

Becrypt OS Management Service

SERVICE DEFINITION

G-CLOUD 15

Contents

Becrypt OS Management Service.....	1
1. Service Overview	4
2. Highlights	4
Key Security Benefits of Becrypt OS, infrastructure software as a service	5
3. Assurance	5
4. Service Definition	6
Base Service Selection.....	6
Becrypt OS+ Device Supply (Pricing on Application).....	7
Device Provisioning/Registration	7
YubiKey Supply and Enrolment.....	7
Dedicated Private Hosting	7
5. Responsibilities.....	8
6. Support Services	10
7. Product Incident & Classification & Resolution.....	11
Incident response targets	12
Service reporting	13
8. Enhanced Support Services	13
9. Vulnerability Management & Patching	14
10. Maintenance / Upgrades / Updates.....	14
11. Service Constraints	15
Planned maintenance.....	15
Exceptional maintenance	15
Emergency maintenance	15
12. Platform Support.....	15
13. Acceptable Usage Policy.....	15
14. Customer Responsibilities	16
15. Training	16

16. About Becrypt	16
--------------------------------	-----------

1. Service Overview

As a trusted supplier of assured solutions to both HM Government and private sector organisations, we recognise the challenges faced in managing enterprise desktop estates.

Becrypt OS is an innovative security-focused operating system, designed to meet cloud, web and virtualised application access requirements, through a secure browser and lightweight application environment.

Becrypt OS provides an intuitive hosted End User Device platform for accessing public or private cloud resources, supporting identity management and segregation between infrastructure management and business service delivery.

Delivered as a fully managed solution, it provides peace of mind over the security, integrity and delivery of the desktop management platform.

2. Highlights

The Becrypt OS Management Service offering includes the following:

- Lower costs – no need to deploy complex management estates for Windows desktops
- Automates application, audit, patch and incident management
- Optimised to support rapid deployment of new Cloud Services
- End to end offering includes both management infrastructure and client software
- Intuitive browser-based End User Device platform
- Simple Web-based estate management reporting
- Supports separation of infrastructure management and service delivery
- Access to Office 365, G Suite, standard and hosted Web Apps
- Compatible with common VDI & VPN clients

Key Security Benefits of Becrypt OS, infrastructure software as a service

- Trusted boot process ensures cryptographic validation of firmware, operating system and all application components. Boots into a 'known good state'
- A light-weight operating system with reduced attack surface, ensures Paradox is not susceptible to common exploits
- Operating System components mounted as read-only to prevent persistent targeted attacks
- Cloud hosted management infrastructure for rapid, automated and transparent patch management
- Architecture ensures high-value, low-volume audit events with SIEM integration

3. Assurance

In most engagements, the customer leads Secure by Design (SbD) assessment activity as part of their governance and assurance processes.

- Suitable for OFFICIAL / OFFICIAL (SENSITIVE) assets
- Becrypt hold ISO9001, ISO27001, ISO14001 and Cyber Essentials Plus certification
- Software developed in the UK with staff cleared from BPSS, SC and DV levels

Higher security Tier options may be available subject to customer requirements and use case.

Becrypt can support customer-led SbD activities through costed Professional Services (PS), for example:

- Workshops with security stakeholders and delivery teams
- Provision of service documentation, design artefacts, and evidence packs appropriate to the deployment
- Support to map service controls to customer assurance needs and operational requirements Secure by Design assessments

Where required, Becrypt can also arrange for assessment activity to be delivered on the customer's behalf via a specialist third party, subject to scope, commercial agreement, and customer requirements.

Note: Formal acceptance, assurance, and classification decisions remain the responsibility of the customer and their governance processes.

