Q-SOLUTION

# Certificate Authority as a Service

Service Description



Crown Commercial Service Supplier

ISO 27001 Certified

CYBER ESSENTIALS PLUS

For more information about our services please contact us:

Tel: +44 (07538) 023530 | email: contact@q-solution.co.uk

or write to:

Customer Services, 2 Tallis Street

London, EC4Y 0AB



**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.

Crown Commercial Service Supplier

Information Security Management System ISO 27001 Certified

CYBER ESSENTIALS PLUS

Q-SOLUTION

# Table of Contents

# 1 Overview

Digital certificates are a well-established, secure and scalable way of providing authentication, digital signature and encryption for a wide range of applications and systems.

Use cases for digital certificates in the Public Sector include:

- Transport Layer Security (TLS) encryption-in-transit, commonly referred to as Secure Socket Layer (SSL) encryption
- mutual TLS (mTLS) for fully authenticated connections to secure systems
- API Gateway mTLS
- Electronic Data Interchange (EDI)
- Virtual Private Network (VPN) site-to-site and remote access via the Internet
- Mobile device and laptop authentication
- User access to secure systems
- Internet of Things (IoT) device authentication
- Code signing

The service offers a cloud-based private Certificate Authority dedicated to each customer, which can be used to issue certificates for a range of use cases such as the examples above.

