



Government Quality Mark

Directory of CESG Claims Tested Mark (CCTM) Awards for Products and Services

May 2008

"In line with Transformational Government Policy and to ensure trust and confidence, Government information systems must use appropriate security products and services which have a minimum assurance of the CCTM."

Central Sponsor for Information Assurance

"If I am going to buy a product or service I need to know that I can trust in it. If I find something that I know will work for us, and it has the CCTM which will also be recognised by our partners, then it's a win-win. As new products go through the CCTM process we hope to end up with a raft of products we know we can trust, choosing the right products also means that our citizen's data should be safe."

David Sifleet, London Borough of Brent, GC Supplement July/August 2007

The CESG Claims Tested Mark (CCTM)- a mark for assurance, a mark for confidence, a mark for quality, a mark to trust.

The CCTM scheme provides a government quality mark for the public and private sectors based on accredited independent testing, designed to prove the validity of security functionality claims made by vendors. The CCTM is designed to assure public bodies that a product or service "does what it says on the box". Additionally, the CCTM scheme provides compliance testing against technical standards for degaussing (data erasure) set by CESG as the National Technical Authority for IA. The CCTM is aimed primarily at products and services to meet IA requirements at Government Impact Levels 1 and 2.

To see details of the claims tested and a test report summary for each product or service in this catalogue visit the Awards page on the CCTM website.

Claims Testing Process

To be awarded the CCTM, each product or service must go through the following process:

- Vendors translate marketing statements about their product or service into claims and produce an Information Assurance Claims Document (ICD)
- Vendor selects and agrees a contract with a Test Laboratory for claims testing.
- Vendor registers with CESG CCTM Secretariat to have their product or service tested against their ICD.
- The Scheme reviews the claims made by the vendor about their product or service, as well as looking at marketing and guidance documentation and accepts the application for claims testing.
- Vendor's chosen CCTM Test Laboratory starts testing the functionality of the product or service against the claims that are made in the ICD and issues a test report.
- If successful the Scheme awards the CCTM for a period of two years for a product and one year for a service. Details are published on the Government website.



Quick Overview of CCTM Awards

Company	Erasure & Disposal	Connection Protection	Integrity Protection	Media & Device Authentication	Media and Information Protection	Network Link Protection
AEP Networks						x
Aladdin			x			
AppSense			x			
Barron McCann	x					
BeCrypt				x	x	
Centennial Software				x		
CGI Group				x		
Credant						
Data Encryption Systems Ltd	x					
Future Technology Industry	x					
HP		x				
IBM					x	
Juniper Networks						x
Message Labs			x			
The National Archives			x			
Netintelligence Limited			x			
Pointsec					x	
R&R Data Managed Services	x					
Reflex Magnetics				x		
Safeboot					x	
SDMS				x		
Secure Wave			x	x		
TruDate Integrity			x			
Ultra Electronics Datel					x	
Ultratec Limited	x					
Whale Communications						x

Descriptors

The following defines the meaning of the categories used in this document.

Connection Protection: focused on protecting Systems, Data and Information in transit at the Application Level

Erasure and Disposal Protection: focused on protecting Data and Information when the Media on which it is contained is to be reused or disposed of

Information Preservation & Investigation: focused on preserving Data and Information for Recovery or Investigative purposes. No Products and Services have yet been awarded in this category

Integrity Protection: focused on protecting Systems, Data and Information from Unauthorised Modification or Deletion, typically at the Application Level

Media & Device Authentication: focused on ensuring that Systems only accept approved media or devices at the Infrastructure Level

Media & Information Protection: focused on ensuring that Data and Information is protected from Unauthorised Access, typically at the Application Level

Network Link Protection: focused on protecting Data and Information in transit at the Communications or Infrastructure Levels

Verification Facilities: focused on ensuring the correct operation of other IA facilities. No Products and Services have yet been awarded in this category

