RocStac™ Cross Domain Security Guard

For G-cloud 9

Roc Technologies Limited, Wharf House, Wharf Street, Newbury, RG14 5AP

T. 01635 581188 F. 0845 647 6001 www.roctechnologies.com info@roctechnologies.com

Service assessment guide

What the service provides

The Roc Cross Domain Security Zone (CDSZ) enables you to securely transfer data between the Roc Assured OFFICIAL (formerly IL2) cloud platform and the Roc Elevated OFFICIAL (formerly IL3) cloud platform, using National Cyber Security Centre (NCSC)-approved cross-domain security patterns.

What the service can help you achieve

- Create secure applications that are accessible to citizens, but ensure data safety
- Reduce your infrastructure and compliance costs, by leveraging Roc's ready-made solutions
- Ensure your solutions are aligned with information security requirements
- Meet changing requirements by controlling and adapting the service

Key service capabilities

- A secure and flexible way to transfer data between your workloads hosted on the Roc Assured OFFICIAL cloud platform and the Roc non-internet connected Elevated OFFICIAL cloud platform
- A choice of services:
    - Roc Guard, which is managed by Roc and delivered as a cloud service
    - The single-tenant Walled Garden, which enables you to deploy your own controls to support a wider range of use cases and traffic flows
- A flexible application process with a self-assessment route for customers with simple implementations; and an assurance review approach with Roc's experienced professionals for more complex implementations
- Independent validation (including NCSC design reviews) that CDSZ is fully aligned with the 14 NCSC Cloud Security Principles and suitable for data classified at OFFICIAL (including OFFICIAL-SENSITIVE)

Why Roc

- UK-based telephone service desk and Network Operations Centre (NOC) function, providing 24/7 support for P1 critical incidents and proactive monitoring, including access to Roc's technical experts
- Platform optimised for OFFICIAL and OFFICIAL-SENSITIVE data and fully aligned to the NCSC 14 Cloud Security Principles
- Extensive independent validation by recognised UK public sector authorities, which enhances the platform's suitability for especially sensitive workloads for organisations within the health, police and defence communities
- Multiple secure UK data centres separated by more than 100km and connected by high-bandwidth, low-latency dedicated connectivity
- UK sovereignty — assured cloud platform delivered by a UK-based company with UK government security-cleared personnel
- Platform hosting workloads exclusively for the UK public sector, creating a known and trusted community of neighbours

- A wide-ranging ecosystem of partners experienced at designing, deploying and supporting workloads that traverse security domains

Cloud characteristics delivered

- Elasticity — you can scale the Roc Guard and Walled Garden solutions horizontally or vertically to adjust for increased traffic flows
- Self-service — you can make changes approved by the compliance team to your Walled Garden without involving the Roc support team
- Measured usage — you will be billed only for what you use as you adjust the number and size of virtual machines (VMs) your solution needs
- Broad networking — connect via DDoS-protected internet; a government community network such as PSN, N3/HSCN, Janet or RLI; or HybridConnect, using your own dedicated circuits
- Resource pooling — both the Roc Guard and the Walled Garden operate within the Roc platform with no need for customer-built solutions

Key characteristics of our service

The Roc Cross Domain Security Zone helps you achieve the goals of the Government Digital Strategy by making government community–facing (for example, PSN) applications available to citizens and industry via the internet. It's ideal for solutions where service accessibility and data security are key underpinning principles.

There are two service options: the Roc-managed Roc Guard, and the self-managed Walled Garden.