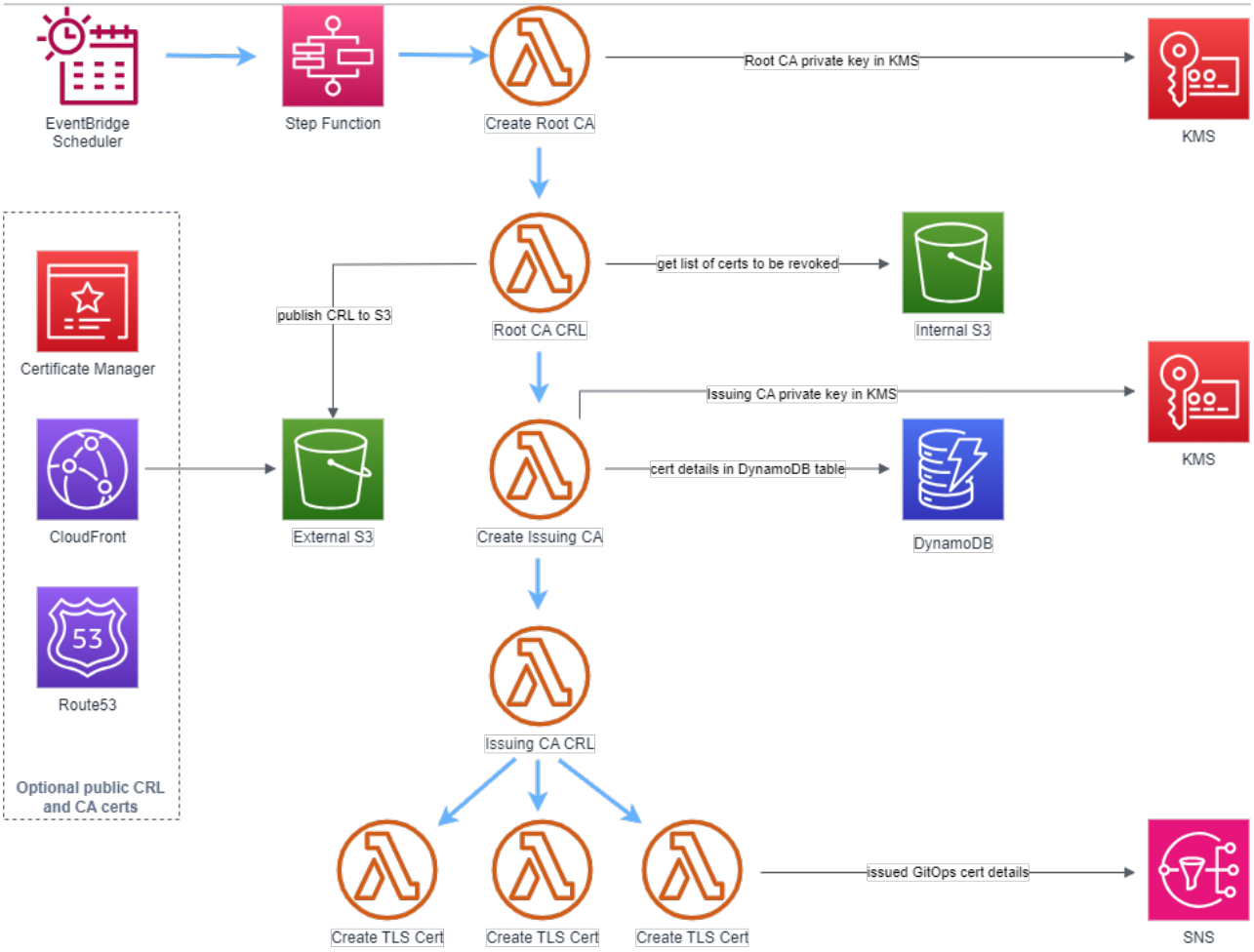
## 1.1 Features

The following features are delivered as part of the Secure Mail as a Service

- Private Certificate Authority service
- Dedicated Root CA / Issuing CA per customer environment
- FIPS 140-2 level 3 hardware protection of CA private keys
- Certificate revocation with optional public CRL distribution points
- Database of issued certificates
- Comprehensive logging and monitoring
- Fully automated certificate issuing option
- GitOps certificate issuing option with approval step
- 99.95% availability

## 1.2 Summary Architecture

The Managed Certificate Authority uses completely serverless infrastructure within AWS as illustrated in the high level architecture overview below.




## 1.3 Monitoring

Monitoring of the infrastructure is performed by Q-Solution as a part of the Managed Service. This includes both System Monitoring and Protective Monitoring.

### System Monitoring and Alerting

System Monitoring involves the monitoring of the underlying services supporting the cloud platform. Thresholds are set for these services to generate automated alerts if they are breached. Details of these thresholds and the alerting and communication with customers will be provided during the on-boarding process and are fully customisable.

### Management Information

Management Information (MI) is provided detailing:

- Number of certificates issued per month and total to date

The MI is provided through a web front end and can be customised to ensure the customer receives the insights relevant to their business.

### Protective Monitoring

The service is governed by a fully managed Protective Monitoring regime supported by our internal security operations team. The service:

- Ensures all systems and services are patched to the latest supported versions
- Measures our technical controls against NIST and ISO27001
- Protects against phishing and malware
- Monitors activity, alerting suspicious behaviour based in the MITRE ATT&CK knowledge base

## 1.4 Security and Information Assurance

Q-Solution operate a comprehensive Cyber Assurance process across all our cloud and corporate IT. Our Assurance Document Set (ADS) aligns with the following HMG & Corporate Policies:

- HMG Security Policy Framework
- NCSC Cloud Security Principles
- NCSC Architectural Patterns
- NCSC Cyber Assessment Framework
- Q-Solution Information Security Policy and sub policies
- ISO/IEC27001 standard
- NIST Cybersecurity Framework
- Government Secure by Design Principles

The following documents support our ADS and can be provided to the customer during the onboarding process

- Information Risk Assessment Report (IRAR) overview document
- Risk Assessment Methodology and Risk Treatment documentation
- ISO/IEC 27001 certification, SoA and audit findings
- Audit Policy
- AWS Well Architected Review
- NCSC Cloud Security Principles
- NCSC Cyber Assessment Framework
- NIST Cybersecurity Framework (Mapped to ISO27001)
- CHECK ITHC report and vulnerability management/mitigation
- Cyber Essentials reports and Action Plan

## 1.5 Limitations

The following are the current limitations of the service.

