



Q-SOLUTION

Secure Messaging as a Service

Service Description



PRINTED COPIES ARE NOT CONTROLLED

© Q-Solution Limited 2026. All rights reserved

Crown
Commercial
Service
Supplier





For more information about our services please contact us:

Tel: +44 (01737) 887229 | email: contact@q-solution.co.uk

or write to:

Customer Services, 2 Tallis Street

London, EC4Y 0AB

© Q-Solution Limited 2026. All rights reserved

The contents of this document are copyright of Q-Solution Limited. All intellectual property rights (including without limitation copyright, moral rights, rights in design and know-how, whether or not registered or capable of registration and whether or not subsisting in the United Kingdom) in the contents of this document are reserved. Any redistribution or reproduction of part or all of this document's contents in any form is prohibited. The contents of this document may not, without Q-Solution Limited's express written permission, be distributed, commercially exploited, or transmitted to outside of your organisation or to a third party.

Disclaimer

Any views, opinions and guidance set out within this document are provided for information purposes only and do not purport to be professional advice. No responsibility or liability is accepted for any errors or omissions in this document or related documents.

1 Overview

Secure Messaging as a Service is a service enabling systems connected to the Internet and PSN Protected network to securely share data with one another. Acting as a secure broker, the service provides Assured message delivery and Management Information reporting out of the box with no additional design, build and deployment overheads.

1.1 Key Features

The features of the service include:

- Secure Message based routing for SOAP, Web Services, FTP/S, HTTP/S protocols
- Content based message routing
- Message persistence enabling assured message delivery
- Internet and PSN gateway connectivity
- Online Management Information
- Accredited to hold up to OFFICIAL data
- Managed Security Operations Centre including Protective Monitoring
- Dedicated 9-5pm Support team (24/365 for P1/P2 incidents)
- 99.95% availability
- Certified against Cyber Essentials Plus and ISO27001:2022
- Data residency within UK Sovereign Data Centres
- Designed and built against NCSC Cloud Security Principles
- Assessed against AWS Well Architected Framework
- Malware Scanning in transit and at rest
- Data Encryption using AES-256 and TLS 1.2/3

Q-Solution will work with the customer to develop specific project requirements associated with message based routing such as prioritised messaging on an as-needs basis and in line with our standard SFIA rate card.

Deployment of these routes will form part of the onboarding process.

1.2 Benefits

Secure Messaging as a Service has the benefits of:

- Migrate systems from secure government networks to a secure Internet connection independently
- Provides assurance of the successful receipt of a message back to the originating system
- Providing schema validation and error reporting, data quality can be dramatically improved
- Provides in-transit and at rest malware scanning
- Message persistence in the event of the receiving system not being available removes a single point of failure ensure originating systems can continue to operate.
- Data encryption based on AWS KMS (AES-256) secures your data throughout
- Employing 100% native cloud technologies ensuring the service is scalable to meet both planned and unexpected increases in demand
- Full messaging auditing and traceability available at the touch of a button
- Reduced CapEx through leveraging of SaaS and pay-per-message
- Accelerate project delivery
- Fully Managed and supported by UK based SC cleared staff
- Account Management, Technical and Security support available
- Receive real time Management Information on desktop and mobile device

1.3 Message Processing

The design of the system is to provide an Assured Message Delivery Service. That is, to be the broker in the exchange of messages between disparate systems across multiple networks, ensuring both message integrity throughout. Key features of the message processing include:

- Response times in the acknowledgement of a message of ~200ms
- Virus scanning of all inbound and outbound messages
- Automated monitoring of system availability and storing of messages for unavailable systems
- Automated replay of stored messages when system become available
- Support for controlled message release as required by customer connected systems
- Built to scale using AWS serverless services

