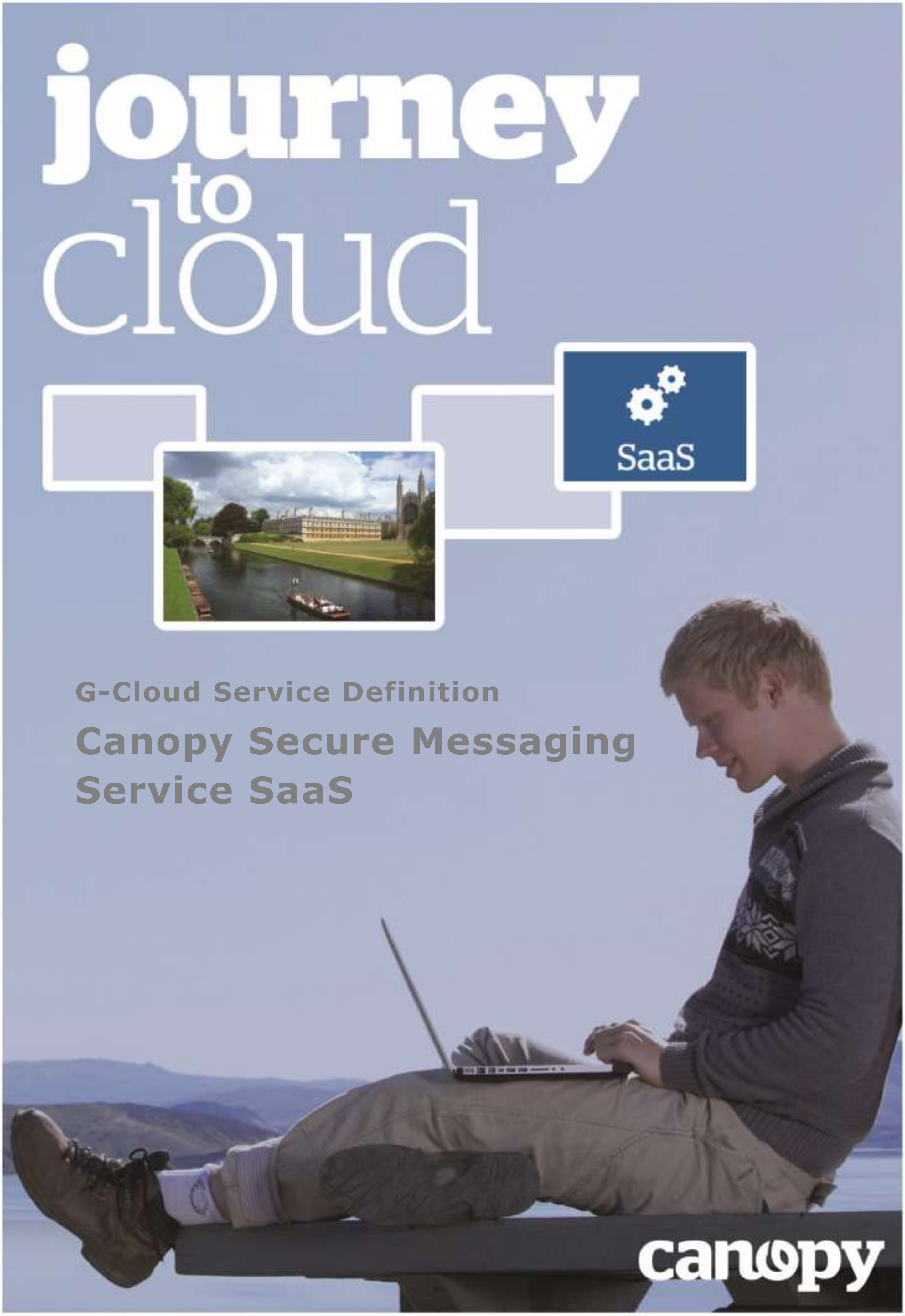


G-Cloud Service Definition

Canopy Secure Messaging Service SaaS

Canopy Secure Messaging Service

The Secure Messaging Service enables your organisation to securely exchange messages between disparate internal and external systems, in an "integrate anything and everything" approach. It is a highly-available highly-secure pay per message messaging service that can both send and receive data up to RESTRICTED and OFFICIAL with the ability to handle all Government approved data standards and connects over the internet, Government Secure Intranet (GSI), Government Convergence Framework (GCF) and Public Service Network (PSN).