- Administrators require an identity within their own organisation's Microsoft Entra ID (formerly Azure AD), which can be used for federated identity - this will be the case if their organisation is a Microsoft 365 customer

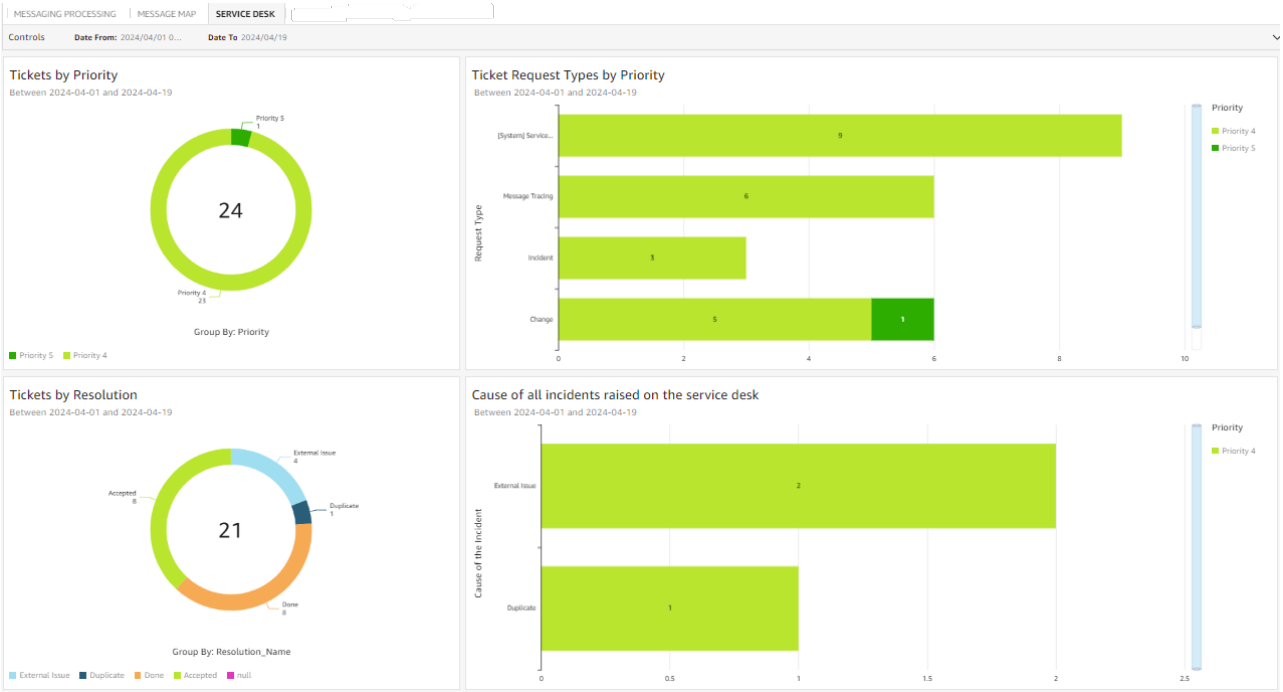
# 2 Certificate Authority Service Management

## 2.1 Overview

Q-Solution provide the overall service management wrap for the secure email service, providing monthly service reports including but not limited to:

- Tickets raised
- Performance against SLA's
- Incident trend types
- Change Management
- Continuous Improvement initiatives

Whilst this is reviewed monthly, our Management Reporting is dynamic and online allowing the customer to view these and other metrics in real time through and online portal.




Our Service Management tooling has a number of APIs available for customers to use to feed service management information into their own analytics platform if required.

## 2.2 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.

## 2.3 SLA Targets

| 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% |
| | 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% |

| Measure | SLA Component | Target Value | SLA Value |
|---|---|---|---|
| | Recovery Time Objective | 30 minutes | 100% |

## 2.4 Availability Targets

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

The service availability outside of core hours allows for patches, change requests and enhancements to be made to the service. When necessary, a scheduled maintenance window will operate with notification of changes published to the Service Desk Portal as well as communicated via the customers preferred channel.

By design, the services provides the necessary resilience to allow patching to occur without service interruption.

# 3 Certificate Authority 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 Response

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.

