Important Information – Please Read

THE DIRECTORY OF INFOSEC ASSURED PRODUCTS

Users of this Directory must be aware that the most up-to-date version of Infosec Assured Products are available at www.cesg.gov.uk

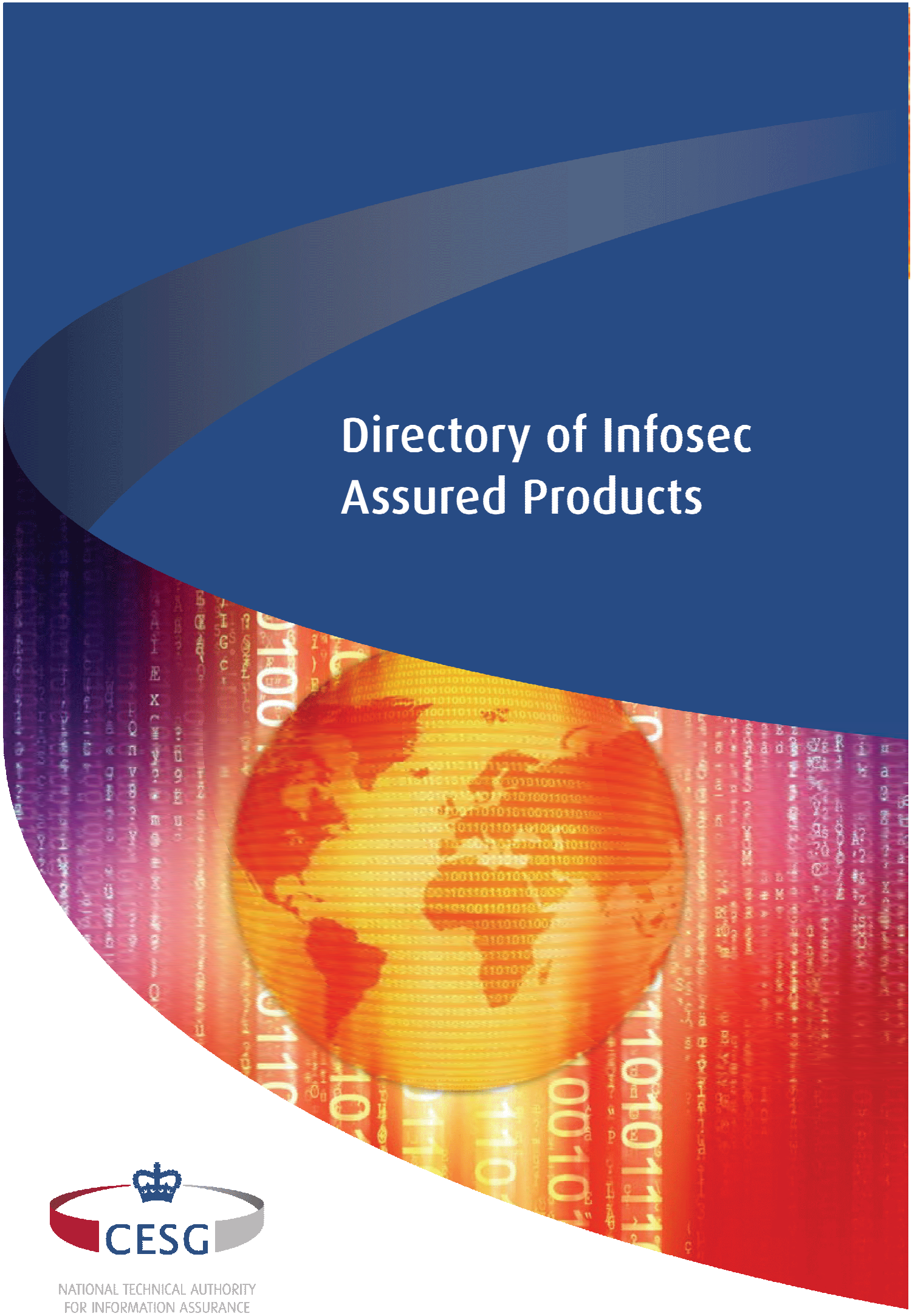
For current information on IA products and their usage please see the individual product entries using the product search facilities at

www.cesg.gov.uk

THIS DOCUMENT WAS CORRECT AT TIME OF PRODUCTION

OCTOBER 2010

Directory of Infosec Assured Products



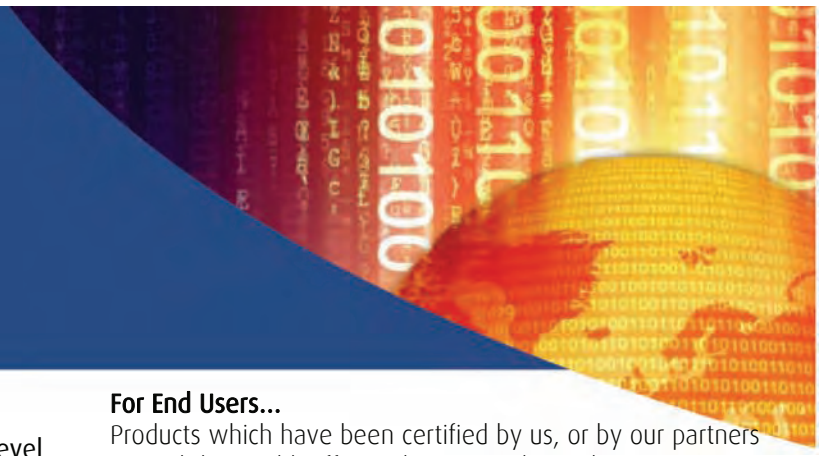
CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Contents

SECTION 1

Introduction



This 'Directory of Infosec Assured Products' is a top-level guide listing all IT security products approved by CESG. The Directory lists products by type, and in addition gives brief details of the means by which products are approved or certified, an overview of the products' features, and the context in which they should be used. There is also a contact list of product vendors.

A downloadable version of the current Directory is available from the CESG website – www.cesg.gov.uk.
As information on assured products is available via the product search facilities at www.cesg.gov.uk, which includes both the Certified Product Search and CESG Assisted Products Service (CAPS) Product Search.

IT products and systems evolve rapidly and are increasingly diverse and complicated. Similarly, customer requirements change and expand to counter new threats and to adapt to new ways of working. CESG has brought together its assurance services under Information Assurance and Consultancy Service (IACS) to offer bespoke solutions to these new security challenges.

In order to be listed in the Directory, a product must have undergone one of the various methods of evaluation and/or certification offered by IACS. IACS provides a seamless service for customers and the IACS management office can provide more in-depth advice and guidance to developers, vendors and end users on the most appropriate solution to meet their assurance requirements.

THE IACS approach

For Developers...

Technical assessors from IACS will work with developers or end users to define the best solution to their assurance requirements. By understanding the developer's goals, IACS can define the most effective assessment package to achieve them. An assessment package could include:

- Internationally recognised Common Criteria (CC) or IT Security Evaluation Criteria (ITSEC) Certification
- Cryptographic approval for HMG
- Tailored Assurance-a toolbox approach to systems assurance

For End Users...

Products which have been certified by us, or by our partners around the world, offer end users ready-made assurance. This allows the customer to determine whether the product is appropriate for his needs. If assurance is required in a system, then a range of packages, including IT Security Health Check, is available.

A brief description of these schemes can be found in the Schemes Annex from page 14.2 more comprehensive details on each scheme are available on the CESG website, www.cesg.gov.uk.

Formal Evaluation and Certification

In the Directory, products will be identified as certified against either CC or ITSEC or in accordance with UK Cryptographic Standards. Certificates are award following extensive testing of the product's IT security features to ensure that those features meet an agreed Security Target. Results of a successful evaluation are published in a Certification Report. This contains additional information and advice on how the certified product should be used and any restrictions that may apply in its configuration or use on specific platforms.

Prospective purchase's of approved products are reminded that the product descriptions in this Directory are only a guide, and that they should consult the supplementary documentation before purchasing, to check the product's suitability. Prospective purchasers of ITSEC/CC products should read both the Security Target and Certification Report of the product. These are available from the vender and can also be downloaded from the CESG website, www.cesg.gov.uk. Prospective purchasers of CAPS products should read both the Security Target and Handling Instructions and are also advised to ensure that the intended usage, implementation and deployment of a cryptographic product is in compliance with National Baseline Policy detailed in HMG Infosec Standard 4.

Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor or CESG www.cesg.gov.uk. Please note that these documents are often Protectively Marked and therefore, available only to recipients with a valid need to know and appropriate storage and handling facilities.

SECTION 1

Introduction

What is a Security Target?

This is a document specifying the security functionality of a product and the assurance level against which it is evaluated as well as a description relating the product to the environment in which it will operate.

Vulnerabilities

Certification is not a guarantee of freedom from security vulnerabilities; there remains a possibility that exploitable vulnerabilities may be discovered after a Certificate has been awarded. Users and prospective purchasers should check regularly whether any security vulnerabilities have been discovered since certification and, if appropriate, should check with the vendor to see if any patches exist for the product. If so they should test and install the Patch.

CESG Sales Approvals

The sale of any CESG-approved cryptographic product is subject to approval by CESG. This is an important process to ensure that cryptographic products are going to appropriate recipients and to ensure that the implementation of cryptography requested is appropriate to the requirement. It is also an important element of the Key production process, ensuring that users receive appropriate Key material for their requirements.

Obtaining Approved Cryptographic Products

Contact details for advice on products and for sales enquires are given in the product listing.

CONTACT DETAILS

Customer Support Office
A2j
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Telephone: +44 (0)1242 709 141
Fax: +44 (0)1242 709 193

Email: enquiries@cesg.gsi.gov.uk
URL: www.cesg.gov.uK

SECTION 2

Access Control

CESG

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor or CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

ITSEC/CC
Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from CESG website.

CCTM
CESG Claims Tested Mark

Prospective purchasers of CCT Mark approved products or services should read both the ICD and Test Report documents available from the CCT Mark website, to ensure the product or service is appropriate for their needs.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0)1242 709141 Fax: +44 (0)1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 2

Access Control

BeCrypt™ Advanced Port Control (APC)

Cryptographic Grade: See Notes

BeCrypt™ Advanced Port Control (APC) is a port control solution designed to prevent the connection and use of unauthorised devices for IBM compatible personal computers running Microsoft Windows XP, Windows 2000 Server and Windows 2003 Server operating systems.

Notes:
BeCrypt™ Advanced Prot Control (APC) does not provide any encryption functionally and does not reduce the Protective Marking (PM) of data on personal computers to a lower level.

Version: 1.0

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0)845 838 2050
Fax:.....+44 (0) 845 838 2060
Email: sales@becrypt.com
URL: www.becrypt.com

BeCrypt™ Connect Protection Version 3.0

CCTM Certificate: 2009/08/0049
Awarded: 4th August 2009 Valid until: 3rd August 2011

BeCrypt™ Connect Protect is an access control solution for Plug and Play devices designed to protect an enterprise from accidental or malicious leakage of private or classified data at Baseline Impact levels IL1 or IL2 or below via unauthorised device connections. BeCrypt™ Connect Protect is configuration using Active Directory, or locally for stand-alone configurations. Device connections are set by device type not bus type and may be set to either 'fill access', 'controlled access', 'read only' or 'no access'. BeCrypt™ Connect Protect can provide further fine grain control with restriction of removable disk drives identified by either vendor model or generated unique identifier.

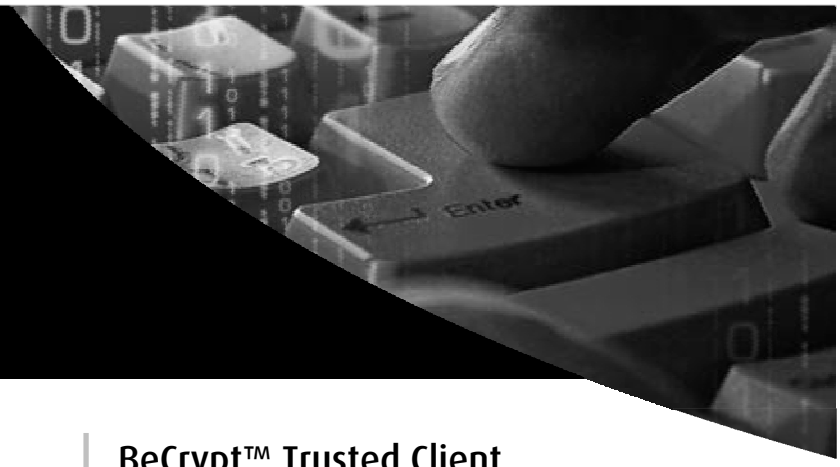
BeCrypt™ Connect Protect audits unauthorised use of devices and optional copying of data in clear to and from otherwise disabled removable media devices.

BeCrypt™ Connect Protect is interoperable with BeCrypt's other products including DISK Protect, PDA Protect and Removable Media Encryption, Combined, they give a compelling data security strategy for an enterprise environment.

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0)1189 880 277
Email: info@becrypt.com
URL: www.becrypt.com

SECTION 2

Access Control



BeCrypt™ Media Client Version 1.1

CCTM	Certificate: 2009/08/0050
Awarded: 4th August 2009	Valid until: 3rd august 2011

BeCrypt™ Media Client Offers a simple and easy way of protecting data at Business Impact levels IL1 or IL2 in transit. Data that is stored on a CD, DVD or USB stick can be vulnerable if unprotected, particularly if the device is lost or stolen. BeCrypt™ Media Client resides on a CD, DVD or USB stick, allowing a recipient to access protected data without needing to install software.

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0) 845 838 2050
Email: info@becrypt.com
URL: www.becrypt.com

BeCrypt™ Trusted Client Platform Version 1.2

CCTM	Certificate: 2007/09/0027
Awarded: 27th September 2007	Valid until: 26th September 2009

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

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0) 1189 880 277
Email: info@becrypt.com
URL: www.becrypt.com

SECTION 2

Access Control

Check Point Endpoint Media Encryption Version 4.93

CCTM Certificate: 2009/02/0043

Awarded: 25th February 2009 Valid until: 24th February 2011

Based on market-leading Pointsec® technologies, Check Point Endpoint Security Media Encryption™ addresses the internal threat from unauthorised copying of enterprise data to personal storage devices and removable media through a powerful combination of port management, content filtering, centralized auditing and management of storage devices, and optional media encryption. Check Point Media Encryption plugs these potential leak points and provides a comprehensive audit-reporting capability of how data files move to and from these devices, giving enterprises complete control of their security policies. Check Point Media Encryption is centrally managed so the solution can be deployed easily across all endpoints. This fine level of granularity over policy settings keeps enterprise in control, allowing them to optimise security while minimizing the effect on user work patterns and IT operational costs.

Check Point Software Technologies Ltd
Unit 4 Lindenwood, Crockford Lane, Chineham Business Park,
Basingstoke, RG 24 8QY, United Kingdom
Telephone: +44 (0)1256 375 460
Email: info@checkpoint.com
URL: www.checkpoint.com

Citrix MetaFrame Presentation Server Version 4.0

COMMON CRITERIA EAL2 Certificate: CRP219 August 2005

CLEF: BT

Citrix Presentation Server provides users with secure access to centrally managed Web, Windows and legacy applications. This access can be from a range of devices over any network connection, including LAN, WAN, dial-up or wireless connection.

Security features include:

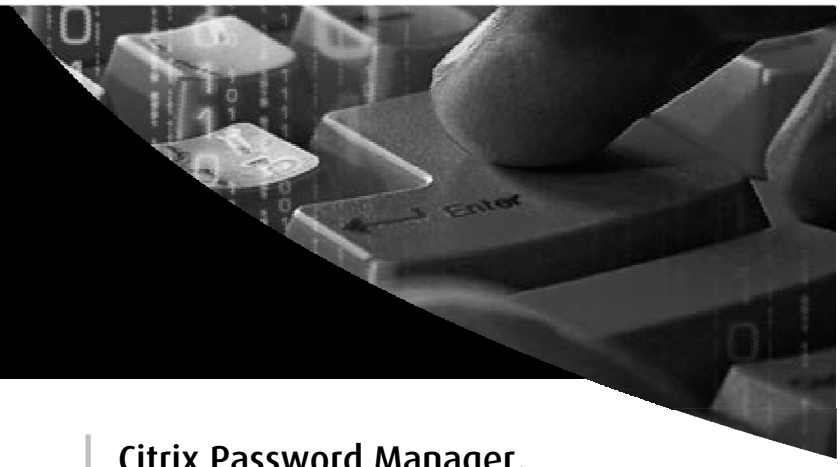
- User authentication by password or smartcard
- Control of access to a managed set of user-specific published applications
- Client/server authentication and encryption of traffic between client and server using TLS.

Citrix Presentation Server allows multiple users to log on and run applications in separate protected sessions on the same server. Servers can be grouped together and managed as a single entity, providing a highly scaleable and flexible means of deploying applications to users.

Citrix System Inc
851 West Cypress Creek Road, Fort Lauderdale, Florida 33309, USA
Point of contact: Millie Price
Telephone: +1 954 229 6401
Fax: +1 954 229 6519
Email: millie.price@citrix.com
URL: www.citrix.com

SECTION 2

Access Control



Citrix® NetScaler®Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0

COMMON CRITERIA EAL2 Certificate: CRP247 September 8

CLEF: SiVenture

The Citrix® NetScaler® NS7000 and NS9010-FIPS Application Switches with Access Gateway Enterprise Edition and Application Firewall are dedicated appliances that accelerate application performance, project web applications from attack, and provide secure application access via Secure Sockets Layer Virtual Private Network (SSL VPN) functionality with policy-based access control.

A NetScaler appliance with activated Access Gateway and Application Firewall software provides secure access from an external network to web-based applications, windows-based applications delivered via Citrix® Presentation Server and Desktop Application delivered via Citrix® XenDesktop. The NetScaler Application Switch, Access Gateway and Application Firewall software elements run on either the NetScaler NS7000 or NS9010-FIPS Application Hardware.

Citrix NetScaler is a solution for enterprise seeking accelerated Web application performance, improved web application security, highly secure application access for users anywhere they work, and increased application availability.

Citrix Systems Inc
4988 Great America Parkway, Santa Clara, California 95954, USA
Point of contact: Michael Badarak
Telephone: +1 408 790 8933
Fax: +1 408 790 8933
Email: michael.badarak@citrix.com
URL: www.citrix.com/

Citrix Password Manager, Enterprise Edition, Version 4.5

COMMON CRITERIA EAL2 Certificate: CRP235 June 2007

CLEF: BT

Citrix Password Manager Enterprise Edition, Version 4.5 (including Citrix Password Manager for Presentation Server) is an enterprise single sign-on (SSO) solution that allows user to access to password-protected applications-whether Windows, Web or host-based-from one single logon. Users authenticate once to the network, and Password Manager automates logons, password changes and password policy enforcement, making connecting to applications easier, faster and more secure.

Security features include:

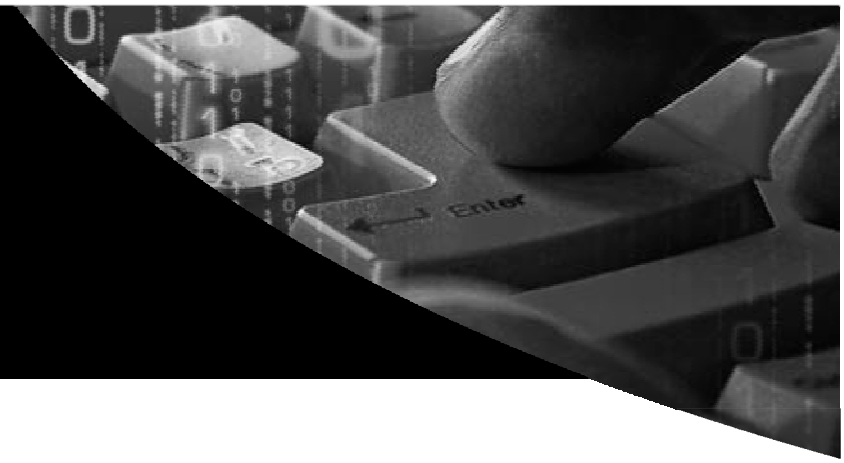
- Support for use authentication using password or smartcard
- Extensive password construction policies
- FIPS-certified encryption for password protection
- Anti-phishing protection
- Mitigation against walk-away breaches
- Auditing of password related events
- The leverage of scalability and resiliency mechanisms built into Windows Active

Directory. Password Manager can also be configured to restrict user visibility to application password, putting password back under the sole control of IT.

Citrix System Inc
851 West Cypress Creek Road, Fort Lauderdale, Florida 33309, USA
Point of contact: Jayram Subrahmanian
Telephone: +1 954 229 6344
Fax: +1 954 940 7701
Email: jayram.subrahmanian@citrx.com
URL: www.citrix.com/

SECTION 2

Access Control



Citrix® Presentation Server Version 4.5

COMMON CRITERIA EAL2 Certificate: CRP241 July 2007

CLEF: BT

Citrix Presentation Server™ is used by more than 180,000 customers to reduce cost for delivering Windows applications. It offers application virtualisation and application streaming delivery methods to enable an exceptional access experience for any user, with ant device, working over any network. With it, organizations can centralize applications and data in secure data centres, reducing costs of management and support, increasing data security, and ensuring fast, reliable performance.