Benefits

Canopy Secure Messaging Service – Software as a Service

- **Lower cost solution**

  Canopy enables cost effective data sharing both internally and externally, and reduces the people overhead of manual intervention by simplifying message flows, removing redundant messages and system interconnects.

- **Business outcome focused**

  Canopy aligns to your business outcomes in a cost-effective manner, so you only pay for successfully delivered messages; and transactional demand rather than reserved resources.

- **Business change flexibility**

  Canopy allows your organisation to be more responsive and flexible to change by removing complex, costly and difficult to change one-to-one interfaces.

- **Business change velocity**

  Canopy allows your organisation to introduce and integrate solutions more quickly, thanks to reusable standardised patterns. This can enable your organisation to realise business benefits sooner.

- **Cloud enabler**

  Canopy supports migration to the cloud by decoupling systems thereby allowing your organisation to benefit from scalable, flexible and cost effective services.

- **Open data**

  Canopy allows your organisation to securely expose data services, such as data enquiry and data update web services, to other government and non-government data consumers.

- **Low barrier to exit**

  Canopy has a very low barrier to exit as off boarding is quick and cheap. There is no cloud lock-in as this service is open standards and open source based.

- **Alignment to Government ICT strategy**

  Canopy aligns with Government ICT Strategies of Cloud, SaaS, open standard, open source, and digital.

Service Summary

What is it?

This software as a service offering is a secure messaging service software solution, configurable for your specific messaging or data transfer services requirements. The secure messaging service is powered by an open source, open standard enterprise service bus built using Red Hat JBoss Fuse. The underlying platform is Pan Government Accredited (PGA) to Impact Level 3 (IL3) and is a cloud solution hosted and supported within the UK.

Features of the service include:

- Secure reliable messaging service software platform for your specific messaging or data transfer services
- Service orchestration, and content and rules based routing
- Message validation, transformation, traceability and auditability
- Ability to prioritise certain messages where required
- Ability to push or pull data between connected end points
- Ability to handle all Government approved data standards, message types and formats.

What makes us unique?

The Canopy Secure Messaging Service is a UK based 24x7x365 highly-available highly-secure pay per message messaging service that enables the exchange of secure messages containing data, up to the HMG protective marking of RESTRICTED and the revised Government Protective Marking Scheme (GPMS) of OFFICIAL, between connected systems.

The service is charged for on the basis of successful message delivery, thereby achieving a business outcome with no minimum volume commitment.

There is a very low barrier to exiting the service with no minimum volume commitment; no contractual tie in period, a quick and cheap off-boarding process supported by our open standard and open source commitments.

Canopy and Atos successfully deliver to key central government, local government, health and transport customers using the people, technology and data centres that are the key ingredients of this service. We are trusted to deliver to our existing customers and we will build this same trust with you by delivering this secure, robust, scalable, flexible, business enabling service.

What's Included

The following list describes the basic components included within the service:

- Secure timely exchange of messages between systems
- A bug fix service for your configured services and settings
- PSN and internet access bandwidth
- Monthly billing and message reporting
- Service management wrapper including incident management
- Standard backup service
- Standard disaster recovery service.

