# IS/IN/IX Series Network Security Data Sheet

## Quadient Mailing System Specification

# Network Security Data Sheet IS/IN/IX

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

## Table des matières

# IS/IN/IX Series Network Security Data Sheet

## 1°) IS/IN/IX MAILING SYSTEMS (MS) PORTS USED

| Application | Ports Used | Protocol |
|---|---|---|
| **Funding Server & OLS** | **53,80,443** | **TCP** |
| EMS / ARM / MAS* | 5353<br>7000 | UDP for discovery TCP for connection |
| **Default Proxy Connection** | **8080** | **TCP** |
| iMeter PC Link (for 280 only) | 8088/8888 | TCP |
| **neoShip** | **SRC (MS): Random DST (PC): 5506** | **UDP** |

*Optional external applications that run on a PC

**NOTE : All local ports are closed until the MS initiates a call**

## 2°) PROTOCOL USED

| Protocol / Application | Information |
|---|---|
| **Cipher Suite** | **DHE_RSA_AES128_SHA1 (TLS 1.0)<br>DHE-RSA-WITH-AES-128-CBC-SHA256 (TLS 1.2)<br>ECDHE-RSA-AES128-GCM-SHA256 (TLS1.2, SMART)** |
| SSL | Uses TLS 1.0 *Mutual Authentication* & X.509 (extensible) self- signed certificates (**1.2 deployed on all the IX range (or by using the ConnectBox device) – 1.3 possible only by using the ConnectBox device**) |
| **DHCP** | **Dynamic and Static configurations on TCP/IP V4.0 (not compatible with V6.0)** |
| DNS | Dynamic and Static configurations (port 53) |
| **Proxy** | **NTLM V1.0 in transparent proxy mode with basic authentication – does not support NTLM V2.0 or Kerberos** |
| NIC Speeds | IS/IM280 \| IS/IM5000-6000 = 10/100Mb/s<br>IN/IS/IM300 \| IN/IS/IM400-700 = 10Mb/s only<br>IX-3/5/7= 10/100Mb/s |
| **MAC OUI** | **00:1B:00 for Quadient Technologies** |

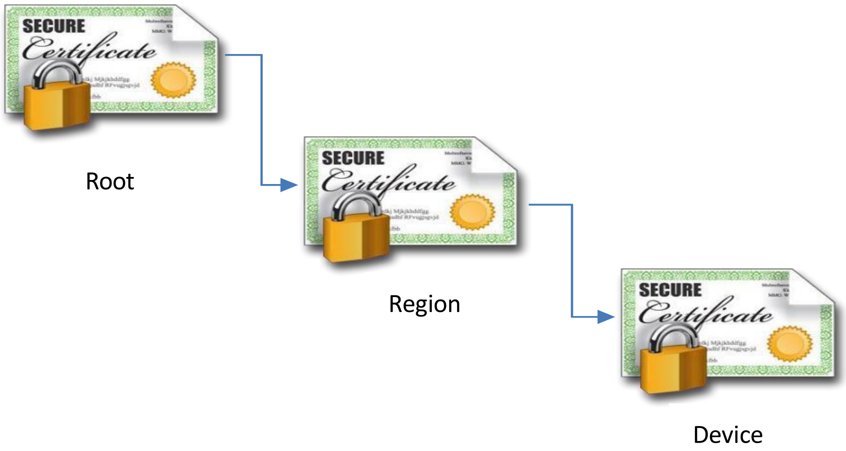
# IS/IN/IX Series Network Security Data Sheet

## RESTRICTIONS

Does not contain a browser
Cannot load 3rd party applications
Cannot integrate any type of *client/server* application
Does not support SNMP, SSH or any other remote management
Does not support 802.1x
Does not support RDP or any type of remote login
Does not support SSL/HTTPS inspection (on firewall)
**If URL Filtering is used (on firewall) an exception or bypass rule may be required (on firewall)**

## 3°) METER/SERVER COMMUNICATION

Quadient maintains its own 3-tier certificate system that enables our meters to connect to our Infrastructure. Since we only communicate with our meters and our meters only communicate with our infrastructure, there is no need for a 3rd party certificate.



The Mailing Systems connect to our Infrastructure using TLS Mutual Authentication. Therefore, our server will not accept any device posing as one of our systems. Further, the mailing systems will not honor any “rogue” servers posing as our infrastructure.

Note : Since our server and mailing system do not accept other certificates, SSL inspection cannot be used to monitor encrypted traffic. The mailing systems would see it as a main-in-the-middle attack and disconnect.

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

### 3.1 °) Data exchanged with Postal and Quadient Servers (Once a month)

Statistics for Post
Ink Level Management
Backup customer data
Diagnostic information for Technical Support
Updates for myquadient on-line reports

### 3.2 °) Manual Calls from mailing system (E-services)

**Ping Server**: is a TCP connect to the Quadient server. It is similar to a Standard call (exchange key with the secure server and then close the connection). When the TCP connect is made, an encrypted tunnel (*TLS V1.0 & TLS V1.2 deployed in some countries*) is created to the Quadient server.

**Test server**: same as Ping server with an exchange of data (less than 1Mb), to ensure the quality of the transaction.

**Standard call**: normal user connection method to our server to download slogan, rate, software update or upload diagnostics, statistics, *MyQuadient* and ink level information.