Security features include:

- User authentication through single sign-on and multi-factor authentication devices
- SmartAccess™ granular access control policies and integrated endpoint analysis
- Client/server authentication and encryption of traffic using Transport Layer Security (TLS)
- Advanced Encryption Standard (AES) support
-

Citrix Presentation Server 4.5, Platinum Edition For Windows is certified to EAL2 augmented by ALC_FLR.2.

Citrix Systems Inc
851 West Cypress Creek Road, Fort Lauderdale, Florida 33309, USA
Point of contact: Jayram Subrahmanian
Telephone: +1 954 229 6344
Fax: +1 954 940 7701
Email: jayram.subrahmanian@citrix.com
URL: www.citrix.com/

Citrix Presentation Server With Feature Release 3

COMMON CRITERIA EAL2 Certificate: CRP201 April 2004

CLEF: BT

Citrix Presentation Server provides users with secure access to centrally managed Web, Windows and legacy applications. This access can be from a range of devices over any network connection, including LAN, WAN, up-up or wireless connection.

Security features include:

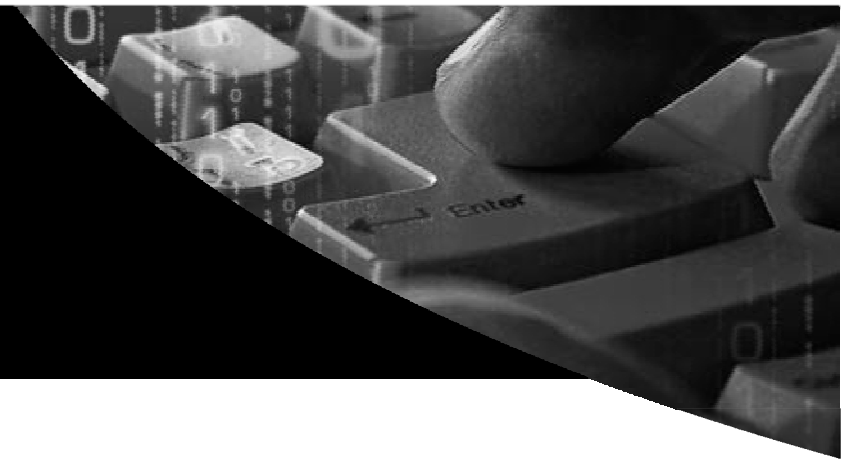
- User authentication by password or smartcard
- Control of access to a managed set of user-specific published applications
- Client/server authentication and encryption of traffic between client and server using TLS

Citrix Presentation Server allows multiple users to log on and run applications in separate protected sessions on the same server. Servers can be grouped together and managed as a single entity, providing a highly scaleable and flexible means of deploying applications to users.

Citrix System Inc
851 West Cypress Creek Road, Fort Lauderdale, Florida 33309, USA
Point of contact: Millie Price
Telephone: +1 954 229 6401
Fax: +1 954 940 6519
Email: millie.price@citrix.com
URL: www.citrix.com/

SECTION 2

Access Control



Excelsior Security Manager Version 1.0

CCTM — Certificate: 2007/09/0030

Awarded: 27th September 2007 — Valid until: 26th September 2009

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.

CGI Group (Europe) Ltd
Broadlands House, Primett Road, Stevenage, Hertfordshire, SG1 3EE
United Kingdom
Telephone: +44 (0)191 515 2666
Email: enquiries@cgigov.com
URL: www.cgigov.com

GUARDIAN ANGEL Version 5.01D1

ITSEC E2 — Certificate: CR9893_2 January 1998

CLEF: BT

Guardian Angel Version 5.01D1 is a 16-bit, pre-DOS loader providing access control mechanisms that prevent data theft and prevent unauthorised usage. Thus preventing:

- Illegal access through user identification and password modules encrypted with the CESG FIREGUARD algorithm
- Unauthorised file access and ownership by User Security Profiles, auditing, and a File Access Control Matrix
- Propagation of malicious code by blocking the copying or activation of unauthorised exactable programs
- The use of unauthorised floppy disks by Disk Certification;

Data encryption is provided using an endorsed implementation of the CESG RED PIKE algorithm. GUARDIAN ANGEL Version 5.01D1 was certified in standalone mode.

Portcullis Computer Security Ltd
The Grange Barn, Pikes End, Pinner, Middlesex, HA5 2EX,
United Kingdom
Point of contact: Alan Romanis
Telephone: +44 (0)208 868 0098
Fax: +44 (0)208 868 0017
Email: consult@portcullis-security.com
URL: www.portcullis-security.com/

SECTION 2

Access Control

HP ProtectTools Authentication Service Version 4.0 & 4.1

Cryptographic Grade: See Notes

HP ProtecTools Authentication Services provides a UK Government approved way of protecting your system from unauthorised access. It strengthens the authentication sub-system by enhancing password processing and incorporating such measures as configurable pass phrase and two-factor login. Authentication Services password processing is enhanced by using UK Government algorithms together with seeding values to produce a customer unique authentication system. This enhanced authentication system can be further configured to impose generated passwords to ensure appropriately strong passwords are used, or a configurable regime of pass phrases can be implemented to provide a more memorable set of authentication parameters with no compromise to security. In addition to the above, Authentication Services contains facilities to manage the change of administrative password, a last successful and unsuccessful login information display, it can be configured to implement multiple login denial and a timed automatic log out of unattended workstations.

Notes:
HP ProtectTools Authentication Services has been approved through CAPS to Baseline grade, however this does not prohibit use on ICT systems that process data for which the assessed impact from loss of confidentiality, integrity or availability is above IL3.

HP ProtectTools Authentications is a technical countermeasure that may be used in conjunction with other physical, procedural, personnel or technical countermeasures for systems at any Impact Level when building a Security Case for the SIRO, SRO accreditor and business users as explained by HMG IA Standard No.1 Part 2.

HP ProtectTools Authentication Services may be used alongside any of the previous products Windows 2000 (SE),Windows XP (SE) or Windows Server 2003 (SE) should it become necessary to increase the size of an installed base that uses one or more of these earlier products.

Version: v4.0, v4.1.

Hewlett Packard Ltd
Secure Solutions Team, 2 Kelvin Close, Birchwood Science Park North, Risley, Warrington, WA3 7PB, United Kingdom
Telephone: +44 (0)1925 841 881
Fax: +44 (0)1925 841 010
Email: protecttools@hp.com
URL: www.hp.com/hps/security/products/

Lumension Device Control Version 4.3.2

Formerly known as Sanctuary Device Control

CCTM Certificate:2099/02/0041
Awarded: 25th February 2009 Vailid until 24rh February 2011

Lumens ion Device Control (formerly known as Sanctuary Device Control) enforces organisation-wide usage policies for removable devices (e.g., USB sticks), removable media (e.g., CDs/DVDs), and data (e.g., read/write, encryption). Using a white list/"default deny" approach, administrations can centrally:

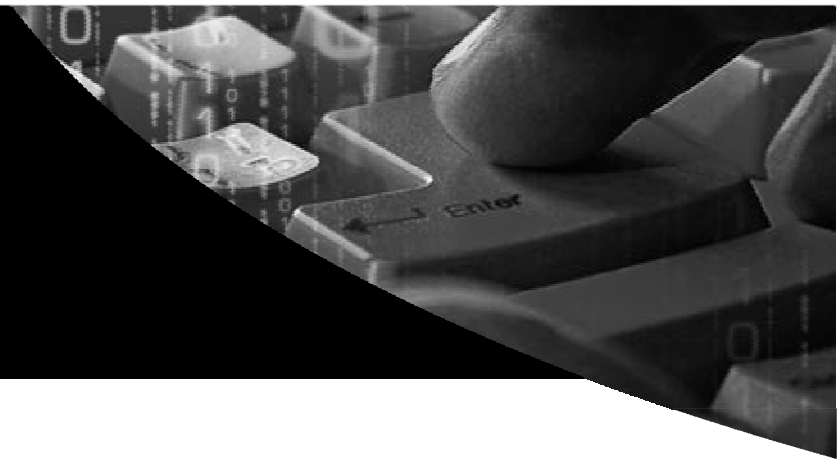
- Control access of "plug and play" devices by class, model and/or specific ID
- Uniquely identify and authorise specific media
- Implement file copy limitations (amount-per-day, time-of-day), file type filtering, and forced encryption
- Apply permissions to specific and/or groups of ports, devices, endpoints and users (both on-line/off-line), including temporary access
- Create role-based Admin Accounts (e.g. regional sites)
- Log either file name or complete file conten
- Create standard & customised reports on system activity to be saved into a repository, shared via email, and/or imported into other applications.

Lumens ion Device Control enables organisations to use productivity-enhancing tools whilst limiting the potential data leakage (and impact thereof).

Lumension
Windsor Place, Faraday Road, Crawley, West Sussex, RH10 9TF
United Kingdom
Telephone: +44 (0)1908 357 897
Email: andrewclarke@lumension.com
URL: www.lumension.com

SECTION 2

Access Control



McAfee Endpoint Encryption for Devices Version 5.0

COMMON CRITERIS EAL4 Certificate: CRP 227 May 2006

CLEF: BT

McAfee Endpoint Encryption for Devices Version 5.0 Client is a Personal Computer (PC) security system that prevents the data stored on a PC's hard disk from being read or used by an unauthorised person. It combines single sign-on user access control with transparent full hard disk encryption to offer effective security for PCs running the Microsoft Windows ™ operating system. Management. deployment and user recovery are handled by a centralised administration server, McAfee Endpoint Encryption Management Centre. Communication between the client software and the administration server is via a cryptographically secure proprietary protocol. McAfee Endpoint Encryption Management Centre is a required system component when using McAfee Endpoint Encryption for Devices Version 5.0

The scope of this EAL4 evaluation is that the McAfee Endpoint Encryption for Devices Version 5.0. The McAfee Endpoint Encryption Management Centre is given the degree of consideration that is reported in the Security Target and Certification Report.

When certified this product was known as "Safeboot Device Encryption for PC Version 5.0 Client". After certification it was rebranded to "McAfee Endpoint Encryption for Devices Version 5.0". The certified product (including its software and documentation) is unchanged.

McAfee, Inc.
3965 Freedom Circle, Santa Clara, CA 95054, USA
Point of contact: Mike Siegel
Telephone: +1 888 847 8766

Reflex Disknet Pro

COMMON CRITERIA EAL2 Certificate: CRP215 April 2005

CLEF: BT

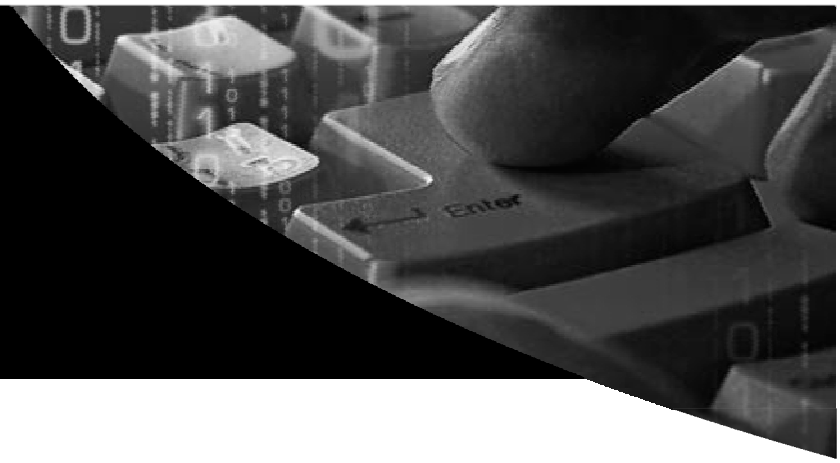
Reflex Disknet Pro is a corporate solution that provides a policy driven mechanism of securing an organisation's information and ensures data integrity. Reflex Disknet Pro provides endpoint security over the use of USB and other memory devices. By managing the use of all I/O devices with Removable Media Manager (RMM) and Port Guard (PG), the system administrator can take back control. Access to devices can be controlled either by denying all access, providing read-only access or allowing full authorised access. Devices are individually authorised ensuring that the content of any newly introduced device complies with your corporate security policy. Furthermore, Reflex Disknet Pro can be used to prevent the download of unwanted file types to the hard disk, network drive or any other attached memory device. This ensures compliance with software licensing and prevents both known and unknown malicious code from getting access to your network.

Notes:
Reflex Disknet Pro is supplied with an additional module Encryption Policy Manager (EPM) which allows for the encryption of removable media where policy dictates. EPM is not part of the Common Criteria evaluation.

Reflex Magnetics Ltd
31-33 Priory Park Road, London, NW6 7HP, United Kingdom
Point of contact: Andy Campbell
Telephone: +44 (0)20 7372 6666
Fax: +44 (0)20 7372 2507
Email: sale@reflex-magnetics.com
URL: www.reflex-magnetics.com/

SECTION 2

Access Control



Secure Data Media Solutions Service Version 1.0

CCTM — Certificate: 2008/12/0040

Awarded: 19th December 2008 — Valid until: 18th December 2009

The SDMS service provides for the supply of premium brand, security marked, printed, accountable and auditable computer, audio and video storage media.

The marking, printing and identification of media can be customised to meet specific customer security requirements.

Packing and distribution is performed within a Government accredited secure location.

Records of despatched products are retained for at least 7 years, to assist in any related incident investigation by the customer.

McAfee, Inc.
3965 Freedom Circle, Santa Clara, CA 95054, USA
Point of contact: Mike Siegel
Telephone: +1 888 847 8766

Trantella Enterprise

COMMON CRITERIA EAL2 — Certificate: CRP214 May 2005

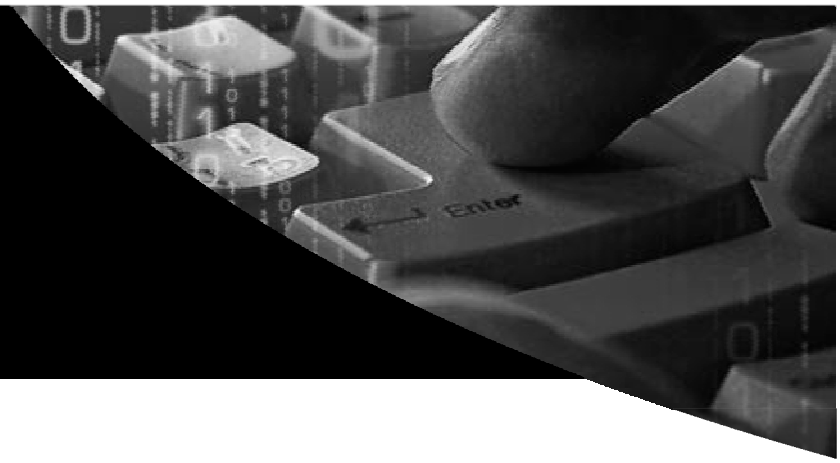
CLEF: Logica

Trantella Enterprise enables business to deploy desktop applications on servers rather than PCs, and delivers secure anywhere access to these applications, from clients equipped with a java enabled browser.

Reflex Magnetics Ltd
31-33 Priory Park Road, London, NW6 7HP, United Kingdom
Point of contact: Andy Campbell
Telephone: +44 (0)20 7372 6666
Fax: +44 (0)20 7372 2507
Email: sale@reflex-magnetics.com
URL: www.reflex-magnetics.com/

SECTION 2

Access Control



Virtual Infrastructure Access Service Version 5.5b

CCTM	Certificate: 2007/06/0024
Awarded: 28th June 2007	Valid until: 27th June 2009

The SDMS service provides for the supply of premium brand, security marked, printed, accountable and auditable computer, audio and video storage media.

The marking, printing and identification of media can be customised to meet specific customer security requirements.

Packing and distribution is performed within a Government accredited secure location.

Records of despatched products are retained for at least 7 years, to assist in any related incident investigation by the customer.

IBM United Kingdom Limited
PO Box 41, North Harbour, Portsmouth, Hampshire, PO6 3AU
United Kingdom
Telephone: +44 (0)207 021 9947
Email: dave_sonerville@uk.ibm.com
URL www-935.ibm.com/services/uk/index.wss/offering/its/a1024853

SECTION 3

Airwave

CESG

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult with vendors on unique functionality and features for each product that is listed.

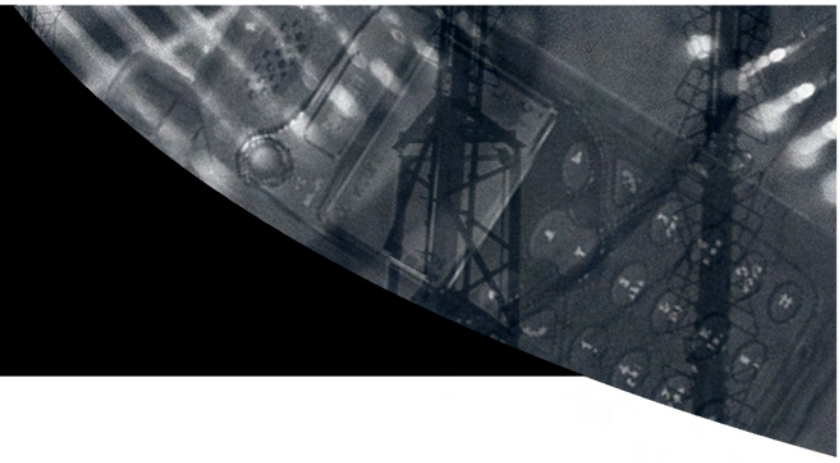
Airwave

The security of Airwave TETRA terminals relies to some extent on the functionality of the Airwave network. For this reason the CAPS Certificates for these products are only valid for use on the Airwave network. The following information identifies vendors which offer a solution for Airwave Users.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0)1242 709141 Fax: +44 (0)1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 3

Airwave



Cleartone CM5000

Cryptographic Grade: Baseline

The Cleartone CM5000 is a mobile TETRA gateway and repeater terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Alogrithm 2 (TEA2) for encryption of the air-interface.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version MR01.212.030

Cleartone Telecomms plc
Pontyfein Industrial Estate, New Inn, Pontypool, NP4 0DQ
United Kingdom
Telephone: +44 (0)1495 752 255
Fax:.....+44 (0)1495 752 323
Email: admin@cleartone.co.uk
URL: www.cleartone.co.uk

Cleartone CM9000P

Cryptographic Grade: Baseline

The Cleartone CM9000P is a mobile TETRA gateway and repeater terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Alogrithm 2 (TEA2) for encryption of the air-interface.