4. Service Definition

Base Service Selection

Service Feature	Silver	Gold	Platinum
Paradox Licensing	✓	✓	✓
Paradox updates & security patches	✓	✓	✓
Enterprise Manager Access	✓	✓	✓
Initial Set-Up (Policies, Applications & Customer Admins)	✓	✓	✓
Service Desk Access (09:00-17:30, Mon-Fri)	✓	✓	✓
Certificate Management	✓	✓	✓
Resilient Configuration Database	✓	✓	✓
Base Application Catalogue	✓	✓	✓
Ongoing Policy Management (Policies, Applications & Customer Admins)		✓	✓
Initial Desktop Config (look and feel)		✓	✓
Additional Application Packaging		✓	✓
User Management / Enrolment		✓	✓
Second and Third Line Support ¹	✓	✓	✓
Dedicated Deployment ²			✓

1 – Support excludes physical desk/user visits

2 – Additional Service Costs Apply – this is based on a high availability resilient deployment

Becrypt OS+ Device Supply (Pricing on Application)

- Becrypt can provide laptop devices as part of the service.
- Becrypt can provide USB sticks for the 'live' variant as part of the service.

Device Provisioning/Registration

- As part of the service, Becrypt can provide provisioning and enrolment services

YubiKey Supply and Enrolment

- Users selecting to take YubiKey as the authentication method can engage Becrypt in provision of the YubiKey
- YubiKey supply is POA

Dedicated Private Hosting

- Becrypt can offer dedicated private infrastructure hosting in a secure data centre for higher assurance requirements

5. Responsibilities

Feature	Becrypt responsibilities	Customer responsibilities
Service desk	Provide service desk support for incidents, changes and service requests; log, track and communicate status.	Provide an up-to-date list of authorised contacts; raise incidents and provide information required for resolution.
Access control and user administration	Provide platform capabilities and processes to support role-based access control and enclave separation.	Define user roles, approve access requests, and manage user lifecycle in line with customer policy.
Hosted applications	Host and operate agreed applications and infrastructure services (where in scope).	Provide licences where required (government/customer furnished) and confirm application requirements and dependencies.
User Authentication	None	Provide support for user authentication issues, such as facilitating automatic or manual password reset for Web applications.
Service Reporting	Provide agreed service reports (for example availability and capacity).	Review reports and raise queries via agreed channels.
Billing and Invoicing	Invoice the Customer for the Charges	Investigate any Becrypt OS Management Service usage discrepancies and communicate them to Becrypt for investigation. Raise Consumption Charges, billing and usage queries via the Service desk.

		Any billing queries in relation to the Consumption Charges will only be dealt with by Becrypt if raised by the Customer within six months of the invoice date being queried.
Becrypt OS Service Reporting Dashboard	Provide the Customer with an initial administration user access to the Paradox Dashboard with appropriate capability defined by the customer. Where appropriate provide Customer access to an online reporting tool for visibility of their Paradox service consumption. Four agreed planned maintenance outages of up to eight hours' duration per year. Becrypt will endeavour to perform any emergency maintenance on the reporting dashboard between the hours of 22:00 and 06:00 Becrypt will endeavour to provide the Customer with at least 24 hours' notice of the intention to perform such maintenance. Notify Customers of scheduled or emergency maintenance of the reporting dashboard via email to the Customer's nominated contact(s).	Allocate user accounts associated with the Becrypt Enterprise Manager Reporting Dashboard. Ensure that all requests for changes to authorised users and groups are sent via Service Request to Becrypt. Ensuring that the Customer's software and or systems are fully licensed as required for the Customer usage and environment.

6. Support Services

Becrypt offers telephone and e-mail technical support for all its products. Support is based in the United Kingdom.

Support Incident: To facilitate communication and obtain effective results, the customer should collect all available information related to the issue they have before raising a support incident.

The information typically required includes:

- Version of product being utilised
- Applications installed
- Incident details - A detailed description of the issue, with the steps required to reproduce it, and the results of any troubleshooting performed
- Relevant logs from BEM and / or syslog's

Becrypt customer support can be contacted by the following means:

Telephone Support	Technical Support assistance and diagnostics provided by a support specialist Telephone: 0345 838 2070 Standard Coverage: Monday to Friday 09:00 to 17:30 Additional Coverage: By arrangement only
E-mail Support	Assistance via a dedicated e-mail address For incidents and technical queries: support@becrypt.com Coverage: this e-mail address is reviewed Monday to Friday 09:00 – 17:30 Additional Coverage: By arrangement only

7. Product Incident & Classification & Resolution

The incident classification scheme outlined below relates to the management of product defects, as opposed to vulnerability management addressed through regular patch set management.

