Becrypt CWE

SERVICE DEFINITION

G-CLOUD 15

Contents

1. Service Overview

Becrypt CWE is a sovereign, secure collaboration environment designed for organisations in Critical National Infrastructure (CNI) and wider government / regulated sectors that need to collaborate at OFFICIAL (including OFFICIAL SENSITIVE) with UK and/or international partners.

Delivered as a fully managed service, Becrypt CWE provides assurance over the security, integrity, and availability of your data and collaboration platform, allowing organisations to rapidly stand-up dedicated productivity environments, onboard partner communities, and reduce the burden on in-house IT.

Outcomes

- Enable secure collaboration across partners, suppliers and internal teams without rebuilding legacy infrastructure.
- Reduce operational burden through a managed service (service desk, security operations, patching and platform management).
- Support rapid onboarding of new users and projects through repeatable, policy-aligned configurations.
- Provide a controlled environment for collaboration artefacts including documents, requirements, designs and engineering data.

High Security Tier options may be available subject to specific customer requirements and use case.

2. What the service provides

Becrypt CWE is designed to support:

- Secure collaboration within a community of interest (internal teams, suppliers, delivery partners)
- Supply chain collaboration where partners may not have data storage or processing at OFFICIAL / OFFICIAL SENSITIVE
- Controlled import/export and cross-domain information sharing (where required) to manage information flows between trust domains, including optional high assurance API-centric cross-domain integration through Becrypt's proprietary High Assurance APP-XD.
- Secure by Design-aligned onboarding and assurance activities, including support for customer Secure by Design assessments where required

- Becrypt CWE can support digital engineering and digital twin programmes by hosting the relevant toolchains that provide this capability.

- Secure by Design-aligned onboarding and assurance support, including costed Professional Services (PS) to support customer-led Secure by Design assessments where required.

3. Secure by Design (SbD) principles and assurance support

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

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. Platform Services (Fully Managed)

Sovereign CWE is delivered as a managed service. Core managed services include:

- Fully managed Security Operations Centre (SOC) capability for monitoring and security response processes
- ITIL compliant service desk with all you would expect - incident, service request, and change handling
- Patch management for platform components and managed services

Operational support services are provided in line with the agreed service scope and can be tailored to customer needs, including reporting, onboarding support, and documented operating procedures.

Service Components and Options

Becrypt CWE is designed to be flexible, allowing the service to be configured to meet different operational, assurance, and collaboration needs. This section describes the service scope at a capability level rather than prescribing a fixed technical implementation.

Core CWE Service Foundation

The service is built on a private cloud foundation, providing isolated compute, networking, and storage resources for each customer community of interest. The platform is designed to support segregation, resilience, and scalability appropriate to secure collaboration environments.

Workspace and access options

Depending on customer requirements, the service can provide secure user workspaces and access mechanisms, for example:

- Centrally managed virtual workspaces
- Secure access from managed or trusted endpoint devices
- Support for different endpoint operating environments, subject to security policy

Endpoint support

The service supports secure collaboration from approved endpoint types. Endpoint options may include:

- Standard enterprise desktop or laptop environments
- Security-hardened operating environments for partner or elevated-risk access
- Mobile access patterns were permitted by policy and solution design

Optional platform capabilities

Additional platform capabilities can be introduced where required, for example:

- Self-service or delegated management features
- Additional capacity, performance, or resilience options
- Customer-specific operational tooling

5. Hosted applications and digital engineering toolchains

The service is designed to be application-agnostic, enabling organisations to bring together the tools they already use, as well as new capabilities introduced over time, within a governed and assured collaboration environment.

Examples of hosted toolchains

- CAD/CAE and engineering tooling (for example SolidWorks and supporting PDM).
- Modelling and analysis tooling (for example MATLAB and Simulink).
- Source control and DevSecOps tooling (for example GitLab).
- Collaboration and content services (for example SharePoint, Teams)

Note: Any application references are illustrative only. The service is intentionally flexible to support evolving toolchains and programme needs without constraining customers to a predefined technology stack.

GPU-enabled desktops

Where required, the service can provide GPU-backed VDI to support low-latency interactive engineering workloads (for example CAD and simulation), sized to the agreed performance profile.

6. Hosted Applications and Toolchains

In addition to the baseline workspace, Sovereign CWE can host or support access to additional applications and toolchains required by the community of interest.

Applications can be delivered as hosted services or provided via government/customer-furnished licences.

Example applications to support buyer imagination (non-exhaustive)

- Productivity and collaboration: Microsoft 365 / Office services, Confluence
- Engineering and design: SolidWorks, MATLAB
- DevOps and delivery: GitHub, Jira

7. Cross-Domain / Controlled Information Sharing

Some collaboration needs require controlled transfer of information between environments with different trust levels (e.g., partner zones, international collaboration, regulated segregation).

Becrypt CWE can be integrated with cross-domain and controlled information sharing capabilities to support:

- Policy-based import/export workflows (e.g., controlled release, audit, approvals)
- Secure API-based integration across trust domains (where required)
- Protection against elevated threats when exchanging information with less trusted environments

Optional high assurance cross-domain capability - APP-XD

Where higher assurance cross-domain integration is required, Becrypt CWE can include APP-XD as an optional extra: a High Assurance API-Centric Cross Domain Solution (CDS) used to support secure API integration across separate network trust domains.