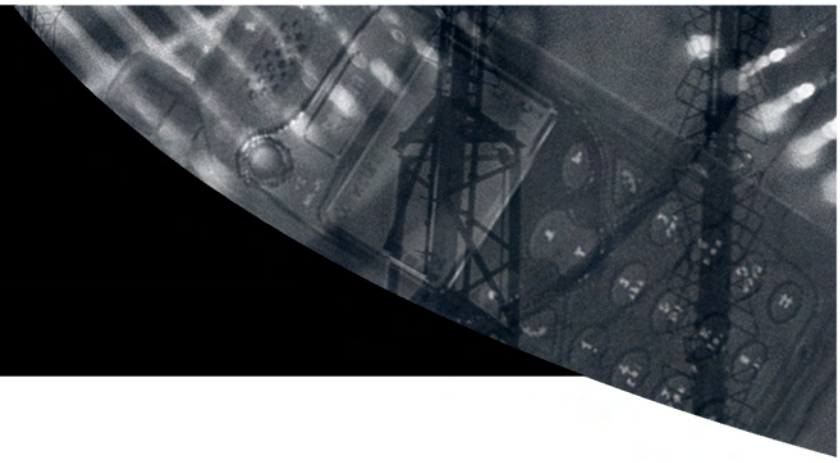
Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version TMP0.80

Cleartone Telecomms plc
Pontyfein Industrial Estate, New Inn, Pontypool, NP4 0DQ
United Kingdom
Telephone: +44 (0)1495 752 255
Fax:.....+44 (0)1495 752 323
Email: admin@cleartone.co.uk
URL: www.cleartone.co.uk

SECTION 3

Airwave



EADS THR880i

Cryptographic Grade: Baseline

The EADS THR880i is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 6.93-5_016

Cassidian
Hiomotie 32, 0038, Helsinki, Finland
Telephone: +385 10 4080 342
Fax: +385 10 4080 931
Email: Oliver.Fischer@Cassidian.com
URL: www.Cassidian.com

EADS TMR880i

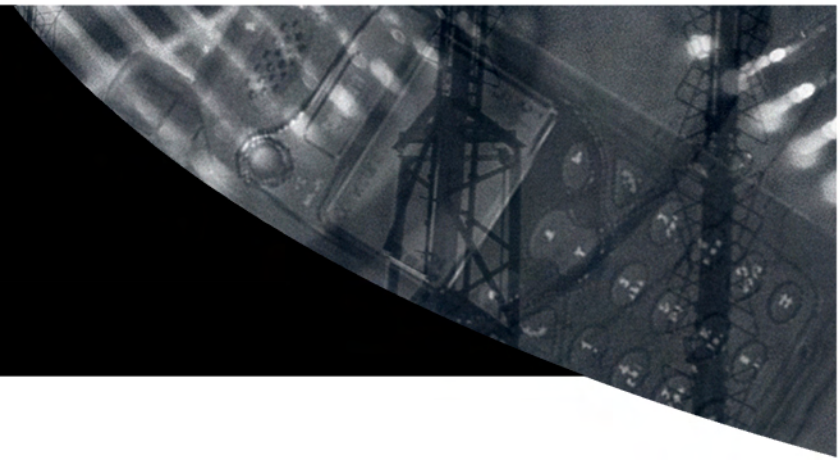
Cryptographic Grade: Baseline

The EADS TMR880i is a mobile TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 6.93-5_016

Cassidian
Hiomotie 32, 0038, Helsinki, Finland
Telephone: +385 10 4080 342
Fax: +385 10 4080 931
Email: Oliver.Fischer@cassidian.com
URL: www.cassidian.com



Motorola MTH800

Cryptographic Grade: See Notes

The Motorola MTH800 is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 5.6.1e, 5.9.1, 5.9.3 & 5.12
TEA2+ UK National – Enhanced Grade Version 5.6.1e, 5.9.1 & 5.9.3

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com

Motorola MTM800

Cryptographic Grade: See Notes

The Motorola MTM800 is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

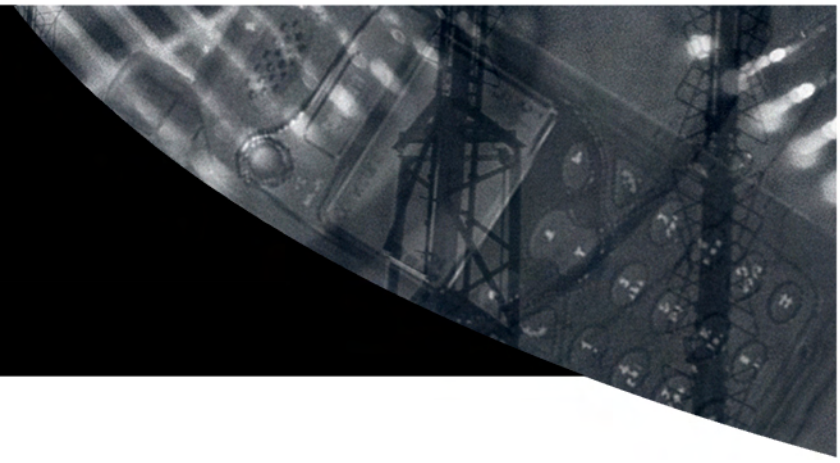
Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 5.6.1e, 5.9.1 & 5.12
TEA2+ UK National – Enhanced Grade Version 5.6.1e & 5.9.1

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com

SECTION 3

Airwave



Motorola MTM800E

Cryptographic Grade: See Notes

The Motorola MTM800E is a mobile TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version MR5.6.1e, MR5.9.1, MR5.9.2 & MR5.12
TEA2+ UK National – Enhanced Grade Version MR5.6.1e, MR 5.9.1 & MR 5.9.2

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com

Motorola MTP850

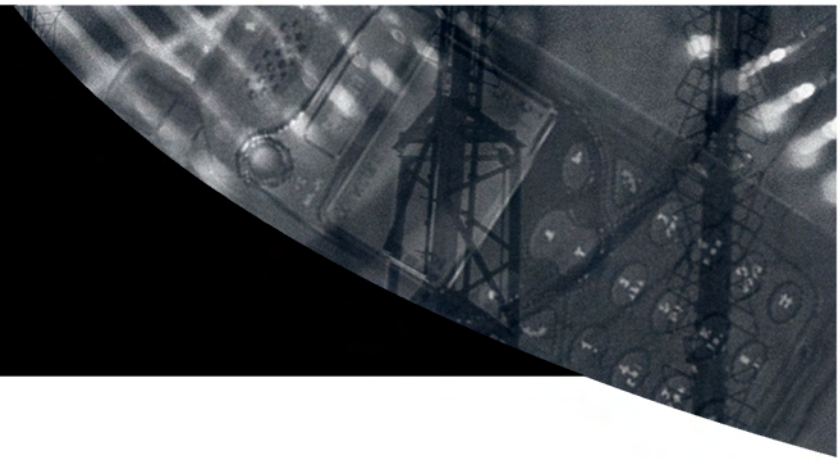
Cryptographic Grade: See Notes

The Motorola MTP850 is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 5.6.1e, 5.9.1, 5.9.3 & 5.12
TEA2+ UK National – Enhanced Grade Version 5.6.1e, 5.9.1 & 5.9.3

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com



Motorola MTP850EX & MTP810EX

Cryptographic Grade: Baseline

The Motorola MTP850EX and MTP810EX are handheld ATEX TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version MR8.6.2 & MR5.12

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com

Motorola TCR1000

Cryptographic Grade: See Notes

The Motorola TCR1000 is a covert TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

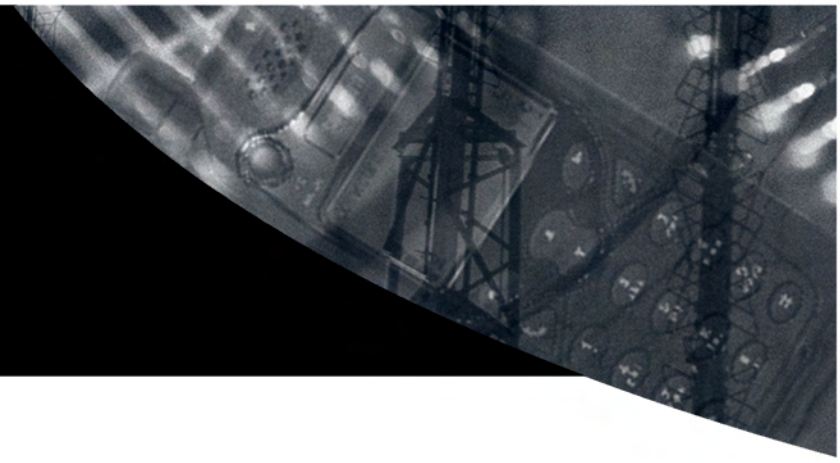
Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.6.1 & 9.12
TEA2+ UK National – Enhanced Grade Version 9.6.1

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com

SECTION 3

Airwave



Motorola TOM100

Cryptographic Grade: Baseline

The Motorola TOM100 is a TETRA modem (for embedment: e.g. into a PDA) that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version MR6.7.1

Motorola plc
Jays Close, Viables, Basingstoke, Hampshire, RG22 4PD
United Kingdom
Telephone: +44 (0)1256 488 126
URL: www.motorola.com

Sepura SRC3300

Cryptographic Grade: See Notes

The Sepura SRG3300 is a covert TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

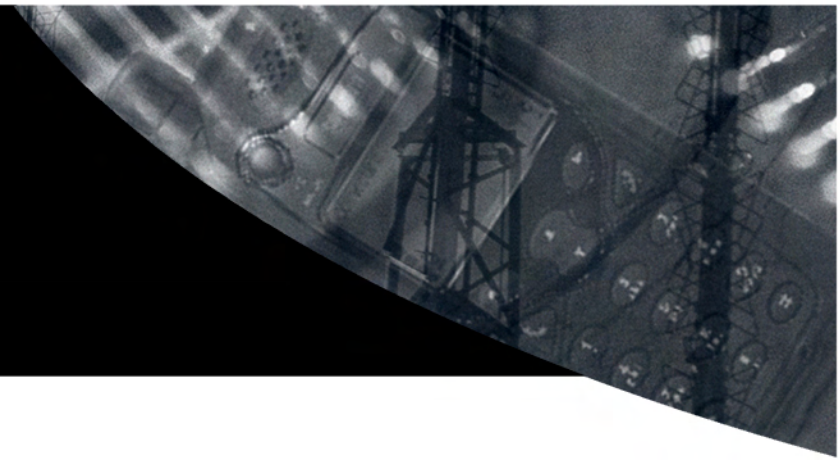
Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015)
TEA2+ UK National – Enhanced Grade Version 9.6. (DEL015)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

SECTION 3

Airwave



Sepura SRG2000

Cryptographic Grade: Baseline

The Sepura SRG2000 is a mobile TETRA gateway and repeater terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 8.8 (DEL009)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

Sepura SRG3500

Cryptographic Grade: See Notes

The Sepura SRG3500 is a mobile TETRA gateway and repeater terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:

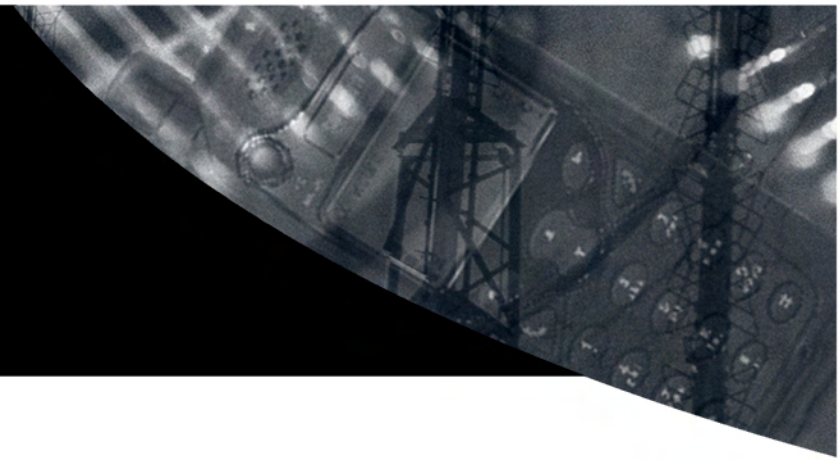
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015) and version 10.0 (DEL009)
TEA2+ UK National – Enhanced Grade Version 9.6. (DEL015) & 9.6 Concession (003)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

SECTION 3

Airwave



Sepura SRG3900

Cryptographic Grade: See Notes

The Sepura SRG3900 is a mobile TETRA gateway and repeater terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015) and 9.5 concession and version 10.0 (DEL009)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

Sepura SRH3500/SRH3800/ SRH3900

Cryptographic Grade: See Notes

The Sepura SRH3500/SRH3800/SRH3900 are handheld TETRA terminals which conform to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

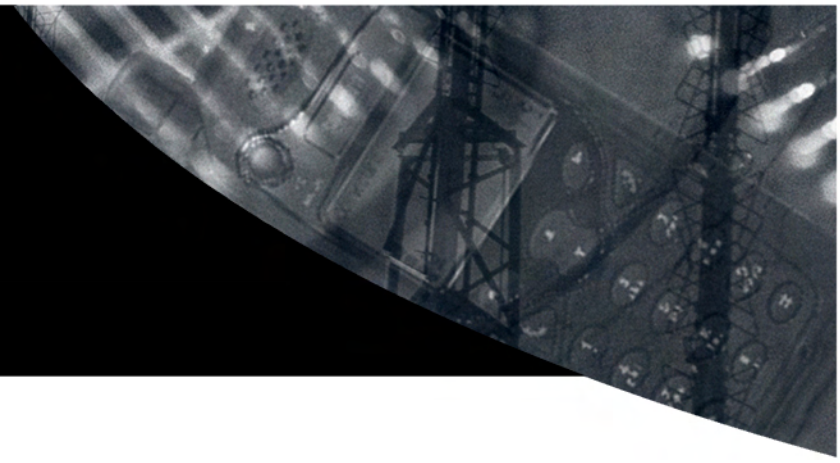
Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015) and version 10.0 (DEL009).
TEA2+ UK National – Enhanced Grade Version 9.6. (DEL015)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

SECTION 3

Airwave



Sepura SRM2000

Cryptographic Grade: Baseline

The Sepura SRM2000 is a mobile TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 8.8 (DEL009).

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

Sepura SRM3500

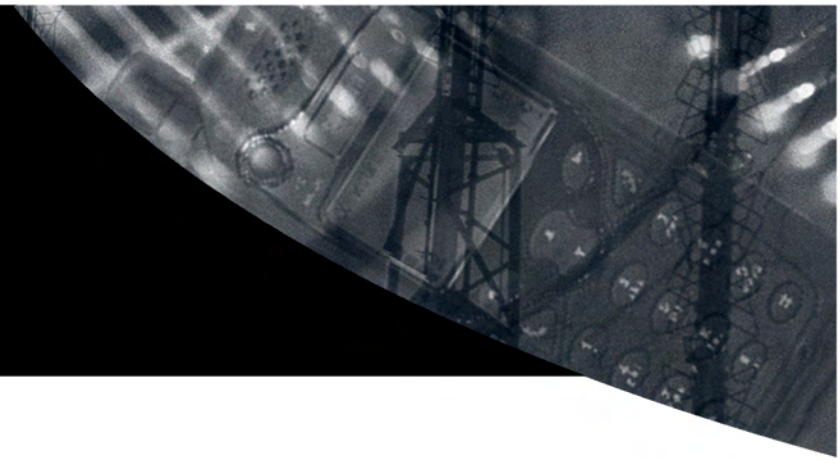
Cryptographic Grade: See Notes

The Sepura SRM3500 is a mobile TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015) and version 10.0 (DEL009)
TEA2+ UK National – Enhanced Grade Version 9.6. (DEL015) & 9.6 Concession (003)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com



Sepura SRP2000

Cryptographic Grade: Baseline

The Sepura SRP2000 is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 8.8(DEL009)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

Sepura STP8000/STP8100

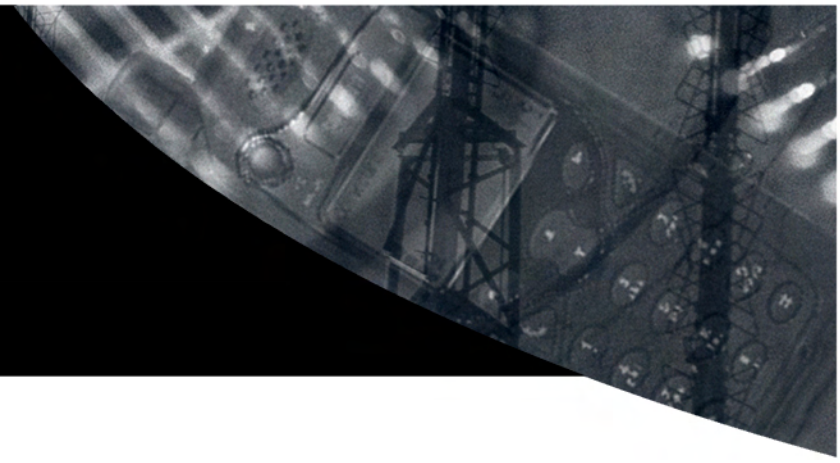
Cryptographic Grade: See Notes

The Sepura STP8000/STP8100 is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface and can additionally use the UK National Algorithm for End-to-End encryption.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015)
TEA2+ UK National – Enhanced Grade Version 9.6. (DEL015)

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com



Sepura STP8200

Cryptographic Grade: See Notes

The Sepura STP8200 is a handheld TETRA terminal that conforms to the ETSI standards and can operate in either Trunked Mode of Operation (TMO) or Direct Mode of Operation (DMO). It utilises the TETRA Encryption Algorithm 2 (TEA2) for encryption of the air-interface
.

Notes:
Prospective purchasers of CAPS approved products are reminded that these product descriptions are a guide only, and that they should consult with vendors for information on unique functionality and features of each product that is listed.

Version: TEA2 only – Baseline version 9.5 (DEL015) and version 10.0 (DEL009).

Sepura plc
Radio House, St. Andrews Road, Cambridge, CB4 1GR
United Kingdom
Telephone: +44 (0)1223 876 000
Fax: +44 (0)1223 879 000
Email: customer.support@sepura.com
URL: www.sepura.com

SECTION 4

Communications

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor or CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

ITSEC/CC
Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from CESG website.

CCTM
CESG Claims Tested Mark

Prospective purchasers of CCT Mark approved products or services should read both the ICD and Test Report documents available from the CCT Mark website, to ensure the product or service is appropriate for their needs.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0)1242 709141 Fax: +44 (0)1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 4

Communications

ALBERCOR
Government use only

Cryptographic Grade: High Grade Top Secret

ALBERCOR is a high-grade cryptographic unit designed to protect traffic to Top Secret Codeword. It can operate in two modes.
Messaging mode: ALBERCOR connects to the messaging system by an asynchronous interface to encrypt addressed messages. It allows the address part through and encrypts the message part, creating an unclassified encrypted message. The transmission system includes a variable delay before the message reaches the destination ALBERCOR for decryption.
Link encryption mode: ALBERCOR has a full duplex connection to another ALBERCOR unit. The interface is essentially a real-time link. The connection can be synchronous or asynchronous, and the equipment can be externally configured to operate over a simplex link.

- Automatic selection of keys for decrypting messages
- Users selectable Traffic Flow Secure, Cypher Text Auto Key and Key Auto Key modes
- Optional plain language (PL) bypass for ACP127 header formats
- Optional message start/end detection
- Separate PL and CY connectors
- Both interfaces are independently V.10/V.11 programmable
- RS232
- Separate RED and BLACK control

ALBERCOR Brochure
Network Encryption
Broadcast Encryption

Ultra Electronics Communication & Integrated Systems
Point of contact: Richard Wall
Telephone: +44 (0)208 813 4545
URL www.ultra-cis.com

AEP Net CA Version 1.0

Cryptographic Grade: Enhanced

The AEP net CA hardware Host Security Module provides the key Storage Management and Certification Authority services for AEP Net family of products. The product processes PKC#10 certificate request and issues X.509V3 certificates using CESG generated signing keys. Certificates are written to an industry standard LDAP. AEP Net CA can also revoke certificates and sign publish an industry standard Certificate Revocation List (CRL) to LDAP. Editing tools are provided for the population and management of generic certificate extension fields

Notes: The AEP Net CA is installed as part of the management system for AEP etc EC/ED/EE20M, EC/ED/EE100M and ED/EE remote encryptor.

AEP Networks
Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts HP2 7BW United Kingdom
Telephone: +44 (0) 7771 924 291
Alt Phone: +44 (0) 1442 458 600
Fax: +44 (0) 1442 458 601
Email: james.tolfree@AEPnetworks.com
URL: www.aepnetworks.com

SECTION 4

Communications

ANWELL
Government use only

Cryptographic Grade: High Grade Top Secret

ANWELL is a self-contained, general-purpose cryptographic equipment for both military and civilian use. It provides protection for traffic on Megastream circuits at data rates of 2.048Mbps and 8.448Mbps

- RED and BLACK G.703/HDB3 interfaces
- 2.048Mbps and 8.448Mbps automatic selection of data rates
- N-type co-axial connectors
- DRUMBEAT or OPUS variants
- Usable in both KAK and CTAK modes
- DRUMBEAT and OPUS versions are interoperable with DRUMBEAT and OPUS versions of EUGENIC when used with a suitable G.703/V.11 converter
- Optional PC-based facility, enabling networking of up to 999 RIU nodes. Each RIU node can support a maximum of 6 ANWELL units.
- Full network control, status monitoring and fault detection
- Ability to perform remote update, change and erase of CV across the entire ANWELL network

Paper tape and UK fill gun socket for loading key variable.

ANWELL Brochure
Link Encryption

Defence Procurement Agency
CASS11, MoD Abbey Wood, Spruce 2a, 1203, Bristol, BS34 8JH, United Kingdom
Telephone: +44 (0) 117 913 3164
Fax: +44 (0) 117 913 3922
Email: cass11@dpa.mod.uk

BEDERAL
Government use only

Cryptographic Grade: High Grade Top Secret

BEDERAL has been designed for UK MoD customers requiring a worldwide message preparation and delivery system for standard military ACP 127 messages to Top Secret Codeword. BEDERAL uses commercial equipment and software for message preparation and delivery systems, and CESG's ALBERCOR for message encryption and decryption. It also uses CESG's NTSE and as an option can be fitted with KILGETTY software for additional workstation security. The ALBERCOR is set up in an asynchronous ACP 127 messaging mode when used within BEDERAL. The ALBERCOR can also be used within other ACP 127 messaging systems by configuring the asynchronous interface and the ACP 127 mode options to suit.

BEDERAL software fit:

- Microsoft NT4 service pack 3 with YK2 additions
- SBL KILGETTY Plus for NT
- SBL NTSE (Security Enhancements)
- Compact CMS Server and CMS Client

BEDRAL hardware:

- Standard laptop/desktop PC where TEMPEST is not an issue, or any PC to the appropriate TEMPEST standard where TEMPEST is an issue.

BEDERAL Brochure
Network Encryption

Ultra Electronics Communication & Integrated Systems
Point of contact: Richard Wall
Telephone: +44 (0) 208 813 4545
URL www.ultra-cis.com

SECTION 4

Communications

BRENT Secure Telephone
Government use only

Cryptographic Grade: High Grade Top Secret

BRENT is a wide-band, fully secure telephone. It is designed to meet UK Government's need for a inter-departmental secure speech system well into the 21sy century. There are three versions of BRENT, these are: BRENT1, ISDN BRENT, X.21 BRENT.