Latest CCTM Awards

Erasure and Disposal

<p>Data Encryption Systems Ltd</p> <p>Certificate number: 2008/05/0036 CCTM awarded: 13th May 2008</p> <p>For more information: www.deslock.com</p>	<p>DESlock+ Ver 3.2.7</p> <p>DESlock+ is a flexible, transparent encryption tool aimed at providing information assurance at Government Impact Levels 1 and 2, for purchase by central government and the wider public sector, particularly the NHS, education, local authorities, police and criminal justice. DESlock+ provides encryption, decryption and deletion of data on Hard disk drives and removable media at file and folder levels, and also the facility to easily Email encrypted data. Each software token holds up to 64 different keys, which can be shared with other users, providing a multilevel solution to Data Security needs</p>
---	---

Products/Services Awarded the CCTM

Connection Protection

<p>HP</p> <p>Certificate number: 2006/05/0011 CCTM awarded: 17th May 2006</p> <p>For more information: www.hp.com/hps/security/ products</p>	<p>HP ProtectTools Email Release Manager Version: 5.0</p> <p>HP ProtectTools Email Release Manager enforces an email security policy by providing facilities to electronically sign, encrypt, and audit emails to ensure your organisation is in control of email activity with minimum impact on users.</p>
---	---

Erasure and Disposal

<p>Barron McCann Technology Ltd</p> <p>Certificate number: 2007/09/0029 CCTM awarded: 27th September 2007</p> <p>For more information: http://www.bemac.com</p>	<p>Managed Service for Secure Destruction of Data on Magnetic Media Version: 1</p> <p>Barron McCann's Secure Data Destruction Service is an end-to-end managed service for dealing with end-of-life IT equipment in central and local government, law enforcement, military and health environments holding data with protective markings of up to and including HMG RESTRICTED. The service offers a data destruction service that ensures data stored on magnetic media such as hard drives and tape is destroyed before the equipment is recycled. Our service allows your organisation to meet both your WEEE and Data Protection Act legal responsibilities.</p> <p>When carrying out the service we follow all relevant security standards in data destruction using CESG approved equipment backed by the CSIA Claim Tested Mark.</p> <p>The service is offered on-site at our secure List-X data destruction facility, or we can carry out the service at your own location anywhere in the UK. All of our data destruction engineers hold at least SC clearances.</p>
<p>Future Technology Industry Ltd</p> <p>Certificate number: 2007/06/0021 CCTM awarded: 13th June 2007</p> <p>For more information: http://www.futuretechnologyindustry.com</p>	<p>Hard Disk Magnetic Crusher Model: HC-3000</p> <p>The consequences of your data being made public are embarrassment, financial loss and reputational loss. To mitigate data theft from discarded computer hard drives and other magnetic recording media, you should destroy the data at source. The HC-3000 is an office-based magnetic media degausser the size of a desktop computer and can be used to clear all data from the media before disposal. When you need a robust security policy, you need a robust end-of-life data destruction process.</p>