1.4 Monitoring

Application Monitoring and Management Information

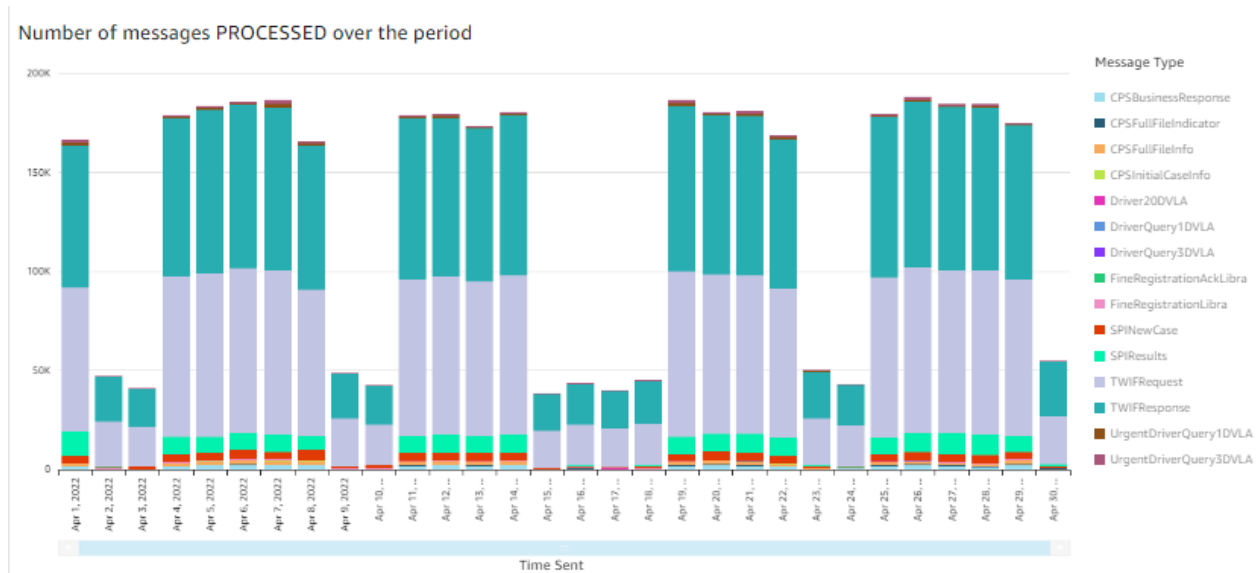
Application Monitoring is provided through SAML based access controls managed by Q-Solution. Reporting is through AWS QuickSuite, accessible to both browser and mobile over the internet and where typical reports include:

- Number of messages processed per hour/day
- Number of messages from/to a given end point

- Maximum, minimum and average message payload sizes over a given time window
- Number of messages by type
- Service Level live view enabling a customer to view in real time, the compliance against SLAs. Includes:
 - Message delivery times
 - System Availability
 - Incident response times
 - Incident durations

These reports can be customised as required by the customer and therefore provide valuable analytics into the user of the service in order to inform key decisions.

An example of the volume of messages processed by type



Further analytics showing the breakdown of messages by sending system



Analytical Information can be presented in a matter of minutes to suit the needs of the business.

Protective Monitoring

The Secure Messaging Service provides all the necessary Protective Monitor and Security Incident and Event Management (SIEM) as required to maintain the Code of Connection to the PSN Protected Network. These include:

- Monitoring for configuration changes
- Threat Detection
- Audit Logging
- Security Alerting and Compliance

Our SIEM and Vulnerability Management tooling as well as our alerting services operate as part of the service to provide this Protective Monitoring capability.

1.5 Security and Information Assurance

Security and your data protection is the foundation of the design of the Messaging and underlying Secure Platform. These are subject to annual independent audits including:

- CHECK approved IT Health Check
- The service and all users/actions are based on the Zero Trust Security Framework
- ISO27001:2022 Information Security Management
- Cyber Essentials Plus
- PSN Code of Connection
- PSN Code of Compliance

In addition to this, the platform provides security in the form of:

- Boundary Malware protection
- User Account auditing and suspicious activity monitoring and alerting
- Ingestion of all AWS service logs into a central Protective Monitoring solution
- Account separation

All staff operating the service are UK based and hold current government SC level security clearance.

Our Information Information Security Policy (available on request) further details our approach to Information Security and the controls we have in place to ensure the highest standards are maintained.

1.6 System Requirements

Sending and receiving systems with message exchange enabled must either be:

- connected to the PSN Protected network, or
- connected to the Internet with a messaging system supporting certificate authentication via mutual Transport Layer Security (mTLS)

2 Secure Messaging SLA

2.1 Support Hours

Support hours for the service desk is between 8am and 6pm, Monday to Friday excluding UK Public Holidays. Our Protective Monitoring and System Monitoring however operates 24/7/365 and will generate alerts throughout this period in the event of any priority incidents occurring. Agreement on how these incidents outside of core hours are resolved will be agreed during the on-boarding process