ISDN BRENT is designed to meet the basic rate access standard (CCITT/I.420) and is ISDN2 compliant. It features an X.21 compatible data-port which supports data transfer at 64kb/s. The port offers data transfer between personal computers, group 3 fax and video conferencing units. Twin secure data port configuration may be selected as required by using the X.21 voice/data port. The BRENT ISDN has been developed to be fully compatible with all other BRENT models (x.21 and BRENT2) and also other products such as the BRUNHILDE gateway. All BRENT telephones automatically set up calls in secure mode. If the corresponding equipment is not a BRENT or does not have its STK inserted, the call will be connected as a non-secure call. BRENT2 is the latest BRENT ISDN upgrade; this contains the inclusion of a red S-Bus for dial-through capability and DTMF. Further details can be found in the BRENT2 brochure. The X.21 Version connects to a digital network via the X.21 port on an existing ISDN telephone. This can allow greater flexibility for use of BRENT in the USA, etc. The BRENT X.21 can only operate in secure mode. All three versions operate using Public Key Cryptography (PKC) and are BABT approved. The BRENT secure telephone currently operates over ISDN telephone technology. However, ISDN is not always readily or cheaply available in some small, remote or mobile locations. BRENT over IP uses an internet protocol adaptor that allows the BRENTS to use a different IP-based bearer technol0gy. Using this IP bearer technology a small number of BRENTS can be linked together, or a remote set of BRENTS can be linked with an existing ISDN infrastructure. For an acceptable level of call quality and availability, the IP bearer infrastructure used for BRENT over IP has to have a good quality of service with respect to bandwidth, packet loss and availability. This can usually be assured through a commercial service level agreement with a service provider or by ownership of the IP network. The IA Technical Programme has sponsored trails of the BRENT over IP technology over IP networks in the UK and Internationally. The vendor also offers a solution for running THAMER over an IP bearer infrastructure.

SELEX Communications Ltd
Liverpool Innovation Park, Baird House, Edge Lane, Fairfield, Liverpool, L7 9NJ, United Kingdom
Point of contact Phil Jones
Telephone: +44 (0) 1512 825 324
Fax: +44 (0) 1512 541 194
Email: phil.jones@selex-comms.com
URL: www.selex-comms.co.uk

CASM CryptServe Version 1.02
Government use only

ITSEC E3.... Certificate: CR9884 March 1989
CLEF: Logica

.

CASM is CESG's Architecture for Secure Messaging project, which provides advice and products to Government Departments and Industry, enabling them to secure their email systems. The CASM CryptServe is one of s a family of products that together provide all the services necessary to protect email over UNCLASSIFIED (unprotected) networks

The CASM CryptServe software package is the product that sits at the heart of CASM and provides all secure cryptographic services required by higher-level applications (as such its use is not limited solely to email products).

CASM CryptServe Version 1.02 has been evaluated to ITSEC E3. The product has been designed for machines with a minimum configuration of an Intel 80386/DX processor with 4MB of RAM.

CESG
A2j, Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, United Kingdom
Point of contact: CESG Customer Support Office
Telephone: +44 (0) 1242 709 1415
Fax: +44 (0) 1242 709 193
Email: enquiries@cesg.gsi.gov.uk
URL www.cesg.gov.uk

SECTION 4

Communications

CATAPAN ATM
Government use only

Cryptographic Grade: High Grade Top Secret

ATM CATAPAN is a high-grade crypto capable of protecting material up to TOP SERCET Codeword which has been designed for use on either a public or private ATM network.

The ATM crypto project began in December 1993 when ATM was emerging as one of the leading WAN protocols being offered by Telecommunications providers.

CATAPAN is a CESG design, but a development contract was let with TRL in August 1996.

DAC (Design Accreditation Certification) was achieved in 2003 and CATAPAN is now in production.

CATAPAN is a Network Crypto-NOT A LINK CRYPTO (although it can be used as a link crypto if only two devices are involved). The network aspect brings many advantages, the main being that you do not need a pair of cryptos on every leased line as is the traditional way of providing secure network services. Instead just a single device at every site, radically reducing the number of cryptos required.

Catapan Brochure

L-3 TRL Technology
Unit 19, Miller Court, Severn Drive, Tewkesbury, Gloucestershire, GL20 8GC, United Kingdom
Point of contact: Malcolm Brown
Telephone: +44 (0) 1684 852 563 or +44 (0) 1684 278 700
Fax: +44 (0) 1684 850 406 or +44 (0) 1684 850 406
Email: Malcolm.Brown@L-3Com.com
URL: www.L-3com.com/TRL

CATAPAN IP

Cryptographic Grade: High Grade Top Secret

IP-CATAPAN is a version of the already successful ATM CATAPAN, which is in widespread use throughout MoD and OGSs. It builds on the proven and reliable CATAPAN chassis, with modifications to the software and firmware, plus specialist IP (Ethernet 10/100Mb/s) Line Interface Modules. No PCB or chassis change enables factory reconfigurability of a device from ATM to IP (or IP to ATM).

Key Features:

- Protection of TS CODEWORD information
- 10/100Mb/s Ethernet with 100BaseF Interface
- 200 concurrent sessions
- IPSec Secure Tunnel Mode using Public Key Cryptography
- Remote Management via SNMPv2
- GKM key material-ECIK/KEK/VECTOR (as ATM-CATAPAN)
- Remote Vector Distribution allowing only yearly manual re-keying
- Local management via LCD/Keypad or via VT100 terminal

A software upgrade has now been approved by CESG enabling DSCP traffic classifications to be preserved across IP CATAPAN allowing customers to support QoS across their secure networks.

Notes:
IP-CATAPAN is a full High Grade (TOPSERCET Codeword) IPv4 network encryptor, designed for installation into any IPv4 network. Contact L-3 TRL Technology for information about additional capability for: IPv6, 1Gb/s and reconfigurable platforms version1.1

L-3 TRL Technology
Unit 19, Miller Court, Severn Drive, Tewkesbury, Gloucestershire, GL20 8GC, United Kingdom
Point of contact: Malcolm Brown
Telephone: +44 (0) 1684 852 563 or +44 (0) 1684 278 700
Fax: +44 (0) 1684 850 406 or +44 (0) 1684 850 406
Email: Malcolm.Brown@L-3Com.com
URL: www.L-3com.com/TRL

Crypto Manager

Cryptographic Grade: Baseline

The Thales Crypto Manager is for use with the Datacryptor Advanced Performance and Datacryptor 2000 network encryptors. Crypto Manager encrypts management traffic between the host management PC and one or more Datacryptor devices. The use of programmable cryptography enables Crypto Manager to support a number of different CESG-approved algorithms and thus provide solutions suitable to protect information classified from RESTRICTED up to SECRET (see Notes). Crypto Manager incorporates advanced anti-tamper technology to avoid the need for it to be protectively marked.

Notes:
Also available in an Enhanced Grade version Protecting information classified as SECRET is based on the conditions described in IS4.

Version 4.01 (HMG) is the latest approved version.

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks HP18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-eseciurity.com
URL: www.thales-esecurity.com/TRL

Crypto Manager

Cryptographic Grade: Enhanced

The Thales Crypto Manager is for use with the Datacryptor Advanced Performance and Datacryptor 2000 network encryptors. Crypto Manager encrypts management traffic between the host management PC and one or more Datacryptor devices. The use of programmable cryptography enables Crypto Manager to support a number of different CESG-approved algorithms and thus provide solutions suitable to protect information classified from RESTRICTED up to SECRET (see Notes). Crypto Manager incorporates advanced anti-tamper technology to avoid the need for it to be protectively marked.

Notes:
Also available in a Baseline Grade version Protecting information classified as SECRET is based on the conditions described in IS4.

Version 4.01 (HMG) is the latest approved version.

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks HP18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-eseciurity.com
URL: www.thales-esecurity.com/TRL

SECTION 4

Communications

CERBERUS Guard Processor LSS Variant Version 1.0
Government use

ITSEC E4.... Certificate: April 1998

CLEF: EDS

The Cerberus Guard Processor is a device to check the messages passed between two processors or networks which communicate using a trusted labelling scheme and while are potentially operating at different security levels or with security restrictions placed upon their interconnection.

The Cerberus Guard Processor checks that the actual security label of a message is contained within a configurable set of permitted labels for a source/destination address pair. Furthermore, if a connection oriented protocol is used, the Cerberus Guard Processor can be configured to permit the initiation of a link by one of the sources/destination address pair only if a message fails any of the checks performed by the Cerberus Guard Processor, a potential security breach is prevented from occurring by the Cerberus Guard Processor stopping any onward transmission of the messages and requiring operator intervention (possibly to include investigation into the cause of the failure).

This product was developed specifically for the MoD's logistic Support system.

EDS Ltd

EDS UK Information Security, Bartley Wood Business Park, 1-3 Bartley Way, Hook Hampshire, RG27 9XA, United Kingdom

Point of contact: Tony Gallagher

Telephone: +44 (0) 1256 742 357

Fax: +44 (0) 1256 742 060

Email: slef@eds.com

URL www.eds.com

Cisco Router Models 1003, 1601, 2501, 3620, 4500M, 4700M, & 7206

ITSEC E2 Certificate CRP 145 March 2001

CLEF: logica

This range of Cisco Routers, running IOS 11.2.16(P), are multifunctional platforms combining dial access, routing, LAN-to-LAN services and multiservice integration of voice and data in the same device. As a modular solution, the Cisco routers have the flexibility to meet both current and future connectivity requirements. The Cisco routers are fully supported by Cisco IOSTM software, which includes LAN-to-LAN routing, data and access security and WAN optimisation. Applications supported are asynchronous and synchronous serial interfaces. This product was evaluated for the MoD's Defence Fixed Telecommunications Service.

Cisco Systems

10 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom

Point of contact: Paul King

Telephone: +44 (0) 20 8824 8349

Fax: +44 (0) 20 8824 8001

Email: pking@cisco.com

URL: www.cisco.com/gobal/UK/solutions/ent/avvid_solutions/security_sol_home.shtml

Cisco Router Models 1003, 1601,1603R, 2501, 3620, 3640, 4500M, & 7206

ITSEC E2 Certificate CRP 157 June 2001

CLEF: logica

This range of Cisco Routers, running IOS 11.2.16(P), are multifunction platforms combining dial access, routing, LAN-to-LAN services and multiservice integration of voice and data in the same device. As a modular solution, the Cisco routers have the flexibility to meet both current and future connectivity requirements. The Cisco routers are fully supported by Cisco IOSTM software, which includes LAN-to-LAN routing, data and access security and WAN optimisation. Applications supported are asynchronous and synchronous serial interfaces. This product was evaluated for the MoD's Defence Fixed Telecommunications Service.

Cisco Systems
10 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom
Point of contact: Paul King
Telephone: +44 (0) 20 8824 8349
Fax: +44 (0) 20 8824 8001
Email: pking@cisco.com
URL: www.cisco.com/gobal/UK/solutions/ent/avvid_solutions/security_sol_home.shtml

Datacryptor 2000 (Synchronous Line Encryptor)

ITSEC E3 Certificate CRP 126 August 1999

CLEF: logica

The Datacryptor 2000 Link product range are encryption devices specifically designed to provide secure communications over circuits at speed of up to 2Mb/s using a variety of line interfaces. The Datacryptor 2000 prevents unauthorised information access and protects against eavesdropping for data transmissions using both private and public networks. The unit provides both tamper evidence and tamper resistance and, once commissioned, will operate automatically without further intervention. The Datacryptor 200 series employ the Thales-e-Security Key Management Scheme to security generates and distribute data encryption keys. This dispenses with the previously time-consuming and laborious tasks associated with secure key management, which significantly reduces the cost of ownership.

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon, Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com/

Communications

Datacryptor 2000

Cryptographic Grade: See Notes

The Thales Datacryptor 2000 range of network encryptors protect classified information in private and public networks. The following models are available:

- Link (leased lines up to 8Mb/s)
- Frame Relay (up to 8Mb/s)

(For higher-speed applications, please see Datacryptor Advanced Performance.) The Frame Relay model is approved for reverse tunnelling. The use of programmable cryptographic enables Datacryptor 2000 to support a number of different CESG-approved algorithms and thus provide solutions to protect information classified from RESTRICTED up to SECRET (see Notes). Datacryptor 2000 incorporates advanced anti-tamper technology to avoid the need for it to be protectively marked.

Notes:
The Datacryptor 2000 is approved at Baseline and Enhanced (Protecting information classified as SECRET is based on the conditions described in IS4)

Version v3.7 (HMG)

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com/

Datacryptor 2000 Application Software Version 3.3

COMMON CRITERIA EAL5 Certificate CRP 208A September 2004
CLEF: logica

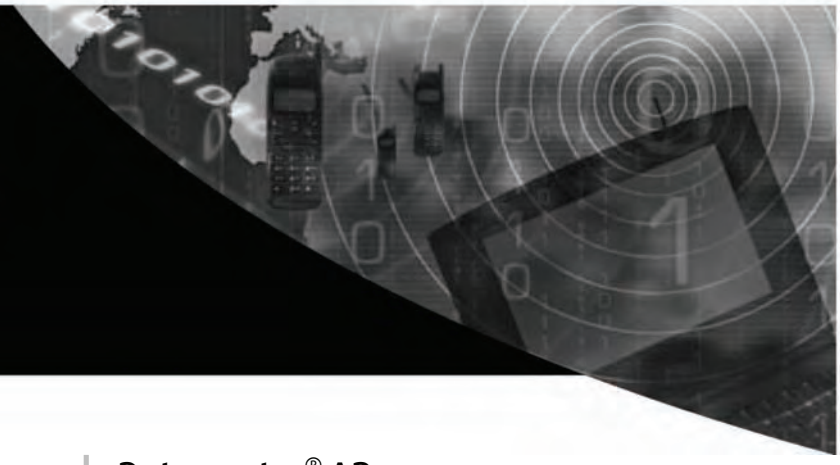
Thales e-Security's Datacryptor 200 is a network encryption product that supports multiple network protocols. It uses Public Key Cryptography techniques to minimise the administrative overhead of key management, and implements sophisticated tamper resistant measures to protect against physical attack in order to safeguard key material and algorithms. The unit also provides integrated secure unit management capability employing the same techniques used for traffic encryption.

Common Criteria Evaluations are confined to the aspects of core functionally that are specified in the Security Target and outlined in the Certification Report. The Security Target for this product is available form Thales e-Security.

This EAL5 certification was achieved concurrently with one at the EAL4 evaluation assurance level.

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 204 161
Mobile: +44 (0) 767123351
Fax: +44 (0) 1844 202 170
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com/

Communications



Datacryptor 2000 Application Software Version 3.3

COMMON CRITERIA EAL4 Certificate CRP 208 September 2004

CLEF: logica

Thales e-Security's Datacryptor 200 is a network encryption product that supports multiple network protocols. It uses Public Key Cryptography techniques to minimise the administrative overhead of key management, and implements sophisticated tamper resistant measures to protect against physical attack in order to safeguard key material and algorithms. The unit also provides integrated secure unit management capability employing the same techniques used for traffic encryption.

Common Criteria Evaluations are confined to the aspects of core functionally that are specified in the Security Target and outlined in the Certification Report. The Security Target for this product is available form Thales e-Security.

This EAL4 certification was achieved concurrently with one at the EAL5 evaluation assurance level.

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 204 161
Mobile: +44 (0) 767123351
Fax: +44 (0) 1844 202 170
Email: ian.danterbs@thales-escurity.com
URL: www.thales-esecurity.com/

Datacryptor® AP

Cryptographic Grade: Baseline

Thales Datacryptor® AP (Advanced Performance) protects classified information in high-speed private and public networks. It is available in a variety of models for IP, Link and Frame Relay networks, and in both rack-mounting and portable form factors. (For full details of the different models, please visit the Thales ISS website.)

IP models operate up to 100Mbps and incorporate a number of advanced features such as Galois/Counter Mode (GCM) for low overhead integrity and anti-replay protection, quality-of-service (QoS) information pass through to support network traffic prioritisation, and hot standby operation for high-availability applications. All models provide a combination of high throughput and low latency.

The use of programmable cryptography enables Datacryptor AP to support a number of CESG-approved algorithms for safeguarding information protectively-marked from RESTRICTED up to SECRET (including reverse tunnelling applications for IP and Frame Relay models). Advanced anti-tamper technology avoids the need for the Datacryptor to be Protectively Marked in certain situations.

Notes:
The Datacryptor AP is approved at Baseline and Enhanced Grade (Protecting information classified as SECRET is based on the conditions described in IS4)

Version 4.01 (HMG)

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 204 161
Mobile: +44 (0) 767123351
Fax: +44 (0) 1844 202 170
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com/

Datacryptor® AP

Cryptographic Grade: Enhanced

Thales Datacryptor® AP (Advanced Performance) protects classified information in high-speed private and public networks. It is available in a variety of models for IP, Link and Frame Relay networks, and in both rack-mounting and portable form factors. (For full details of the different models, please visit the Thales ISS website.)

IP models operate up to 100Mbps and incorporate a number of advanced features such as Galois/Counter Mode (GCM) for low overhead integrity and anti-replay protection, quality-of-service (QoS) information pass through to support network traffic prioritisation, and hot standby operation for high-availability applications. All models provide a combination of high throughput and low latency.

The use of programmable cryptography enables Datacryptor AP to support a number of CESG-approved algorithms for safeguarding information protectively-marked from RESTRICTED up to SECRET (including reverse tunnelling applications for IP and Frame Relay models). Advanced anti-tamper technology avoids the need for the Datacryptor to be Protectively Marked in certain situations.

Notes:
The Datacryptor AP is approved at Baseline and Enhanced Grade (Protecting information classified as SECRET is based on the conditions described in IS4)

Version 4.01 (HMG).

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com

DCV1000

Cryptographic Grade: In evaluation

The DCV1000 is the first model in the Datacryptor Vox (DCVox) family of secure telephony solutions that features soft programability and advanced anti tamper protection, The DCV1000 is a High Grade desktop telephone that supports both PSTN and VoIP (Voice over IP) infrastructures. The first release includes a SCIP (Secure Communications Interoperability Protocol) profile for secure voice and data transfer up to TOP SECRET. Additional soft-loadable profiles will be made available in the future, including a SCIP profile for UK Eyes traffic. The DCV100 is designed to hold a minimum of two profiles concurrently.

TBC on Completion of Evaluation

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com

SECTION 4

Communications

Ectocryp Black

Cryptographic Grade: High Grade Top Secret IN EVALUATION

Ectocryp Black is a secure voice gateway implementing the Secure Communications Interoperability Protocol (based on FNBDT). It enables the connection of SCIP (FNBDT) compliant devices to existing secure speech networks, providing up to 120 channels of secure voice over a standard PSNI network.

Notes:
Fully interoperable with US FNBDT and future NATO SCIP equipment ith the advantage of being infield re-programmable.

Version 1.1.

EDS Defence & Security Systems Limited
EADS, Quadrant House, Celtic Springs, Coedkernew Newport, South Wales, NP10 8FZ, United Kingdom
Point of contact: Steve Allum
Telephone: +44 (0) 1633 715 990
Fax: +44 (0) 1633 715 200
Email: steve.allum@eads.com
URL: www.eads.com

Ectocryp Blue

Cryptographic Grade: High Grade Top Secret

Ectocryp Blueis a high assurance internet protocol encryptor (HAIPE) IS Version 3 compliant network encryptor, providing information assurance services for Ipv4 and Ipv6 networks. Providing 1gbps throughput. It enables assured connection of private networks across cheaper public networks, including the Internet.

Notes:
Fully interoperable with all tested HAIPE compliant-equipment (Version 1.3.5 and later), advantage of being infield re-programmable.

Version Release1, 1.1 and 1.2.

EDS Defence & Security Systems Limited
EADS, Quadrant House, Celtic Springs, Coedkernew Newport, South Wales, NP10 8FZ, United Kingdom
Point of contact: Steve Allum
Telephone: +44 (0) 1633 715 990
Fax: +44 (0) 1633 715 200
Email: steve.allum@eads.com
URL: www.eads.com

SECTION 4

Communications

EC100M

Cryptographic Grade: Baseline

The AEP Net EC100M protects IP traffic across networks and provides 2x100Mb/s network interfaces designed to achieve close to 100Mb/s full duplex (200Mb/s throughput). The encryptor provides both data confidentially and source authentication for network traffic enabling Virtual Private Network (VPN) communications. The use of IETF standard transport protocol allows the encrypted traffic to be routed across non-IP networks e.g. ATM, xDSL, MPLS Frame Relay, ISDN, Satcom and Radio links.

The encryption system employs a central management station for key management and distribution and encryptor and network configuration enabling fit and forget operation for the encryptors themselves. Approved for Data Separation, Reverse Tunnelling and Closed User Groups.

Notes.
The EC100M provides identical functionally to/interoperation with the AEP Net EC20M. (Note, these use the same key material).

Version: v1.3, v1.4, v1r4.2

AEP
Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts., HP2 7BW, United Kingdom
Point of contact: James Tolfree
Telephone: +44 (0) 7736 643 853 0r +44 (0) 1442 458 600
Fax: +44 (0) 1442 458 601
Email: james.tolfree@AEPnetworks.com
URL: www.aepnetworks.com/

EC20M

Cryptographic Grade: Baseline

The AEP Net EC20M protects IP traffic across networks. The encryptor provides both data confidentiality and source authentication for network traffic enabling Virtual Private Network (VPN) communications. The products can be deployed as an IP Security Gateway at the network interface or at the workstation to support end-to end or data separation requirements. The use of an IETF standard transport protocol allows the encrypted traffic to be routed across non-IP networks e.g. ATM, xDSL. MPLS, Frame Relay, ISDN, Satcom, and Radio Links

The encryption system employs a central management station for key management and distribution and encryptor and network configuration enabling fit and forget operation for encryptors themselves. Version 5 and later approved for Data Separation, Reverse Tunnelling and Closed User Groups.