Incident & Request Classification. The incident shall be classified by the Customer and Becrypt according to the following classification:

Severity Levels	
Severity 1	▪ Your organisation experiences a complete loss of service, and the situation is an emergency – causing high levels of adverse impact to the business. ▪ There is no viable workaround, later version or patch available.
Severity 2	▪ Your organisation is severely impacted, but operations can continue in a restricted fashion. ▪ There are widespread symptoms across your organisation, affecting many users. ▪ A major product feature is not working in the manner that was intended.
Severity 3	▪ Your organisation is impacted, but operations can continue. ▪ There are limited symptoms across your organisation. ▪ Loss of functionality or performance, but users may continue to use the product.
Severity 4	▪ There is limited impact or inconvenience on your organisation's daily activities. ▪ There are only isolated symptoms within your organisation. ▪ Minor loss of functionality, but users may continue to use the software.
Severity 5	▪ Does not affect your organisation's ability to conduct business. ▪ Product and/or documentation enhancement request. ▪ All other requests. Eg, new users, access change, device provisioning, etc.

Multiple incidents or requests reported by a single Customer shall be treated as separate tickets.

Every new incident & request will be logged on Becrypt's IT Service Management system and a reference number will be assigned for tracking purposes. The ticket number will be communicated to the Customer and should be quoted in all future communication.

All incident details and history will be logged on to Becrypt's incident management system. Incident reports may be provided upon request.

Incident response targets

Priority	Target response time	Target performance	Resolution
P1 – Major	30 minutes	95%	Restore services or get to a point that a reduction in severity level applies
P2 – High	1 hour	90%	Restore services where possible; an effective workaround may be found, or a patch supplied that alleviates the business impact as soon as possible. Fix may be incorporate into the next minor release
P3 – Medium	3 hours	80%	A short-term workaround will be investigated and implemented if possible. A longer-term fix may be incorporated into the next major release or upgrade
P4 – Low	17 hours	75%	A short-term workaround will be investigated and implemented if possible. Fix will be incorporated into the next major release or upgrade
P5 - Minor	26 hours	70%	Process request. Possible candidate for a future release (dependent on request)

Priority 1 incidents **must** be raised by telephone. All other priorities can be raised by either telephone or email.

If necessary, Becrypt may provide an on-site diagnosis. If on-site visits identify that the root cause (reported by the Customer) was due to factors other than the Becrypt products, Becrypt reserves the right to charge the Customer. These charges would be Becrypt's published time and materials rate, and any out-of-pocket expenses for such support.

Internal procedures are in place to escalate any outstanding incidents to Becrypt's Customer Support Management, Senior Management Team, and Executive.

Service reporting

Report type	Description	Frequency
Capacity and availability	Provides information on service availability and capacity.	Monthly (or as agreed)

Consumers of the service are also able to run (at a frequency of their choosing) their own reports from the service dashboard. Custom filter reports are categorised by the following filters:

- Devices
- Device Groups
- Device Logs
- Policies
- Domains
- Messages
- Audits
- Users

8. Enhanced Support Services

Becrypt can provide Enhanced Support Services on an ad hoc basis, as requested by the Customer. This may include but not limited to Consultancy, Development, On-site Installation and Training. These services may be charged at Becrypt's current applicable rate plus related expenses, as mutually agreed upon in advance between Becrypt and the Customer. The provision of Enhanced Support Services shall be subject to the availability of qualified and (if appropriate) security-cleared personnel.

9. Vulnerability Management & Patching

Becrypt undertakes daily reviews of published software Vulnerabilities, using public vulnerability databases, open-source scanning tools and security notices, which are then cross-checked against the product components. The corresponding software fixes are collated to create a quarterly software update package, which is made available to customers within approximately 90 days of vulnerability fix publication.

If a vulnerability is identified as critical or involving privilege escalation capability, then the vulnerability shall be urgently assessed by Becrypt and may trigger an urgent patch management process; where we inform our customers of the exact nature of the risk, provide any immediate mitigations that might be applied before ensuring that a patch release for the affected product is produced within 30-days of the fix being made available.

