



Secure Messaging

SECURE COLLABORATION

**SERVICE DEFINITION
DOCUMENT**

JANUARY 2026

46 Donegall Pass

Belfast, BT7 1BS

Email Stiona (sales@stiona.com)

Tel: +44 (0) 2890 322011



Contents

1. Secure Messaging Overview	2
2. Service features	3
2.1. Citizen & User Entry Points (“Who Interacts”).....	4
2.2. Message configuration and Published Service features	4
2.3. The Platform (“Secure Foundations”)	5
3. Onboarding and Offboarding	7
3.1. Onboarding	7
3.2. Offboarding	7
3.2.1. End of contract data extraction	8
4. The Digital Toolkit Platform	9
4.1. Platform Security Architecture	9
4.2. Disaster Recovery	10
5. The Stiona Managed Service	11
5.1. Service Level Agreements (SLAs).....	11
5.2. Support and Service Management	12
6. Additional Professional Services – For Information Purposes.....	14
6.1. Mobilisation services	14
6.2. Enhanced Configuration & Solution design services	14
6.3. Data Services	14
6.4. Payment Services.....	15
6.5. Enhanced Support/Extended hours.....	15
6.6. Business Continuity planning & support	15
6.7. Business security risk management support	15
6.8. Custom development services.....	16
6.9. Hosting Services.....	16

1. Secure Messaging Overview

Secure Messaging is a ***no-code 'Commercial off-the-Shelf' (COTS) secure collaboration solution*** - a cloud-hosted encrypted communication service enabling secure exchange of messages and documents with internal teams, organisations and public recipients. Supports multiple verification types, audit history, attachments and message threads. Fully managed with configurable retention and ISO27001-aligned controls, with integration available through APIs and UI components. The service is hosted in our Azure Digital Toolkit platform and can be fully supported by our managed service.

2. Service features

The Secure Messaging service offers extensive configuration customisation and messaging features to a variety of users.