Notes.
The EC20M provides identical functionally to/interoperation with the AEP Net EC100M. (Note, these use the same key material).

Version v4.1, v4.2, v4.3, v5.3, v5.4, v1r4.2

AEP
Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts, HP2 7BW, United Kingdom
Point of contact: James Tolfree
Telephone: +44 (0) 7736 643 853 0r +44 (0) 1442 458 600
Fax: +44 (0) 1442 458 601
Email: James.tolfree@AEPnetworks.com
URL: www.aepnetworks.com/

ED100M

Cryptographic Grade: Enhanced

The AEP Net ED100M protects IP traffic across networks and provides 2x100Mb/s network interfaces designed to achieve close to 100Mb/s full duplex (200Mb/s throughput). The encryptor provides both data confidentially and source authentication for network traffic enabling Virtual Private Network (VPN) communications. The use of IETF standard transport protocol allows the encrypted traffic to be routed across non-IP networks e.g. ATM, xDSL, MPLS Frame Relay, ISDN, Satcom and Radio links. The encryption system employs a central management station for key management and distribution and encryptor and network configuration enabling fit and forget operation for the encryptors themselves. Approved for Data Separation, Reverse Tunnelling and Closed User Groups.

Notes.
The ED100M provides identical functionally to/interoperation with the AEP Net ED20M and AEP Net ED Remote encryptors. (Note, these use the same key material).

Version: v1.3, v1.4, v6.1, v6r3, v6r5

AEP
Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts, HP2 7BW, United Kingdom
Point of contact: James Tolfree
Telephone: +44 (0) 7736 643 853 0r +44 (0) 1442 458 600
Fax: +44 (0) 1442 458 601
Email: James.tolfree@AEPnetworks.com
URL: www.aepnetworks.com/

ED20M

Cryptographic Grade: Enhanced

The AEP Net ED20M protects IP traffic across networks. The encryptor provides both data confidentiality and source authentication for network traffic enabling Virtual Private Network (VPN) communications. The products can be deployed as an IP Security Gateway at the network interface or at the workstation to support end-to end or data separation requirements. The use of an IETF standard transport protocol allows the encrypted traffic to be routed across non-IP networks e.g. ATM, xDSL. MPLS, Frame Relay, ISDN, Satcom, and Radio Links. The encryption system employs a central management station for key management and distribution and encryptor and network configuration enabling fit and forget operation for encryptors themselves. Version 5 and later approved for Data Separation, Reverse Tunnelling and Closed User Groups.

Notes.
The ED20M provides identical functionally to/interoperation with the AEP Net ED100M and AEP Net ED Remote encryptors. (Note, these use the same key material).

Version v4.1, v4.2, v4.3, v5.3, v5.4, v6.1, v6r3, v6r5

AEP
Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts., HP2 7BW, United Kingdom
Point of contact: James Tolfree
Telephone: +44 (0) 7736 643 853 0r +44 (0) 1442 458 600
Fax: +44 (0) 1442 458 601
Email: James.tolfree@AEPnetworks.com
URL: www.aepnetworks.com/

SECTION 4

Communications

ED Remote

Cryptographic Grade: Enhanced

The AEP Net ED Remote provides IP layer communications security for remote access users. The system employers a central management station for key management and distribution and encryptor and network configuration, enabling fit and forget operation for the remote units. The system also offers assured compromise control for lost or stolen units. AEP Net ED Remote encryptors can be deployed in a stand-alone system or can be integrated into AEP Net protected networks.

Notes:
The Net ED Remote interoperates with AEP Net ED100M and AEP Net ED20M encryptors (Note, these use the same key material).

Version: v1.1, v1r3, v1r4

AEP Networks
Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts, HP2 7BW, United Kingdom
Point of contact: James Tolfree
Telephone: +44 (0) 7736 643 853 0r +44 (0) 1442 458 600
Fax: +44 (0) 1442 458 601
Email: James.tolfree@AEPnetworks.com
URL: www.aepnetworks.com/

Enterprise CATAPAN

Cryptographic Grade: High Grade Top Secret IN EVALUATION

Enterprise-CATAPAN (BID/2470/1) is the next generation 1/10Gbps High Grade IP network encryption device. A member of the highly successful CATAPAN family of products.
Key features include:

- Sovereign High Grade SECRET & TOP SECRET reprogrammable platform
- 1 Gbps and 10Gbps interfaces
- NPM ACCESEC when not operational
- HAIPE-IS v3.1 with UK Traffic Protection Suite
- Fully interoperable with Mini-CATAPAN
- In-field reprogrammable
- Easy to configure.

Notes: Up to 100Gbps duplex throughout. Key management system compliant with the latest CESG Key management specifications and procedures.

L-3 TRL Technology
Unit 19, Miller court, Severn Drive, Tewkesbury, Gloucestershire, GL20 8CD, United Kingdom
Point of contact: Malcom Brown
Email: Malcolm.Brown@L-3Com.com
Telephone: +44 (0) 1684 852 889
Alt Phone: +44 (0) 1684 278 700
Fax: +44 (0) 1684 850 406
Alt Fax: +44 (0) 1684 852 599
URL: www.L-3com.com/TRL

Entrust/Authority From Entrust/PKI Version 5.0

COMMON CRITERIA EAL3 Certification: CRP141 March 2000

CLEF: BT

Entrust/ Authority is the core component of an Entrust public Key infrastructure. Acting as the Certification Authority (CA), Entrust/Authority issues X.509 public Key certificates and performs key and certificate management functions, including:

- Creating certificates for all public keys
- Creating encryption key repairs for users
- Enforcing an organisation's security policy

Entrust/Authority includes other capabilities to ensure the security of an organisation including:

- Ability to interoperate with other Entrust CAs or with other vendors' CA products
- Ability to support and maintain a strict PKI hierarchy and peer-to-peer relationships with other CAs
- Flexible configuration of what administrators and users can do
- Ability to change the distribution setup information to users and to specify the authorisation code lifetime
- Ability to specify either RSA (1024 or 2048) or DSA 10024 as the CA signing algorithm and CA signing key size
- Ability to renew the CA signing key pair before it expires and to recover from possible CA key compromise.

Entrust
Unit 4 (First Floor), Napier Court, Napier Road, Reading, RG1 8BW
United Kingdom
Point of contact: Ian wills
Telephone: +44 (0) 118 953 3000
Fax: +44 (0) 118 935 3001
URL: www.entrust.com

EUGENIC
Government use only

Cryptographic Grade: High Grade Top Secret

EUGENIC is a self-contained, general purpose cryptographic unit for civilian and limited military use. It is fitted at the terminal ends of a point-to-point communications circuit and provides protection for traffic using synchronous, duplex V.10/V11 lines, operating at a data rate in the range of 1.2kb/s up to 10Mb/s.

- RED interface V.10 and V.11 synchronous
- BLACK interface V.11 synchronous
- 1.2kb/s to 100Mb/s using external LINE or STATION clock
- PAT 105 connectors
- DRUMBEAT or OPUS variants
- Usable in both KAK and CTAK modes
- Interoperable with compatible ANWELL variants used with a suitable V.11/G703 converter
- Front panel provides local and remote change/update variable
- Paper tape and UK fill gun socket for loading key variable.

Ultra Electronics Communications & Integrated Systems
Point of contact: Richard Wall
Telephone: +44 (0) 208 813 4545
URL: www.ultra-cis.com

HALCYON Version 11
Government use only

Cryptographic Grade: High Grade Top Secret

HALYCON is a high-grade data link encryptor that will provide end-to-end protection of traffic up to and including TOP SECRET UK EYES. Using the very latest cryptographic algorithms developed by CESG, which offer significant future-proofing, the device is compact, rugged and facilitates secure communications in duplex mode at a data rate of 32Kbps to 34Mbps. It will interoperate with a variety of standard communications interfaces including X.21, V11, G703 (E1 and E3) and is suitable for replacing many legacy BID equipments. The unit can be deployed in both tactical and strategic environments and has been designed for 19 inch rack mounting with removable flanges. Main characteristics are:

- Automatic Synch Recovery
- GKM and EKMS compatible
- Two hour Keymat backup
- Tolerates double satellite hop delays
- Operates in high error environments
- Local Management via a VT100 terminal or front panel
- Remote Management using SNMPv3
- Available as a purchase or on managed service
- Low power, 20W dissipation

Notes: BIDC/2520/1n1

Version: v1.0

SELEX Communications Ltd
Innovation House, Baird House, Edge Lane, Fairfield, Liverpool.
L7 9NJ, United Kingdom
Poc: Phil Jones
Email: Phil.jones@selex-comms.com
Telephone: +44 (0) 1512 825 324
Fax: +44 (0) 1512 541 194
URL: www.selex-comms.co.uk

HALCYON G.703

Cryptographic Grade: High Grade Top Secret

HALYCON is a high-grade data link encryptor that will provide end-to-end protection of traffic up to and including TOP SECRET UK EYES. Using the very latest cryptographic algorithms developed by CESG, which offer significant future-proofing, the device is compact, rugged and facilitates secure communications in duplex mode at a data rate of 32Kbps to 34Mbps. It will interoperate with a variety of standard communications interfaces including X.21, V11, G703 (E1 and E3) and is suitable for replacing many legacy BID equipments. The unit can be deployed in both tactical and strategic environments and has been designed for 19 inch rack mounting with removable flanges. Main characteristics are:

- Automatic Synch Recovery
- GKM and EKMS compatible
- Two hour Keymat backup
- Tolerates double satellite hop delays
- Operates in high error environments
- Local Management via a VT100 terminal or front panel
- Remote Management using SNMPv3
- Available as a purchase or on managed service
- Low power, 20W dissipation

Notes: BIDC/2520/1n1
Version : v1.0, v1.1, v1.2

SELEX Communications Ltd
Innovation Park, Baird House, Edge Lane, Fairfield, Liverpool.
L7 9NJ, United Kingdom
POC: Phil Jones
Email: Phil.jones@selex-comms.com
Telephone: +44 (0) 1512 825 324
Fax: +44 (0) 1512 541 194
URL: www.selex-comms.co.uk

SECTION 4

Communications

HANNIBAL SecureTelephone Government use only

Cryptographic Grade: High Grade Top Secret

HANNIBAL is a secure ISDN (Integrated Services Digital Network) telephone capable of protecting voice and data over EURO ISDN up to TOP SECRET. Its design is based on the BRENT wide-band telephone-developed by CESG as the lead product of a programme to meet UK Government's need for an inter-departmental secure speech system well into the 21st Century. HANNIBAL has been developed from BRENT to satisfy the needs of a wider market in Europe. HANNIBAL retains the user-friendly features of BRENT that combine reliable security with convenient operating procedures. The addition of a RED ISDN SO bus gives HANNIBAL the flexibility to connect directly to compatible commercial equipment while maintaining secure functionality and dial-through capability. Features:

- HANNIBAL's user-friendly operation allows secure calls to be established automatically when a Secure Telephone Key (STK) is inserted in each equipment. The unique user STK provides secure call authentication and ensures low key management overhead.
- HANNIBAL is equipped with RED ISDN SO bus, which provides a transparent connection to the EURO ISDN. HANNIBAL can also be used to provide secure dial-up connectivity between LANs.
- HANNIBAL uses both ISDN B channels, providing a dedicated speech channel and a secure 64kbs data port, or two secure 64kb/s data ports, which can be operated simultaneously. Independent network operation and encryption are provided on each user channel.
- A unique Call Bypass Monitor ensures only selected D channel signalling messages are passed to the network
- Commercial EURO ISDN SO interface compatible equipment, plus applications such as ISDN video conferencing and personal computers may be connected directly to HANNIBAL.
- Call progress information supplied by the network is displayed on the LCD, and presented to the user application

Additional features: single key dial, last number redial, mute button, and International Telecom approval.

SELEX Communications Ltd
Innovation Park, Baird House, Edge Lane, Fairfield, Liverpool.
L7 9NJ, United Kingdom
POC: Phil Jones
Email: Phil.jones@selex-comms.com
Telephone: +44 (0) 1512 825 324
Fax: +44 (0) 1512 541 194
URL: www.selex-comms.co.uk

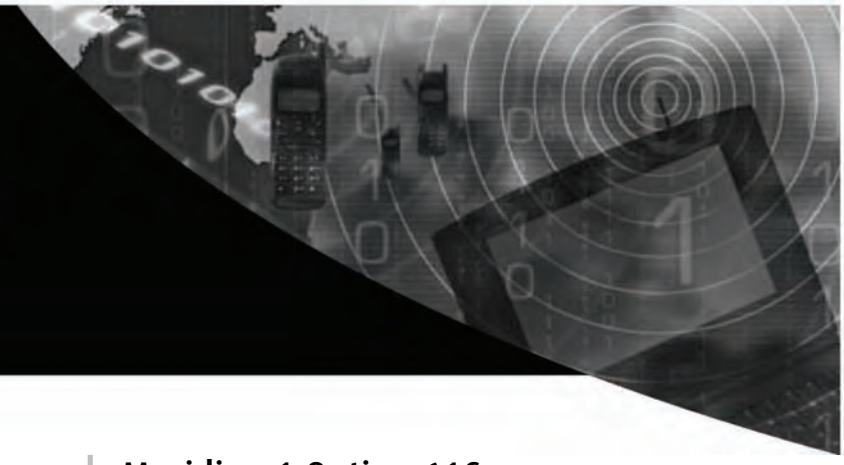
IPCRESS Network IP Crypto

Cryptographic Grade: High Grade Top Secret

IPCRESS is an IPv6 High Grade Internet Protocol Cryptographic equipment developed by Selex Communications, Secure Systems Division. IPCRESS acts as a Security Gateway, broadly in accordance with the IPSec ESP Tunnel Mode security architecture defined in RFC 2401 and RFC 2406. User IP packets traverse an untrusted BLACK WAN infrastructure as the encrypted payload of an outer encapsulating IP packet. All operational traffic keys are generated using strong PKC techniques, with an authentication overlay that permits multiple communities of interest to share a common Black network, each community acting as a Virtual Private Network (VPN).

- High Grade encryption of TOP SECRET Codeword traffic
- Strategic use
- IPv6
- Interoperable with IPv4
- 10/100Mb/s ethernet
- GKM compatible-ETD key fill
- Public Key Cryptography
- Secures Communities of Interest
- Local Management via a VT100 compatible terminal
- Remote Management using SNMPv3
- Up to 512 simultaneous sessions
- IPv4 variant in development
- EKMS key management also in development
- 1Gb+ variant development.

SELEX Communications Ltd
Innovation Park, Baird House, Edge Lane, Fairfield, Liverpool.
L7 9NJ, United Kingdom
POC: Phil Jones
Email: Phil.jones@selex-comms.com
Telephone: +44 (0) 1512 825 324
Fax: +44 (0) 1512 541 194
URL: www.selex-comms.co.uk



KITCHENMAID
NATO & Allies Government use only

Cryptographic Grade: High Grade Secret

KITCHENMAID is a High Grade cryptographic module to protect traffic up to SECRET.
KITCHENMAID is a card set that operates as a component part of Link 11 Tactical Data Link equipment, allowing halfl-duplex encryption and decryption at 45 and 9600 bits per second. It employs standard 24-bit data frame used in link 11 communications. It provides interoperability with the KG-40A and the KG-40AR and is approved for NATO operations.

Key Features:

- Crypto Variable (CV) management functions, allowing filling and validity checking of traffic CVs into up to four stores
- Switching amongst four stores for traffic CVs.
- Facility for battery backup of CVs and the associated management.
- Local and remote Erasing (Zeroizing) of CVs
- Anti-tamper features erases CVs if host equipment is removed from its mounts
- Operator indication of crypto alarms.

Ultra Electronics Communications & Integrated Systems
Point of contact: Richard Wall
Telephone: +44 (0) 208 813 4545
URL: www.ultra-cis.com

Meridian 1 Option 61C (22.46) Switch

ITSEC E2 Certificate: CRP163 February 2002
CLEF: Logica

The Meridian Option 61C, running software Version 22.46, is a Software Stored Program Control Digital Switch. Utilised as a platform for integrated voice and data, Meridian Option 61C delivers sophisticated messaging, call centre and computer telephony integration (CTI) applications for Asynchronous Transfer Mode (ATM) technology. These support WAN bandwidth consolidation, transport and delivery of multimedia communications. When configured as part of a communications network the switch prevents subscribers from gaining access to the management system and thus provides an assured separation between subscribers and management traffic. This product was evaluated for the MoD's Defence Fixed Telecommunications Service.

Nortel Networks
Maidenhead Office Park, Westvaco Way, Maidenhead, Berks
SL6 3QH, United Kingdom
Point of contact John Ducey
Telephone: +44 (0) 1628 432 799
Mobile: +44 (0) 7710875078
Fax: +44 (0) 1628 438 032
Email: jducey@nortelnetworks.com
URL: wwwnortelnetworks.com

Milgo Link/2 Multiplexer

ITSEC E2 Certificate: CRP155 March 2001

CLEF: Logica

The Milgo Link/2 Multiplexer, running software Version 11. is a fully-featured, high performance TDM networking product. It provides voice, data and image transmission integration with extensive subrate date multiplexing support. With extensive I/O functionality, it also provides unified network management with an integrated TIME/View 2000 network management system (Version 10.006). This product was evaluated for MoD's Defence Fixed Telecommunications Service.

NextiraOne Management SAS
28, avenue Victor Hugo, 75116, Paris, France
Telephone: +33 (0) 1 72 29 10 00
Fax: +33 (0) 1 72 29 12 00
URL: www.nextiraone.com

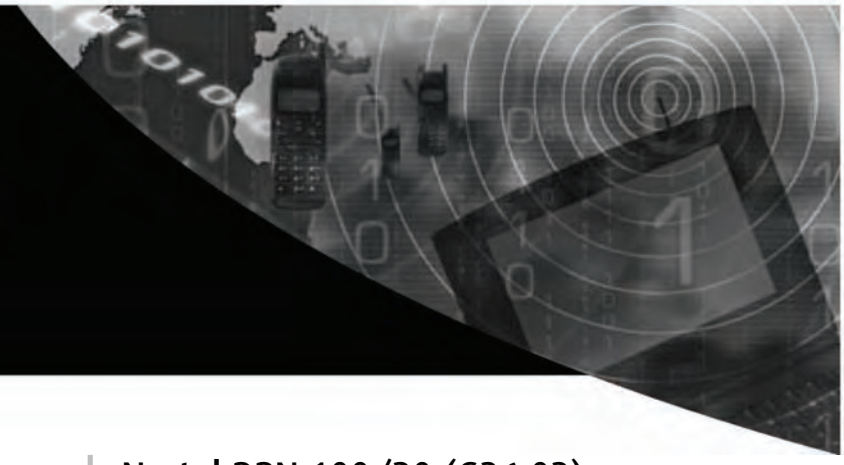
Milgo Synchrony ST-1000 & ST-20 Multiplexer

ITSEC E2 Certificate: March 2002

CLEF: Logica

The Synchrony ST-1000 and ST-20 Multiplexer, running software Version 3.2.2.3, are multiservice platforms providing circuit, frame or cell transport techniques for routing, bridging and SNA functionality. Spare bandwidth is dynamically allocated to both burst traffic, as well as contending voice, video or other constant bit rate traffic. The evaluation included the Synchrony network management system (software Version 3.1.3). This product was evaluated for MoD's Defence Fixed Telecommunications Service.

NextiraOne Management SAS
28, avenue Victor Hugo, 75116, Paris, France
Telephone: +33 (0) 1 72 29 10 00
Fax: +33 (0) 1 72 29 12 00
URL: www.nextiraone.com



Mini CATAPAN

Cryptographic Grade: High Grade Top Secret

Mini CATAPAN (BID2420/1) is the next generation, Pocket-sized, High Grade IP network encryption device. A member of the highly successful CATAPAN family of products.
Key features include:

- Sovereign High Grade SECRET & TOP SECRET reprogrammable platform.
- For Tactical, Desktop and Strategic deployment
- NPM ACCSEC when not Operational
- HAIPE-IS v3.1 with UK Traffic Protection Suite
- Small Form Factor (Pocket Sized)
- Lightweight
- Low Power
- Rugged Design
- Easy to Configure

Notes:
100Mbps duplex throughput. Key management system compliant with latest CESG Key Management specifications and procedures.
BID2420/2 is the CESG TEMPEST approved version of mini-CATAPAN.
This has been certified to SDIP-27 level A.