**System Synchronization**: same as Standard call.

### 3.3 °) Duration of call

Between 1-10 minutes (depending on customer network)

## 4°) MAILING SYSTEM OS

The Mailing Systems (MS) use two proprietary versions (locked) of operating system software:

| Model | Windows CE 5.0 | Linux |
|---|---|---|
| IS/IM 280 | ✓ | |
| IS/IM 330/350 | ✓ | |
| IS/IM 400 series | ✓ | |
| IS/IM 5000/6000 | ✓ | |
| IN-360/600/700/750* | ✓ | ✓ |
| IX-3/5/7 series | | ✓ |
| IX-9 series | | ✓ |

**Systems after July 2017 arrive with a Linux board*

Both operating systems *do not* allow any third-party software to be loaded. Any drivers must be signed and incorporated into a software release by Quadient R&D. All software updates are in a special format that cannot be read by any other computer or software. New software is only released by Quadient through our service organization.

IX machines are running a proprietary Operating System based on Linux which uses its own TCP/IP implementation.

## 5°) ADDITIONAL THINGS THE OS SOFTWARE WILL NOT DO

Does *not* connect to or embed an email client or server
Does *not* include or allow a web server or browser
Does *not* offer access to the BIOS
Does *not* offer access to a command prompt, root directory or registry
Will *not* download or propagate a virus or worm
Is *not* susceptible to a **man-in-the-middle attack** due to TLS protocol

## 6°) TLS VULNERABILITIES & MITIGATIONS

### 6.1 °) POODLE Attack SVE-2014-3566

The POODLE attack or 'Padding Oracle On Downgraded Legacy Encryption' is a vulnerability for TLS 1.0 using web browsers and web servers. The vulnerability requires the use of cipher-block chaining mode (CBC) and SSL 3.0 between the target device (PC with web browser) and the web server.

The attack complexity is high and requires the attacker to have some control over the web browser. Further, they have to establish an effective man-in-the-middle (MITM) exploit. In addition, multiple failed connection attempts have to be sent to the server to 'downgrade' to SSL 3.0 (or lower).

**Mitigation**

***First***, the Quadient Spine server does not offer the ability to downgrade to any SSL protocol.

***Second***, our mailing systems/server do not use RC4 in the cypher suite.

***Third***, our mailing systems do not have a web browser and will not allow any third-party devices/sites to connect.

***Lastly***, our server and the mailing system use mutual authentication – this prevents a MITM attack.

### 6.2 °) BEAST Attack SVE-2011-3389

The Beast attack is a client-side SSL attack that uses a Man-in-the-middle (MITM) attack to decrypt HTTPS (SSL) sessions using browser components such as JavaScript, HTML5 Websocket API, Java URLConnection API, or the Silverlight WebClient API.

**Mitigation**

***First***, our mailing systems do not have a web browser and will not allow any third-party devices/sites to connect. Further, neither JavaScript nor any Web API can be run on the mailing systems.

***Lastly***, our server and the mailing system use mutual authentication – this prevents a MITM attack.

### 6.3 °) Ripple 20

A new set of vulnerabilities, known as **Ripple 20**, have been discovered by the JSOF laboratory. These zero-day vulnerabilities affect a low-level TCP/IP software library developed by Treck, Inc and used in a large variety of IOT devices.

***Our range of connected Franking Machines, IS, IN, IX, does not use this library.***

- IS/IN machines are running a proprietary Operating System based on Windows CE which uses its own TCP/IP implementation.
- IX machines are running a proprietary Operating System based on Linux which uses its own TCP/IP implementation.
- Postal Secure Devices or meters inside the Franking Machines do not communicate directly with the outside world and use the TCP/IP capabilities of the Franking Machines in which they are installed in.
- Our “Connect by Quadient” box is running a proprietary Operating System based on Linux which uses its own TCP/IP implementation.

Given these facts, our machines are not vulnerable to the attacks targeted at the Treck, Inc library.

### 6.4 °) DUKH

In the last few days, Quadient Postal Secure Devices have been cited in a number of communications regarding a new vulnerability, known as the DUHK Attack.

The origin of this vulnerability resides in the Random Number Generator (RNG) used by the Postal Secure Devices (PSD) or meters, the ANSI X9.31 RNG, and its seed key. An attacker who would acquire the seed and a direct output of the RNG could discover the key elements of the algorithm and simulate its processes, allowing him to generate all the random

numbers, past and future, of the RNG. It is thus imperative that the seed remains secret. The attack is based on the fact that some hardware manufacturers would simply hard-code the seed key in the device firmware, which could be downloaded and disassembled.
Based on the https://duhkattack.com/ site, a device is vulnerable if 4 conditions are met:

- It uses the X9.31 RNG;
- The seed key is hard-coded into the firmware;
- It uses the output of the RNG to generate cryptographic keys;
- Some of the generated random numbers are used unencrypted in a transmission (case of the handshake in SSL/TLS).

Since the beginning of the IJ and IS projects, our Postal Secure Devices or meters, up to version 28 included, use the ANSI X9.31 RNG. However, since the beginning, the seed used by our meters has never been hard-coded into the firmware of the devices. The seed is generated by an outside system (a computer called the manufacturing server) at the factory, in a secure environment,  using its own Random Number Generator. This RNG comes from a FIPS module (certificate 313) in the Microsoft .Net Framework 2.0.
The security code of the Manufacturing Server can be traced up to 2007 and has not been modified since. The first versions of our meters in the USA date back to 2008.