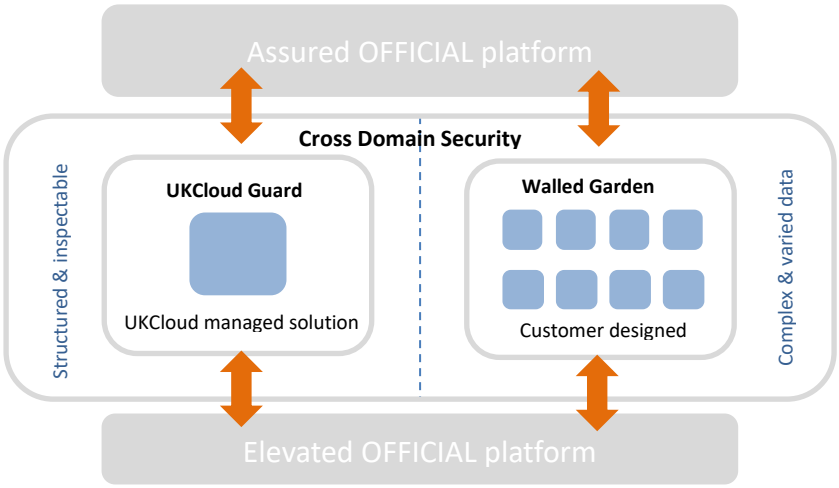
Roc Guard

We provide a secure, scalable managed Roc Guard that supports structured and inspectable HTTP-based data flows. This option provides an immediately available solution to support simple use cases, such as applications designed to make inspectable web services calls between the security domains.

Walled Garden

We provide self-service access to the Cross Domain Security Zone so that you can design, implement and manage your own Walled Garden, using technology and application services of your choice. We provide an assurance wrap by managing firewalls between the security zones and ensuring you use appropriate risk management to understand and mitigate identified risks.

The Walled Garden is ideal for organisations that require more control and flexibility over what is passed between security domains, to support a wider range of use cases.



Pricing and packaging

Roc Guard

The Roc Guard is priced as per the table below. Once the consumption of the service reaches the next pricing tier, all usage for the month will be charged at that lower price.

Data volume	Monthly price	Dual site
Starter Pack (1TiB)	£500	£500 per month
Next 4000GiB	£0.50 per GiB	
5001GiB+	£0.10 per GiB	

Walled Garden

The self-managed Walled Garden is priced with a baseline monthly fee plus a fee per VM per hour, depending on the VM size and inclusion of Snapshot protection options, as follows:

Baseline (per DC / month)	£500

VM (per hour)				
	2GHz vCPU	RAM (GiB)	POWER	
Tiny	1	2	£0.12	+
Small	2	4	£0.15	
Medium	4	8	£0.26	
Medium High Memory	4	16	£0.40	
Large	8	16	£0.50	
Large High Memory	8	32	£0.75	
Tier 1 Apps Small	8	48	£1.05	
Tier 1 Apps Medium	8	64	£1.39	
Tier 1 Apps Large	8	96	£1.85	

VM Protection [2]	
14-day snapshot	28-day snapshot
£0.07	£0.07
£0.12	£0.12
£0.19	£0.19
£0.25	£0.25
£0.35	£0.35
£0.60	£0.60
£0.85	£0.85
£1.05	£1.05
£1.55	£1.55

Block Storage (per GiB/per month)[6] [7]	
Tier 1	£0.25
Tier 2 [4]	£0.10

+

Block Storage Protection (per GiB/per month)	
£0.20	£0.30
£0.10	£0.20

Licensing										
VM Size	Microsoft Windows Server OS		Microsoft SQL Standard [3]		Microsoft SQL Enterprise [3]		Microsoft RDS		Red Hat Enterprise Linux	Bring Your Own Subscriptions
	£ / hour / VM	Academic £ / hour / VM	£ / hour / VM	Academic £ / hour / VM	£ / month / VM	Academic £ / month / VM	SAL Licence per month	Academic SAL Licence per month	Subscribe through Roc £ / hour / VM	
Micro, Tiny VM	£0.012	£0.002	£0.266	£0.054	£725.70	£195	£4.19	£0.44	£0.04	No charge
Small VM	£0.023	£0.003								
Medium VM	£0.046	£0.007								
Medium High Memory	£0.046	£0.007								
Large VM, Large High Memory, Tier 1Apps	£0.135	£0.020	£0.513	£0.15	£1460.25	£390			£0.09	

[2] You must choose the same protection option for both VMs and storage.
[3] SQL Enterprise is bought on a monthly basis: you must report the quantity of SQL Standard and Enterprise licences that you need each month to Roc.
[4] 60GiB of Tier 2 storage is included in the pricing for all VMs while they are powered on. For VMs in powered-off state, consumed storage will be charged at the prevailing rate.
[6] Consumed storage includes VM catalogue images and snapshots.
[7] VMs with additional allocated storage will be charged at the prevailing storage rate regardless of their powered-on/off state.
[8] If you wish to host Oracle solutions on our platform, please consult our Cloud Architects, or consider our Dedicated Compute or Enterprise Compute Cloud – Oracle services, to avoid licensing issues.

For all services above, billing is per unit or part thereof.