10. Maintenance / Upgrades / Updates

Becrypt's annual subscription charge includes access to all support services and future product updates and discretionary upgrades. Major upgrades (including large changes in functionality or new system architecture) may be offered at additional cost. Standard upgrades can be requested by customers who are currently registered for maintenance / subscription services. Becrypt software release version numbers follow the commonly used MAJOR, MINOR, PATCH format, e.g., Becrypt OS+ v4.1.3. The release notes for a specific version will also include a Build Number, included for internal tracking purposes.

Major releases: On average, Becrypt produces a major release of its core products every twelve to twenty-four months. The exception to this rule is the Becrypt OS solution which has a four-year major release cycle that tracks Ubuntu's Long Term Support release schedules. These releases typically include large feature updates and/or significant underlying system changes.

Minor releases: On average, Becrypt has a minor product release of the core products approximately every three months (90 days). This release variant is likely to include a combination of feature updates, bug fixes and non-urgent vulnerability updates as per our vulnerability and patch management commitments.

Patch releases: These releases may include small specific fixes or critical security fixes as per our vulnerability and patch management commitments.

New products: Becrypt's annual subscription / maintenance charge does not cover new products to be developed by Becrypt.

11. Service Constraints

Planned maintenance

A scheduled maintenance window may be used monthly between 19:00 and 06:00 (UK). Changes to the day will be notified with at least 24 hours' notice.

Exceptional maintenance

Where non-emergency maintenance is required outside the scheduled window, Becrypt will provide not less than 7 days written notice. Downtime resulting from exceptional maintenance with appropriate notice may be excluded from availability calculations.

Emergency maintenance

To resolve major issues relating to service stability or security, unplanned maintenance may be necessary. Becrypt will provide as much notice as reasonably possible, advising customers of any likely impact.

12. Platform Support

Becrypt undertakes product testing on a variety of standard platform hardware and software configurations for which Becrypt endeavours to provide support. However, because so many platforms are available, it is impossible to guarantee that a specific one will be supported. Becrypt technical support should be contacted for further details of specific platform support and restrictions. Where a customer requirement exists for deployment of Becrypt software with non-standard or currently un-tested components or platforms, advice should be sought from Becrypt support prior to product deployment.

13. Acceptable Usage Policy

The services will be subject to Becrypt's Acceptable Use Policy ("AUP") which is available upon request. The purpose of the Policy is to outline those actions which are either strictly prohibited or are considered unacceptable by Becrypt in particular or by the wider IT environment in general, whether they be committed wilfully, inadvertently or innocently, and to define the sanctions which may be imposed by Becrypt upon Customers in violation of this Policy.

The Customer shall be responsible for always complying with the AUP and ensuring that all consumers of the service shall be made aware of the AUP.

14. Customer Responsibilities

The customer responsibilities will be as follows:

- Procurement, maintenance and management of any Customer data communications lines not identified in the Technical Specification. This shall need to be properly defined and provided according to the appropriate code of connection
- Administration, management and control of Users access to the data stored on the Paradox Edge Service
- Should Becrypt determine that the Customer's usage of the Paradox Edge Service is not compliant with best practice guidelines, the Customer must comply with Becrypt's reasonable requests for change.

15. Training

User documentation is available for relevant service components. Training is not included as standard but can be provided as a professional services engagement subject to additional charges.

16. About Becrypt

Becrypt is a UK-based cyber security specialist delivering high-assurance products and managed services to government and critical national infrastructure organisations.

As an agile London-based SME with over 25 years of cyber security expertise, Becrypt designs and delivers trusted security solutions aligned with government-accredited platforms and standards. We enable our customers to safely and rapidly deploy mobile endpoint and cloud technologies, enhancing operational flexibility, agility, and productivity.

Becrypt supports government and critical national infrastructure organisations with a comprehensive portfolio of security solutions and services, ranging from funded research and development to commercially available products and flexible managed services.

For enquiries: sales@becrypt.com or 0845 838 2080