Products/Services Awarded the CCTM

Erasure and Disposal

<p>Future Technology Industry Ltd</p> <p>Certificate number: 2007/06/0022 CCTM awarded: 13th June 2007</p> <p>For more information: http://www.futuretechnologyindustry.com</p>	<p>Hard Disk Magnetic Crusher Model: COMBO</p> <p>The consequences of your data being made public are embarrassment, financial loss and reputational loss. To mitigate data theft from discarded computer hard drives and other magnetic recording media, you should destroy the data at source. The Combo's dual function will magnetically degauss and physically destroy the magnetic media to clear all data before disposal. When you need a robust security policy, you need a robust end-of-life data destruction process.</p>
<p>Future Technology Industry Ltd</p> <p>Certificate number: 2007/08/0025 CCTM awarded: 6th August 2007</p> <p>For more information: http://www.futuretechnologyindustry.com</p>	<p>Hard Disk Magnetic Crusher Model: HC-7800</p> <p>The consequences of your data being made public are embarrassment, financial loss and reputational loss. To mitigate data theft from discarded computer hard drives and other magnetic recording media, you should destroy the data at source. The HC7800 is a high-power magnetic media degausser which and can be used to clear all data from the media before disposal. When you need a robust security policy, you need a robust end-of-life data destruction process. Additionally, HC7800 has large storage which can be accommodated up to 15" Laptop PC and erase the data without taking the hard drive from the Laptop PC.</p>
<p>R & R Data Managed Services Ltd</p> <p>Certificate number: 2007/02/0018 CCTM awarded: 27th February 2007</p> <p>For more information: www.datarecovered.com</p>	<p>Secure Destruction of Data on Magnetic Media Version: 1</p> <p>Our unique mobile Data Destruction Service makes it easy for clients to comply with their statutory duty to securely remove data classified at RESTRICTED and below from obsolete and surplus IT equipment and media. The data destruction process can be part of the quality and security policy of any organisation, allowing proof of compliance with security needs and the law. In addition, the media can be safely destroyed in an environmentally approved way to comply with statutory disposal requirements.</p>
<p>Ultratec Ltd</p> <p>Certificate number: 2007/09/0026 CCTM awarded: 14th September 2007</p> <p>For more information: http://www.ultratec.co.uk</p>	<p>Secure Destruction of Data on Magnetic Media Version: 1</p> <p>This service provides cost effective Secure Data Destruction on your site for a variety of magnetic data storage media. This service uses a CESG approved degausser to remove all data on media marked RESTRICTED or below. This service is operated by our own Defence Vetting Agency Security Check ('SC') engineers. Van, Engineer, and equipment will arrive on the customer site. If the option for environmentally compliant (WEEE directive) disposal of the processed media has been taken, then the engineer will remove the media for smelting and refining. A certificate detailing all media processed is issued on completion.</p>

Products/Services Awarded the CCTM

Integrity Protection

<p style="text-align: center;">Aladdin</p> <p>Certificate number: 2007/03/0019 CCTM awarded: 7th March 2007</p> <p style="text-align: center;">For more information: www.aladdin.com</p>	<p>eSafe Version: 5.2</p> <p>Founded by pioneers in the anti-malware industry and grounded in ongoing product innovation and patented technologies, eSafe provides strong content security solutions with the capacity, manageability, scalability and reliability to effectively protect against Internet-borne threats -- reducing risk and increasing productivity.</p>
<p style="text-align: center;">MessageLabs Ltd</p> <p>Certificate number: 2007/10/0032 CCTM awarded: 5th November 2007</p> <p style="text-align: center;">For more information: http://www.messagelabs.com</p>	<p>MessageLabs Anti-Virus Service Version: 5.1</p> <p>MessageLabs Anti-Virus email service provides protection against email threats, such as viruses and Trojans, saving businesses valuable time and resource otherwise spent dealing with unwanted outbreaks and the associated clean up.</p> <p>The service uses multiple commercial virus scanners to identify existing threats and Skeptic™, MessageLabs predictive proprietary technology. Skeptic is supported by an internationally recognised anti-virus team who researches and identifies new threats and pre-emptively updates the service to offer up-to-date 24x7x365 protection.</p> <p>With 99.999% availability and backed by a service level agreement which offers compensation in the very unlikely event that a virus reaches your network, the service is run in secure data centres on multiple sites to ensure continuous availability in the event of a disaster. Even with MessageLabs global infrastructure client email can still be guaranteed to be scanned within certain countries or regions to ensure compliance with data protection legislation and specific client requirements.</p>
<p style="text-align: center;">NetIntelligence Ltd</p> <p>Certificate number: 2007/11/0031 CCTM awarded: 30th October 2007</p> <p style="text-align: center;">For more information: http://www.netintelligence.com</p>	<p>Ni Enterprise Manager Version: 5.0</p> <p>IT user management & control gets the hosted service treatment, with Ni Enterprise Manager offering a simple way of enforcing endpoint policy regardless of the physical location of the users.</p> <p>An 'all in one software as a service' solution that combines core physical security functionality of anti virus/spyware, firewall, web filtering, IM & P2P control, asset management, with comprehensive end point usage reporting, Ni Enterprise Manager offers a truly unique 'plug and play' web based management, protection and control service. Ni Enterprise Manager enables the central application and enforcement of policies across de-perimeterised networks and physical boundaries.</p>