Connectivity options

Roc provides one of the best connected cloud platforms for the UK public sector. We offer a range of flexible connectivity options that enables access to our secure platform by virtually any government user community or system. The variety of government, public and private networks is shown in the following diagram:

Connection type	DDoS-protected internet	PSN Assured	PSN Protected	N3/HSCN	Janet	Hybrid Connect	RLI
Starter pack price (per month)	FREE	FREE	£250	£250	FREE	N/A	N/A
Subsequent price (per GB outbound)	FREE	£0.25	£1.00	£1.00	FREE	N/A	N/A
Set-up fee	N/A	N/A	N/A	N/A	N/A	£2,000	£2,000

Please refer to the pricing guide for all options and details.

PSN Assured: The general-purpose unencrypted Public Services Network. Connected to most central, local and devolved government organisations.

N3/HSCN: The NHS National Network. Connected to all health and social care organisations nationwide.

Janet: The UK's research and education network. Connected to all education organisations and research councils.

PSN Protected: Encrypted higher-security Public Services Network. Connected to legacy IL3 networks including GSI, PNN, CJX, GSE, GSX and others.

HybridConnect: Supports a variety of flexible private connectivity options. Enables connection to Crown Hosting (CHDC) and other third-party facilities.

RLI: A high-security network for defence and industry partners. Connection to RLI is subject to extensive vetting and approval from the MoD.

Discount and purchase schemes

There are two discount or purchase schemes — see below. You can find full details of each one in our pricing guide.

Option 1: Commitment discount

Commit to spending a specific minimum amount each month for a minimum of 12 months and receive a discount based on the total spend committed.

Option 2: Cloud Credits

Purchase Cloud Credits upfront and redeem them against UKCloud services over a maximum two-year period. This enables you to effectively commit your CAPEX or budget spend in advance, with monthly usage deducted from the balance until depleted.

An SLA you can trust

We understand that UK public sector organisations need a dependable service that demonstrates value to stakeholders, which is why we offer one of the best SLAs on G-Cloud.

What's more, we back our SLA with Service Credits. If we fall short of our agreement, we'll compensate you with Service Credits so that you can be confident that we have a financial incentive to deliver on our promises.

The table below outlines the SLA and Service Credit details. For more in-depth information, see the terms and conditions.

Service level agreement	99.90%

Portal level agreement	99.90%
Availability calculation	Availability is calculated based on the number of hours in the billing month (for example, 744 hours for months with 31 days), excluding any planned and emergency maintenance.
Measurement of SLA	Unavailability applies to the Roc Guard or the underlying Cross Domain Security Zone infrastructure due to a fault recognised at the IaaS layer, data centre facilities, physical firewalls or routers.
Key exclusions	The following are examples of what is not covered by the SLA: • The fault is within the customer's control (such as VM configuration, customer networks, application logic) • Faults within external connectivity providers (for example DDoS-protected internet, PSN, Janet or N3/HSCN) and components colocated at Roc
Service Credit	10% of monthly spend on the Cross Domain Security Zone. 1% of monthly spend per 1% below service level target or part thereof for the Roc API and Portal.

Supporting documents and resources

This service definition aims to give you enough information about the service, options and pricing to support your G-Cloud procurement process. The following documents, available on request or from the Roc Portal, should provide any additional information you need:

- Service scopes provide more details about our services; they also cover service options, such as the Mass Transfer Facility and Cloud Enablement
- FAQs for each service aim to answer the most common questions
- Datasheets/factsheets provide a high-level description of each service
- Blueprints provide examples and instructions for how to use the Roc Assured Cloud platform
- How to guides provide step-by-step instructions for specific actions and tasks on the platform, including the use of the Portal and interacting with Roc support teams

In addition, we have:

- Cloud Architects who can help you understand how this service can address your requirements
- Over 240 partners who can provide professional and managed services

Try before you buy

Owing to complex assurance requirements, a trial service is not available.

The small print

The appendix to this service definition provides a summary of the service terms. For full terms and conditions, refer to the Terms and Conditions document, available from the Digital Marketplace.

Appendix

Ordering and invoicing

The service can be ordered via the G-Cloud Framework and must be supported by a valid purchase order.

Billing for the service is monthly in arrears based on either the amount of traffic sent through the Roc Guard or the consumption of resource during the month for the Walled Garden.

