

Becrypt Trusted Client

Inexpensive Secure Mobility and Remote Access

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 employees and contractors 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 security and compliance strategy.

The Challenge of De-perimeterization and Unmanaged Remote Endpoints

As organizations seek to increase efficiency and flexibility by providing their staff with mobile capabilities, some aspects of data security are put at risk.

Existing solutions can be costly and cumbersome or can provide access at the expense of security. People accessing the corporate network from an unmanaged PC could inadvertently introduce viruses, Trojans and other malware. In addition, there is little control over what data is accessed and where it is saved. Data could be saved on the insecure hard disk of a home PC for example or on CDs/DVDs/USB devices, exposing organizations to multiple security threats.

Trusted Client Overview

Trusted Client is a device that allows people to work securely from a desktop or laptop that can boot to USB. It addresses the inherent risks of allowing unmanaged connections to an organization'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 endpoint.

A secure environment is easily launched by inserting the Trusted Client device into a USB port and re-booting. The user is then provided with a secure interface, web browser, email access and standalone applications. Trusted Client is fully configurable to each organization's individual requirements. Employees no longer need expensive laptop hardware with bloated and insecure applications for remote access. Instead they can be issued a USB flash drive with only the necessary applications configured, resulting in a more secure and portable method for obtaining secure mobility.

As well as being used for remote access and telecommuting, Trusted Client can also be used in Business Continuity scenarios, either as a secure remote access device, or as a standalone secure environment.

How is it Different?

Unlike other security and virtualization solutions, Trusted Client's innovative use of technology creates a secure environment utilizing the host PC where the native hard drive is never accessed. Only the PC's memory and processor are used. The hard drive is completely bypassed so that no data can be leaked and no malware can infect the corporate network. Any data that is saved to Trusted Client is automatically protected with FIPS 140-2 certified encryption that protects all data on the USB device in the event of loss or theft.

Fast Facts

- Secure mobility from unmanaged PCs
- Encrypted operating environment
- Low cost solution
- Secure network access
- Data is encrypted

How it Works

Trusted Client was designed with a modular approach to enable the inclusion and customization of third party components. It is configurable to include only pre-approved applications, and to restrict the user to approved IP destinations, ports, and protocols, such as the corporate intranet, virtual private network (VPN) or specific remote servers.

The end user can use the Trusted Client device from any PC. The user boots from the USB device and an authentication prompt is then displayed on the host PC's screen, asking for a username and password, or optional two-factor authentication such as a CAC/PIV smartcard. After successful authentication, the device automatically decrypts and the device operating system is loaded, creating a secure environment on the USB drive, utilizing the host machine's CPU, RAM, display and peripherals such as mouse and keyboard.

Trusted Client supports the use of multiple popular applications like Firefox, OpenOffice and Skype, as well as terminal services, such as Citrix, Microsoft, VMWare VDI, giving users a familiar interface and offering easy integration with existing systems.

The hardened Trusted Client operating system has no access to the internal drives of the machine, allowing the user to work safely regardless of any malicious software that may be present on the host. This feature also prevents any data from being leaked outside of the Trusted Client environment. If authentication fails, the device cannot be booted and the data on it cannot be accessed, as the whole device is encrypted with Pre-Boot Authentication for access control.

Trusted Client is quick to boot up and once authenticated, the encryption is completely transparent to the end user. If an end-user forgets their Trusted Client password, secure device recovery is achieved through a challenge/response process, 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 remotely disabled should they be lost, stolen or the user's rights revoked.

Becrypt Trusted Client

At a glance

Features	Benefits
Secure remote network access enables users to work safely from any unmanaged PC* <small>*PC must be able to boot from USB</small>	Enables secure mobility to provide better service to customers and better work/life balance for employees and contractors.
Working environment is totally isolated from the host machine	Zero exchange of data from USB drive to and from native hard drive significantly reduces the risk of data loss or data leakage
Encrypted operating system and data storage – data saved to Trusted Client is automatically encrypted	Device and any data saved is securely protected from unauthorized access in the event of loss or theft of the USB drive
Optional strong authentication (two-factor) including CAC/PIV smartcards for federal workforce	Government-approved authentication options make Trusted Client suitable for protecting sensitive information
Open Source software is hardened and customized to customer requirements and loaded on an off-the-shelf USB flash drive	Extremely cost effective solution with low hardware costs (particularly when compared with alternatives like company-issued laptops or PDAs). No additional license fees for the operating system
Out-of-the-box integration with major internet browser, Citrix and Microsoft Terminal Services, among other available applications	Familiar look and feel for users reduces training overhead. Rapid startup time with fast access to applications boosts user acceptance
Fully configurable with easy inclusion of additional plug-in applications	Highly configurable to meet business requirements of each individual organization
Enterprise central management for Trusted Client deployments	Low operational overhead 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 256bit

PKCS 11 FIPS 201 smartcards

Password hashing: SHA-256

Certifications

Trusted Client uses Becrypt's Cryptographic Library which is FIPS 140-2 certified

Trusted Client is currently undergoing Common Criteria evaluation

Trusted Client achieved UK CESG Claims Test Mark (CCTM) in October 2007



Minimum System Requirements

USB Bootable X86 platform

For more information please call (877) 221-7775, email info@becrypt.com or visit www.becrypt.com

Becrypt Inc. 225 Franklin Street, 26th Floor Boston, MA 02110

Becrypt is a global leading supplier of innovative Information Assurance solutions and services, providing secure, feature rich, out of the box products that are government-certified and suitable for all industry sectors. Through technology and OEM partnerships Becrypt enables third-party solutions with encryption and other data security capabilities. Becrypt has offices in Boston, USA, London, UK and Sydney, Australia serving clients worldwide.

© Copyright 2009 by Becrypt. All Rights Reserved. The Becrypt logo and trademarks are owned by Becrypt Limited. No material may be reproduced for any purpose, private or commercial, without prior written permission from Becrypt Limited.