Optional cross-domain applications (requires APP-XD)

All cross-domain applications below are optional and are predicated on the customer taking the optional APP-XD capability. They are available only where APP-XD is in scope for the deployment. Where customers need specific collaboration workflows across domains of trust, Becrypt CWE can include optional applications and services that integrate with cross-domain controls.

Becrypt VDI Guard (requires APP-XD)

Becrypt VDI Guard is an optional capability to protect remote access services by validating network traffic for remote sessions (e.g., RDP/VDI), helping defend against advanced and zero-day threats targeting remote access.

Key capabilities include:

- Comprehensive remote access protection through traffic validation
- Secure partner collaboration using managed partner devices without exposing core assets to compromised endpoints
- A Zero Trust model where every connection is validated before reaching sensitive networks
- Designed for elevated threat environments and critical services

Becrypt Calendar Sync (requires APP-XD)

Becrypt Calendar Sync is an optional application and service to enable controlled exchange of calendar information between calendars in different trust domains (for example, synchronising between ‘high-side’ and ‘low-side’ environments).

Key capabilities include:

- Automated synchronisation across domains of trust
- Policy enforcement to restrict or redact content (e.g., Free/Busy only, location controls, subject removal/obfuscation)
- Compatibility with Microsoft Exchange and Microsoft 365 (with planned support for other platforms)
- Secure authentication, encryption, and identity mapping, with centralised management and self-enrolment

Becrypt Mail (requires APP-XD)

Becrypt Mail is an optional secure email and messaging platform for controlled exchange of information across different levels of trust and information sensitivity, including scenarios involving government-classified systems.

Key capabilities include:

- End-to-end encryption between high-side email services and partner-accessible users
- Policy controls to restrict recipients and prevent unauthorised forwarding
- Optional support for attachment import/export controls and audit
- No data stored on partner client devices, with monitoring and audit of security-related events

8. Use cases and who it is for

Becrypt CWE is typically used where multiple organisations must collaborate securely within a defined community of interest.

- Secure collaboration across prime, partner and supplier organisations, including non-government organisations working with government or CNI.
- Engineering collaboration requiring GPU-enabled desktops for CAD/CAE workloads and low-latency interactive applications.
- Programme delivery teams needing governed document collaboration, requirements management and controlled import/export of data.
- Organisations requiring segregated environments (enclaves) for separate projects, teams or data domains.

9. Service architecture and components

Sovereign CWE is underpinned by high assurance security components and managed cloud operations.

Security components (examples)

- Document / email marking and labelling controls to support user awareness and handling requirements.
- Encryption services for data protection in transit and at rest.
- Endpoint and platform anti-malware protection.

Note: specific component selection is dependent on the required assurance profile and customer context.

Segregation and sovereignty

The service is delivered with dedicated and segregated resources for the customer community, co-located in secure data centres. Data residency, access controls and operational processes are designed to support UK sovereignty requirements where required.

10. Collaboration with partners and suppliers

Where collaboration is required with users who do not have access to an OFFICIAL or OFFICIAL SENSITIVE endpoint, Becrypt CWE can provide secure access patterns based on Becrypt OS privileged access workstations (PAWs) and controlled remote access.

Partner onboarding and access control

Access is granted to named individuals, using role-based access control and project or enclave separation. Customer security controllers can define who can access each enclave and what services are available.

Privileged access workstations (optional)

For elevated-risk collaboration scenarios, a hardened access device or operating environment (Becrypt OS) can be used to provide explicit device trust for partner users, aligned to NCSC guidance for PAWs.

11. Assurance and compliance

Becrypt CWE is designed to support assured collaboration at OFFICIAL, including OFFICIAL SENSITIVE where required. Assurance artefacts and security documentation can be made available to support customer risk owners and security teams through Secure by Design processes.

Assurance approach

- Independently validated secure policy configurations (where applicable).
- Security documentation to support customer accreditation and risk decisions.
- UK-cleared staff and secure operational processes (subject to contract).

High Security Tier options may be available subject to specific customer requirements and use case.

12. Roles and responsibilities

The table below summarises typical responsibilities. Responsibilities are finalised in the contract and statement of work.

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.
Reporting	Provide agreed service reports (for example availability and capacity).	Review reports and raise queries via agreed channels.

13. 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 re-produce 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

14. 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 request. 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

15. Enhanced Support Services

Becrypt can provide Enhanced Support Services on an ad hoc basis, as requested by the Customer. This may include but not be 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.

16. 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.

17. 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.

18. 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 hour's 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.

19. 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 deployment.

20. Acceptable use and customer responsibilities

Acceptable use

Use of the service is subject to Becrypt's Acceptable Use Policy (AUP), available on request. Customers are responsible for ensuring their users understand and comply with the AUP.

Customer responsibilities

- Provide and manage customer communications lines not included in the service scope, in line with relevant connection codes and policies.
- Manage user access approvals and ensure only authorised users can access customer data in the service.
- Comply with reasonable security requests where customer usage is not aligned to best practice or agreed policy.

21. 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.

22. 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.

Enquiries: sales@becrypt.com