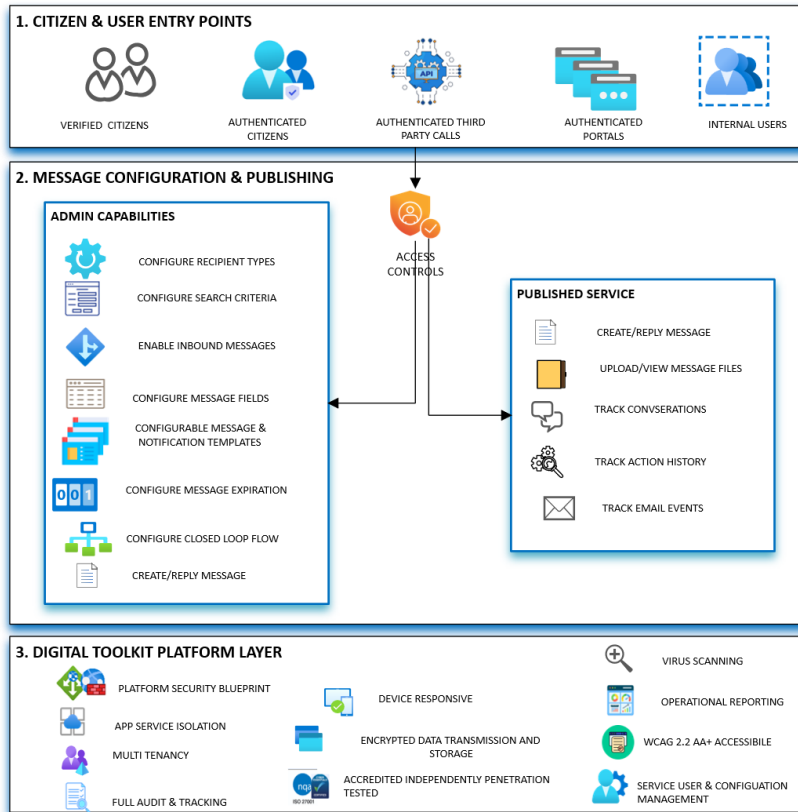


Diagram summary: The diagram illustrates the Secure Messaging capabilities available to a variety of audiences. Authorised citizens and admin users enter via configured verification methods (e.g. Email or SMS), authenticated portals, or internal admin interfaces. Administrator capabilities include configuring recipient authorisations required, message fields, message flows, message expiration, message search capabilities and message and message notification templates. Authorised service users can then use the published service to create or reply to messages including uploading any message attachments, view messages and track message status, conversations, all message event audits and email notifications issued. All uploaded files are virus scanned and the platform ensures the message and service data remains accessible, device responsive and securely encrypted at all times through tenancy management, service isolation, and platform configuration management.

2.1.Citizen & User Entry Points (“Who Interacts”)

The Secure Messaging service can be published to a variety of citizen and user entry points including:

- **Verified citizens** – the platform supports issuing of secure messages to citizens who verify SMS or Email verification. These are typically one-way messages to individuals where only basic information is known.
- **Authenticated citizens** – the platform supports a variety of authentication providers including ADFS (Windows), Azure ID (Entra), Username and Password with SMS verification, NIDA and OpenID providers such as GOV.UK One. This can be extended
- **Authenticated portals** – the service can be configured to send messages to individuals or multiple users within role-based portals for distinct external user groups (e.g., organisations, solicitors, partner bodies). Using the platform’s *multi-tenant architecture*, each group is securely and logically separated from others, ensuring data isolation and controlled access. Each portal enables the group to manage its own administrators and users, giving them autonomy over user provisioning and access management while maintaining full separation and security between tenants.
- **Internal users** – the platform provides comprehensive service administration features for internal users, tailored through role-based access controls. Depending on their assigned role, users can configure secure messaging features and create and manage message conversations.

The platform integrates with the organisation’s authentication provider via the identity service to deliver **Single Sign-On (SSO)** for provisioned internal administrative users. Once authenticated, permissions are applied based on role, ensuring users only access the features relevant to their responsibilities.

2.2.Message configuration and Published Service features

Secure Messaging internal users with the appropriate role can configure:

1. **Message Recipient types:** aligned to authentication mechanisms
2. **Message Flow:** one way or two-way messaging can be enabled.
3. **Message unique reference fields:** to link to existing business process reference identifiers

4. **Email and message templates:** Message recipients are notified of a waiting message by email. The format of these can be tailored to include business specific information if required. Service and email logos and branding can be configured within the platform.
5. **Message Expiration:** If enabled is by default set to 3 months but can be configured on a message-by-message basis
- **Message search criteria:** options for search fields can be enabled/disabled
6. **Message format and fields:** including options to prepopulate and disable sender email, HTML format messaging etc

Once configured, the service can be published to the target user entry point(s). The published service will have configured features including:

Message creation/reply – Message creation and reply from citizen and user entry points as configured by the service configuration administrator.

Secure file exchange – Files can be securely uploaded and attached to messages from both the sender and receiver (if configured), with configurable allowable file types and virus scanning on upload to protect both parties and the platform.

Track Conversations – Service administrators and message senders and receivers can view message statuses and track all messages within conversations.

Track Action History – Secure Messaging encapsulates all secure communications within one service, so all message actions from both the citizen and admin are tracked and visible to administrators within an action history ensuring all actions remain auditable.

Track Email Events – All Secure messaging email notifications for messages are tracked and visible to administrators within an email events history view, again ensuring all actions remain auditable.

2.3.The Platform (“Secure Foundations”)

The Secure Messaging service is provisioned on the Digital Toolkit platform hosted on the Stiona Toolkit Azure Cloud as standard. Should the business require the service to be hosted on a business owned instance, please see 6.9 Hosting Services.