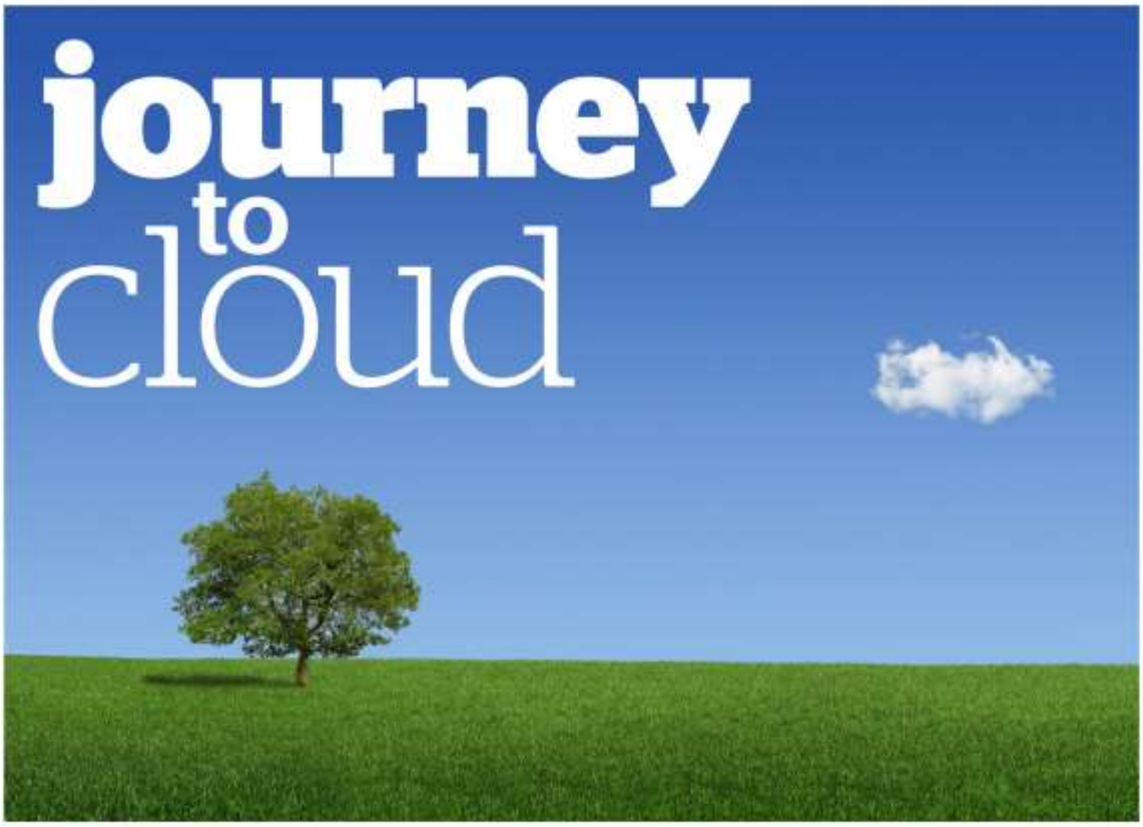
Who Can Benefit

The Secure Messaging Service enables your organisation to securely exchange messages between disparate internal and external systems. Amongst other use cases, the Canopy solution enables public services agencies to:

- Connect public-facing services to back-end systems
- Connect multiple organisations that need to securely share and exchange data of different security classifications (at up to RESTRICTED or OFFICIAL security classifications)
- Connect systems for the exchange of biometric or biographic information, checks and notifications
- Connect case working systems, passport systems, and identity systems
- Automatically extract 'pull' information from other systems (data collection)
- Automatically send 'push' information to other systems (data propagation).

Furthermore, the solution is "backwards compatible" meaning that it is flexible and will meet the requirements of existing services and legacy system connections.

canopy



About Canopy

Canopy focuses on your business goals. We focus on the technology so you can focus on what it can do for your company. Our offerings range from cloud infrastructure and private cloud to platform offerings, application development and strategic consultancy.

We help you enrich your business
It's that simple. Canopy is the end-to-end cloud services provider, enabling customers to get the most from the cloud, through world-class datacenter and consulting services. Powered by the leading technology and continuous innovation from leaders in the IT sector - Atos, EMC, and VMware - Canopy helps you reimagine tomorrow's business.

Our secure on and off premise private clouds give you access to the fast-growing ecosystem of essential cloud-based business solutions, best practices and processes you need to compete today, and in the future. We help you bring all your clouds under one set of processes, one environment, one Canopy.

www.uk.atos.net/g-cloud

canopy
the atos cloud

Contents

1. Introduction

1.1 Service summary

The Secure Messaging Service enables your organisation to securely exchange messages between disparate internal and external systems, in an "integrate anything and everything" approach. In summary, the service:

- is a unique highly-available highly-secure pay per messaging service that can both send and receive data
- powers the exchange of secure messages containing data up to RESTRICTED and OFFICIAL
- gives the ability to handle all Government approved data standards connects over the internet, Government Secure Intranet (GSI), Government Convergence Framework (GCF) and Public Service Network (PSN).
- is secure, flexible, robust and scalable.

