Technical Product Overview

Becrypt
Enterprise Manager

High Assurance Secure Endpoint Solutions

Becrypt Enterprise Manager (BEM) is a robust and centralised security management system that provides full management of Becrypt's Secure Endpoint Solutions.

Designed with usability in mind, it provides a seamless and straightforward experience for efficient administration of complex tasks.

Built with UK Government

HM Government

becrypt

Becrypt
Enterprise Manager

A powerful, centralised, management solution

Becrypt Enterprise Manager (BEM) is a robust and centralised security management system, enabling users to effortlessly deploy, configure, maintain, update and manage Becrypt OS, OS+, Yubikeys and DAS products. Operating as a web-based management console, BEM offers accessibility from any web browser-enabled device. It supports installation and access from various locations, whether via internet connectivity, a VPN, an internal network or an air-gapped network, all while ensuring the management control through a set of defined BEM user roles and assignments.

How it works

All Becrypt OS managed devices establish and maintain an encrypted connection with BEM, ensuring secure communication. These devices regularly check-in with BEM to stay synchronised. When a policy is modified or created on BEM, the corresponding updates are distributed to all devices assigned to that policy, enabling mass-management across all managed endpoints. In the event of a temporary disconnection from BEM, devices will seamlessly catch up with pending updates as soon as they regain communication.

It is important to note that losing connection to BEM does not hinder device functionality. Once a device has received its assigned policy and is operational, it continues to function independently until further updates are received.

BEM provides a comprehensive overview of registered devices, offering valuable insights such as their last communication status, currently assigned policies, and a complete activity log (showing only important activities). Audit events, including password changes, key requests, and user recovery, are centrally logged, allowing multiple administrators from different locations to access and review them. All data is securely stored in a centralised database facilitating easy backup and recovery procedures.

BEM integrates with existing network services; enabling directory/certificate services, logging servers, and email servers to synchronise with ease. It can be configured to utilise existing identity and certificate services or leverage its own built-in services.

Functionality

Becrypt's family of secure endpoint products are managed in BEM and available as snap-in modules. Each product is configured individually using the respective first-time setup wizard. Users are then able to start utilising the power of BEM alongside the product.

- **Becrypt OS (formerly known as Paradox)**

An ultra-secure lightweight operating system that gives a full user experience at a fraction of the risk.

- **Becrypt OS+**

This enhanced version of Becrypt OS builds upon its existing strength and incorporates additional security features, making it suitable for use at Secret and Top-Secret tiers.

- **Becrypt DAS (Device Authentication Service)**

Provides a secure connectivity for applications and services communicating across diverse and high-risk networks and when accessed externally.