Moreover, the seed is stored inside the cryptographic memory of the meter. This memory is protected, both by software and hardware, against tampering, as described in our Security policy:

| | | | |
|---|---|---|---|
| **RNG (ANSI X9.31)** | **Key generation; with 16 bytes seed/seed key (externally generated by FIPS validated module and imported into the PSD in secure factory environment); based on AES 128 as transition function** | **[AES-128 Key]** | **1217** |
| **Algorithm/Key size(s) required per Postal Authority/Postal Standard: United States Postal Service** | | | |

| Name | Algorithm/Key Size | Description/Usage | Generation | Storage | Distribution | Zeroization |
|---|---|---|---|---|---|---|
| **Common CSPs (independent of country configuration)** | | | | | | |
| Master Secret Key | AES CBC 128 bits | Internally encrypt & decrypt PSD's critical security parameters | Internally ANSI X9.31 RNG | In plaintext tamper protected memory | N/A | - Invocation of "Zeroize CSPs" service<br>- breach of flex circuit triggers "Zeroize CSPs" service.<br>- PSD temperature over 84°C triggers "Zeroize CSPs" service (EFP measure)<br>- Failure of a self-test triggers "Zeroize CSPs" service |
| RNG Seed | ANSI X9.31<br>128 bits | Current status of the seed used by the Approved RNG. | N/A | In plaintext tamper protected memory | Entered in factory | |
| RNG Key | ANSI X9.31 AES 128 bits | Key used by the Approved RNG underlying encryption algorithm | N/A | In plaintext tamper protected memory | Entered in factory | |
| TLS Communication Private Key | RSA PKCS # 1 v1.5 2048 bits | Authenticates messages and data output from the PSD during TLS Handshake Protocol | Internally ANSI X9.31 RNG | Encrypted | N/A | Rendered unusable by zeroization of "Master Secret" |

In case of an intrusion in the meter, the memory is entirely erased and the seed is lost.

The attack being based on the presence of a hard-coded seed in the device firmware, **our Postal Secure Devices or meters are not subject to the DUHK vulnerability**.

The next generation of meters (version 30 for IMI postal specification) will not be concerned by the vulnerability. The ANSI X9.31 RNG has been replaced by the AES based CTR DRBG as recommended by the NIST SP800-90A specification.

### 6.5 °) Spectre Meltdown

Following the recent findings on potential exploits using processor speculative execution (known as Spectre and Meltdown, referenced CVE-2017-5753, CVE-2017-5715 and CVE-2017-5754), here are the latest information regarding our range of connected Franking Machines.

The current range of IS/IN machines uses either a Samsung S3C2410 processor or an Atmel A91SAM9260, both based on the Arm 9 architecture. Based on information provided by Arm, this generation of architecture **is NOT vulnerable to any these exploits.**

The upcoming range of machines, the IX range running on a Quadient-specific OS based on Linux, uses an Altera Cyclone V, based on the Arm Cortex-A9 architecture. According to Arm, this generation is potentially vulnerable to CVE-2017-5753 and CVE-2017-5715 (Spectre) but **is NOT vulnerable to CVE-2017-5754** (Meltdown).

However, in order to exploit the Spectre vulnerability, an attacker must be able to execute his own code on the Franking Machine, which is strictly made impossible by design:

- Quadient machines can only execute authenticated programs which come directly from the Quadient server;
- Communication between the Franking machine and the Quadient server is protected using TLS security protocols (1.0 or 1.2, depending on the current Postal requirements) with both encryption and mutual authentication;
- The programs themselves are signed and authenticated by Quadient private PKI.

Based on these information, **it is impossible to exploit any of these vulnerabilities on our range, current or upcoming, of Franking Machines.**

### 6.6 °) Apache Log4j vulnerability

A serious alarming and easily exploitable Security Vulnerability was made public on *Thursday, December 09th 2021*.
Called "**Log4Shell**", it concerns a tool massively used in applications and web services and can allow to execute remote code on a targeted server.

**WHAT IS Log4j?** In this case, Log4j is a library in the Java language that is used to record the activity (the "logs") of an application. It can be used, for example, to make sure that a program is working properly and, if not, to note in a file error reports each time a part of the code has a problem.

**WHAT IS THE ISSUE WITH Log4j?** it is possible to ask the application to take code from another server and execute it and in the worst case, "this vulnerability allows to take full control of the server as an administrator".

**→The Apache Foundation released a patch on Friday December 10th, 2021 to fix the vulnerability←**

Since the alert, we have made all necessary verifications and implemented corrective patches made available to ensure the integrity of our systems. Please be aware that **we have not identified any risk of this event impacting our production services or any customer data entrusted to us.**

Based on these information, our solutions **MAS**, **OLS** and **Postalcore** are not impacted by this vulnerability. **It is impossible to exploit any of these vulnerabilities on our range, current or upcoming, of Franking Machines**. Because none of our embedded software runs JAVA, Apache or log4j.

We are committed to bringing you the most up to date information to keep you secure

## 7°) TLS STATUS & CONNECTBOX (LINK0 BOX) INTRODUCTION

All Alpha / Delta & Rodin machines (IS / IN range) are communicating using TLS 1.0 with the corresponding spine(s) available in each country.