This software as a service offering is a secure messaging service software solution, configurable for your specific messaging or data transfer services requirements. This service includes a bug fix service for your configured services and settings. The secure messaging service is powered by an open source, open standard enterprise service bus built using Red Hat JBoss Fuse.

The underlying platform is Pan Government Accredited (PGA) to Impact Level 3 (IL3) and is a cloud solution hosted and supported within the UK. An on premise 'private cloud' solution in your data centres can be implemented if required.

Benefits

- Aligns to your business outcomes in a cost-effective manner, so you only pay for:
  - successfully delivered messages
  - transactional demand rather than reserved resources
- Enables cost effective data sharing both internally and externally
- Allows your organisation to be more responsive and flexible to change by removing complex, costly and difficult to change one-to-one interfaces
- Improves the speed, quality and accuracy of data e.g. ensuring that messages are sent in the correct format, using validation
- Supports migration to the cloud by decoupling systems which allows your organisation to benefit from scalable, flexible and cost effective services
- Allows your organisation to securely expose data services, such as data enquiry and data update web services, to other government and non-government data consumers
- Reduces the effort and management overhead of manual intervention by simplifying message flows, removing redundant messages and system interconnects
- Allows your organisation to introduce and integrate solutions more quickly, thanks to reusable standardised patterns. This can enable your organisation to realise business benefits sooner.

Key characteristics:

- Pay per successfully delivered message
- No minimum volume per customer
- Low barrier to exit as off boarding is quick and cheap
- No cloud lock-in as this service is open standard and open source
- Secure reliable messaging service software platform for your specific messaging or data transfer services
- Message traceability and auditability
- Ability to prioritise certain messages where required
- Ability to push or pull data between connected end points
- Ability to handle all Government approved data standards, message types and formats
- Aligns with Government ICT Strategies of Cloud, SaaS, open standard, open source, and digital.

1.2 How this product can be used

This product has been designed to be used in a variety of different ways, including providing one-to-one or one-to-many connections between internal systems.

Furthermore, this product can be used to share and exchange data between your organisation's systems and other external organisation's systems.

Examples of practical uses include,

- Connecting public-facing services to back-end systems
- Connecting multiple organisations that need to securely share and exchange dataConnecting systems between different security classifications (at up to RESTRICTED or OFFICIAL security classifications)
- Connecting systems for the exchange of biometric or biographic information, checks and notifications
- Connecting case working systems, passport systems, and identity systems
- Automatically extracting 'pull', information from other systems (data collection)
- Automatically sending 'push' information to other systems (data propagation).

Furthermore, the solution is "backwards compatible" meaning that it is flexible and will meet your existing services and legacy system connection requirements.

Your services will connect to the Canopy Secure Messaging Service over your preferred access method (internet, GSI, GCF or PSN). The Canopy Secure Messaging Service will be configured to link into the endpoints that you specify, and rules will be set based on your business and technical requirements.

Canopy Secure Messaging Service has been flexibly designed to work with various rules including either 'push' (messages are sent immediately) or 'pull' (recipients can extract the message when convenient) depending on your desired business processes.

2. Service overview

Canopy Secure Messaging Service is a UK based 24x7x365 highly-available highly-secure pay per message service that enables the exchange of secure messages containing data, up to the HMG protective marking of RESTRICTED and the revised Government Protective Marking Scheme (GPMS) of OFFICIAL, between connected systems. The messages can be exchanged over the internet, Government Secure Internet (GSI), Government Convergence Framework (GCF) and Public Service Network (PSN). The messages can be encrypted in transit and digitally signed. Messages received by the service are digitally validated as having been sent from a trusted source, and checked for malicious threats.

The underlying platform is Pan Government Accredited (PGA) to Impact Level 3 (IL3) and is a cloud hosted solution in the UK, supported by SC cleared engineers. The system is secured with a security gateway that assures the integrity of the data and mitigates malicious attacks such as Distributed Denial of Service (DDoS), XML injection, virus and Trojans. An on premise ‘private cloud’ solution in your data centres can be implemented if required.