- **Yubikey Manager**

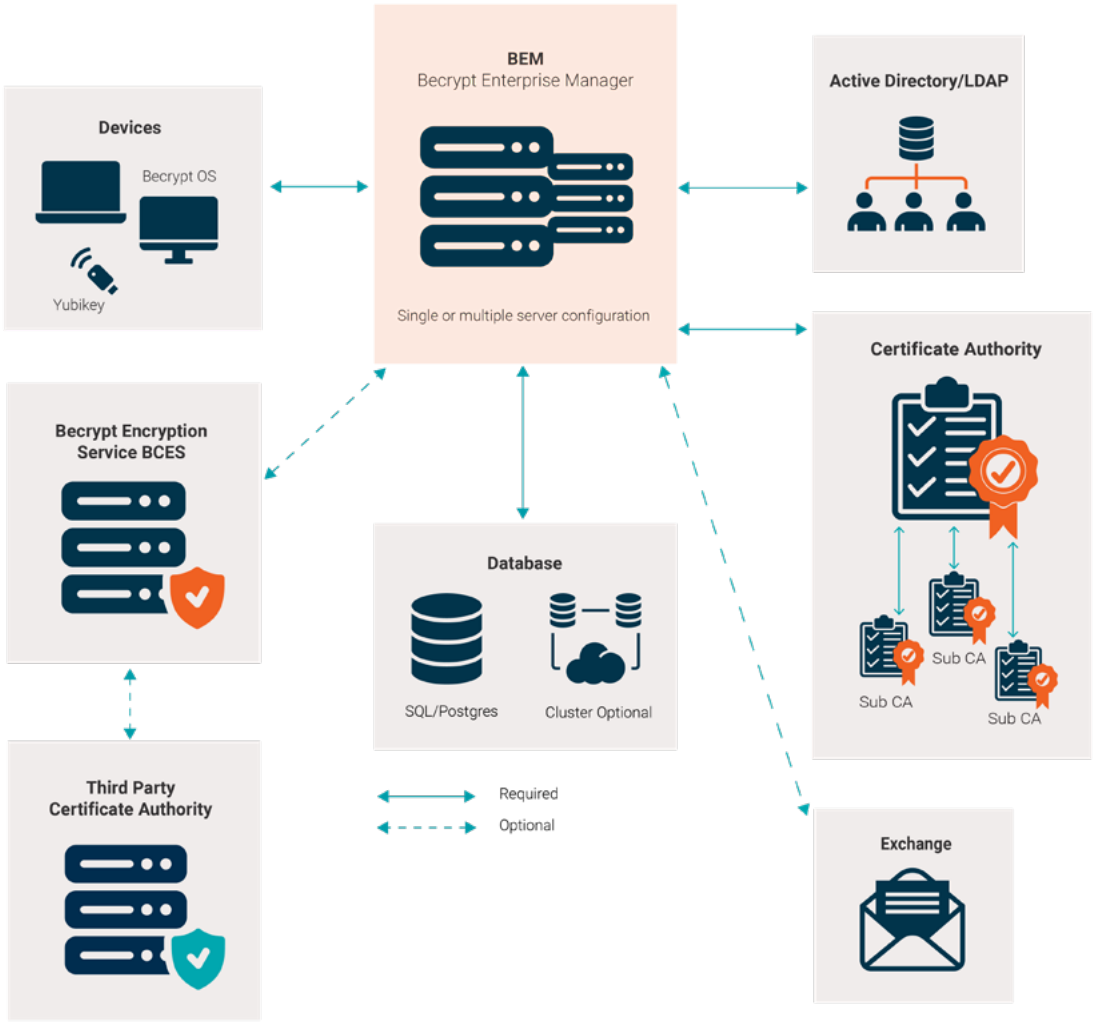
A powerful tool allowing users to self-enrol their Yubikey devices while granting administrators full control over Yubikey management tasks such as PIN resets, device re-enrolment, and user certificate renewal.

- **Access**
  - BEM is hosted on a web front-end, meaning physical access to the service can be restricted to suit the business requirements.
  - BEM can be made available publicly, or access can be restricted to certain networks groups.
  - BEM can be accessed from any device with web browser capabilities so it is easy and efficient for changes to be made on the go.
  - 2FA to the BEM console can be mandated by policy.
- **User Roles**
  - Super User – Manages organisational assets and can access all functionality.
  - Operator – Can manage and access all User and Device functionality.
  - Registrator – Credentials can only be used to register devices to BEM.
  - Becrypt OS+ Device Group Operator (Becrypt OS+ only) – Can manage allocation of Becrypt OS+ devices to Device Groups.
- **Integration**
  - Integrates with existing database services, MS MSQL or PostgreSQL.
  - Integrates directly with identity services such as active directory or other LDAP servers (to allow for creation and management of BEM users and security groups).
  - Microsoft CA Services and HSM's can be integrated to provide certificate and key management services.
  - The different products also offer integration with other services such as syslog, AWS S3/ min.io object storage and more.
- **Management**
  - With the web front-end being hosted on IIS, BEM can be easily managed alongside other IIS web services.
  - Custom Reporting.
  - Audit Logs.
  - Scheduler service + tracking.
  - Import/Export functionality.
  - Database maintenance tools.
  - Licence Management.