All machines from the Zenith (IX-3, IX-5 & IX-7) & Nova (IX-9) ranges are communicating using TLS 1.2 with the corresponding spine(s) available in each country if the Zenith/Nova ranges have been launched in the corresponding country.

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

Version 1.6 IPSS © 2023 Quadient. All rights reserved.
p. 12

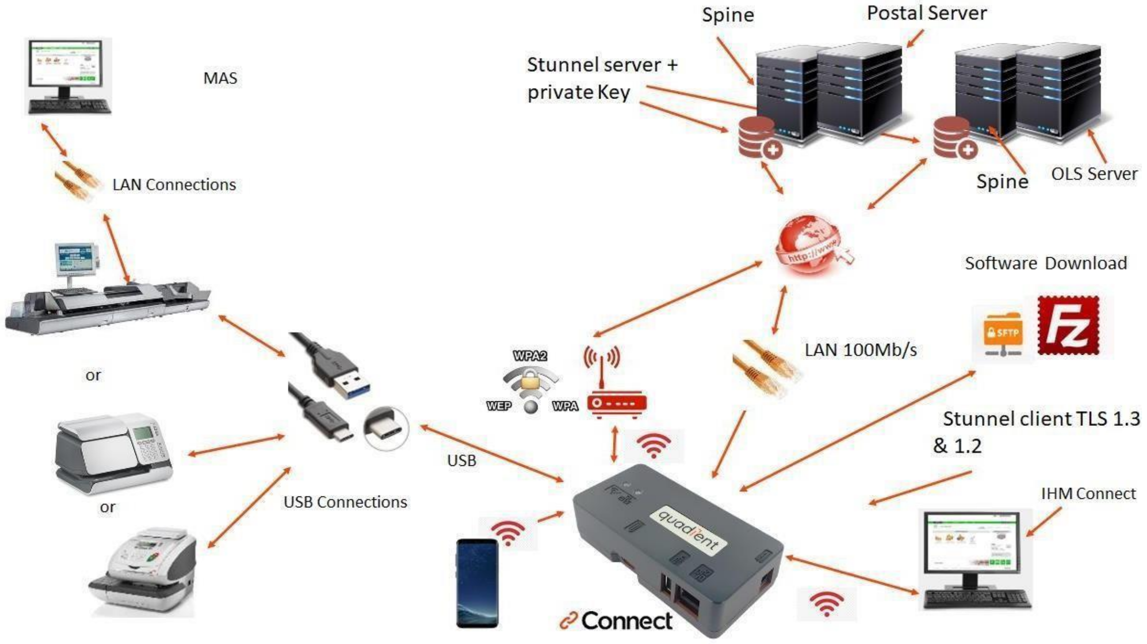
# IS/IN/IX Series Network Security Data Sheet

Please note : For the NOVA range, the franking machine can use a wireless connection to connect to the network & IPV6 is enabled for all SW versions except for the USA where the IPV6 available since SW version N US V1.1r0.0.

If the Zenith range (IX range) is not launched yet in your country, the only way to be able to communicate using TLS 1.2 is by using our Quadient product called the ConnectBox (called as well LINK0 box), which is a physical box to which a franking machine is connected to overcome the TLS 1.0 issue if the product has been launched in your country as well.

ConnectBox physical box

Depending on the needs, this ConnectBox can either be connected by LAN or Wifi to the customer network and this box and here is an overview of the ConnectBox :



Overview of the ConnectBox used in TLS 1.2 or 1.3

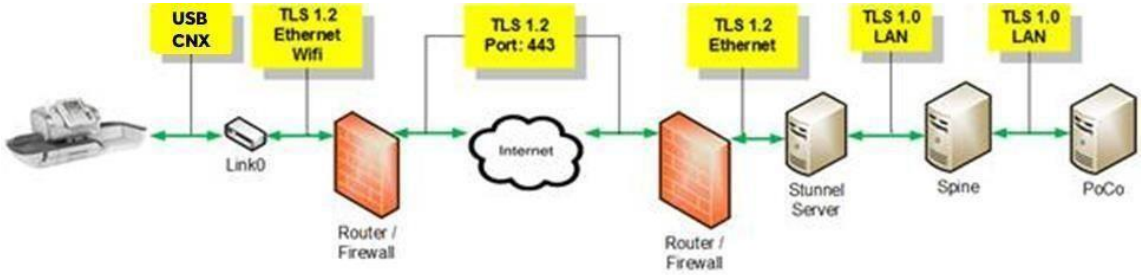
To be noted : This ConnectBox can as well allow to communicate using TLS 1.3 if needed (it's just a case to be checked on the ConnectBox configuration screen) and this product is our only way to be able to use TLS 1.3. To be able to use TLS 1.3, the ConnectBox Software should be version 13.7 or higher & Stunnel software version server 5.59 or higher.

When using the ConnectBox, The software Stunnel client is Embedded in the ConnectBox to provide a universal TLS/SSL tunneling service TLS1.2 and uses public-key cryptography with  to secure the SSL connection and authenticated via a certificate.

It is mandatory for the client's IT to make sure that the port 443 is accepted on the sftp.link0-neopost.com address.

The communication channel between stunnel client and server are encrypted via TLS 1.2 protocol, it's simple authentication by using encrypted algorithm in the connection of the standard port 443.