The system is powered by an open source, open standard enterprise service bus (ESB) built using Red Hat JBoss Fuse which has a request, response and notification service that can be either synchronous or asynchronous.

The service has the capability to support a range of industry standards including JMS 1.1, TCP, SSL, UDP, MQTT, AMQP (tech preview) and multicast transport protocols plus others including Ajax, REST, SOAP, WSDL, JAX-WS, WS-Security and WS-Reliable Messaging.

Based on the National Institute of Standards and Technology (NIST) definition this product is an application accessible from a programme interface where the customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or individual application capabilities except for user-specified application configuration and settings. The user-specific application configuration and settings are your specific messaging or data transfer services configuration and settings. A bug fix service is provided for your specific messaging or data transfer services configuration and settings.

Service management is included within the charges and is fully ITIL aligned.

Your Service’s Complexity

The complexity of the service is based on the total number of message attributes used within your service. An attribute is a field within a message.

	Simple	Medium	Complex
Total number of message attributes used within your service	<1000	1001 to 2999	3000 to 6000

Message Delivery

The Canopy Secure Messaging Service has been designed to align to business outcomes of successful message delivery within a timely manner based on your specific services' complexity (see above and section 9), or no charge is applicable. The service will:

- Attempt to deliver, retry, and then if still unsuccessful, provide an error message to the sender
- Send message receipts to confirm the successful submission of a message. This feature can be turned off if required.

An example of a reason for non-delivery could be that the target system is unavailable.

Key functions of the service are:

- Content and rules based routing
- Synchronous and asynchronous messages handling
- Message schema validation
- Message transformation
- Queuing and temporary persistence of messages
- Secure reliable messaging
- Service orchestration
- Content splitting, filtering and complex event processing
- Support of many message formats including Open Standards
- Support for transactions and files
- Support for scheduled, throttled, blocked, and held messages.

Bug Fixing Service

Bug fixes for the secure messaging service software solution and underlying platform are included within the pay per message pricing model. As part of the Canopy Secure Message Service there is an inclusive service of discrete bug fixing (involving modifications to the Customer Content) to address problems on your specific services' configuration or settings. Key functions of the bug fixing service are:

- Analysis of problems identified that prevent successful processing or delivery of messages
- Modification of configuration or settings, testing and deployment of the relevant fix, which will follow standard ITIL practices.

Benefits of the bug fixing service option include:

- Faster completion of business process as messages are processed faster
- Enhanced service as more messages are successfully exchanged.

If you do not wish to make use of this bug fixing service then you may choose to opt-out. If you choose to opt-out you will need to ensure an equivalent service is supplied.

2.1 Service Roadmap

The future service roadmap will deliver:

- Enhanced Management Information
- User administration portal.

Both features are eue to be available in 2015.

No features are being retired.

Additionally Atos offer the following complementary offerings to further configure this product:

- Solution Architecture and Design, Service ID: 4.G4.0261.230
- Business Intelligence Dashboards and Analytics, Service ID: 4.G4.0261.212
- Software Development Services, Service ID: 4.G4.0261.231
- Solution Architecture and Design, Service ID: 4.G4.0261.230
- Data Extract Transform and Load (ETL) and Data Migration, Service ID: 4.G4.0261.245
- Mobile Solutions Development, Service ID: 4.G4.0261.203
- Atos Shared Hosting IaaS, Service ID: 3.G2.039.002
- Atos Shared Hosting PaaS, Service ID: 3.G2.039.042.

3. Information assurance

The underlying platform is Pan Government Accredited (PGA) to Impact Level 3 (IL3).

Departmental accreditation will be required for our specific messaging or data transfer services configuration and settings.

The service can transport messages up to and including HMG protective marking of RESTRICTED and the revised Government Protective Marking Scheme (GPMS) of OFFICIAL.

The architecture and location of the service is capable of being accredited to carry data at a higher protective marking than RESTRICTED or OFFICIAL.

4. Backup/restore and disaster recovery

Backup

Standard backup of the service and all configuration and settings is provided as follows:

- 6 incremental backups per week
- 1 full backup per week
- Backups retained for 28 days as the data is transitory
- Backups retained on local site and offsite

Backup may be further enhanced by utilising Atos’ Platform as a Service (IL3) G-Cloud offering.