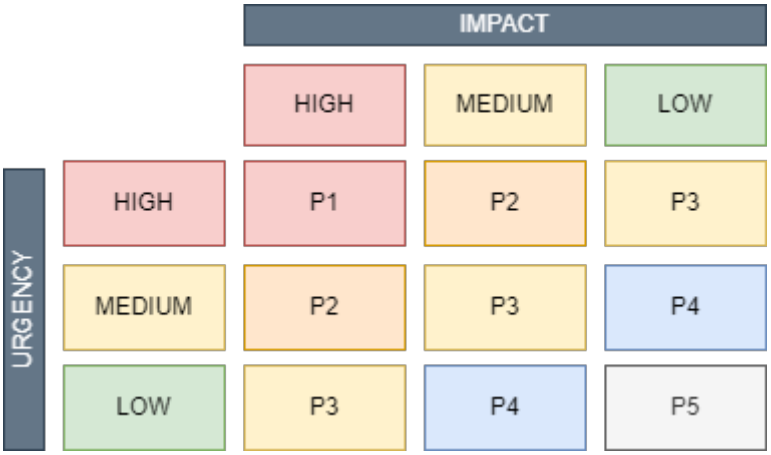
| Category | Description |
|---|---|
| High (H) | • The damage caused by the Incident increases rapidly.<br>• Work that cannot be completed by staff is highly time sensitive.<br>• A minor Incident can be prevented from becoming a major Incident by acting immediately. |
| Medium (M) | • The damage caused by the Incident increases considerably over time. |
| Low (L) | • The damage caused by the Incident only marginally increases over time.<br>• 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.<br>• A large number of customers are affected and/or acutely disadvantaged in some way.<br>• The damage to the reputation of the business is likely to be high.<br>• Someone has been injured. |
| Medium (M) | • A moderate number of staff are affected and/or not able to do their job properly.<br>• A moderate number of customers are affected and/or inconvenienced in some way.<br>• 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.<br>• A minimal number of customers are affected and/or inconvenienced but not in a significant way.<br>• The damage to the reputation of the business is likely to be minimal. |

The diagram below defines the Priority assigned to incidents raised.




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.

# 4 Certificate Authority Pricing

## 4.1 Billing and Charging

Our charging model for Certificate Authority as a Service is designed to be simple and cost effective. With that goal in mind, the charges for the platform consist of

- On-Boarding setup charge
- Monthly charge based on number of certificates issued
- Initial Organisation setup fee

## 4.2 Onboarding Charge

The initial onboarding charge is associated with working alongside the customer to setup their solution. The charges associated with this will be for Professional Services and typically involve one or more of the following roles:

- Technical Delivery Management
- Service Management
- Security Architect
- DevOps engineer

Rates can be found in the supporting Q-Solution SFIA Rate Card.

## 4.3 Certificate charging

Charges are based on monthly certificate volumes as detailed below

| **Volume** | **Price per certificate** | | |
|---|---|---|---|
| **certificates / year** | 30 day validity | 90 day validity | 1 year validity |
| > 1,000,000 | £0.02 | £0.05 | £0.20 |
| 100,001 - 1,000,000 | £0.04 | £0.13 | £0.50 |
| 10,000 - 100,000 | £0.08 | £0.25 | £1.00 |

Note that there is a minimum volume for the services of 10,000 certificates (1 year validity)

## 4.4 Organisation setup fee

There is an initial setup fee for each new organisation of £4,900, this covers:

- Creation of CA environment for customer

- Set up of administrator users via identity federation
- Creation and configuration of Git repository for customer's GitOps certificate management process

The standard organisation standard setup fee does not include setup of automated API access to the Certificate Authority service, or professional services work to integrate with customer systems and services. This is covered by the additional organisation onboarding charge (above).

## 4.5 Education pricing

We do not offer separate pricing for educational bodies.

## 4.6 Sector Pricing

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

## 4.7 VAT

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

## 4.8 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 requirements outside the scope of the standard Certificate Authority as a Service offering. Any such requirement will be agreed with the customers during the onboarding process.