



Government Quality Mark

Directory of CSIA Claims Tested Mark Awards for Products and Services

August 2007

"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 CCT Mark."

Harvey Mattinson, CSIA- Head of Assurance and Standards

"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 CCT Mark from the CSIA which will also be recognised by our partners, then it's a win-win. As new products go through the CCT Mark 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 CSIA Claims Tested (CCT) Mark - a mark for assurance, a mark for confidence, a mark for quality, a mark to trust.

The CCT Mark 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 CCT mark is designed to assure public bodies that a product or service "does what it says on the box". Additionally, the CCT Mark scheme provides compliance testing against technical standards for degaussing (data erasure) set by CESG as the National Technical Authority for IA. The CCT Mark 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 CCT Mark website.

Claims Testing Process

To be awarded the CCT Mark, 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 CSIA 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 CCT Mark 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 CCT Mark 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 CCT Mark 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			
BeCrypt				x	x	
Centennial Software				x		
Future Technology Industry	x					
HP		x				
IBM					x	
Juniper Networks						x
Message Labs			x			
Pointsec					x	
R&R Data Managed Services	x					
Reflex Magnetics				x		
Safeboot					x	
Secure Wave			x	x		
Ultra Electronic Datel					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

Products/Services Awarded the CCT Mark

Connection Protection

<p>HP</p> <p>Certificate number: 2006/05/0011 CCT Mark 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>Future Technology Industry Ltd</p> <p>Certificate number: 2007/06/0021 CCT Mark 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>
<p>Future Technology Industry Ltd</p> <p>Certificate number: 2007/06/0022 CCT Mark 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 CCT Mark 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>

Products/Services Awarded the CCT Mark

Erasure and Disposal

<p>R & R Data Managed Services Ltd</p> <p>Certificate number : 2007/02/0018 CCT Mark 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>
--	--

Integrity Protection

<p style="text-align: center;">Aladdin</p> <p>Certificate number : 2007/03/0019 CCT Mark awarded: 7th March 2007</p> <p>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;">AppSense</p> <p>Certificate number: 2005/10/0004 CCT Mark awarded: 21st October 2005</p> <p>For more information: www.appsense.com</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 style="text-align: center;">Message Labs</p> <p>Certificate number: 2006/04/0007 CCT Mark awarded: 26th April 2006</p> <p>For more information: www.messagelabs.com</p>	<p>Anti-Virus Service Version: 5.1</p> <p>MessageLabs Anti- Virus e-mail service provides protection against e-mail threats, such as viruses and Trojans, saving business valuable time and resource otherwise spent dealing with unwanted outbreaks and the associated clean up.</p>
<p style="text-align: center;">Secure Wave</p> <p>Certificate number: 2005/09/0002 CCT Mark awarded: 8th September 2005</p> <p>For more information: www.securewave.com</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>

Products/Services Awarded the CCT Mark

Media and Device Authentication

<p>BeCrypt</p> <p>Certificate number: 2006/04/0009 CCT Mark awarded: 26th April 2006</p> <p>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>BeCrypt</p> <p>Certificate number: 2005/09/0001 CCT Mark awarded: 8th September 2005</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>Centennial Software</p> <p>Certificate number : 2006/08/0012 CCT Mark awarded: 5th September 2006</p> <p>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>Reflex Magnetics</p> <p>Certificate number: 2005/11/0005 CCT Mark awarded: 7th November 2005</p> <p>For more information: www.reflex-magnetics.com</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 CCT Mark awarded: 8th September 2005</p> <p>For more information: www.securewave.com</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>

Products/Services Awarded the CCT Mark

Media and Information Protection

<p style="text-align: center;">BeCrypt</p> <p>Certificate number : 2006/10/0014 CCT Mark 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 CCT Mark 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 CCT Mark 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; • Simplified Portal presentation <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 CCT Mark 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 CCT Mark

Media and Information Protection

<p style="text-align: center;">Pointsec</p> <p>Certificate number : 2006/10/0015 CCT Mark 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 : 2006/09/13 CCT Mark 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 : 2007/06/23 CCT Mark 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 CCT Mark

Network Link Protection

<p>AEP Networks</p> <p>Certificate number : 2006/11/0016 CCT Mark 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 : 2007/03/0020 CCT Mark 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 CCT Mark can be used in the Public Sector for networks carrying information up to Restricted data.</p>
<p>Whale Communications</p> <p>Certificate number: 2006/02/0006 CCT Mark awarded: 27th February 2006</p> <p>For more information: www.whalecommunications.com</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 CCT Mark Scheme has appointed six 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 CCT Mark website:

www.cctmark.gov.uk

TEST LABORATORY	CATEGORIES OF CLAIMS TESTING
	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 CCT Mark Scheme go to www.cctmark.gov.uk

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

Please write to:
CCT Mark Secretariat
CSIA
Cabinet Office
26 Whitehall
London
SW1A 2WH

General Enquiries: 020 7276 5029