Version: v1.0

L-3 TRL Technology
Unit 19, Miller Court, Severn Drive, Tewkesbury,
Gloucestershire, GL20 8GD United Kingdom
Point of contact Malcolm Brown
Telephone: +44 (0) 1684 852 889 0r +44 (0) 1684 278 700
Fax: +44 (0) 1684 850 406 or +44 (0) 1685 852 599
Email: Malcolm.Brown@L-3Com.com
URL: www.L-3com.com/TRL

Nortel DPN 100/20 (G36.03) Switch

ITSEC E1 Certificate: CRP142 March 2000
CLEF: Logica

The Nortel DPN 100/20 switch, running software Version G36.03, is used within the Defence Fixed Telecommunications Service designed to form part of a packet switched data communications service. Its purpose is to provide the interface between user lines and the network. It can be configured either as an Access Module (AM) or a Resource Module (RM). The latter serves trunks, providing dynamic routing tables, whereas the former serves links and link/trunk interfaces. This product was evaluated for the MoD Defence Fixed Telecommunications Service.

Nortel Networks
Maidenhead Office Park, Westacott Way, Maidenhead, Berks
SL6 3QH, United Kingdom.
Point of contact: John Ducey
Telephone: +44 (0) 1628 432 799
Mobile: +44 (0) 7710 875 078
Fax: +44 (0) 1628 438 032
Email: hdmahony@nortel.
URL: www.nortel.com

SECTION 4

Communications

Nortel Multservice Switch 15000, Version 8.2

COMMON CRITERIS EAL3 IN EVALUATION

CLEF: BT

Nortel Multiservice Switch (MSS) 15000 is an Asynchronous Transfer Mode (ATM)-based data device that can be deployed as a backbone for existing MSS edge node networks or as a service provider ATM backbone node. It also delivers a range of standards-based interfaces and services, including IP<>MSS 15000 nodes provide multi-protocol routing services and simultaneously support voice, data, video and image traffic. MSS systems provide security that includes user ID and password protection, link to an external RADIUS server for authentication, command and event logging, in-band or out-of-band management, accurate routing of traffic and separation of all traffic streams form one another.

Nortel MSS 15000, Version 8.2, is in evaluation to EAL3 augmented by ALC_FLR.3.

Nortel Networks
Maidenhead Office Park, Westacott Way, Maidenhead, Berks SL6 3QH, United Kingdom.
Point of contact: Hugh Mahoney or Simon Wilson
Telephone: +44 (0) 1628 432 511 or 3434 566
Email: hdmahony@nortel.com
siwilson@nortel.com
URL: www.nortel.com
Http://products.nortel.com

Nortel PASSPORT 6480 (5.0.16) Switch

ITSEC E1 Certificate: CRP143 March 2000

CLEF: Logica

The Nortel Passport switch, running software Version 5.0.16 is used within Defence Fixed Telecommunications Service designed to form part of a packet switched data communications service. Its purpose it to support high capacity services on the network. It provides access protocol support for Frame Relay, Asynchronous Transfer Mode and LAN interconnect. This product was evaluated for the MoD's Defence Telecommunications Service

Nortel Networks
Maidenhead Office Park, Westacott Way, Maidenhead, Berks SL6 3QH, United Kingdom.
Point of contact: John Ducey
Telephone: +44 (0) 1628 432 799
Mobile: +44 (0) 7710 875 078
Fax: +44 (0) 1628 438 032
Email: hdmahony@nortel.
URL: www.nortel.com

OMGEA Version 7.20 Increment 7.0
Government Use

ITSEC E3 Certificate: CRP230 June 2006

CLEF: Logica

OMEGA is a multi-level secure message-handling product (Functionality Class FB1) which provides a full range of network and secure messaging facilities.

Features include:

- MAC, DAC and application of security labels
- Drafting, release control, distribution, delivery, routing, servicing and correction of messages with full provision of accountability, arching and traceability
- Acceptance and generation of almost all message formats including ACP127 and X.4000 (1984 and 1988).

Fujitsu Ltd
Point of contact: John Reynolds
Telephone: +44 (0) 870 853 3157
Fax: +44 (0) 1256 844 759
Email: john.reynolds@services.fujitsu.com
URL: www.services.fujitsu.com

Oracle HTTP Server (OHS) 10g (10.1.2)

COMMON CRITERIA EAL4 Certificate: CRP243 January 2007

CLEF: Logica

Oracle HTTP Server (OHS) provides Key infrastructure for serving the internet's HTTP protocol.

OHS returns responses for both process-to process and human generated requests from browsers. Key aspects are its technology, its serving of both static and dynamic content and its integration with both Oracle and non-Oracle products.

OHS is based on the open source technology Apache 2.0, which accommodates the newest Internet Protocol, Ipv6. OHS also provides an application firewall capability, via the open source product mod_security.

OHS serves static content directly or via standard interfaces, e.g. WebDAV. Languages such as Java and PLSQL are supported for content generation.

Oracle Corporation
Security Evaluations Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA,United Kingdom.
Point of contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com
or shaun.lee@qracle.com
URL: otn.oracle.com/deploy/security/seceval/content.html

SECTION 4

Communications

Oracle Identity and Access Management 10g

COMMON CRITERIA EAL4 Certificate: CRP245 June 2008

CLEF: Logica

Oracle Identity and Access Management is a product suite that allows enterprise to mange the end-to-end lifecycle of user identities, and provides users with secure, fine-grained access control to enterprise resources and assets.

The suite includes the following products:

- Oracle Access Manager-an access control system which provides a full range of identity and access control functions including single sign-on; access control; auditing; policy management; and delegated administration.
- Oracle Internet Directory-a general purpose LDAP directory service
- Oracle Virtual Directory-a service that provides a virtualised directory containing the information from many heterogeneous systems

Oracle Identity and Access Management 10g Release 3 (10.1.4.0.1) has been evaluated to EAL4 augmented by ALC_FLR.3.

.

Oracle Corporation

Security Evaluations Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA,United Kingdom.

Point of contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@qracle.com

URL: otn.oracle.com/deploy/security/seceval/content.html

Oracle Identity Federation Version 10g Release 3

COMMON CRITERIA EAL4 IN EVALUALTION

CLEF: Logica

Oracle Identity Federation is a standalone, self-contained federation server that supports federated identity management to enable single sign-on and authentications in a multiple-domain identity network. Federated identity management is the evaluation of the single sign-on paradigm in response to users' growing needs for access to computing resources and services that reside outside their own company's boundaries. In a federated environment, enterprises offering such a service can reliably obtain identity information about an individual or other entity from user's home organisations or security domain.

Oracle Corporation

Security Evaluations Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA,United Kingdom.

Point of contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@qracle.com

URL: otn.oracle.com/deploy/security/seceval/content.html

Oracle Internet Directory 10g

COMMON CRITERIA EAL4 Certificate: CRP244 June 2008
CLEF: Logica

Oracle Internet Directory is a general purpose LDAP directory service that enables fast retrieval and centralised management of information about dispersed users and network resources.

Oracle Internet Directory has a unique multi-threaded, multi-process, multi-instance process model that combines LDAP v3 with the high performance, scalability, robustness, and availability of the Oracle Database server.

Oracle Internet Directory runs as an Oracle Database application, for which the database holds the directory data.

Oracle Internet Directory 10g (10.1.4.0.1) has been evaluated to EAL4 augmented by ALC_FLR.3.

.

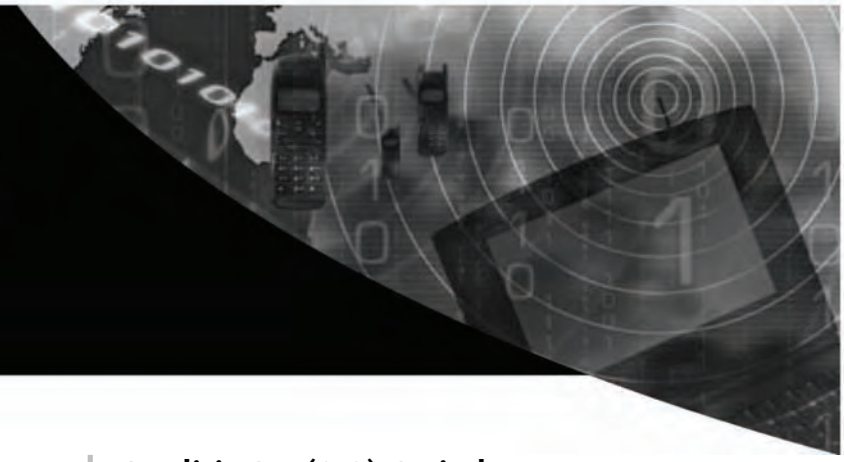
Oracle Corporation
Security Evaluations Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA,United Kingdom.
Point of contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com
or shaun.lee@qracle.com
URL: otn.oracle.com/deploy/security/seceval/content.html

Oracle Internet Directory 10g

COMMON CRITERIA EAL4 Certificate: CRP210 February 2005
CLEF: Logica

Oracle Identity Directory (OID) Release 10g (9.0.4.) is a scalable, robust LDAP V3-compliant directory service that runs as an application on the Oracle9i Database Server. It is a vital component in the Oracle Identity Management infrastructure. OID implements several authentication levels and allows access to the directory to controlled through the use of access control lists. It also offers sophisticated password policy management capabilities and facilities to permit directory events to be selected by directory administrator and subsequently audited. Tools for manipulating large volumes of LDAP data and for directory administration are provided.

Oracle Corporation
Security Evaluations Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA,United Kingdom.
Point of contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com
or shaun.lee@qracle.com
URL: otn.oracle.com/deploy/security/seceval/content.html



Realitis DX (6.1) Switch

ITSEC E2 Certificate: CRP162 February 2002
CLEF: Logica

The Realitis DX, running software Version 6.1, is a Software Stored Program Control Digital Switch. Utilised as a platform for integrated voice and data, the Realitis DX supports Industry's standard interface and open communications standards, such as ISDN and IP. When configured as part of a communications network the switch prevents subscribers from gaining access to the management system and thus provides an assured separation between subscribers and management traffic. This product was evaluated for the MoD's Defence Telecommunications Service.

.

Siemens Communications Ltd
Technology Drive, Beeston, Nottingham, NG9 1LA,
United Kingdom.
Point of contact: Stuart Jesson
Telephone: +44 (0) 115 943 0300
Fax: +44 (0) 115 943 9610
Email: stuart.jesson@marconiselenia.com
URL: www.siemenscomms.co.uk

Realitis DX (8.0) Switch

ITSEC E2 Certificate: CRP202 March 2004
CLEF: Logica

The Realitis DX Switch is a Software Stored Program Control Digital Switch. Utilised as a platform for integrated voice, data and video, Realitis DX Switch supports Industry's standard interface and open communications standards, such as ISDN and IP based multimedia. When configured as part of a communications network the switch prevents subscribers from gaining access to the management system and thus provides an assured separation between subscribers and management traffic. This product was evaluated for the MoD's Defence Telecommunications Service

Siemens Communications Ltd
Technology Drive, Beeston, Nottingham, NG9 1LA,
United Kingdom.
Point of contact: Stuart Jesson
Telephone: +44 (0) 115 943 0300
Fax: +44 (0) 115 943 9610
Email: stuart.jesson@marconiselenia.com
URL: www.siemenscomms.co.uk

Realitis DX Switch

ITSEC E2 Certificate: CRP183 June 2003

CLEF: Logica

The Realitis DX Switch is a Software Stored Program Control Digital Switch. Utilised as a platform for integrated voice, data and video, Realitis DX Switch supports Industry's standard interface and open communications standards, such as ISDN and IP based multimedia. When configured as part of a communications network the switch prevents subscribers from gaining access to the management system and thus provides an assured separation between subscribers and management traffic. This product was evaluated for the MoD's Defence Telecommunications Service.

.

Siemens Communications Ltd
Technology Drive, Beeston, Nottingham, NG9 1LA,
United Kingdom.
Point of contact: Stuart Jesson
Telephone: +44 (0) 115 943 0300
Fax: +44 (0) 115 943 9610
Email: stuart.jesson@marconiselenia.com
URL: www.siemenscomms.co.uk

SAFEDIAL+

Cryptographic Grade Enhanced

Thales SafeDial+ is a hardware encryption device for protecting classified communications between computers across a variety of public networks, both fixed and dial-up. SafeDial+ is primarily intended as a remote access solution (e.g. for home-workers to connect to their office network), but can also be used for ad hoc point-to-point communication links. The following transmission media are supported via a range of optional modems and adapters:

- PSTN (analogue telephone network)
- ISDN
- GSM (mobile phone network)
- IP (e,g, broadband – see Notes)

Housed in a tamper-resistant Type II PC Card, SafeDial+ fits directly into a laptop PC or connects to a desktop PC through an optional serial adapter. A 16-slot rack is available for central site installations. SafeDial+ employs a CESG-approved algorithm and, once installed, requires only a password for normal operation. Unique session keys are generated automatically each time it is used, removing the need for time consuming key creation, updating and distribution tasks. SafeDial+ is not protectively marked.

.

Notes:
Use of SafeDial+ over IP networks may be subject to certain limitations outside the UK – please contact CESG for details. Please contact CESG regarding continued availability of a Baseline Grade Version.

Version 1.529

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, Hp18 9EQ, United Kingdom
Point of contact: Ian Danter
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 208 550
Email: ian.danter@thales-escurity.com
URL: www.thales-esecurity.com/

Safegate Version 2.0.2

COMMON CRITERIA EAL3 Certificate: CRP139 January 2000
CLEF: Logica

Safegate (Version 2.0.2) is a firewall that serves as a single point connecting a private network to a hostile network (e.g. the internet) and is designed to eliminate various kinds of potential threat attack on a private network through the hostile network. Safegate has an Internet Protocol packet filtering function, an application gateway function (non-transparent and transparent) and a security management function which contains the audit functions. The IP packets filtering function permits or denies the transmission of IP packets through Safegate from the hostile network and the private network according to filtering rules defined by an authorised administrator. The transparent gateway (TCP,UDP,ICMP,FTP, Telnet and various multimedia services) allows a direct connection between a client on the private network and a host on the Internet. The non-transparent gateway (only FTP and Telnet services) allows simultaneous sessions between the client on the private network and the Internet host. Auditing functionality allows information on packet filtering and the application gateway to be logged, an alert to be sent to the administrator on detection of an invalid packet, monitoring by the administrator and viewing by the administrator.

Fujitsu Ltd
Point of Contact: Takehiko Yahagi
Telephone: +81 45 472 9379
Fax: +81 45 472 93690
Email: t-yahagi@jp.fujitsu.com
URL: www.fujitsu.com/

SECTERA Secure Mobile Telephone
Government Use Only

Cryptographic Grade High Grade Secret

The General Dynamics Sectéra GSM is the medium-term solution for secure mobile telephony in HM Government. The Sectéra GSM is a commercial handset incorporating 2.5 generation GPRS enhanced data services in non-secure mode. A clip-in module provides secure voice and secure data up to SECRET using the GSM data service. As a Future Narrow Band Digital Terminal (FNBDT) product, the Sectéra GSM is Compatible with HMG's next generation secure architecture for mobile and desktop telephony. As well as secure data, recent upgrades provide interoperability between up to 4 user groups including the Combined Communications Electronics Board and NATO.

The Sectéra GSM, used with the Sectéra Wireline Terminal, can be used in locations where mobile phones are otherwise not permitted. Small and portable, the Wireline Terminal can be connected to a PC or standard desktop handsets.

When high assurance secure communications are required in remote areas where terrestrial communications are not available, the Sectéra BDI (Black Digital Interface) Terminal provides end-to-end voice and data security for digital communications.

Sectéra BDI Terminal protects communications for a variety of satellite applications, including Iridium, Inmarsat, Globalstar and Thuraya satellite phones. The terminal has also been enhanced to provide secure data rates up to 128 Kb/s over landline digital networks when connected to an ISDN adapter. Additionally the terminal can be used to secure voice and data for mobile phones and other AT-compatible communications devices.

Secetra Brochure
End_use Cryptographic Equipment
All enquiries regarding Sectera should be emailed to:
Sectera@gchq.gsi.gov.uk

CESG
Room A2j, Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, United Kingdom
Point of contact: Customer Support Office
Telephone: +44 (0) 1242 709 141
Fax: +44 (0) 1242 709 193
Email: enquiries@cesg.gsi.gobv.uk
URL: www.cesg.gov.uk

SECTION 4

Communications

SELEX Communications MPS

COMMON CRITERIA EAL4 Certificate: CRP207 July 2004

CLEF: Logica

MPS115 and MPS145 (Software Version 1.4 pack 2) are part of a family of multiprotocol, multi-level secure digital switches built up in mixed ATM/IP technology and designed in compliance with ITU-T and ATM Forum Standards with additional cell hardening features essential in military applications. The TOE comprises a large set of ATM and Interworking interfaces that can be equipped in a flexible way in order to assure a full integration and interoperability with civilian and military ATM, IP, ISDN, STANAG/EUROCOM networks and IT products, deployed both in tactical and strategic scenarios.

Information Flow Control policy is enforced by the TOE for all the available subscriber facilities and switched user traffic, both native and in transit, and is based on hierarchical security levels and on security profiles individually associated to registered subscribers, networks and plugged-in traffic interface. Access Control policy is enforced by the TOE for the access to the management data and is based on manager user roles with different privileges that can be associated to TOE's Administrators for both local and remote management activities.

The TOE preserves secure state during operations with automatic recovery capabilities, assuring complete separation between the different subscriber, security domains and between management and control planes; all the security relevant events are detected, maintained and traced back to Administrators as auditable data.

SELEX Communications

Secure Systems Division. Wavetree Boulevard, Wavetree Technology Park, Liverpool, L7 9PE, United Kingdom

Telephone: +44 (0) 151 282 5300

Fax: +44 (0) 151 254 1194

URL: www.selx-comms.co.uk

SGSS

Cryptographic Grade: See Notes

The Thales SGSS is a Programmable Infosec Module (PIM) consisting of a secure hardware platform and secure bootstrap (application loading) process. The use of programmable cryptography enables the SGSS to support a number of different CESG-approved algorithms and thus provide solutions suitable to protect information classified from RESTRICTED up to SECRET (see Notes).

Notes:

Available in both Baseline Grade and Enhanced Grade versions. Protecting information classified as SECRET is based on the conditions described in Security Notice S(E)N 03/03. Products containing this module will require evaluation in their own right.

Version: Bootstrap v2.4.3 software and issue 3a hardware

Thales e-Security

Meadow View House, Crendon Industrial Estate, Long Crendon, Aylesbury, Bucks, HP18 9EQ, United Kingdom

Point of contact: Ian Danter

Telephone: +44 (0) 1844 201 800 or

Fax: +44 (0) 1844 201 570

Email: ian.danter@thales-esecurity.com

URL: www.thales-esecurity.com

SHELLEYAN II
Government Use Only

Cryptographic Grade: High Grade Top Secret

SHELLEYAN II is a high-grade cryptographic unit designed to protect data to Top Secret Codeword.

It can operate in either of two modes:

Messaging mode: SHELLEYAN II is connected to the messaging system by an asynchronous interface to encrypt addressed messages. It allows the address part through and encrypts the message part, creating an unclassified encrypted message. The transmission system includes a variable delay before the message reaches the destination SHELLEYAN II for decryption.

Link encryption mode: SHELLEYAN II has a full duplex connection to another SHELLEYAN II unit. The interface is essentially a real-time link. The connection can be synchronous or asynchronous, and the equipment can be externally wired to operate over a simplex link.

SHELLEYAN II is interoperable with all other versions of SHELLEYAN.

CESG
Room A2j, Hubble Road, Cheltenham, Gloucestershire, GL51 0EX,
United Kingdom
Point of contact: Customer Support Office
Telephone: +44 (0) 1242 709 141
Fax: +44 (0) 1242 709 193
Email: enquiries@cesg.gsi.gobv.uk
URL: www.cesg.gov.uk

SYMONS (SHELLEYAN III)
Government Use Only

Cryptographic Grade: High Grade Top Secret

SYMONS is a high-grade cryptographic unit designed to protect data to Top Secret Codeword.

SYMONS communications functionally and cryptography are identical to SHELLEYAN II.

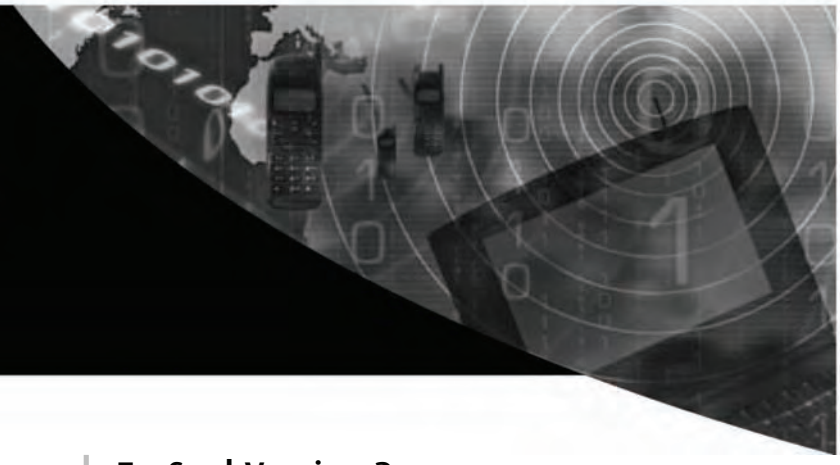
Additional features of this device are that SYMONS is smaller, lighter and specifically developed for mobile and desktop applications, as well as rack mounting via a rack-mounting unit.

SYMONS is AC or DC powered.