Products/Services Awarded the CCTM

Integrity Protection

<p>TruData Integrity Ltd</p> <p>Certificate number: 2007/11/0033 CCTM awarded: 8th November 2007</p> <p>For more information: http://www.tru-dataintegrity.com</p>	<p>TruSeal Version: 2.0</p> <p>The Tru Data Integrity TruSeal product provides a solution to the question of what happens to information once it leaves the originator; the product provides a means of ensuring that copies of original data continue to hold evidential weight even once they have moved into the hands of third parties. The product delivers proof (in line with BIP0008) of integrity and origin, for legal and Information Integrity purposes, by sealing data and ensuring that the seal remains with all copies of data, regardless of ownership or location.</p>
<p>The National Archives</p> <p>Certificate number: 2008/02/0035 CCTM awarded: 27th February 2008</p> <p>For more information: http://www.nationalarchives.gov.uk</p>	<p>Digital Record Object Identification (DROID) Version: 3.0</p> <p>Departments and other public bodies are unclear about the depth and breadth variations in file formats in use for electronic records.</p> <p>To support an ongoing identification and monitoring of this information, the National Archives has produced:</p> <ul style="list-style-type: none">• The PRONOM technical registry which provides a way of identifying file formats• The DROID (Digital Record Object Identification) tool to perform trusted, automated batch identification of file formats, using both file extension and byte sequence signatures from PRONOM to identify and report file format versions of digital files <p>These tools were joint winners of the 2007 Digital Preservation Award sponsored by the Digital Preservation Coalition, and DROID has been awarded the government's CSIA Claims Tested (CCT) Mark, Certificate Number 2008/02/0035 which independently validates the trusted nature of the product.</p>

Products/Services Awarded the CCTM

Media and Device Authentication

<p style="text-align: center;">BeCrypt</p> <p>Certificate number: 2006/04/0009 CCTM awarded: 26th April 2006</p> <p style="text-align: center;">For more information: www.becrypt.com</p>	<p>Connect Protect Version: 2.0</p> <p>Connect Protect 2.0 introduces further functionality over its predecessor version 1.6.2. Version 2.0 now allows finer grained control over external memory devices and provides support for audited file copies to and from otherwise restricted removable media.</p>
<p style="text-align: center;">BeCrypt</p> <p>Certificate number: 2007/09/0027 CCTM awarded: 27th September 2007</p> <p style="text-align: center;">For more information: http://www.becrypt.com</p>	<p>Trusted Client Platform Version: 1.2</p> <p>BeCrypt™ Trusted Client Platform is a secure portable computing environment that can be used on unmanaged and unsecured computers. The platform is an enterprise security solution designed to ensure reduced operational risk by protecting information on bootable USB flash devices on which critical information could be compromised if lost or stolen. It is a solution that is easy to design, deploy and support in line with organisational security requirements. Implementation and ongoing management can be achieved with a low Total Cost of Ownership.</p>
<p style="text-align: center;">Credant Technologies, Inc.</p> <p>Certificate number: 2008/02/0034 CCTM awarded: 18th February 2008</p> <p style="text-align: center;">For more information: www.credant.com</p>	<p>Credant Mobile Guardian Enterprise Edition Version 5.2.1</p> <p>CREDANT Mobile Guardian (CMG) Enterprise Edition is a scalable mobile security and management software platform that enables organizations to easily secure and manage disparate mobile & wireless devices from a single management console. CREDANT Mobile Guardian provides strong authentication, Intelligent Encryption, usage controls, and automated key management that guarantees data recovery. With CREDANT deployed, organizations can easily increase the speed of business execution by enabling business processes to reduce the risk of going mobile safely “go mobile”.</p>
<p style="text-align: center;">Centennial Software</p> <p>Certificate number : 2006/08/0012 CCTM awarded: 5th September 2006</p> <p style="text-align: center;">For more information: www.centennial-software.com</p>	<p>DeviceWall Version: 4.01</p> <p>DeviceWall facilitates the granular management of endpoint communications ports, removable media and other peripheral devices in accordance with security privileges assigned to groups and users in the Control Center. DeviceWall manages all common device types, including USB drives, CDs, PDAs and other external data storage devices. Where appropriate, DeviceWall can further secure files legitimately copied to USB flash drives by automatically encrypting the data.</p>
<p style="text-align: center;">CGI Group (Europe) Ltd</p> <p>Certificate number: 2007/09/0030 CCTM awarded: 27th September 2007</p> <p style="text-align: center;">For more information: http://www.cgigov.com</p>	<p>Excelsior Security Manager Version: 1</p> <p>Excelsior Security Manager provides a comprehensive identity management platform for Local Authorities for providing registration and authentication features. It provides the flexibility for Local Authorities to make their own decisions on authentication solutions, while at the same time delivering out of the box compatibility with other government initiatives.</p>