2.2 Service Level Agreement Target

Measure	SLA Component	Target Value	SLA Value
Incident Response time	P1 Response time	10 minutes	100%
	P2 Response time	30 minutes	100%
	P3 Response time	1 Hour	100%
	P4 Response time	8 Hours	100%
Incident Restoration time	P1 Restoration time	1 Hour	98%
	P2 Restoration time	4 Hours	100%
	P3 Restoration time	24 Hours	100%
	P4 Restoration time	3 Days	100%
Incident Resolution time	P1 Resolution time	4 Hours	98%
	P2 Resolution time	8 Hours	98%
	P3 Resolution time	3 Days	98%
	P4 Resolution time	7 Days	98%
Change Management	Emergency Change	12 Hours	100%
	Standard Change	2 Days	100%

Measure	SLA Component	Target Value	SLA Value
	Planned Maintenance Notification	14 Days	100%
Problem Management	Root Cause Analysis Delivery	1 Day	98%
Availability	Monthly Availability	99.95%	100%
Business Continuity	Recovery Point Objective	Zero hours	100%
	Recovery Time Objective	30 minutes	100%

2.3 Availability Target

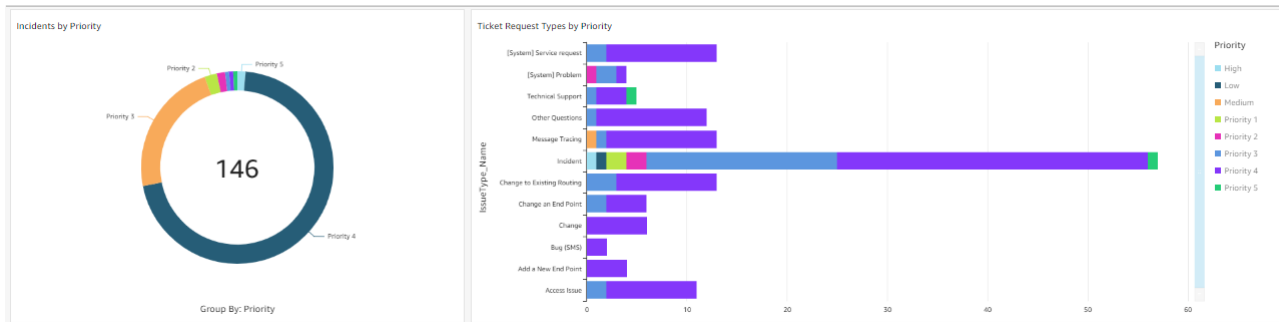
Type	Measurement	SLA (over month)
Availability	Availability of the Messaging Application during working hours (8am to 6pm, Monday to Friday excluding Bank Holidays)	99.9%
	Availability of the Messaging Application outside of working hours.	99.5%
Service Desk	Monday to Friday, 8am to 6pm excluding UK Public Holidays	See Secure Messaging Incident Management

The Secure Messaging Service availability outside of core hours allows for Change Requests and enhancements to be made to the service. A scheduled maintenance window will operate typically between 8pm and 10pm with notification of changes published to the customer portal as well as communicated via the customers preferred channel.

All changes to the service are automated using Infrastructure as Code and Continuous Integration processes. The above SLA for out of hours availability allows for approximately 1 deployed per week (assuming a 30 minute outage) if required.

2.4 Reporting

Service Owners are able to view real-time information on the status of tickets and incidents over customised periods of time as depicted below



Customers are able to view over the internet, the status of all tickets raised by themselves and/or associated with the organisation they belong to

Limitations

The following are the current limitations of the service. We do however encourage customers to review these pages and the dashboard for changes made to the service as we aim to continually improve the capacity, availability and overall service provision.

- Individual message sizes are limited to 6Mb
- Message throughput is restricted to 500 messages per second based on message sizes of 100k

3 Secure Messaging Incident Management

Users of the service have two channels for raising incidents on the service:

- Email
- Online Portal

Emails can be sent to a centralised email address that will generate a ticket to be triaged and raised with the support desk. Alternatively, a portal is available that allows users to raise specific service requests directly, ensuring the information required by the service desk is provided and therefore a quick response to the incident can be achieved.

3.1 Incident

Incident Management and the response to incidents is defined through a combination of two factors:

- Urgency of the incident
- Impact of the incident

Incident Urgency

The *urgency* of the incident is defined as how quickly a resolution to an incident is required.

Category	Description
High (H)	• The damage caused by the Incident increases rapidly. • Work that cannot be completed by staff is highly time sensitive. • A minor Incident can be prevented from becoming a major Incident by acting immediately.
Medium (M)	• The damage caused by the Incident increases considerably over time.
Low (L)	• The damage caused by the Incident only marginally increases over time. • Work that cannot be completed by staff is not time sensitive.