Disaster recovery

As this is a cloud service there will be no charge for messages lost during a disaster situation.

This service is deployed across two data centres in an active-passive configuration. In other words all messages are managed by the primary data centre with failover to the standby data centre in the event of a disaster. Customers are therefore abstracted from the failure. The target restore time objective (RTO) is 48 hours.

Connected systems are required to queue new messages during a disaster situation and to re-send “lost” messages when the service is returned to operation.

Disaster recovery can be enhanced by utilising Atos’ Platform as a Service (IL3) G-Cloud offering.

5. On-boarding and off-boarding

Integration of CSMS into the Customer's existing solutions has been designed to be as simple as possible.

5.1 On-boarding

The on-boarding project can take between 2 weeks and 4 weeks depending on your service's complexity.

	Simple	Medium	Complex
Before go live ▸ Release to production and disaster recovery ▸ Operational Acceptance Testing ▸ Knowledge transfer	1 week	2 weeks	4 weeks
After go live ▸ Early life support ▸ Service acceptance	1 weeks	2 weeks	4 weeks
Total number of weeks	2 weeks	4 weeks	8 weeks

In advance of the on-boarding project, Canopy will provide a pre-requisites document and a step by step guide.

Knowledge transfer will be a series of workshops covering an overview, documentation, functional requirements, testing procedures, deployment and support processes.

5.2 Off-boarding

To off-board, a Customer will switch their systems to point to another messaging service and allow the in-flight messages to complete. This final processing duration is dependent on customer specific configuration.

Once all in-flight messages have completed the off-board process is complete and no data will persist in the CSMS.

An alternative off-boarding approach is to shut the system down and make the connected systems resend messages to the new messaging service.

If the Customer requires a copy of the message audit logs for security auditing, a copy can be provided at an additional charge.

6. Pricing

The pricing for Canopy Secure Messaging Service is based on the complexity of your service(s):

Set-up		
On-boarding	**Price**	**Frequency**
On-boarding	£30,000	One time cost per service
Customer project	**Price**	**Frequency**
Assisting customer project	SFIA rate card	One time cost

Run			
Price per message per month £			
Message Banding*	**Simple**	**Medium**	**Complex**
1 to 500,000	£0.096	£0.101	£0.106
500,001 to 1,000,000	£0.052	£0.056	£0.060
1,000,001 and above	£0.032	£0.036	£0.040

Off-boarding			**Frequency**
Copy of audit data	£500	price per copy	One time cost
Knowledge Transfer to other party		SFIA rate card	One time cost

* Message Banding based on total number of messages with a customer across all their services

7. Service management

Support is provided by UK Based security cleared staff (to SC clearance) and is delivered via ISO27001, ITIL and HMG certified services. Full details of the service are provided as part of the on-boarding process.

The service is monitored 24x7 for any issues and our support teams will respond and deal with these issues as they arise.

The CSMS will provide the following ITIL service functions:

- Availability Management
- Capacity Management
- Change Management
- Continuous Service Improvement
- Demand Management
- Incident Management
- Major Incident Management
- Monthly Service Reporting
- Problem Management
- Release Management
- Service Management.

Service reporting and management information

A daily report will be emailed to the Customer detailing the volume of messages processed.

A monthly report will be provided to the Customer detailing the following:

- Chargeable message volumes
- Non-chargeable message volumes
- Message error rate
- Forward schedule of patching
- Defects analysed as part of the bug fixing service, resolution status and any hot fixes applied.

8. Service constraints

The CSMS service is limited to:

- Exchanging messages with a maximum size of 3MB.

9. Service levels

Messaging Service

Message delivery will be near instantaneous and the following service levels are an indication of worst case.