Roc will issue invoices as follows:

- At point of order for up-front fees and service options
- Annually in advance for pre-payment fees
- Monthly in arrears for monthly fees

Payment can be made by direct bank transfer (BACS/CHAPS).

Onboarding

Setting up a new customer within the Roc Portal will typically be completed within 4 hours from acceptance of order.

Customers will have two options when purchasing a CDSZ service.

- A light-touch design review/self-assessment route for customers with simple implementations, or those who are experienced at designing secure solutions.
- An assurance-wrap style approach with Roc's experienced professionals for more complex implementations or those customers who would like support and guidance when developing their solutions.

Both options require the same submission documentation to enable Roc to provision the service.

When you apply for a CDSZ service, you must provide the following documents to show that you have identified and mitigated for any risks:

- Details of your proposed implementation that covers the intended design in the CDSZ, the Assured and Elevated VDCs you are connecting to and data flows.
- Evidence of acceptance of risk from the data owning organisation.
- An explicit statement that the solution has been reviewed by a named Roc Cloud Architect or that you do not require a review.
- If you're connecting to a PSN Protected enabled VDC, proof of PSN compliance

Validation of inclusion of appropriate documentation for a self-assessment service request will happen in 4 hours.

Deployment time following validation is 5 days. This includes the setup and configuration of customer specific firewall requirements.

Roc will create the customer's Primary Administrator account and send the customer a Welcome Pack which includes the URL for the Roc Portal for access to the Knowledge Centre and service management function.

Once enabled, the customer's Primary Administrator can create additional administrator users and configure the Cross Domain Security Zone virtual data centre (such as virtual networks, virtual firewalls, virtual machines, OS provisioning and application configuration) as required.

Resources to support the assurance wrap approach activity will be assigned within 10 days of order acceptance.

Due to the variable nature of this service, full onboarding of the customer organisation including enrolment of all users and end-user devices will take an indeterminate amount of time.

If you choose an assurance wrap review for your proposed implementation, the Roc compliance team and Cloud Architects will work with you to help identify risks on your platform. This includes:

- Review of design and data flow with a Cloud Architect.
- Advice and guidance for how to design secure solutions
- Conversation between Roc SIRO and customer SIRO or nominated representative covering risk management and mitigation
- Review of ITHC scope and summary with a Cloud Architect

Roc takes no ownership or responsibility for the implementation or running of components specific to the customer's own solution or ownership for any risks to the data.

Roc reserves the right to charge SFIA day rate charges for time spent on customer projects if you disengage with the assurance wrap review process before completion.

Roc has created a number of videos, help guides, manuals and FAQs to help train and instruct users so that they are up and running quickly and easily. These are available within the Knowledge Centre, accessed via the Roc Portal.

In addition, you will be assigned a Customer Success Manager (CSM) to provide any assistance required during the first 90 days of the service.

Roc also has a large ecosystem of partners who can deliver additional services, such as support and professional services. Roc would be pleased to introduce you to the right partner to suit your needs.

Data migration

For service migration, Roc allows existing data to be migrated to and from the Walled Garden virtual data centre.

Roc can also help facilitate a bulk migration to the platform using offline data ingest and extraction — please ask Roc for details.

Service management

Roc will allocate a Technical Account Manager (TAM) to provide you with an assigned point of contact. The TAM will provide additional assistance with reporting and incident escalation, at all times following Roc's ISO20000-certified ITIL-based process framework.

For organisations that require a managed service, Roc has a mature and active partner ecosystem that can provide value-added services such as consultancy, training and on-going custom managed services. Roc will be pleased to make an introduction on request.

Service constraints

The Roc Cross Domain Security Zone can be used only for connectivity between Roc services such as Enterprise Compute Cloud and Hadoop in the Cloud.

The constraints below will be applied as standard to the Roc guard. For customers purchasing the walled garden, Roc strongly advises that those using this service apply the following constraints to protect their own applications and data:

- Configuration and management of application services in both the low- and high-security domains must be hardened, with regular security patches applied
- Application services must use appropriate anti-malware software which is regularly updated
- Only specified traffic types will be allowed via a Roc-managed whitelist
- The data owning organisation must understand and accept the residual risks associated with this solution

Roc will adhere to the following in terms of maintenance windows:

"Planned Maintenance" means any pre-planned disruptive maintenance to any of the infrastructure relating to the service. Planned Maintenance activity may result in periods of degradation or loss of availability depending on the nature of the activity required. In such cases, Roc shall provide affected customers with at least fourteen (14) days' advance notice of the Planned Maintenance.