Products/Services Awarded the CCTM

Media and Device Authentication

<p style="text-align: center;">SDMS Ltd</p> <p>Certificate number: 2007/09/0028 CCTM awarded: 27th September 2007</p> <p style="text-align: center;">For more information: information@sdms.uk.com</p>	<p>Secure Data Media Solutions Service Version: 1</p> <p>The SDMS service provides for the supply of premium brand, security marked, printed, accountable and auditable computer, audio and video storage media.</p> <p>The marking, printing and identification of media can be customised to meet specific customer security requirements.</p> <p>Packing and distribution is performed within a government accredited secure location.</p> <p>Records of despatched products are retained for at least 7 years, to assist in any related incident investigation by the customer.</p>
--	--

Products/Services Awarded the CCTM

Media and Information Protection

<p style="text-align: center;">BeCrypt</p> <p>Certificate number : 2006/10/0014 CCTM awarded: 23rd October 2006</p> <p style="text-align: center;">For more information: www.becrypt.com</p>	<p>Disk Protect Version: 4.1</p> <p>BeCrypt™ DISK Protect is a feature rich enterprise security solution designed to ensure reduced operational risk by protecting information on mobile devices and smart media on which critical information could be compromised if lost or stolen. It is a flexible and scalable solution that is easy to design, deploy and support in line with organisational security requirements on a range of Windows™ platforms. Implementation and ongoing management can be achieved with a low Total Cost of Ownership.</p>
<p style="text-align: center;">BeCrypt</p> <p>Certificate number : 2006/11/0017 CCTM awarded: 30th November 2006</p> <p style="text-align: center;">For more information: www.becrypt.com</p>	<p>PDA Protect Version: 4.1</p> <p>BeCrypt™ PDA Protect is a feature rich enterprise security solution designed to ensure reduced operational risk by protecting information on mobile computing devices on which critical information could be compromised if lost or stolen. It is a flexible and scalable solution that is easy to design, deploy and support in line with organisational security requirements on a range of Windows CE platforms. Implementation and ongoing management can be achieved with a low Total Cost of Ownership.</p>
<p style="text-align: center;">IBM United Kingdom Ltd</p> <p>Certificate number : 2007/06/0024 CCTM awarded: 28th June 2007</p> <p style="text-align: center;">For more information: www-935.ibm.com/services/uk/index.wss/offering/its/a1024853</p>	<p>Virtual Infrastructure Access Services Version: 5.5b</p> <p>The IBM Virtual Infrastructure Access Services product allows authorised users to connect through any Java enabled Web browser securely over the internet to an enabled application within their enterprise. The solution combines portal, Thin client, messaging, and security technologies delivered through a single, consistent delivery framework founded upon a standard and scalable set of Internet architecture principles. IBM Virtual Infrastructure Access Services is an effective way of delivering distributed infrastructure solutions featuring:</p> <ul style="list-style-type: none"> • Single Sign On; • Single Logical Access point; one entry point allows greater control; <p style="padding-left: 40px;">Simplified Portal presentation</p> <p>Note: The scope of the claims testing is the IBM Virtual Infrastructure Access Services product infrastructure only. Testing of client specific applications on the IBM Virtual Infrastructure Access Services infrastructure has not been undertaken.</p>
<p style="text-align: center;">Pointsec</p> <p>Certificate number: 2006/04/0008 CCTM awarded: 26th April 2006</p> <p style="text-align: center;">For more information: www.pointsec.com</p>	<p>PC Enterprise Workplace Edition Version: 5.2.2</p> <p>Pointsec for PC combines enforceable mandatory access control and strong encryption to create an advanced enterprise security solution. User credentials and confidential data remain private, enabling organisations and agencies to take advantage of today's mobile PC technology without compromising security.</p>