Key performance Indicator	Target Value	What happens if exceeded	Reporting Requirement
Messages delivered, measured 24 hours a day 365 days a year, except during planned maintenance windows	100% within or equal to x* hours based on receipt and delivery of each message as logged by the billing engine	Message is not chargeable	Chargeable and non-chargeable messages are reported in the monthly service report

* see the following table for the definition of x

Your service's complexity	Message delivery within (x)
Simple	1 hour
Medium	2 hours
Complex	4 hours

Bug Fix Service

Key performance Indicator	Target Value	What happens if exceeded	Reporting Requirement
Bug fix analysis	Analysis performed within or equal to y* hours based on identification/report of the problem.	Messages no not processed ad as result of the defect continue not to be chargeable	Bug fix analysis and any related incident and problem records will be reported as part of the monthly service report

* see the following table for the definition of y

Your service's complexity	Analysis performed within (y)
Simple	4 hour
Medium	8 hours
Complex	12 hours

Incident Hours

The following support hours are provided as part of the services detailed above:

- Standard Working Hours/Days – Monday to Friday 08:00 to 18:00 excluding public holidays.(clock stops outside service hours)
- Out of hours support will be provided 24x7 for priority 1 and 2 incidents only

Incident Classification

The following table defines the incident classification for priority 1 and 2 incidents.

Priority Level	Impact	Description	Result
P1	Critical	System Down	The Service cannot operate due to failure of the CSMS in the Production environment.
P2	Serious	Major Disruption	The main software function of the Service operates but is disrupted (i.e. has an impact on the end result of the software) due to failure of the CSMS in the Production environment.

Maintenance Windows

Maintenance windows for this service are monthly and will be published within the forward schedule of change in the Monthly Service Report and follow ITIL processes. It is anticipated that the maintenance windows will be on Thursdays between 7pm -10pm and as agreed at weekends.

10. Financial recompense

To minimise the cost to users, Canopy does not provide service credits for use of the service. All Canopy services are provided on a reasonable endeavours basis. Please refer to G Cloud terms and conditions.

In accordance with the guidance within the GPS G-Cloud Framework Terms and Conditions, the Customer may terminate the contract at any time, without cause, by giving at least thirty (30) Working Days prior notice in writing. The Call Off Contract terms and conditions and the Canopy terms will define the circumstances where a refund of any pre-paid service charges may be available.

11. Training

Training can be provided at the rates defined in our Skills for the Information Age (SFIA) rate card that was submitted as part of our G-Cloud submission.

12. Ordering and invoicing process

Ordering this product is a straightforward process.

Please forward your requirements to the email address GCloud@canopy-cloud.com Canopy will prepare a quotation and agree that quotation with you, including any volume discounts that may be applicable.

Once the quotation is agreed, Canopy will issue the customer with the necessary documentation (as required by the G-Cloud Framework) and ask for the customer to provide Canopy with a purchase order.

Once received, the customer services will be configured to the requirements as per the original quotation.

For new customers, additional 'new supplier' forms may need to be completed.

Invoices will be issued to the customer and Shared Services (quoting the purchase order number) for the services procured. On a monthly basis, Canopy will also complete the mandated management information reports to Government Procurement Services detailing the spend that the customer has placed with us. Cabinet Office publish a summary of this monthly management information at:

http://gcloud.civilservice.gov.uk/about/sales-information/.

13. Termination terms

13.1 By consumers (i.e. consumption)

Termination shall be in accordance with:

- The G-Cloud Framework terms and conditions
- Any terms agreed within the Call Off Contract under section 10.2 of the Order Form (termination without cause) where the Government Procurement Service (GPS) guidance states 'At least thirty (30) Working Days in accordance with Clause CO-9.2 of the Call-Off Contract'
- Canopy Supplier Terms for this Service as listed on the G-Cloud CloudStore.

For this specific service, by default Canopy ask for at least thirty (30) Working Days prior written notice of termination as per the guidance within the GPS G-Cloud Framework Terms and Conditions.

13.2 By the Supplier (removal of the G-Cloud Service)

Canopy commits to continue to provide the service for the duration of the Call Off Contract subject to the terms and conditions of the G-Cloud Framework and Atos Supplier Terms.

14. Data restoration / service migration

Data restoration

On-boarding will include the introduction of configuration data.

Configuration can be restored from backup.

Service Migration

Should the service be terminated the off-boarding process described in Section 5 will be invoked. Due to the nature of the service all data is transitory i.e. once messages are processed there is no data migration requirement.

