

## Becrypt Media Client

Becrypt Media Client is a software based file encryption solution that protects data whilst in transit on any removable media such as CDs, DVDs or USB devices, as well as supporting secure ZIP file and email attachment encryption.

**Becrypt Media Client offers a simple and easy way of protecting data in transit. Data that is stored on a CD, DVD, ZIP file or USB stick can be vulnerable if unprotected, particularly if the device is lost or stolen. Media Client resides on any removable Device or Zip file with a zero footprint approach, allowing a recipient to access protected data without needing to install software.**

### Protecting data in transit

Data is most at risk of being lost when taken outside of the physical boundaries of the organisation.

Increasingly, mobile working employees are required to work offsite and data needs to be transported on removable media. CDs also offer a low cost, easy to use storage solution, whereby data can be easily copied or downloaded with no regard to the security implications. Similarly, data can be easily transferred to a USB stick and taken off the premises.

With data being easily accessed and copied, organisations are increasingly finding that they need to put in place security measures to protect information. Furthermore, with new legislation requiring compliance with data protection measures, never has the issue of data security been more important to address.

### Media Client Overview

Media Client is a software based file and folder encryption solution that protects data while in transit on removable media. The data can be very quickly encrypted and saved to removable media, as an email attachment, or standard zip file, and shared with a recipient with no further need for Becrypt software to be installed on the recipient's computer.

Password protection built into the software ensures that access to the data is authorised. In the event of the password being forgotten or unknown, data remains totally secure – files or folders can be seen, but no filenames or extensions revealing the data type.

### How it works

Files are encrypted and written to external media, file or email using the Encrypted Media Writer. As part of the process, the disc is protected with a passphrase by the user that conforms to a policy set by the system administrator, and a copy of the Encrypted Media Reader is written as a small executable program. Password/passphrases can be configured to the required complexity to meet the organisation's individual requirements

When the authorised recipient of the protected data opens it on his or her computer they simply run the reader and authenticate to access the information.

The media reader prompts the user to enter the passphrase. If the passphrase is entered correctly, the user may decrypt the files and then open and view them in the normal way. If the passphrase is entered incorrectly, the reader remains locked and, although the user can see the files via Windows Explorer, all filenames, including the file extensions, are hidden.

Should a passphrase or password be lost or forgotten a system administrator with access to the corresponding certificate that contains the private key that was used to perform the encryption, will be able to access the data without knowing the password.

Writing the encrypted files and folders to the CD/DVD device is performed by Media Client, so there is no requirement for third party CD/DVD burning software.

### Fast Facts

- File encryption
- Protects Data in transit on CDs, DVDs or USB devices
- Supports encrypted ZIP file creation
- Supports Email attachment encryption\*
- Easy to use and easy to handle & share data safely
- Zero footprint
- CAPS approved – secures data at RESTRICTED

# Becrypt Media Client

## At a glance

Features	Benefits
Simple easy to use interface enables folders/files selected by the user to be encrypted and written to the media with a passphrase	Non-technical users can easily secure data to the chosen removable media
Secure ZIP File creation	Securely transfer data without the need for physical media
Email Attachment Encryption*	Easily protect data attached to emails
Event log generates automatic audit trail	Provides a transparent view of data being exported by the user
Files (file extensions) and folder names are hidden for data confidentiality	Unauthorised viewers (with incorrect password) can see files but are prevented from knowing the data type
Zero footprint design and extractor application on protected media	Data can be encrypted quickly by the sender and read by the recipient's PC (with passphrase) with no need to have Becrypt software installed
Data recovery facility using certificates	Enables straightforward access to data by administrator if the password is forgotten or unknown
In built integrity/verification of media content	Protects content from being tampered with while in transit. If the file contents have been altered the recipient will not be able to extract the data
Files are written to CDs/DVDs/USB media from within Media Client	No need for additional third party CD/DVD burning software
Includes support for Recipient Certificates*	Removes the need for passphrases and allows automatic decryption by the recipient.

## Certification

CAPS approved to RESTRICTED (Impact Level 3)

\*Not available in the CAPS edition



## For more information please visit [www.becrypt.com](http://www.becrypt.com)

**Headquarters:** Becrypt Limited, 90 Long Acre, Covent Garden, London, WC2E 9RA, United Kingdom Tel: +44 (0) 207 557 6502 Fax: +44 (0) 207 557 6599

**United States:** Becrypt Inc, 1600 Tysons Boulevard, 8th Floor, McLean, Virginia 22102, USA Tel: +1 (877) 221 7775 Fax: +1 (703) 245-3001

**Australia:** Becrypt Pty, Level 12, 1 Pacific Highway, North Sydney, NSW 2060 Tel: +61 (0) 2 9959 1961 Fax: +61 (0) 2 9959 3003

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

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

[www.twitter.com/becrypt](https://www.twitter.com/becrypt)