Products/Services Awarded the CCTM

Media and Information Protection

<p style="text-align: center;">Pointsec</p> <p>Certificate number : 2006/10/0015 CCTM awarded: 30th October 2006</p> <p style="text-align: center;">For more information: www.pointsec.com</p>	<p>Pointsec for Pocket PC</p> <p>Pointsec™ for Pocket PC combines enforceable mandatory access control and strong encryption to create an advanced enterprise security solution. This has been proven under the CSIA Claims Tested Scheme, on Windows 2003 Mobile for Pocket PC. User credentials and confidential data remain private, enabling organisations and agencies to take advantage of today's mobile PC technology without compromising security.</p>
<p style="text-align: center;">Safeboot</p> <p>Certificate number : 2006/09/0013 CCTM awarded: 5th September 2006</p> <p style="text-align: center;">For more information: www.safeboot.com</p>	<p>Safeboot Device Encryption for PC/Laptop Version: 5.0</p> <p>SafeBoot® Device Encryption™ for PC/Laptop uses strong access control and pre-boot authentication for both users and machines to prevent unauthorized access to PCs and laptops. Encryption and decryption on hard disk drives are performed on the fly, in a process which is transparent to the user, with virtually no performance degradation. SafeBoot® Device Encryption™ for PC/Laptop also offers secure hibernation, password rules (for content, length, etc.), and extensive central management capabilities integrated into existing enterprise tools and Active Directory.</p>
<p style="text-align: center;">Ultra Electronics Datel</p> <p>Certificate number : 2007/06/0023 CCTM awarded: 28th June 2007</p> <p style="text-align: center;">For more information: www.ultra-datel.com</p>	<p>Syntaxis Shared Collaborative Working Environment Service Version: 2.7</p> <p>Ultra Electronics Datel recognises that team working is crucial to many modern enterprises. Teams are often geographically dispersed and reliant on modern technology for communication. With time being one of today's most precious resources; there's a requirement for teams to share information and knowledge safely and securely in real time.</p> <p>By use of the Syntaxis product, Ultra Eletronics Datel provides a Secure Collaborative Working Environment to a wide cross-section of Industry and Government customers, delivering real time collaborative working.</p> <p>Syntaxis not only enables joint Government and/or Industry to communicate freely on engagements, but allows teams to share material and contribute to work-in-progress, providing project stakeholders with the right information at the right time in the right place.</p> <p>Accessible from the Internet, the RLI and the GSI, Syntaxis provides the flexibility needed for all stakeholders, regardless of location, to contribute.</p>

Products/Services Awarded the CCTM

Network Link Protection

<p>AEP Networks</p> <p>Certificate number : 2006/11/0016 CCTM awarded: 30th November 2006</p> <p>For more information: http://www.aepnetworks.com</p>	<p>AEP Netilla Security Platform</p> <p>The AEP Netilla Security Platform (NSP) is an SSL VPN appliance that enables organisations to simply, securely, and cost effectively provide users with browser-based access to corporate applications and files from through the security and convenience of a web browser. With any browser enabled computer, telecommuters, branch office employees, business partners and a mobile sales force can quickly and securely reach virtually any resource used in your business.</p>
<p>Juniper Networks</p> <p>Certificate number : 2007/04/0020 CCTM awarded: 24th April 2007</p> <p>For more information: www.juniper.net</p>	<p>Juniper Networks Secure Access Family Version: 5.4R2.1</p> <p>The Juniper Secure Access 4000/6000-FIPS appliances can be deployed to provide secure, anywhere, anytime remote access services to public sector employees from a wide variety of end devices and locations. By leveraging the advanced client endpoint assessment features, administrators can provide many levels of differentiated access, consistent with a centralised security policy. Ease of integration into existing AAA environments makes the SA an extremely compelling solution to support Web, Application and Network connectivity for a remote workforce. Following CSIA guidelines and subject to a risk assessment and accreditor approval, the SA4000FIPS and SA6000FIPS, combining FIPS 140-2 Level 3 and the CCTM can be used in the Public Sector for networks carrying information up to Restricted data.</p>