15. Customer responsibilities

The following lists the Customer’s responsibilities in relation to this service:

- End to end service integration
- On-boarding
  - Provision of Customer Content (e.g. your service’s configuration and settings), documentation and knowledge transfer workshops
  - Participation in service acceptance activities
  - Carrying out your departmental accreditation
  - Provision of early life support for a period defined in section 5
  - The Customer must reconfigure the Customer’s own network, infrastructure and systems to connect to this service. And the customer is responsible for ensuring any of the connected systems are configured to connect to this service. Where appropriate, this includes provision of a GSI or GCF to PSN bridge.
  - Compliance with this service’s code of connection and operational rules such as:
    - Service hours of receiving systems
    - Maximum files sizes
    - Adherence to the specific interface definitions supported by the system
    - Connected systems are required to queue new messages during a disaster situation and to re-send “lost” messages when the service is returned to operation
- Run
  - The service is dependent on the Customer’s Service Desk, ITIL tooling and management of ITIL processes.
  - The service is dependent on the Canopy support teams having access to the Customer’s Service Desk and ITIL tooling.
  - Demand forecasting and reasonable notice for any changes that may impact this service
  - Provision of bug fix environments and any other environments required
  - The service is dependent on the Canopy support team having continued access to the Customer’s bug fix environments
  - User acceptance testing for any bug fixes
  - If you choose to opt-out of this service’s bug fix service then you will need to ensure an equivalent service is supplied
  - Integrity of message format and payload sent to the service
- Off-boarding
  - Provision and collection of media for a copy of your audit data in compliance with relevant security procedures.

16. Technical requirements

Connectivity

The messages can be exchanged over the following networks

- Internet
- Government Secure Intranet (GSI) via the customer’s GSI to PSN bridge
- Government Convergence Framework (GCF) via the customer’s GCF to PSN bridge
- Public Service Network (PSN) which is directly connected to the CSMS infrastructure.

The bandwidth and latency requirements are dependent on the characteristics and volume of messages the Customer wish to exchange and the number of systems the Customer wish to connect with.

Capability to support a range of industry standards including SMTP, JMS 1.1, TCP, SSL, UDP, MQTT, AMQP (tech preview) and multicast transport protocols plus others including Ajax, REST, SOAP, WSDL, JAX-WS, WS-Security and WS-Reliable Messaging.

Message error rate

The service provided to each customer has a maximum message error rate of 0.05% of message volumes, where message errors are not caused by the CSMS. The error rate is calculated over a calendar month. The error rate is set to ensure the quality of connected system messages is kept to a reasonable standard and the service can be priced economically. We would typically expect the message error rate to be substantially less than this number.

Bug Fixing Service environments

The requirements specification of these environments will be provided during on-boarding.

17. Trial service

A trial service is not currently available.

However, we would be happy to assist the Customer to carry out a proof of concept. The following G-Cloud products would be utilised for the above task:

- Atos Architecture Consulting, and Security Consulting
- Atos Test and Development platform
- Atos Shared Hosting Trusted Agile Infrastructure
- Atos Cloud Professional Services for Solution Design and testing.

18. Glossary

Term	Description
AMS	Application Management and Support
BaU	Business as Usual
CESG	Information Assurance arm of GCHQ (Communications-Electronics Security Group)
CLAS	CESG Listed Adviser Scheme
CR	Change Request
CMDB	Configuration management database
CMS	Content Management System
COTS	Commercial off-the-shelf
DIS	Departmental Interface Server
DoS	Denial of Service
DR	Disaster Recovery
E&B	Extend and Blend Programme
FCO	Foreign and Commonwealth Office
FMOP	Free Movement of Persons
FWSM	Firewall Service Modules
GCHQ	Government Communications Headquarters
GPMS	Government Protective Marking Scheme
GSI	Government Secure Intranet
IA	Information Assurance
ITF	Integrated Test Facility
ITIL	Information Technology Infrastructure Library (ITIL) is a set of concepts and practices for Information Technology Services Management (ITSM),
ITHC	Information Technology Health Check
MIS	Management Information System
OS	Operating System
PaaS	Platform as a Service
PID	Project Initiation Document, as defined in PRINCE2
PM	Project Manager
PSN	Public Service Network

Term	Description
RMADS	Risk Management and Accreditation Documentation Set
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
TBC	Team Based Case-working system
VLAN	Virtual Local Area Network
XML	Extensible Markup Language

journey to cloud

uk.atos.net/g-cloud