If during Planned Maintenance there is a loss of availability outside the scope described in the planned maintenance notification to the service, an SLA event will be triggered, but excluded from Service Credits.

"Emergency Maintenance" means any urgent maintenance required to prevent or mitigate against any event compromising the infrastructure relating to the service. Whenever possible, Roc shall: a) provide affected customers with at least six (6) hours' advance notice and b) carry out the emergency maintenance between the hours of 00:00 and 06:00 (UK local time) Monday to Friday or between the hours of Saturday 00:00 to 06:00 (UK local time) on Monday, (including bank holidays) unless there is an identified and demonstrable immediate risk to customer environment(s). Emergency Maintenance may result in periods of degradation or loss of availability depending on the nature of the activity required.

If during Emergency Maintenance there is a loss of availability to the service, an SLA event will be triggered. This time will be excluded from the availability calculation but will be included in monthly service reporting related to the service.

Technical requirements

Customers must ensure that systems in both security domains meet the requirements of this service:

- Recommended use of a CPA-approved data-at-rest encryption solution
- Recommended use of anti-malware software (regularly updated) to reduce risk of malicious code execution on the servers
- Recommended use of an enterprise audit and monitoring service by the customer organisation to ensure security events are centrally logged and reviewed
- Recommended implementation of a Incident Response plan by the customer organisation to respond to security incidents such as loss of data confidentiality

Customers will require appropriate network connectivity such as DDoS-protected internet access or accredited connectivity such as a government secure network to our platforms. Connectivity via the DDoS-protected internet, a government secure network (PSN, JANET or N3/HSCN) or private leased line is available but may incur additional charges if the hosting of CPE routers is required — see the pricing section for more details. Where they are required, customers are responsible for procuring and managing appropriate devices or software to meet the requirement for data security over the various forms of connectivity.

Customer responsibilities

The control and management of access and responsibilities for end users including appropriate connectivity, security and accreditation if required. If access is required over government secure networks such as N3/HSCN, Janet, RLI or PSN (including legacy networks), the customer is responsible for adhering to the relevant Code of Connection (CoCo) and for providing evidence of their CoCo to Roc upon request. Roc is unable to provide access to secure networks where such evidence has not been provided by the customer.

Satisfying their customer and internal assurance teams that suitable technology controls in both the low-side and high-side domains (such as Protective Monitoring, anti-malware and security patches) will be implemented and maintained.

We recommend ensuring a suitably scoped IT Security Health Check against the application using the Cross Domain Security Zone is performed.

We recommend keeping evidence that suitable and ongoing assurance process and governance regime are implemented and maintained to ensure that risks are regularly reviewed and controls are regularly audited for effectiveness.

Providing access requirements between the Cross Domain Security Zone and customer solutions (firewall ports).

Managing security incidents related to the use of this service (for example, data breach).

The customer is also responsible for ensuring only lawful data that supports the UK public sector is stored and processed by applications on this environment, and that they fully comply with the Roc Security Operating Procedures (SyOPs) and other information assurance requirements as specified in the Roc System Interconnect and Security Policy (SISP) and associated accreditation documentation sets.

Termination

Terms

The Roc Guard option is subject to a minimum term of one month.

The Walled Garden option is subject to a minimum term of one month.

Customers are required to provide notice of termination of not less than 30 working days.

At the point of termination, customers must ensure that they have extracted any required data from the Walled Garden virtual data centre as Roc will ensure all customer data, accounts and access will be permanently deleted. These will not be able to be subsequently recovered or restored.

Costs

An Early Exit charge will be payable if the Roc Guard contract is terminated within the minimum term. The Early Exit charge will be equal to the cost of three months' service less payments already made.

There are no termination costs for the Walled Garden. Customers are responsible for extracting their own data from the Enterprise Compute Cloud service if required.

Customers are responsible for extracting their own data from the platform if required.

Roc may make an additional charge for transferring data out of the service.

Offboarding

Prior to terminating the contract, the customer is able to transfer all their data out of the solution (for example using the Roc API to retrieve data).

When the organisation terminates its agreement with Roc, Roc ensures all of the organisation’s data is deleted.

Roc

Roc Technologies Limited, Wharf House, Wharf Street, Newbury, RG14 5AP

T. 01635 581188 www.roctechnologies.com info@roctechnologies.com