Incident Impact

The *impact* of the incident is defined by what impact this incident is having on live operations and specifically the number of users and/or systems affected.

Category	Description
High (H)	- A large number of staff are affected and/or not able to do their job. - A large number of customers are affected and/or acutely disadvantaged in some way. - The damage to the reputation of the business is likely to be high. - Someone has been injured.
Medium (M)	- A moderate number of staff are affected and/or not able to do their job properly. - A moderate number of customers are affected and/or inconvenienced in some way. - The damage to the reputation of the business is likely to be moderate.
Low (L)	- A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort. - A minimal number of customers are affected and/or inconvenienced but not in a significant way. - The damage to the reputation of the business is likely to be minimal.

The diagram below defines the Priority assigned to incidents raised.

		IMPACT		
		HIGH	MEDIUM	LOW
URGENCY	HIGH	P1	P2	P3
	MEDIUM	P2	P3	P4
	LOW	P3	P4	P5

Response times for Priority incidents are defined in the [Service Level Agreement Target](#) section

Please note that as part of the On Boarding process, our Incident Management as well as our Problem Management processes will be shared with the customer and integrated into their own operating model as necessary.

Following the onboarding process, the Secure Messaging Service Design will be shared and where necessary, customised with the customer.

4 Secure Messaging Pricing

4.1 Billing and Charging

Our charging model for the Secure Messaging as a Service is designed to be simple and cost effective. With that goal in mind, the charges are based on:

- Initial setup charges
- Connection charge
- Message numbers, size and volume discount per sending system

4.2 Initial setup charges

If initial custom setup is required for the customer then this shall be charged based on the standard SFIA rate card and aligned to an initial onboarding plan.

4.3 Connection Charge

This connection charge is levied for each sending endpoint required and covers activities such as:

- Firewall/Security Group amendments
- Enrolling the end point into the service wrap
- Testing connectivity to the end point

There is a £1,000 charge for each end point connection. The process for onboarding a new end point (as well as the definition of an 'end point') is defined in the On Boarding Process Manual. Where complex end points require additional support, this will be agreed with the client at the initial onboarding and be charged at our standard SFIA rate cards.

4.4 Message numbers, size and volume discount

The remainder of the charges for the service are based on the number of messages sent from and grouped by a given source, the protocol used and the message size over a calendar month. A volume based discount is applied to these charges as defined in the tables below. The charges, as detailed in the Customer On Boarding Procedures, include the configuration of:

- Customers specific data retention policies
- Message persistence requirements

Volume p/m			Price per Message/Size (k)/Month				
From	To	Discount	1-25	26-100	101-250	251-500	501+
1	10,000	0%	£0.0343	£0.0429	£0.0515	£0.0601	£0.0686

Volume p/m			Price per Message/Size (k)/Month				
10,001	50,000	15%	£0.0292	£0.0365	£0.0438	£0.0511	£0.0583
50,001	150,000	25%	£0.0257	£0.0322	£0.0386	£0.0450	£0.0515
150,001	500,000	35%	£0.0223	£0.0279	£0.0335	£0.0390	£0.0446
500,001	2,000,000	45%	£0.0189	£0.0236	£0.0283	£0.0330	£0.0378
2,000,001	4,000,000	60%	£0.0137	£0.0172	£0.0206	£0.0240	£0.0275
4,000,001	6,000,000	70%	£0.0103	£0.0129	£0.0154	£0.0180	£0.0206
6,000,001	Above	70%	£0.0103	£0.0129	£0.0154	£0.0180	£0.0206

4.5 Discounts

Discounts are available based on message volumes as defined above.

4.6 Education pricing

We do not offer separate pricing for educational bodies.

4.7 Sector Pricing

We do not differentiate our pricing across different sectors or bodies.

4.8 VAT

All prices within this document are exclusive of VAT, which will be applied at the prevailing rate.

4.9 Indexation

The Supplier may increase the Charges on an annual basis with effect from each anniversary of the contract start date in line with the percentage increase in the Consumer Prices Index (CPI) in the preceding 12-month period.

“Consumer Prices Index” means the Consumer Prices Index as published by the Office for National Statistics from time to time, or failing such publication, such other index as the parties may agree most closely resembles such index.

Other Charges

Q-Solution reserves the right to apply additional charges based on the standard SFIA rate card in support of customers messaging requirements outside the scope of the Secure Messaging as a Service offering. Any such requirement will be agreed with the customers during the onboarding process.