Key Benefits and Uses

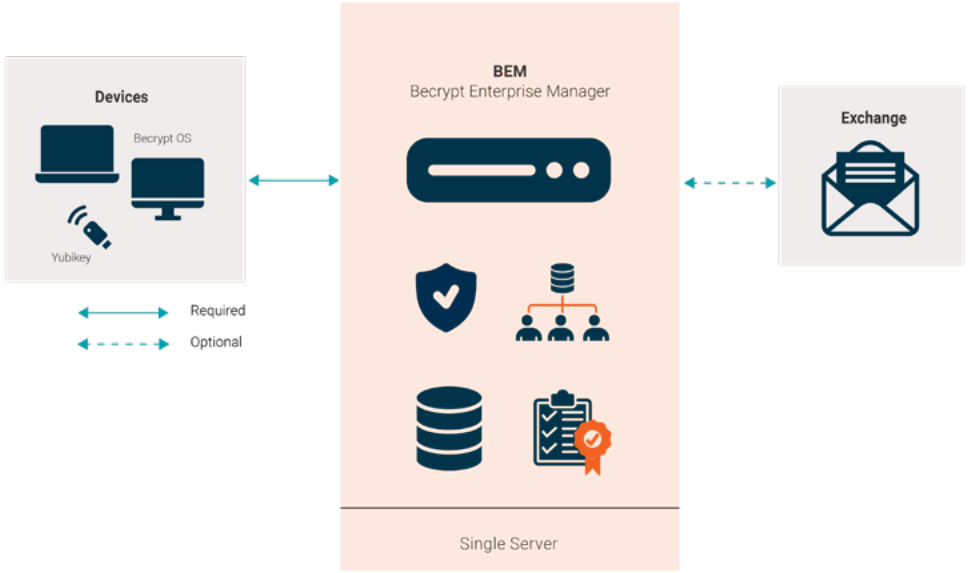
- BEM, being the management platform for Becrypt OS, is used across a wide variety of verticals such as:
  - Government infrastructure
  - Critical National Infrastructure
  - Federal agencies
  - Other security conscious commercial organisations
- Precise security controls and functionality allow for full control over any managed device.
- Ensures all devices are in a healthy and secure state.
- Streamlines the management of all devices:
  - New devices can be automatically deployed based on policies, reducing manual configuration
  - Important security updates can be pushed out to thousands of devices instantly
  - Groups containing configuration and application policies are used to manage devices
  - Device configuration changes can be pushed out to groups instantly
  - New applications and application updates can be pushed out to groups instantly
- Should a device be lost or stolen, its encryption status can be ascertained immediatly and therefore the risk of the data assessed.
- Replacement devices can be fully configured replicating previous device state completely remotely, reducing costs and downtime.
- Supports Zero Trust Architectures
- Certified for use at all tiers, complies with a range of security certifications, assured via thorough security reviews and government-rated penetration tested.

Classic BEM and relating services diagram



BEM in a box option

Simplified deployment for small/tactical deployments and POCs.



Specifications and Requirements + “What is under the hood”

Supported devices:

- Becrypt OS Device
- Becrypt OS+ Devices
- Yubikey Smart Cards

Supported Servers for BEM Installation

- Windows Server 2019 64 bit
- Windows Server 2022 64 bit
- Windows Server 2025 64 bit

Infrastructure:

- Active Directory Server
- Certificate Authority Server
- Microsoft SQL Server 2014
- Microsoft SQL Server 2019
- Microsoft SQL Server 2022
- Microsoft SQL Express
- PostgreSQL 13

VPNs

- Cisco Anyconnect VPN
- Strongswan VPN
- Palo Alto GlobalProtect VPN
- OpenVPN

Pre-Requisites

- .NET 4.7.2 Framework
- .NET Core 8.# Hosting Bundle
- Visual C++ Redistributable for Visual Studio 2019
- IIS 8.5 or later

Software Supplied

- BEM Web.msi
- BCES.msi
- bem_config.yml
- bces_config.yml
- XSDs for APP-XD integration

Hardware (minimum recommended specs)
Per 5000 Devices

- 8gb memory
- 120gb disk
- 1x 2.5 GHz processor
- 1x network interface

Why Becrypt?

With a heritage of creating National Cyber Security Centre-certified products, Becrypt is a trusted provider of endpoint cybersecurity software solutions. Becrypt helps the most security conscious organisations to protect their customer, employee and intellectual property data. It has an established client base which includes governments (central and defence), wider public sector, critical national infrastructure organisations and SMEs.

As one of the early pioneers in device encryption software to today being first to market with a unique desktop operating system, Becrypt continues to bring innovation to endpoint cyber security technology. A recognised cyber security supplier to the UK government, Becrypt's software also meets other internationally accredited security standards. Through its extensive domain and technical expertise, Becrypt helps organisations optimise the use of new technologies and BEM facilitates users to effortlessly deploy, configure, maintain, update and manage Becrypt's Secure Endpoint Solutions products to deliver the security required for the modern age.

Find out more about Becrypt

Call us: 0845 838 2080
Email us: info@becrypt.com

View us on: becrypt.com
Follow us on: @Becrypt
Support us on: Becrypt
Follow us on: Becrypt_Ltd

becrypt