This product was developed under the CESG Assisted Products Service (CAPS).

SYMONS now has full TEMPEST certification and Design Acceptance Certificate

Compucat Europe Ltd (Manufacture)
The Mews, 18-20 Church Gate, Thatcham, Berkshire, RG19 3PH,
United Kingdom
Telephone: +44 (0) 1635 863 777
Fax: +44 (0) 1635 863 557
Email: info@compucat.co.uk



THAMER
NATO & Government Use Only

Cryptographic Grade: High Grade Top Secret

.THAMER is a low cost point-to-point link encryption unit which protects data to Top Secret Codeword. It operates across fixed links at data rates up to 2.084Mb/s. It has been designed to minimise the cost of link security both in terms of initial purchase and continued ownership. It is suitable for both desktop and rack mounted applications.

THAMER employs tamper protection and detection methods which, when combined with the removal of the access control device, enables THAMER to be left unattended in a secure site.

- Full duplex point-to-point synchronous high grade data encryption
- Automatic key generation and distribution using Public Key Cryptography
- Plug-in Line Interface Modules (LIMs) allow user to select exact configuration required without the expense of additional unwanted options.
- Current LIM options are RS-232 and V.11 and G703
- Simple access control device
- No routine key changes
- Fit and forget
- Small and portable

SELEX Communications
Innovation Park, Baird House, Edge Lane, Fairfeild, Liverpool, L7 9NJ, United Kingdom
POC: Phil Jones
Email: phil.jones@selex-comms
Telephone: +44 (0) 7801 715 696
Fax: +44 (0) 1512 541 194
URL: www.selex-comms.co.uk

TruSeal Version 2

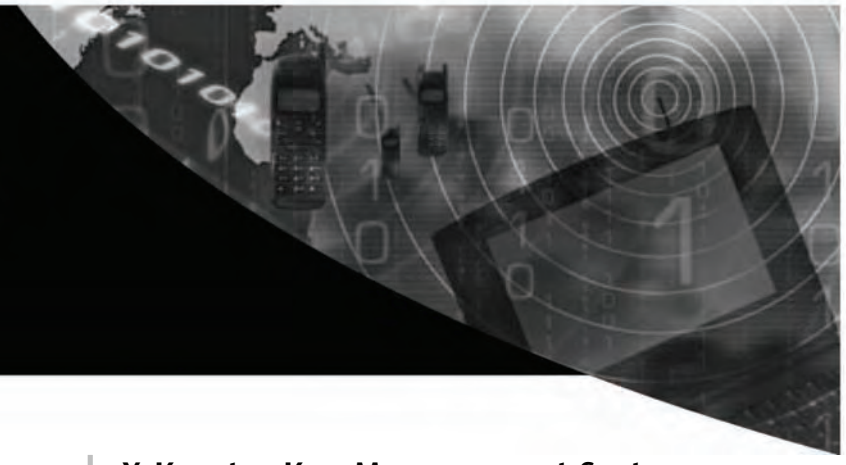
CCTM Certificate: 2007/11/0033
Awarded: 8th November 2007 Valid until: 7th November 2009

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 or 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.

Tru Data Integrity Limited
Registered Office, Acorn House, Oaks Business Park, Oaks Lane, Barnsley, South Yorkshire, S71 1HT, United Kingdom

Sales Office:
93-95 Gloucester Place, London, W1U 6JQ, United Kingdom
Telephone: +44 (0) 870 251 7100/ +44 (0) 20 7487 8389
Email: a.thomas@tru-dataintegrity.com
URL: www.tru-dataintegrity.com

Communications



X-Kryptor Client to PDA

Cryptographic Grade: Baseline

X-Kryptor Client for PDA is a secure client for Windows Mobile 5 network communications. The software encrypts IP Packets over WLAN and 3G connections using approved implementations of the AES algorithm with 128 bit key. The X-Kryptor Client for PDA will communicate with a standard X-Kryptor Gateway and can be used concurrently alongside XP and Windows 2000 X-Kryptor Clients.The Client can also be configured to target multiple X-Kryptor Gateways or used in Dynamic Mode which will locate X-Kryptor Gateway's automatically.

Version: BMS1664, BMS1665

Barron McCann Technology Ltd
Bemac House, Fifth Avenue, Letchworth, Herts, SG6 2HF,
United Kingdom
Point of Contact: Peter Alderson
Telephone: +44 (0) 1462 482 333
Fax: +44 (01462 482 112
Email: petera@bemac.com
URL: www.x-kryptor.com/

X-Kryptor Key Management System

Cryptographic Grade: Baseline

The solution for X-Kryptor Clients and X-Kryptor Gateways to receive key material updates automatically over the air. It will support many thousands of Clients and Gateways in multiple separate encryption domains. A comprehensive range of support and training services are available to ensure the successful implementation of KMS. The system has been designed to ensure that customers can migrate to a KMS environment at a pace appropriate to their needs.

Version: v1.0, BMS1797-2

Barron McCann Technology Ltd
Bemac House, Fifth Avenue, Letchworth, Herts, SG6 2HF,
United Kingdom
Point of Contact: Peter Alderson
Telephone: +44 (0) 1462 482 333
Fax: +44 (01462 482 112
Email: petera@bemac.com
URL: www.x-kryptor.com/

X-Kryptor Network Encryption Gateway & VPN Client

Cryptographic Grade: Baseline

X-Kryptor is a dedicated Network Encryption Gateway providing domain based security. The device has two active 10/100Mb LAN interfaces which create a secure network domain. Multiple secure domains can be created through the interconnectivity of multiple X-Kryptors or via client devices running the X-Kryptor Secure Device Driver Client (SDD). The encryption technique uses the AES algorithm with a 128 bit key. Data throughput speeds supported are 25Mb/s and a 100Mb/s.

X-Kryptor supports any TCP/IP network infrastructure including:

- Wireless
- GPRS/3G
- Satellite
- Bluetooth
- Traditional LAN/WAN technologies

Communications across the network can be in either TCP encryption mode or within a TCP based VPN tunnel Supported client operating systems include:

- Windows 2000
- Windows XP

Version:

- X-Kryptor Lite
- X-Kryptor 25
- X-Kryptor 100

Firmware:

- BMF0930-4, non RSA version, BMF0931-4 RSA version

X-Kryptor Client:

- Installer (BMI102-2, non RSA version, BMI103-2 RSA version

Barron McCann Technology Ltd
Bemac House, Fifth Avenue, Letchworth, Herts, SG6 2HF,
United Kingdom
Point of Contact: Peter Alderson
Telephone: +44 (0) 1462 482 333
Fax: +44 (01462 482 112
Email: petera@bemac.com
URL: www.x-kryptor.com/

SECTION 5

Databases

CESG

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

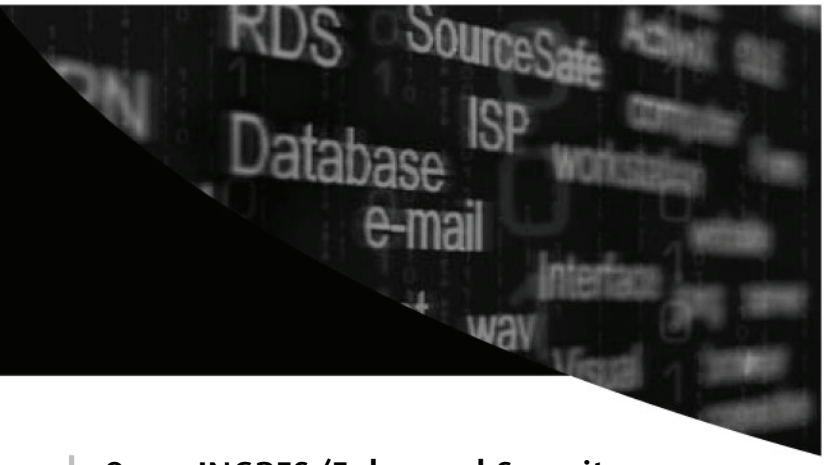
ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0)1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 5

Databases



INFORMIX-Online Dynamic Server Version 7.23

ITSEC E2 Certificate: CR96-95 March 1998

CLEF: Logica

INFORMIX-Online Dynamic Server Version 7.23 is a multi-threaded database server designed to exploit the capabilities of both symmetric multiprocessor (SMP) and uniprocessor architectures to deliver database scalability, manageability and performance. It provides transaction processing and decision support through parallel data query (PDQ) technology, high availability, data integrity, mainframe-calibre administration and client/server. IT supports informix's entire range of SQL-based application development tools and a large number of third party tools. Designed to be portable across E2/F-C2 UNIX platforms, tailoring to specific platforms involves changes to a small and well defined set of source modules requiring a minimal amount of re-evaluation. The product was evaluated on DEC UNIX V4.0c.

IBM United Kingdom
Mailpoint BDF22W, 2New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom
Point of Contact: Andy Legge
Telephone: +44 (0) 20 8818 1017
Fax: +44 (0) 20 8818 1017
Email: andy.legge@uk.ibm.com
URL: www.ibm.com/software/data/informix/

Open INGRES/Enhanced Security 1.2/01

ITSEC E3 Certificate: CRP146 July 2000

Open INGRES/Enhanced Security 1.2/01 is a fully featured multi-level Relational Database Management System offering an ANSI compliant SQL interface. In addition to the standard Discretionary Access Controls (DAC), it provides Security Auditing and Mandatory Access Control (MAC) features. When used in conjunction with an F-B1 operating system it is intended to provide security for systems requiring F-B1 functionality. INGRES/Enhanced Security acts as a vital component of a secure system by providing a set of database security functions that cover the areas of Identification, DAC, MAC, Accountability, Audit and Object Reuse. When used with an F-C2 operating system, OpenINGRES 1.2/01 provides F-C2 functionality, in applications where there is no requirement for MAC.

Computer Associates
Point of Contact: Jim Callaghan
Telephone: +44 (0) 1753 242 200
Fax: +44 (0) 1753 242 500
Email: jim.Callaghan@ca.com
URL: www.ca.com

SECTION 5

Databases

Oracle Application Server 10g

COMMOM CRITERIA EAL4 Certificate: CRP223 May 2006

CLEF: Logica

Oracle Application Server 10g is a standards-based, mission-critical platform designed for unbreakable reliability, high availability and predictable scalability in an integrated, service orientated architecture.

The scope of the certification covers Oracle containers for J2EE (OC4J) and Oracle Internet Directory (OID)'

The OC4J is fully J2EE 1.3 compliant, uses a standard JDK 1.4 Java Virtual Machine and provides complete support for JSPs, Servlets, Enterprise JavaBeans, Web services and J2EE services. It utilises the OID with the addition of Java API

OC4J offers a complete Java Authentication and Authorisation Service (JAAS) including role-based access control, authentication and JAAS Delegation.

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

Oracle Database 10g Enterprise Edition

COMMOM CRITERIA EAL4 Certificate: CRP221 September 2005

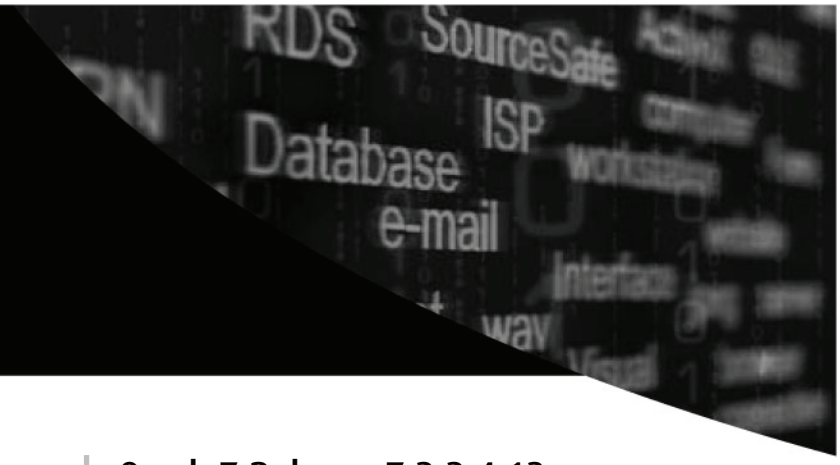
CLEF: Logica

Oracle Database 10g Enterprise Edition is the first Relational Database Management System designed for Grid Computing. Providing advanced security and functionality for multi-user, distributed database environments. Oracle 10g, Release 10.1.0 is evaluated against the Database Management System protection profile. In addition to the security functions listed for Oracle9i, Release 2, Oracle 10g supports Enterprise User Security including Enterprise Privilege Administration and Password Authenticated Enterprise Users. It has extensible fine-grained auditing and enhanced administrator auditing. Oracle 10g supports secure connections from Oracle 10g database to older database versions.

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

SECTION 5

Databases



Oracle Label Security 10g

COMMOM CRITERIA EAL4 Certificate: CRP222 September 2005

CLEF: Logica

Oracl10g Label Security (OLS).is a security option for the Oracle Database 10g Enterprise Edition Release 10.1.0. It mediates users' access to data via their assigned authorities and labels, allowing data separation by sensitivity within single databases.

OLS augments traditional government-centred multi-level security and B1 products. It extends classifications and compartments with groups and, exploiting facilities within Oracle10g's Virtual Private Database feature, provides for multiple policies on the same database.

Interfaces are provided for creating and managing policies, enforcement options, data labels and user label authorisations, and for protecting individual tables or schemas. OLS also supports releasabilities (or nationality caveats).

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

Oracle7 Release 7.2.2.4.13

COMMOM CRITERIA EAL4 Certificate: CRP103 September 1998

CLEF: Logica

Oracle 7 is a Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environments. Oracle7, Release 7.2.2.4.13, when used in conjunction with an operating system of ITSEC F-C2 or greater, provides database security for systems that require F-C2 functionality. Oracle7, Release 7.2.2.4.13, was evaluated against the Commercial Database protection profile. The main security functions are identical to those given in the Oracle7, Release 7.2.2.4.13, ITSEC E3 evaluation entry.

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

SECTION 5

Databases

Oracle8 Release 8.0.5.0.0

COMMOM CRITERIA EAL4 Certificate: CRP106 October 2000

CLEF: Logica

Oracle8 is an Object/Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environments. Oracle8, Release 8.0.5.0.0, when used in conjunction with an operating system incorporating the Controlled Access Protection (or the equivalent ITSEC F-C2 functionality) provides database security for the systems that require C2 functionality. Oracle8, Release 8.0.5.0.0, was evaluated against the Database Management System protection profile. In addition to the security functions listed for Oracle7, Release 7.3.4.0.0, Oracle8 also supports mutual authentication of database, single sign-on, password management, data dictionary protection, global roles and X.509 certificate based authentication.

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

Oracle8i Label Security

COMMOM CRITERIA EAL4 Certificate: CRP169 May 2002

CLEF: Logica

Oracle8i Label Security (OLS) is a security option for the evaluated Oracle8i Object/Relational Database Management System (enterprise Edition). It mediates users' access to data via their assigned authorities and labels, allowing data separation by sensitivity within a single database.

OLS adds to traditional government-centred Multi Level Security and B1 products. It extends classifications and compartments with groups and, exploiting the facilities provided by Oracle8i's VPD, provides for multiple policies on the same database.

Interface are provided for creating and managing policies, enforcement options, data labels and user label authorisations, and for protecting individual tables or schemas.

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

SECTION 5

Databases

Oracle8i Release 8.1.7.0.0

COMMOM CRITERIA EAL4 Certificate: CRP158 July 2001

CLEF: Logica

Oracle8i is an Object/Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environment. Oracle8i, Release 8.1.7.0.0, has been evaluated against the Database Management System protection profile. In addition to the security functions listed for Oracle8i, Release 8.0.5.0.0, Oracle8i also supports security policies for fine-grained access control, application specific security context, invoker's and definer's rights to permit separation of programmed logic from privileges and data and integration with LDAP-based directory services.

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

Oracle9i Label Security

COMMOM CRITERIA EAL4 Certificate: CRP179 September 2003

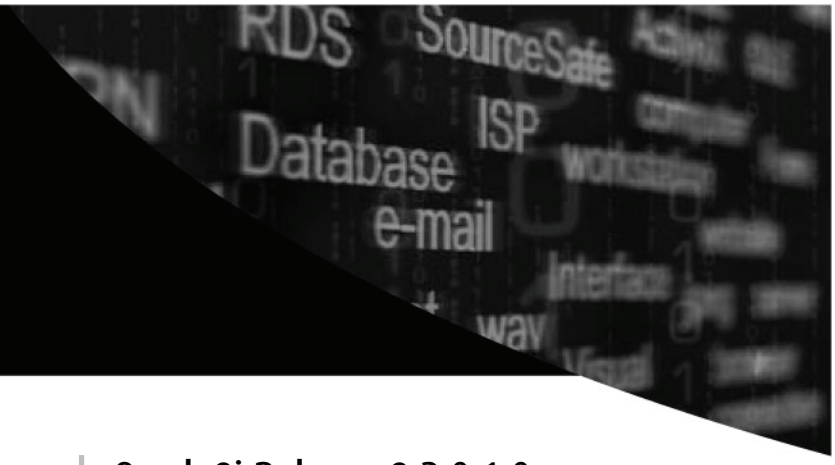
CLEF: Logica

Oracle9i Label Security (OLS) is a security option for the Oracle9i Release 2 Object/Relational Database Management System (Enterprise Edition). It mediates users' access to data via their assigned authorities and labels, allowing data separation by sensitivity within single databases. OLS augments traditional government-centred Multilevel Security and B1 products. It extends Classification and compartments with groups and, exploiting facilities within Oracle9i's VPD, provides for multiple policies on the same database. Interfaces are provided for creating and managing policies, enforcement options, data labels and user label authorisations, and for protecting individual tables or schemas OLS also supports releaseabilities (or nationality caveats). The product was certified running on Sun Solaris 8 and Microsoft Windows NT 4.0 (The product was subsequently certified running on SuSE Linux)..

Oracle Corporation
Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom
Point of Contact: Shaun Lee
Telephone: +44 (0) 118 924 3860
Fax: +44 (0) 118 924 3171
Email: seceval_us@oracle.com or shaun.lee@oracle.com
URL: otn.oracle.com/deploy/security/seceval.html

SECTION 5

Databases



Oracle9i Label Security on SUSE Linux

COMMOM CRITERIA EAL4 Certificate: CRP212 February 2005

CLEF: Logica

Oracle9i Label Security (OLS) is a security option for the Oracle9i Release 2 Object/Relational Database Management System (Enterprise Edition). It mediates users' access to data via their assigned authorities and labels, allowing data separation by sensitivity within single databases. OLS augments traditional government-centred Multilevel Security and B1 products. It extends Classification and compartments with groups and, exploiting facilities within Oracle9i's VPD, provides for multiple policies on the same database. Interfaces are provided for creating and managing policies, enforcement options, data labels and user label authorisations, and for protecting individual tables or schemas OLS also supports releaseabilities (or nationality caveats). The product was certified running on SuSE Linux. (The product was previously certified running on Sun Solaris 8and Microsoft Windows NT 4.0).

Oracle Corporation

Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom

Point of Contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@oracle.com

URL: otn.oracle.com/deploy/security/seceval.html

Oracle9i Release 9.2.0.1.0

COMMOM CRITERIA EAL4 Certificate: CRP178 September 2003

CLEF: Logica

Oracle9i is an Object/Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environment. Oracle9i, Release 9.2.0.1.0, has been evaluated against the Database Management System protection profile. In addition to the security functions listed for Oracle8i, Release 8.1.7, Oracle9i supports security applications roles (roles that can only be enabled by authorised PL/SQL packages) and adds new privileges. Oracle9i also extends the auditing facilities offered by supporting fine-grained auditing and by increasing the auditing performed on the SYS.user and users connected as SYSDBA and SYSOPER. The product was certified running on Sun Solaris 8 and Microsoft Windows NT 4.0. (The product was subsequently certified running on SuSE Linux).

Oracle Corporation

Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom

Point of Contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@oracle.com

URL: otn.oracle.com/deploy/security/seceval.html

SECTION 5

Databases

Oracle9i Release 9.2.0.1.0
SUSE Linux

COMMOM CRITERIA EAL4 Certificate: CRP211 February 2005

CLEF: Logica

Oracle9i is an Object/Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environment. Oracle9i, Release 9.2.0.1.0, has been evaluated against the Database Management System protection profile. In addition to the security functions listed for Oracle8i, Release 8.1.7, Oracle9i supports security applications roles (roles that can only be enabled by authorised PL/SQL packages) and adds new privileges. Oracle9i also extends the auditing facilities offered by supporting fine-grained auditing and by increasing the auditing performed on the SYS.user and users connected as SYSDBA and SYSOPER. The product was certified running on SuSE Linux. (The product was subsequently certified running on Sun Solaris 8 and Microsoft Windows NT 4.0).