Lapsed CCTM Awards for Products/Services

Integrity Protection

<p>AppSense</p> <p>Certificate number: 2005/10/0004 CCTM Lapsed: 20th October 2007</p>	<p>Application Manager Version: 6.0</p> <p>AppSense Application Manager blocks the execution of all unauthorized software, including executable viruses, trojans, spyware, P2P and hacking tools.</p>
<p>Secure Wave</p> <p>Certificate number: 2005/09/0002 CCTM Lapsed: 8th September 2007</p>	<p>Sanctuary Standard Edition Version: 2.8.0</p> <p>Sanctuary Application Control provides total control over the execution of all applications on Microsoft based networks. Sanctuary Application Control Desktop works on the basis that the use of all executables is denied unless authorised.</p>

Media and Device Authentication

<p>BeCrypt</p> <p>Certificate number: 2005/09/0001 CCTM Lapsed: 7th September 2007</p>	<p>Connect Protect Version: 1.6.2.5</p> <p>Connect Protect is an enterprise Plug and Play device access control solution designed to secure desktop or laptop computers from data leakage via devices such as USB memory sticks, removable disk drives and printer.</p>
<p>Reflex Magnetics</p> <p>Certificate number: 2005/11/0005 CCTM Lapsed: 6th November 2007</p>	<p>Reflex Disknet Pro Version: 4.50.1</p> <p>Reflex Disknet Pro manages the use of all I/O devices allowing granular access to devices; denying all access, providing read-only access or allowing full authorised access and full content management.</p>
<p>Secure Wave</p> <p>Certificate number: 2005/09/0003 CCTM Lapsed: 7th September 2007</p>	<p>Sanctuary Device Control Version: 2.8.7</p> <p>Sanctuary Device Control extends the standard Windows security model to control I/O devices. Based on the White List concept, device access for users is not allowed by default.</p>

Network Link Protection

<p>Whale Communications</p> <p>Certificate number: 2006/02/0006 CCTM Lapsed: 27th February 2008</p>	<p>Whale Intelligent Application Gateway <i>(Previously called e-Gap Remote Access Appliance Vers: 3.1)</i></p> <p>Whale's Intelligent Application Gateway is an enterprise-class SSL VPN that enables organisations to simply, securely, and cost effectively provide users with browser-based access to corporate applications and files from anywhere.</p>
--	--

Accredited Test Laboratories








The CCTM Scheme has appointed seven test laboratories to validate the security functionality claims of products and services submitted to the Scheme.

Vendors can approach these test laboratories to:

- Provide advice and assistance in preparing their claims document.
- Undertake the claims testing of their product or service

For more information please consult the Test Laboratories page of the CCTM website:

www.cctmark.gov.uk

TEST LABORATORY	CATEGORIES OF CLAIMS TESTING
	Generalist
	Generalist
	Generalist
	Generalist
	Generalist, Specialist - Hardware and Smartcard testing, Data Erasure (CESG Degaussing Lower Level)
	Generalist
	Generalist and Specialist testing – Anti Virus



For more information about the CCTM Scheme go to www.cctmark.gov.uk

You can e-mail us at: secretariat@cctmark.gov.uk

Please write to:
CCTM Secretariat
35 Endell Street
London
WC2H 9BA

General Enquiries: 020 7240 7220