The Digital Toolkit is a public cloud shared services platform that provides a suite of **reusable services** backed by a core set of management microservices including Identity management, Service User Management, Configuration Management, Notifications Management, Payments services, Business and Portal Admin services. This provides Secure Messaging the following service capabilities:

Device responsive – All secure messaging features are available on both desktop and mobile; however, some complex configuration screens and tracing through conversations are easier to navigate on a larger desktop screen. There is no reduction in security or access controls across devices, ensuring consistent performance and functionality for all users.

Virus Scanning – All message document uploads are virus scanned before being uploaded into the secure platform for attachment to secure messages.

Audit – the platform audits and tracks user interactions and provides an event history for tracking as part of message event detail.

Accessibility – Secure Messaging is accessibility tested and independent verified at WCAG 2.2 AA and we are actively working towards AAA conformance.

Multi language support – Secure Messaging provides limited multi language support for citizen forms. It does not provide multi language support for business admin forms, just published citizen forms.

Operational Reporting – An optional reporting module can be enabled, and service reports can be enabled at additional cost. See section 6.8 Custom development services.

The **platform is ISO27001 and ISO9001 accredited** and is built on a highly secure proven architecture which provides isolation of resources through autoscaling, load balancing, and logically separated multi-tenant architecture. Each customer's environment is allocated dedicated or appropriately partitioned compute, storage, and database resources, ensuring that performance is not affected by activity from other users. This ensures **consistent, reliable performance for all customers**.

The Secure Messaging service application is accessible from **supported web browsers** and does not require the Buyer to manage or control the underlying cloud infrastructure (unless linked to the Buyers own infrastructure by request).

3. Onboarding and Offboarding

3.1. Onboarding

We provide comprehensive online user documentation to help users begin using the Secure Messaging service. As part of standard service delivery, we will:

1. ***Publish the service to the target user groups*** (e.g. Citizen Portal, Authenticated citizen etc)
2. ***Configure the chosen authentication mechanism*** (if already supported by the platform identity service, additional integrations will cost extra)
3. ***Configure the service user roles*** applicable to each user group.
4. ***Create the initial 'Super' Admin users.***

Additional onboarding and mobilisation services are available at extra cost, including support with service and organisation configuration and message flows, business process mapping, forms configurations design, data migration, and remote or onsite user training. We can also assist with user testing preparation and execution to ensure a smooth and successful rollout where required. We highly recommend that for complex implementations that you consider mobilising our forms configuration design service support.

3.2. Offboarding

At the end of the contract, we provide a structured offboarding process to ensure a smooth transition. Included in the contract price are:

1. ***export of customer data*** in an Azure SQL supported format,
2. ***account closure***
3. ***revocation of user access for all user groups.*** This can be phased if required.

Users retain full ownership of their data.

Additional-cost services include assisted data migration, bespoke export formats, extended access beyond the contract end date, or support with transition to another supplier. All end-of-contract activities follow agreed security and data-retention requirements.

3.2.1. End of contract data extraction

All user data is ***encrypted in transit and at rest*** and stored in an Azure SQL database. Stored user details can be extracted in several ways. As standard, we provide a complete CSV export of all customer data at the end of the contract at no additional cost. Service configuration can be exported as JSON at any time. Additional export formats or structured migration support can be provided on request, subject to Azure SQL capabilities and may incur extra cost. All data extractions are delivered securely and follow agreed timelines and data-retention requirements.

