#becrypt

Becrypt Trusted Client

Secure low cost remote working

Trusted Client is Becrypt's innovative answer to the IT Manager's dilemma of providing low-cost, secure remote access to corporate networks so that staff can work safely from any location. Trusted Client significantly reduces the risk of data loss and data leakage and is an invaluable tool to support and enforce a comprehensive Information Assurance strategy.

Trusted Client Overview

Trusted Client is a device that allows people to work securely from a PC that has a network connection. It addresses the inherent risks of allowing unmanaged connections to an organisation's secure networks and data. By providing cost effective and highly secure access for mobile workers Trusted Client is an easy to use solution that can transform an unmanaged machine into a secure access point.

Simply by inserting the Trusted Client device into a USB port and re-booting, a secure environment is launched, providing a user interface, web browser, email access and standalone applications. Trusted Client is fully configurable to each organisation's individual requirements. Staff no longer need laptops for home or occasional remote working, instead they can be issued with an inexpensive USB flash drive which is more secure and easier to carry.

As well as being used for remote access, home working and occasional off-site working, Trusted Client can also be used in Business Continuity scenarios, either as a secure remote access device, or as a standalone secure environment, should the corporate network fail.

How is it different?

Unlike other solutions, Trusted Client's innovative use of technology creates a secure environment on the host PC where the hard drive is never accessed. Only the PC's memory and processor are used. The hard drive is bypassed so that no data can be leaked and no malware can infect the network. Any data that is saved to Trusted Client is automatically encrypted or Trusted Client can be configured to be a read-only device so that no data can be saved.

How it works

Trusted Client has been designed with a modular approach to enable third party components to be built. It is configurable to include only pre-specified applications, and to restrict the user to approved IP destinations, ports, and protocols, such as the corporate intranet, virtual private network (VPN) or specific hosts. Once the configuration of Trusted Client has been decided, a single install file is created allowing an organisation to quickly and securely build devices that are unique to their needs.

Next the Trusted Client device is built, this can be done by the end user themselves, or by an administrator or other central function. For optimum performance a standard 2 GB or greater USB memory stick is required. The configuration of Trusted Client specific for your organisation, may be held in a central secured zone for access by staff. To create the device, the end user or administrator sets up an initial username and password and inserts the USB memory stick. The Becrypt software then generates a unique 256bit AES encryption key and uses this to encrypt the device and copy the relevant files, producing the Trusted Client.

Fast Facts

- Secure working from unmanaged PCs
- Encrypted operating environment
- Low cost solution
- Secure network access
- Data is encrypted
- CCTM and Common Criteria

The end user then can use the Trusted Client from an internet connected PC. They boot from the USB device, an authentication screen will be displayed, asking for username and password. After successful authentication, the device automatically decrypts and the device operating system is loaded creating a secure environment on the host machine.

Trusted Client utilises standard browsers, Citrix and Microsoft Terminal Services, giving users a familiar user interface and offering easy integration with existing systems. The Trusted Client operating system has no access to the internal drives of the machine, allowing the user to work safely regardless of the malicious software that maybe present on the host. This feature also prevents any data from being leaked outside of the Trusted Client environment. If authentication fails, the device can not be booted and it can not be accessed as the whole device is encrypted.

Trusted Client is quick to boot up and the encryption is completely transparent to the end user. The strong user authentication features include an embedded strong password generator, and the device can be configured to work with additional tokens, providing secondary authentication of any user. Should a password be forgotten, secure device recovery through a challenge/response processes is possible, ensuring that the original password is never compromised.

Central management functionality ensures low operational overhead. Trusted Client deployments can be managed centrally so that individual devices may be repudiated remotely should they be lost, stolen or the user's rights revoked.

Having completed their work session, the user simply shuts down the host PC and removes the Trusted Client USB device, no trace of session is left on the host PC.

#becrypt

Becrypt Trusted Client

At a glance

Features	Benefits
Secure remote network access enables users to work safely from any unmanaged PC	Flexible and mobile working capabilities to provide better service to customers, and work/life balance for users
Working environment is totally isolated from the host machine	Absolutely no transference of data significantly reduces the risk of data loss or data leakage
Encrypted operating system and encrypted data storage – data saved to Trusted Client is automatically encrypted	Device and any data saved securely protected from unauthorised access
Strong authentication with additional dual authentication options and 256 bit AES encryption	Government grade security options make Trusted Client suitable for protecting virtually any commercial information
Based on Open Source software and loaded on an off-the-shelf USB flash drive	Extremely cost effective solution with low hardware costs (particularly when compared with alternatives like laptops or PDAs), and no additional license fees for the operating system
Out of the Box integration with standard browsers, Citrix and Microsoft Terminal Services	Familiar look and feel for users reduces training overheads and rapid start up time giving fast access boosts user acceptance
Fully configurable with easy inclusion of additional plug-in applications	Highly configurable to meet business requirements of each individual organisation
Central Management facilities for device deployment and repudiation	Low operational overheads and the ability to 'kill' a Trusted Client device remotely should it be lost, stolen or the user's rights revoked

Standards and Protocols

Symmetric Encryption: AES 256 bit
Smart Cards: PKCS #11, FIPS 201
Password hashing: SHA-256

Certification

Trusted Client achieved CESG Claims Test Mark (CCTM) in October 2007 and Common Criteria certification in November 2009
FIPS 140-2 Trusted Client uses Becrypt's Cryptographic Library which is FIPS 140-2 level 1 certified

Minimum system requirements

USB Bootable X86 platform

For more information please call 0845 838 2050 or +44 (0) 20 3145 1050, or visit www.becrypt.com

Becrypt Limited, 90 Long Acre, Covent Garden, London WC2E 9RA. www.becrypt.com info@becrypt.com

Becrypt is a leading supplier of innovative Information Assurance solutions and services with operations in the UK and US. Becrypt provides secure, feature rich, out of the box products suitable for all industry sectors, and is the largest supplier of encryption technology to the UK Government, Ministry of Defence and UK Police.