

#becrypt



# Secure Collaborative Working Environment



Everything 365™

 [info@becrypt.com](mailto:info@becrypt.com)

 0845 838 2050

 [www.becrypt.com](http://www.becrypt.com)

Becrypt Ltd, Artillery House, 11-19 Artillery Row, London SW1P 1RT, United Kingdom

## Introduction

Becrypt's Secure Collaborative Working Environment (CWE) has been designed to meet an enterprise need for secure online collaboration, supporting video, voice and Microsoft Office productivity tools. Based on Becrypt's market-leading [Everything 365™](#) managed service offering, the platform integrates 'best in class' collaboration tools configurable to meet a range of customer requirements.

Becrypt provide a unique level of service flexibility, providing optional self-service application hosting through a managed infrastructure as a service (IaaS) platform, with an open architecture ensuring customers avoid vendor lock in and continue to benefit from sustained competitiveness and efficiencies.

Ideal for organisations looking to reduce IT costs, increase time to value, or securely collaborate with third-party organisations, the CWE is available as either a UK Sovereign private cloud-hosted service, or within public cloud. The extensible CWE platform is built from proven technology components, architectures and service capabilities that have been accredited at both Government Official and Secret, and are widely used across government and partners to simplify risk management while delivering a first-class user experience.

## Collaboration and Productivity

As standard, the CWE employs a Microsoft Office Online Server, with Exchange, SharePoint and Terminal Services, delivering browser-based access to familiar office productivity (Word, PowerPoint and Excel) and Email services. An integrated open source VoIP, Video and Instant Messaging platform provides an intuitive secure communications environment, with Microsoft Skype for Business as an optional service configuration.

Service options include project management and rich collaboration using either an Atlassian Jira instance, or OpenProject dependent upon customer requirements.

Each CWE is hosted by default as a single tenancy within a secure private UK data centre. Where customer constraints allow, Becrypt can offer multi tenancy environments and a public-cloud hosted CWE.

## Infrastructure as a Service

To support evolving or bespoke customer requirements, Becrypt can optionally provide a flexible pool of co-located compute, storage and networking. A self-service portal provides administrative compute and data storage access, supporting the commissioning, deployment and configuration of additional applications and services. Customer defined templates are used to constrain workloads to authorised images and networking configurations.

The platform provides extensive monitoring and reporting, and rich APIs to support automation and integration. Becrypt provide bespoke consultancy resource in line with customer requirements, calling on the company's extensive UK-based software development, DevOps, IT and security resources. To mirror CWE redundancy, bespoke services may be optionally replicated to a second UK data centre.

## Why choose Becrypt CWE? - Security and Flexibility

With over 20 years of experience of providing security products and services to government and their partners, Becrypt are today a leading supplier of High Assurance capability. Through NCSC funded research and development, we have helped shape both the architectures and technologies now in use across government and the critical national infrastructure, to support remote working, collaboration and mobility up to Secret. We provide security and architectural support and advice; managed services both directly and through partners; security monitoring; and bespoke engineering services all informed by our security pedigree, while delivering the user experience that even our most security-conscious customers now demand.

For a CWE however, security should not detract from the key advantages of leveraging cloud technologies: the flexibility to scale and adapt services to evolving demand. Becrypt ensure a number of principles are adhered to, to maintain flexibility and attractiveness of service offering:

### Avoid vendor lock-in

Becrypt's customers are retained through service delivery excellence, not vendor lock-in. Our CWE is not dependent on proprietary IPR, and we ensure our customers can maintain a migration path for service capability and data to other private or public sector platforms and providers if needed.

### Tailor to customers' needs

We have a track record that spans the delivery of small agile projects for government, through to supporting large-scale strategic programmes: from the rapid provisioning of new capability in sandpit environments for customers such as the National Cyber Security Centre, to supporting collaborative transition to large scale deployments.

### Private "cloud of clouds"

To leverage competition and innovation, organisations typically engage multiple public cloud providers, so we help consumers of high assurance private clouds to adopt an equivalent model. Becrypt can work with other data centre and service providers, using federated identity management and secure connectivity to appropriately accredited platforms to allow CWE customers to transparently access service capability from other cloud providers through a common service window.

### Secure expansion of user community

The CWE allows user identity management to be augmented with strong device identity management, allowing organisations to have confidence in the health of endpoint devices as the CWE community grows. When optionally used with the [Paradox Operating System](#), accredited up to Secret, new users or partners accessing the CWE can inherit a secure endpoint platform with minimal overhead, simplifying risk management as the size and diversity of the user community expands, and providing complete confidence in the health of endpoint estates, irrespective of broader partner cyber maturity.

### Secure mobile compatibility

Working with partners within the UK High Assurance sector, Becrypt have supported the development and deployment of secure mobile architectures, with smartphones now deployed and in use within the defence community at Secret. Becrypt's CWE is compatible with High Assurance architectures, allowing integration of mobile platforms, while maintaining security or accreditation status.

## Service Features

- Familiar and easy to use productivity tools
- Rich collaboration platform with voice, video, messaging and planning environments
- Extensible IaaS platform with control and accountability through managed infrastructure as code
- Federated identity management enables optional secure connectivity to additional cloud platforms
- Layered security architecture includes managed VPN and Firewalls configured to NCSC guidelines
- Dedicated Security Operations Centre with 24/7 security monitoring
- A range of multi-factor user authentication options
- Optional endpoint security provided by the government accredited Paradox Operating System
- Service access restricted to authorised devices with optional device health measurement
- High availability and site replication for disaster recovery
- Self-service or managed user and device enrolment
- Device application & policy management
- Service infrastructure management
- Software vulnerability and patch management
- Reporting
- Incident Management

## Information Assurance

Becrypt's standard CWE offering is hosted within UK-based private data centre, managed by cleared UK staff. Becrypt have a track record of delivering a range of desktop, remote working, collaboration and mobile services at Official Sensitive and above, both directly and through select UK partners.

Becrypt support system accreditation activities, providing appropriate documentation support.

## On Boarding

Becrypt can advise on relative advantages and disadvantages of open source versus proprietary communication and planning tools, including consideration of integration with existing corporate IT where required.

User authentication, security policy, support and governance processes are agreed, allowing an initial CWE capability to go live within weeks. Becrypt provide a dedicated team of consultants, architects and engineers to support service expansion and evolution in line with evolving customer requirements.

Structured training is delivered in line with customer requirements, to build and develop competencies for self-service management and administration as well as productivity and collaboration tool familiarity as required.

## About Becrypt

[Becrypt](#) is an agile London-based UK SME with almost 20 years' experience of disruptive innovation in cyber security. We supply governments and security-conscious commercial organisations, large and small, with a range of security solutions and services - from funded research, to commercially available products and flexible managed services.

Adopting emerging technology, be that cloud or mobile, is about enabling business value and improving user experience. Technology should be designed to be secure by default, simplifying informed risk management. We leverage relationships with government and the 'High Assurance' communities to deliver technologies and services designed for elevated threat environments, and available for all.

From our heritage in data and device encryption, our solutions span operating system security, mobile device management, secure voice, cross-domain and cloud security. We turn government and private-sector funded research into market-leading commercially available products and services.

#becrypt