For the Stunnel server, the communications are protected by a certificate, this certificate using RSA key 2048 bits Encryption SHA-2.



Using the ConnectBox / Link0 box to communicate with TLS 1.2

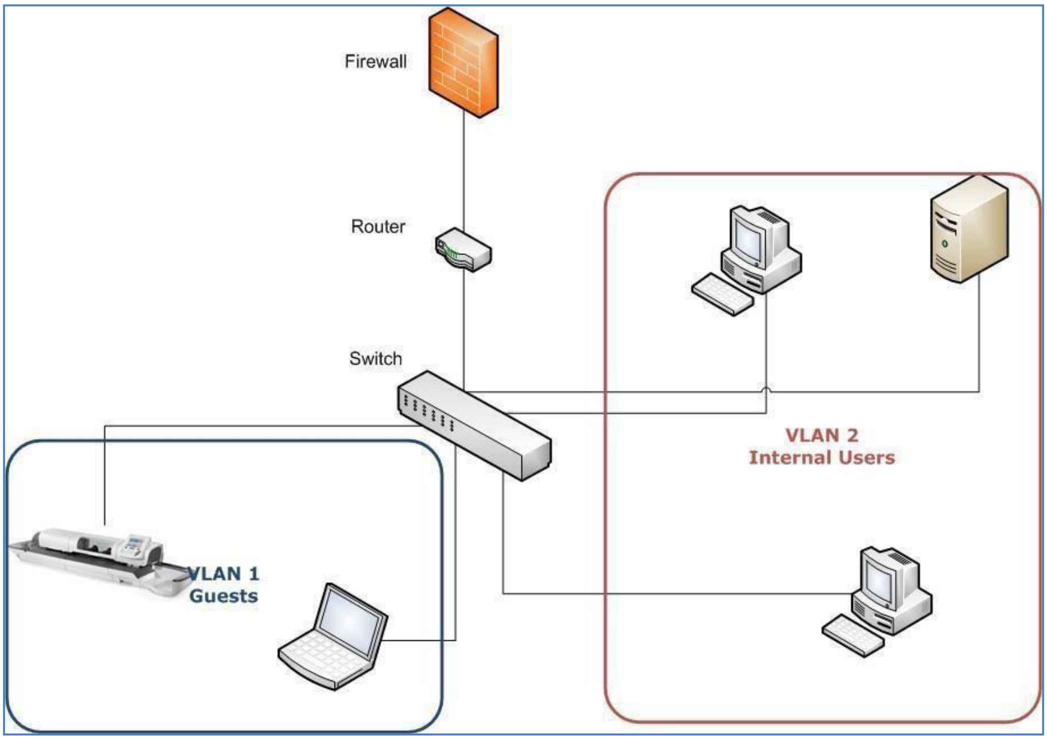
## 8°) ALTERNATIVE NETWORK CONFIGURATIONS

Some IT managers may not feel comfortable allowing our meters on their network for fear of infiltration by a virus or hacker. Therefore, we offer a solution that can allow our Mailing Systems on the customer network and alleviate some of the concerns that IT may have.

# IS/IN/IX Series Network Security Data Sheet

## 8.1°) VLANs

The use of a VLAN is a known way of segmenting a network. Moreover, it is an effective way of securing internal servers and data. By creating a VLAN that only has access to the internet an IT manager mitigates the risk of successful breach of internal company resources. Many of our customers have setup “Guest” networks that allow our Mailing Systems (MS) to connect to our servers without giving the MS access to internal customer resources. See network diagram below.



As shown in the diagram above, allocating a network segment for the Mailing System assures that network resources are shielded from possible intrusion by malicious software or users.

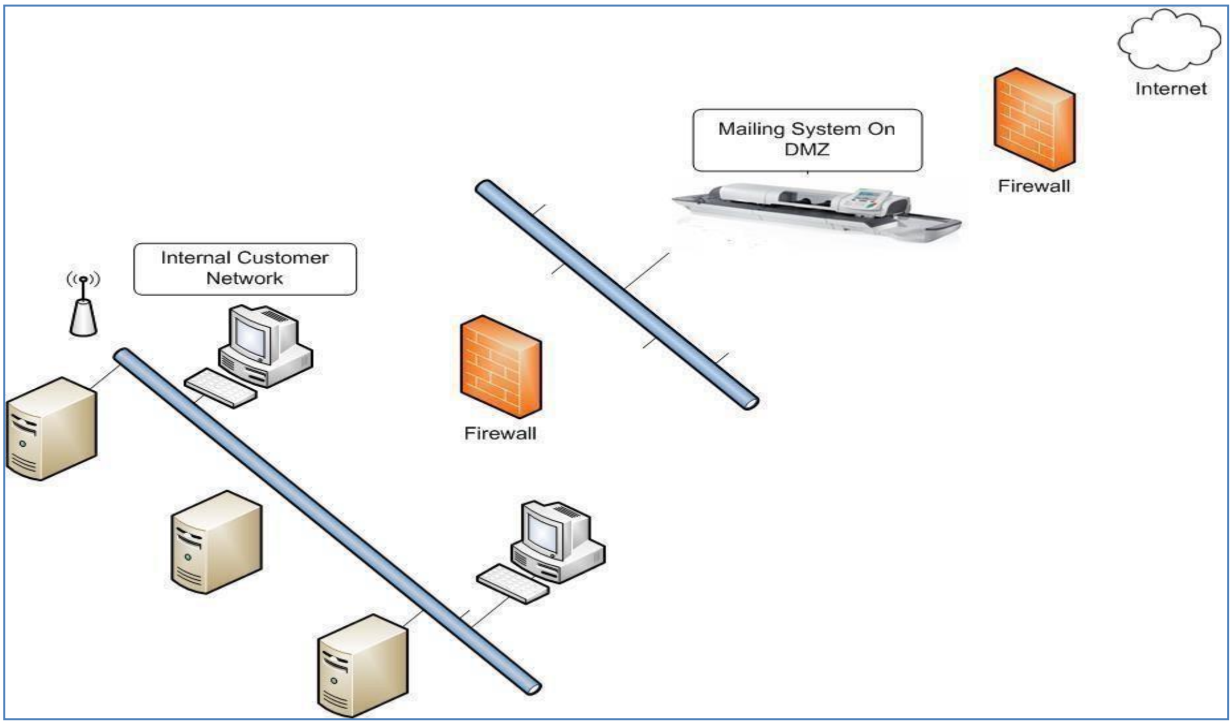
*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