4. The Digital Toolkit Platform

The Digital Toolkit platform is designed using a ***multi-layered security architecture that protects customer data, ensures resilient operation, and meets the security expectations of public sector organisations.***

4.1. Platform Security Architecture

1. **Hosting** – The Secure Messaging service runs in a high-availability architecture across Azure UK South and West data centres, with real-time replication of databases and file stores using geo-redundant services and SQL Failover Groups
2. **Network** – Network protections include
 - a. Private network or public sector network
 - b. TLS (Version 1.2 or above)
 - c. IPsec or TLS VPN gateway
3. **Identity & Access Management** – Is managed by the platform Identity service and includes
 - a. Authentication via Azure AD / the customer's configured identity provider
 - b. Single Sign-On (SSO) for internal admin users
 - c. Role-Based Access Control (RBAC) enforced at platform and application layers
 - d. Principle of least privilege for all roles
 - e. MFA enforced through the customer's IdP
4. **Multi tenancy security** – The platform supports multi tenancy and manages this through:
 - a. Logical separation of tenants within the platform
 - b. Strict segregation of data access paths
 - c. Tenant-specific roles, permissions, and boundaries
 - d. Isolation of workflows, forms, and case data
 - e. Isolation tested and validated during assurance activities
5. **Application Security** – We ensure the platform itself is built securely including
 - a. Logical separation of tenants within the platform
 - b. Strict segregation of data access paths
 - c. Tenant-specific roles, permissions, and boundaries
 - d. Isolation of workflows, forms, and case data
 - e. Isolation tested and validated during assurance activities

6. **Data Security** – Data is encrypted in transit and at rest in UK data centres. Database access is controlled by private networking and firewalls.
7. **Logging, Monitoring & Alerting** – Proactive monitoring and detection including real time anomaly detection and security alerts, extensive audit logging for authentication, data access and administrative actions.
8. **Vulnerability & Patch Management** – Regular penetration testing with a product roadmap including patch application for infrastructure components and scheduled application release with security updates if required.
9. **Data Protection & Compliance** – Compliance with UK GDPR and Data Protection Act 2018 including secure data management, retention and disposal processes. DPIA support additional cost services available if requested.

4.2. Disaster Recovery

Disaster Recovery capabilities are built into the Digital Toolkit platform as part of the **standard service**. The platform is hosted within Microsoft Azure UK regions using a resilient architecture designed to maintain availability in the event of a component or site-level failure. The standard DR capability includes:

1. **Resilient, multi-zone architecture**
2. **Encrypted, automated backups**
3. **Defined recovery objectives (RTO/RPO)**
4. **Platform-level failover processes** - Infrastructure and core platform services are configured with automated failover or rapid redeployment processes to minimise downtime in the event of failure.
5. **Regular (annual) testing and validation** - DR processes are periodically tested as part of ISO platform assurance activities to ensure recovery procedures remain effective
6. **Secure data restoration**

These Disaster Recovery capabilities relate to the resilience and recoverability of the Digital Toolkit platform itself. Stiona's support for customer-specific Business Continuity planning, operational continuity processes, or wider organisational risk management is not included as part of the standard service and is available as an optional, additional-cost professional service.

5. The Stiona Managed Service

Support for the Secure Messaging service is provided via ***the Stiona Managed Service from 08:00–18:00, Monday to Friday excluding Northern Ireland bank and public holidays.***

Standard Support ***includes email/ticket assistance and knowledge base access to user guidance material at no additional cost.*** Premium Support (optional) is available at additional cost and provides 24/7 phone/email support, faster SLAs, and access to a dedicated Technical Account Manager or Cloud Support Engineer, with pricing agreed per contract.

5.1. Service Level Agreements (SLAs)

Standard Secure Messaging support service SLA are highlighted below. Please contact us for full details of the Stiona Managed Service including definitions of priority levels and incident/problem management escalation processes.

Impact on service	Response Time	Resolution Time (Support)	Resolution Time (Defect)
Critical – P1	30 minutes	4 hours or as agreed by problem diagnosis	8 hours
High – P2	1 hour	6 hours or as agreed by problem diagnosis	32 hours
Moderate – P3	2 hours	8 hours or as agreed by problem diagnosis	Next planned release
Minor – P4	4 hours	12 hours or as agreed by problem diagnosis	Next planned release

Table 1 - Service Level Agreements

5.2.Support and Service Management

As standard, the Secure Messaging service support cost covers platform support and Secure Messaging incident/problem management including:

