In addition, the hard coded URL of the UGW may become the most frequently addressed URL within the organization. This is due to the scheduled and event-related communications between eRDS and the Canon server. To ensure uninterrupted performance of the imageWARE Remote services, it is important that this URL remains unchanged and will not be blocked.

Power

Power outages or device shutdowns by employees will result in an interruption of data transmission. No meter information can be transmitted to the UGW if the device is off. Upon return of power, the eRDS will start communicating with the UGW server again.

Image Data

The eRDS is not capable of sending or receiving image data. The types of data collected and submitted by the eRDS function are described in “Network Security”, Table 1.

Failures

After network failures or power outages, eRDS will automatically start communicating with the Canon server once the situation is corrected. Execution of another “communication test” is not required.

Data Storage Time

UGW

Meter data will be stored in the Universal Gateway database for 12 months, however only the most recent meter data is accessible for download from the Web Portal by the service provider.

Service information/statistics are currently stored for 6 months. This storage time may be modified in the future.