# IS/IN/IX Series Network Security Data Sheet

## 8.2°) DMZ

This method is very similar to creating a VLAN, however, instead of using switches it is accomplished with routers. A DMZ is a "De-militarized Zone" and is a borrowed term from the military. It designates a danger zone where there is little security. In networking, a DMZ is created to allow a server or system to be seen by the internet with only a firewall to limit access and provide security. Most web servers operate in this fashion.

So, the suggestion is to put our Mailing System on the DMZ and allow it to be seen externally. The machine will not accept requests or load any software so the chances that it will get compromised are slim. In the event that it does get compromised, it has been shielded from the rest of the internal network.



Both methods offer similar results and further protection can be achieved by combining them. It is beyond the scope of this article to describe how to setup any of these configurations. Since different networks are configured using different equipment, steps to any of these solutions may vary.

**It Is up to IT managers to investigate and determine the best configuration for their network.**

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

### 8.3°) About the POE

There are 2 kind of devices :

- Active POE
- Passive POE

The active POE launch a machine recognition in order to know if this machine can support the POE, if not : it deactivate the POE in the transmition.
The passive POE Passive doesn't take into account the machine state and send the POE in the transmition every time.

Our franking machine do not support the passive POE.
Except for the IX-9; which has a specific RJ45 connector.

## 9°) SMART application

In some countries, UK & US (as of July 2022), machines can be connected to an external application called SMART.

For information, The iX Series Mailing Systems are the ONLY Mailing Systems supported to integrate into the S.M.A.R.T. application. For an iX Mailing System to communicate with S.M.A.R.T., the Mailing System MUST have a valid contract for WebRemoteControlAuthorization in OLS.

Every time a S.M.A.R.T. session attempts to connect to a Mailing System, O.L.S. validates that the contract is active and the Mailing System is available to be controlled.

The Remote Control Service manages secured access to the Mailing System over the internet and ensures access between users and their corresponding Mailing System. R.C.S. is composed of several Amazon Web Services (A.W.S.) components. R.C.S. has two access points (one per region). S.M.A.R.T. and the Mailing System manage the access point depending on the ZIP Code configured on the PSD

To use the SMART application with your franking machine, you will need to install the Device Manager Software. The Device Manager is a local application that allows S.M.A.R.T. to communicate with locally attached hardware, such as printers and scales. In addition, the use of the Simple Integration feature requires Device Manager. **Device Manager requires local administrator access for installation and potential firewall settings. Device Manager communication does not support proxy server communications.**

# IS/IN/IX Series Network Security Data Sheet

S.M.A.R.T. is a web browser-based application for shipping and mailing system control. See above for supported web browsers and configurations