Platform costs cover:

1. **Live Support** including:
 - a. Incident Management & Reporting
 - b. Routine infrastructure maintenance
 - c. Bug fixing and security upgrade patching
 - d. Annual external Security Assurance Testing support and remediation
2. **Proactive optimisation** including:
 - a. Backups and disaster recovery
 - b. Automated transaction volume monitoring and scaling
 - c. Automated service health checks with configurable service availability alerts
3. **Platform governance** including:
 - a. Disaster recovery planning
 - b. User role reviews and MFA compliance

Incident/Problem management support includes:

1. Access to the **Stiona Service Desk for logging incidents** during standard support hours.
2. **Incident triage and prioritisation** based on severity and impact.
3. **Response and resolution** of service incidents, including workarounds where needed.
4. **Restoration of normal service** following platform issues or outages.
5. **Identification of recurring or underlying issues** impacting stability or user experience.
6. **Implementation of permanent fixes or corrective actions** to prevent recurrence (where within platform or service scope).

Stiona can provide a comprehensive Managed Service that covers all aspects of support and service management for the Digital Toolkit platform. This includes incident resolution, request fulfilment, system monitoring, change control, release management, and ongoing communication with the customer to ensure stable and reliable service performance.

Additional support and service management are available at additional cost. See section 6.5 Enhanced Support/Extended hours.

6. Additional Professional Services – For Information Purposes

Stiona can also offer the following service and customer delivery support services at additional cost:

6.1.Mobilisation services

Stiona can provide customers with additional support throughout the delivery period from contract award to the point the service becomes operational and under Managed service scope. This includes

1. Project/Programme planning and co-ordination
2. Planning and guided User Acceptance Testing
3. Implementation planning
4. Data migration support
5. Customer engagement support
6. Training materials and delivery via multiple channels
7. Change Management activities

6.2.Enhanced Configuration & Solution design services

We offer additional design services that go beyond standard onboarding into deeper implementation work including:

1. Advanced workflow design and optimisation
2. Advanced Form design and configuration services
3. Integration and design workshops
4. Requirements gathering / discovery sessions
5. Process mapping and business process re-engineering

6.3.Data Services

We offer additional data management services including:

1. Complex data migration support (multiple sources, data transformations and complex cleansing)
2. Legacy system extraction consultancy
3. Data modelling and design

6.4.Payment Services

We offer additional payment management services including:

1. Assistance in establishing the payment product catalogue configuration
2. Integration to payment provider(s) other than Worldpay or Gov.UK Pay
3. Additional payment reporting

6.5.Enhanced Support/Extended hours

We can offer enhanced or extended support on request including:

1. Extended service desk hours
2. Out of hours incident response
3. Priority Service levels with faster SLAs
4. Scheduled Evening/ Weekend maintenance windows
5. Extended proactive monitoring and notifications
6. Regular service review reporting and meetings

6.6.Business Continuity planning & support

We offer additional business continuity planning and support services including:

1. Helping the customer write or update their BC plan
2. Running BC workshops with stakeholders
3. Scenario modelling and impact assessments
4. Establishing customer playbooks or continuity checklists

6.7.Business security risk management support

We offer additional business security risk management services including:

1. Threat and risk assessments
2. Security policy development
3. Governance and compliance reviews
4. Support in meeting internal audit requirements

6.8. Custom development services

We offer additional custom development services including:

1. Bespoke module or feature development
2. Custom reporting/dashboard creation
3. Custom front-end design for forms and portals
4. Branding and UX improvements
5. Enhanced document management and bundling solutions
6. Enhanced Reporting services linked to service dashboards

6.9. Hosting Services

As standard, the Secure Messaging service will be provisioned and hosted on the Stiona Digital Toolkit. We can also provision the Digital Toolkit platform and Secure Messaging service onto another business Azure subscription at additional cost if required. Custom URL(s) and/or DNS configuration would be additional.