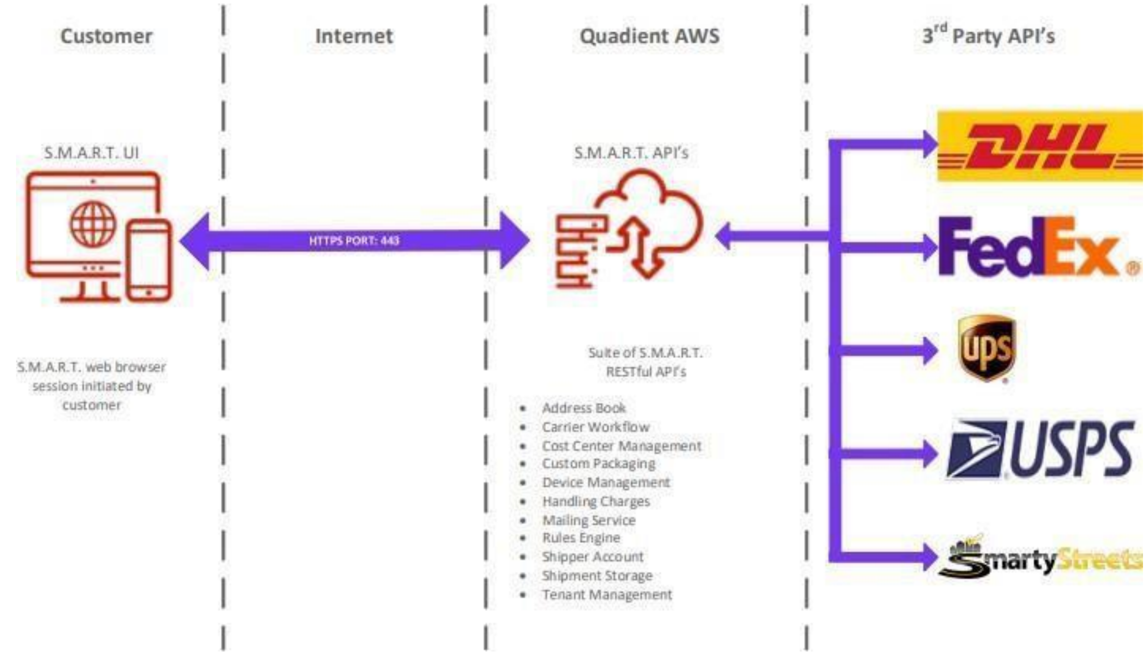
Windows Firewall may prevent the various modules and Carrier utilities from communicating. Ensure the following ports are open for communication. S.M.A.R.T. utilizes Device Manager to communicate with devices (printers and scales). The communications between the Mailing System and R.C.S. and Device Manager and socket.io require mutual SSL authentication. Devices and software that disrupt mutual SSL authentication cause connection interruptions between S.M.A.R.T. and the attached peripherals. SSL Inspection and proxy servers are two examples of this type of disruption.

Port Requirements:

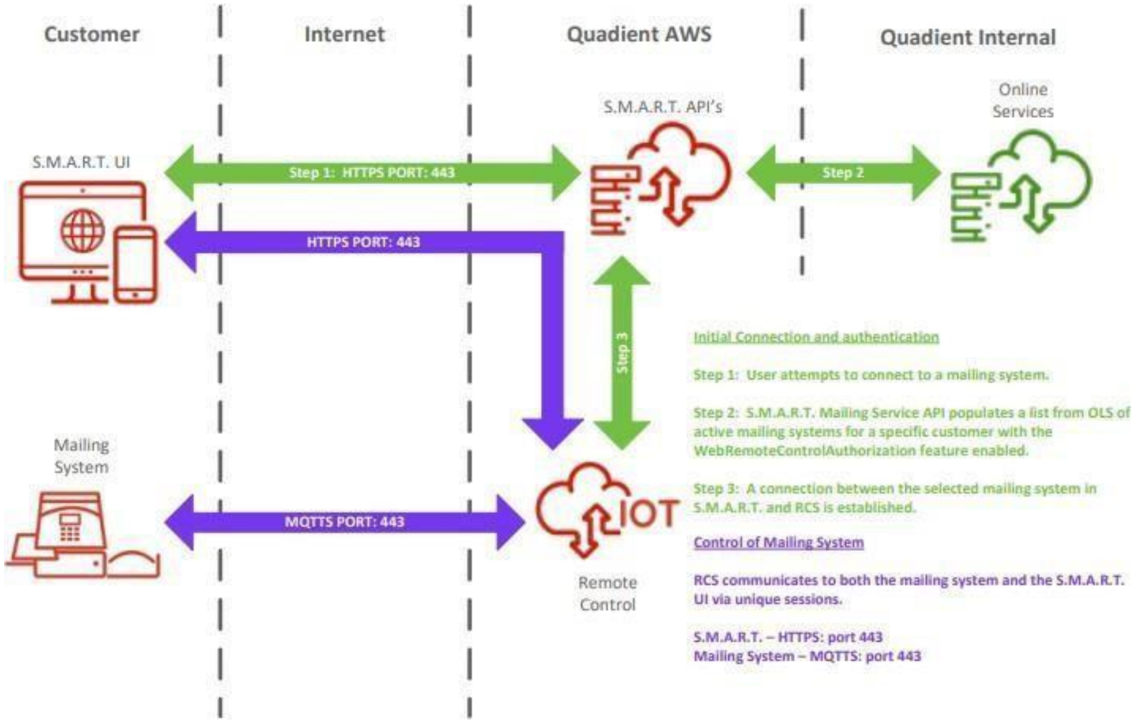
• Port 80 - HTTP Internet communications automatically redirect to Port 443 for security
• Port 443 - HTTPS Internet communications (secured)

The mailing system always initiates outgoing Internet connections.
All outgoing communications from the iX Mailing System are TLS1.2.
An initiated connection creates two communication tunnels for these data exchanges:

• For Machine connection to A.W.S.: ⎫ ECDHE-RSA-AES128-GCM-SHA256 with 2048 bit for R.S.A. keys • For Machine connection to Quadient Servers ⎫ Key Exchange: 1024, RSA 1536/2048 ⎫
Cipher Suite: DHE_RSA_AES128_SHA256 ⎫
Mac: HMAC-SHA-256



SMART Communication Diagram



Initial Connection and authentication

Step 1: User attempts to connect to a mailing system.

Step 2: S.M.A.R.T. Mailing Service API populates a list from OLS of active mailing systems for a specific customer with the WebRemoteControlAuthorization feature enabled.

Step 3: A connection between the selected mailing system in S.M.A.R.T. and RCS is established.

Control of Mailing System

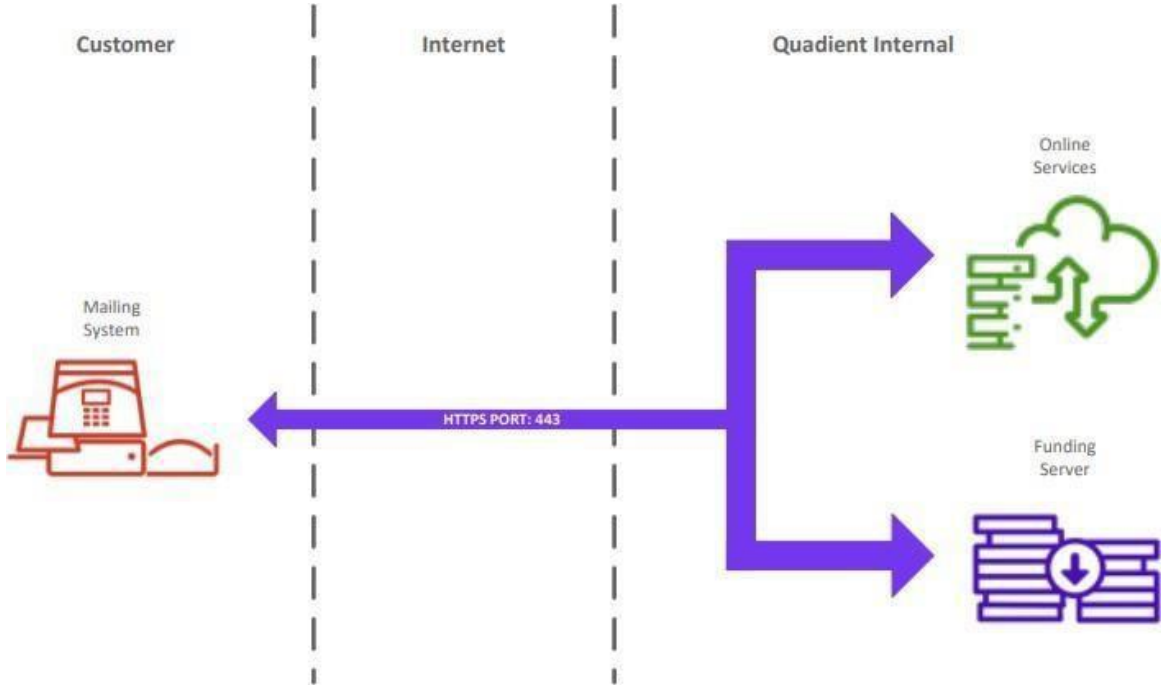
RCS communicates to both the mailing system and the S.M.A.R.T. UI via unique sessions.

S.M.A.R.T. – HTTPS: port 443
Mailing System – MQTTS: port 443

SMART with franking machine communication diagram

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

# IS/IN/IX Series Network Security Data Sheet



Mailing System Communication Diagram

## 10°) MORE INFORMATION

**Server communication process**:

When the mailing system needs to connect to our servers, it opens a secure communication tunnel, based on TLS V1.0 protocol & TLS V1.2*, over the Internet to the Quadient server.
The mailing system uses the same port used for HTTPS (Hypertext Transfer Protocol Secured), i.e. **port 443**.

**The mailing system doesn’t integrate an email client/server**. Mail spamming is not possible from the mailing system because it doesn't integrate any email client or server.

**Remote access from the LAN to the mailing system is not possible : I** nternet connections are always initiated by the mailing system and never from the Network toward

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*

the mailing system. These are either initiated manually by the user or automatically by the mailing system (normally once a month).

**Communication ports are used only during communication with Quadient Servers :** The ports used to communicate with our Servers are only open during data transfer. When the communication is finished, the port on the mailing system is closed.

**DMZ** The Mailing system can be installed on the **DMZ** or **Guest network**. This will prevent the firewall from blocking communications if URL Filtering is used on it.

**WiFi** An optional wireless adapter is available from Quadient, for connection to a customer’s existing WiFi network.
The WiFi is embarqued in the IX-9 series and is limited to 2.4G

## FAQ

**1- Regarding security updates (whether for Windows CE or your application),**
**what is the process and the associated network flows?**

Our machines are approved by the Post Office: in this context, the software of the franking machine must be validated. It is a long and complex process that does not allow regular updates like on PCs. This software includes the Windows CE system base, like the drivers, like the application.

The OS (Windows CE) does not allow downloading of software other than that approved by the Post. These software (defined in a proprietary format) are signed. There are no specific security updates made on our machines.

The security algorithms used are independent of the OS and are managed in the application (TLS, ...)

**2- Could you also confirm that the Windows CE system pedestal is still supported by Microsoft?**

No there is no more support from Microsoft, but security releases are not managed through Microsoft support

**3- Is your system integrated with Active Directory?**

There is no integration with an active Directory

**4- Regarding system and application accounts, what are they and how will they be managed?**

There is no access through system / application accounts.

Access controls on the machine are made by User / Supervisor / Technician access.

Access to servers is validated by TLS verification using an X509 certificate

*No part of this document may be reproduced or distributed in any form or by any means without the express permission of an authorized representative of Quadient. This manual and all information contained therein, is confidential and may only be disclosed as necessary to support customer use of the equipment.*