Oracle Corporation

Security Evaluations Managers, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom

Point of Contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

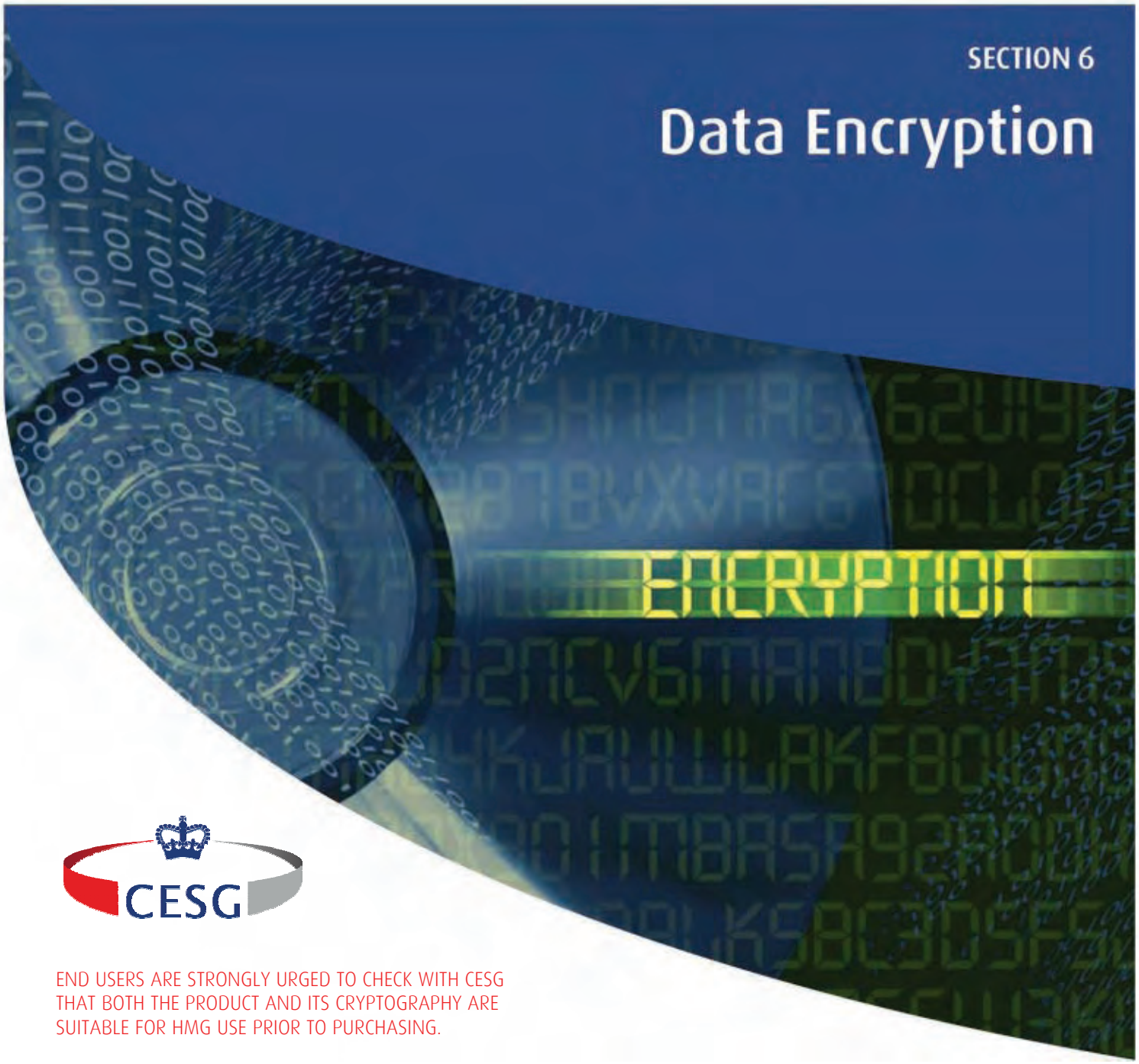
Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@oracle.com

URL: otn.oracle.com/deploy/security/seceval.html

SECTION 6

Data Encryption



CESG

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor or CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 6

Data Encryption

BeCrypt DISK Protect Baseline

Cryptographic Grade: Baseline

BeCrypt's DISK Project Baseline product provides encryption for fixed disk or removable media devices. For selected disks and media, full-disk encryption is provided, allowing all data and the operating systems to be encrypted, in accordance with Government standards for data protection. Boot-time authentication is provided, using the CESG LOGFIRE algorithm. Optional token-based secondary authentication is supported using a range of smartcards and USB tokens. Following user authentication, encryption is transparent, and the user needs to take no further action. All data written to disk is automatically encrypted using AES. Removable device support includes Memory sticks, USB drives, and Firewire drives. The product support multiple users per machine, and options are provided to support secure key delivery and auditing. Installation is via a standard Windows MSI, Windows 2000, Windows XP and MS Vista are supported.

Version: v3.1 (Build 3.1.1.38), v3.2.1, v3.3, v3.3.1, v3.3.2

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0) 845 838 2050
Fax: +44 (0) 845 838 2060
Email: sales@becrypt.com
URL: www.becrypt.com

BeCrypt DISK Protect Enhanced

Cryptographic Grade: Enhanced

DISK Protect Enhanced is a highly secure, CESG accredited, software solution that provides transparent, total disk encryption of a hard disk or disks for Personal Computers. The product also provides access control to the PC itself and to the removable drives (e.g. floppy disk) supported by the PC.

DISK Protect Enhanced has been developed under the CAPS scheme to provide security assurance coupled with reduced physical handling requirements for PCs containing Protectively Marked information. DISK Protect Enhanced is designed to protect against data compromise due to theft or loss of the computer.

Total disk encryption ensures ALL data, including system and page files are automatically encrypted and decrypted transparently, so the user is assured that information is protected at all times.

Access control is provided by means of a user name, user password and personalised cryptographic token. The token is read via a USB port reader. All key material is supplied by CESG.

DISK Protect Enhanced may be configured to satisfy any local security policy by means of an easy-to-use Administration Tool, which provides full on-line help. The product supports up to four users, with privileges being configurable on an individual basis.

Notes

- DISK Protect Enhanced will reduce the Protective Marking of a laptop (when powered off) as follows.
- TOP SECRET to SECRET, SECTRET to RESTRICTED, CONFIDENTIAL/RESTRICTED to UNCLASSIFIED
- Disk Protect Enhanced is available for Windows 2000 and Windows XP

Version: v3.03, v3.04, v3.05

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0) 845 838 2050
Fax: +44 (0) 845 838 2060
Email: sales@becrypt.com
URL: www.becrypt.com

SECTION 6

Data Encryption

BeCrypt Media Client

Cryptographic Grade: Baseline

BeCrypt Media Client enables the transfers of data on CD, USB media and flash using file encryption. The solution can ensure the integrity of data and enable secure sharing with authorised third parties.

Version: v1.0, v2.0

BeCrypt Ltd
90 Long Acre, Covent Garden, London, WC2E 9RA
Telephone: +44 (0) 845 838 2050
Fax: +44 (0) 845 838 2060
Email: sales@becrypt.com
URL: www.becrypt.com

Datacryptor Model 3

Cryptographic Grade: High Grade Top Secret IN EVALUATION

The Thales Datacryptor Model 3 is a High Grade encryption platform to protect classified information in high-speed private or public networks. Datacryptor Model 3 will initially be available as a High Grade Top Secret IPv4 Encryptor, at 100Mbps or 1Gbps. Datacryptor Model 3 is expected to be approved for Reverse tunnelling.

Notes:

Datacryptor Model 3 will be soft upgradeable to HAIPIS version 3 and above. Including IPv6. A link version is also in development.

Thales e-Security
Meadow View House, Crendon Industrial Estate, Long Crendon,
Aylesbury, Bucks, HP18 9EQ, United Kingdom
Point of Contact Rob Stubbs
Telephone: +44 (0) 1844 201 800
Fax: +44 (0) 1844 201 570
Email: rob.stubbs@thales-esecurity.com
URL: www.thales-esecurity.com

SECTION 6

Data Encryption

Eclypt Baseline

Cryptographic Grade: Baseline

Eclypt Baseline secures CONFIDENTIAL or RESTRICTED data via one 15-character Clearview password. All CONFIDENTIL data saved to an Eclypt Baseline drive is reduced to RESTRICTED when the computer is powered off or the drive unplugged. RESTRICTED data is reduced to NOT PROTECTIVELY (NPM). The product has a lifetime Key.

Eclypt Baseline Drives are available in two variants:

- Internal Eclypt
  - Drive Direct replacement for the existing hard disk
  - Easily retro-fitted or available factory fitted
  - Available in both SATA and PATA variants
  - Available in both Rotating (HDD) and Solid State (SDD) Variants
- External USB Drive (Freedom)
  - Quick "plug & play" USB connectivity
  - Data can be securely backed up or transported
  - Available in both Rotating (HDD) and Solid State (SDD) Variants
- Protect every single sector with 256-bit AES encryption
- Store no Plain Text
- Compatible with all operating systems, applications and patches
- Support imaging, partitioning and diagnostic applications
- Support multiple users (up to 128)
- Require no ongoing maintenance and, following authentication, are transparent to the user
- Life time key, there is no need to change the key
- Requires no specialist IT knowledge
- Encrypts and decrypts data transparently and with no noticeable effect on the computer performance

Elcypt Technology integrates sophisticated authentication, entire disk encryption and data storage into tamper-resistant hardware that safeguards data. This provides instant data protection without any adverse performance degradation. Data is protected even if lost or stolen.

Eclypt Baseline reduces RESTRICTED to NOT PROTECTIVELY MARKED.

Notes:

The following Security Procedures also apply to v3.3: Eclypt HMG Issue no 2.0, January 2010. This docurment can be requested from enquiries@cesg.gsi.gov.uk or the CESG Information Assurance Portfolio (IAP) website.

Version: v3.1, v3.2, v3.3

Stonewood Electronics Limited

Sandford Lane, Wareham, Dorset, BH20 4DY United Kingdom

Point of Contact Jayde Oakley

Telephone: +44 (0) 1929 554 400

Fax: +44 (0) 1929 552 525

Email: jayde.oakley@stonewood.co.uk

URL: www.eclypt.com

www.stonewood.co.uk

Eclypt Baseline Plus

Cryptographic Grade: Baseline

Eclypt Baseline Plus secures CONFIDENIAL or RESTRICTED data via one 15-character Clearview password.CONFIDENTIAL data saved to an Eclypt Baseline Plus drive is reduced to RESTRICTEd when the computer is powered off or the drive unplugged. RESTRICTED data is reduced to NOT PROTECTIVELY MARKED. This product has a lifetime Key

.

Eclypt Baseline Plus Drives are available in two variants:

- Internal Eclypt Drive
  - Direct replacement for the existing hard disk
  - Easily retro-fitted or available factory fitted
  - Available in both SATA and PATA variants
  - Available in both Rotating (HDD) and Solid State (SDD) variants
- External USB Drive (Freedom)
  - Quick "plug & play" USB connectivity
  - Data can be securely backed up or transported
  - Available in both Rotating (HDD) and Solid State (SDD) Variants
- Protect every single sector with 256-bit AES encryption
- Store no Plain Text
- Compatible with all operating systems, applications and patches
- Support imaging, partitioning and diagnostic applications
- Support multiple users (up to 128)
- Require no ongoing maintenance and, following authentication, are transparent to the user
- Life time key, there is no need to change the key
- Requires no ongoing maintenance and no specialist IT knowledge
- Encrypts and decrypts data transparently and with no noticeable effect on the computer performance

Elcypt Technology integrates sophisticated authentication, entire disk encryption and data storage into tamper-resistant hardware that safeguards data. This provides instant data protection without any adverse performance degradation. Data is protected even if lost or stolen.

Eclypt Baseline Plus reduces CONFIDENTIAL to RESTRICTED and RESTRICTED to NOT PROTECTIVELY MARKED.

Notes:

The following Security Procedures also apply to v3.3:Eclypt HMG Issue No 2.0, January 2010. This document can be requested from enquiries@cesg.gsi.gov.uk or the CESG Information Assurance Portfolio (IAP) website.

Version: v3.1, v3.2, v3.3

Stonewood Electronics Limited

Sandford Lane, Wareham, Dorset, BH20 4DY United Kingdom

Point of Contact Jayde Oakley

Telephone: +44 (0) 1929 554 400

Fax: +44 (0) 1929 552 525

Email: jayde.oakley@stonewood.co.uk

URL: www.ecypt.com

www.stonewood.co.uk

SECTION 6

Data Encryption

Eclypt Enhanced

Cryptographic Grade: Enhanced

Eclypt Enhanced secures Top Secret data via a Touch-Memory-Token and one Clearview password. Data saved to an Eclypt Enhanced drive is reduced by two levels when the computer is powered off or the drive unplugged. TOP SECRET data is reduced to CONFIDENTIAL, SECRET data to RESTRICTED, CONFIDENTIAL data to NOT PROTECTIVELY MARKED (NPM) and RESTRICTED data to NPM. This product has a lifetime key.

.

Eclypt Enhanced Drives are available in two variants:

- Internal Eclypt Drive
  - Direct replacement for the existing hard disk
  - Easily retro-fitted or available factory fitted
  - Available in both SATA and PATA variants
  - Available in both Rotating (HDD) and Solid State (SDD) variants
- External USB Drive (Freedom)
  - Quick "plug & play" USB connectivity
  - Data can be securely backed up or transported
  - Available in both Rotating (HDD) and Solid State (SDD) Variants
- Protect every single sector with 256-bit AES encryption
- Store no Plain Text
- Compatible with all operating systems, applications and patches
- Support imaging, partitioning and diagnostic applications
- Support multiple users (up to 128)
- Life time key, there is no need to change the key
- Requires no ongoing maintenance and no specialist IT knowledge
- Encrypts and decrypts data transparently and with no noticeable effect on the computer performance

Elcypt Technology integrates sophisticated authentication, entire disk encryption and data storage into tamper-resistant hardware that safeguards data. Data is protected even if lost or stolen.

Eclypt Enhanced reduces Protective Marking by two levels i.e. TOP SECRET to CONFIDENTIAL, SECRET to RESTRICTED, CONFIDENTIAL and RESTRICTED to NOT PROTECTIVELY MARKED.

Stonewood Electronics Limited
Sandford Lane, Wareham, Dorset, BH20 4DY United Kingdom
Point of Contact Jayde Oakley
Telephone: +44 (0) 1929 554 400
Fax: +44 (0) 1929 552 525
Email: jayde.oakley@stonewood.co.uk
URL: www.eclypt.com
www.stonewood.co.uk

Flagstone Baseline

Cryptographic Grade: See notes

Flagstone Baseline secures RESTRICTED data via a 9-character Clearview password. All data saved to a Flagstone Baseline drive is reduced to NPM when the computer is shut down. This product has a 5 year Key life.

Flagstone Drives:

- Protect every single sector with 128-bit AES encryption
- Store no Plain Text
- Are secure, robust and compatible with all operating systems, applications and patches
- Support imaging, partitioning and diagnostic applications
- Are intended as a direct Hard Disk Drive replacement for all computers
- Are available in both SATA and PATA variants
- Can be easily retro-fitted and are available factory fitted
- Require no ongoing maintenance and, following authentication, are transparent to the user

Flagstone Technology integrates sophisticated authentication, entire disk encryption and data storage into temper-resistant hardware that safeguard data. This provides instant data protection without any adverse performance degradation. Data is protected even if lost or stolen.

Notes: Flagstone Baseline is approved to reduce RESTRICTED to NOT PROTECTIVELY MARKED.

The Flagstone range is approaching end-of-life and should not be used for new projects. New projects should use the Eclypt range, which is based on the established Flagstone technology. For details, please see the entries for Eclypt is available as an internal hard drive and also as a range of USB connected storage products, see www.stonewood.co.uk

Version 1.10

Stonewood Electronics Limited
Sandford Lane, Wareham, Dorset, BH20 4DY United Kingdom
Point of Contact Robert Palmer
Telephone: +44 (0) 1929 554 400
Fax: +44 (0) 1929 552 525
Email: rpalmer@stonewood.co.uk
URL: www.flagstonesecure.co.uk
www.stonewood.co.uk

SECTION 6

Data Encryption

Flagstone Baseline Plus

Cryptographic Grade: High Grade Top Secret

Flagstone Baseline Plus secures CONFIDENTIAL and RESTRICTED data via a 9-character Clearview password. Confidential data saved to a Flagstone Baseline Plus drive is reduced to RESTRICTED when the computer is shut down. RESTRICTED data is reduced to NPM. This product has a 5 year Key life.

Flagstone Drives:

- Protect every single sector with 128-bit AES encryption
- Store no Plain Text
- Are secure, robust and compatible with all operating systems, applications and patches
- Support imaging, partitioning and diagnostic applications
- Are intended as a direct Hard Disk Drive replacement for all computers
- Are available in both SATA and PATA variants
- Can be easily retro-fitted and are available factory fitted
- Require no ongoing maintenance and, following authentication, are transparent to the user

Flagstone Technology integrates sophisticated authentication, entire disk encryption and data storage into temper-resistant hardware that safeguard data. This provides instant data protection without any adverse performance degradation. Data is protected even if lost or stolen.

Notes: Flagstone Baseline Plus is approved to reduce CONFIDENTIAL to RESTRICTED and RESTRICTED to NOT PROTECTIVELY MARKED.

The Flagstone range is approaching end-of-life and should not be used for new projects. New projects should use the Eclypt range, which is based on the established Flagstone technology. For details, please see the entries for Eclypt is available as an internal hard drive and also as a range of USB connected storage products, see www.stonewood.co.uk

Version 1.10

Stonewood Electronics Limited
Sandford Lane, Wareham, Dorset, BH20 4DY United Kingdom
Point of Contact Robert Palmer
Telephone: +44 (0) 1929 554 400
Fax: +44 (0) 1929 552 525
Email: rpalmer@stonewood.co.uk
URL: www.flagstonesecure.co.uk
www.stonewood.co.uk

Flagstone Enhanced

Cryptographic Grade: See notes

Flagstone Enhanced secures up to TOP SECRET data via one Touch Memory-Token and one Clearview password. Data saved to a Flagstone Enhanced drive is reduced by two levels when the computer is shut down. TOP SECRET is reduced to CONFIDENTIAL, SECRST data to RESTRICTED, CONFIDENTIAL data to NPM and RESTRICTED data to NPM. This product has a lifetime Key.

Flagstone Drives:

- Protect every single sector with 128-bit AES encryption
- Store no Plain Text
- Are secure, robust and compatible with all operating systems, applications and patches
- Support imaging, partitioning and diagnostic applications
- Are intended as a direct Hard Disk Drive replacement for all computers
- Are available in both SATA and PATA variants
- Can be easily retro-fitted and are available factory fitted
- Require no ongoing maintenance and, following authentication, are transparent to the user

Flagstone Technology integrates sophisticated authentication, entire disk encryption and data storage into temper-resistant hardware that safeguard data. This provides instant data protection without any adverse performance degradation. Data is protected even if lost or stolen.

Notes: Flagstone Enhanced reduces Protective Marking by two levels i.e. TOP SECRET to CONFIDENTIAL, SECRET to RESTRICTED, CONFIDENTIAL and RESTRICTED to NOT PROTECTIVELY MARKED.

The Flagstone range is approaching end-of-life and should not be used for new projects. New projects should use the Eclypt range, which is based on the established Flagstone technology. For details, please see the entries for Eclypt is available as an internal hard drive and also as a range of USB connected storage products, see www.stonewood.co.uk

Version 1.10

Stonewood Electronics Limited
Sandford Lane, Wareham, Dorset, BH20 4DY United Kingdom
Point of Contact Robert Palmer
Telephone: +44 (0) 1929 554 400
Fax: +44 (0) 1929 552 525
Email: rpalmer@stonewood.co.uk
URL: www.flagstonesecure.co.uk
www.stonewood.co.uk

SECTION 6

Data Encryption

MessageLabs Policy Based Encryption Service

CCTM Certificate 2009/07/0048

Awarded 6th July 2009 Valid until 5th July 2011

MessageLabs Policy Based Encryption service enables an administrator to create flexible rules for the encryption of outbound emails, preventing the loss of confidential data through both accidental or deliberate emailing activity and facilitating regulatory compliance. Recipients can access encrypted emails in their inbox or retrieve them from a secure web portal without requiring any specific knowledge or tools.

The service can be enhanced by incorporating MessageLabs Anti-Virus scanning service which will protect the network from Malware attacks such as viruses, worms, Trojans and phishing. With 99.995% availability and best of breed FIPS 140 – 2 certified Identity Based Encryption engine, the service is run in secure data centres on multiple site to ensure continuous availability in the event of a disaster.

MessageLabs Ltd
1240 Lansdown Court, 3 Gloucester Business Park, Gloucester, GL3 4AB, United Kingdom
Telephone: +44 (0) 1452 627 627
Email: info@messagelabs.com
URL: www.messagelabs.com

MXI Stealth M600

Cryptographic Grade: Baseline

MXI Security's Stealth M600 encrypted USB Security device is a fully managed AES hardware encrypted USB drive providing a secure mechanism for the storage and transfer of data without the need for installation of drivers or special privileges. Its hardware-based security , strong password authentication and advanced management functionality ensure the enforcement of CESG approved authentication methods to protect valuable data and identity credentials.

Version: v1..0.0.9

MXI Security: A Division of Memory Experts International
Saracen House, Swan Street, Old Isleworth, Middlesex, TW7 6RJ, United Kingdom
Point of Contact Simon Roe
Telephone: +44 (0) 208 758 9600
Fax: +44 (0) 208 758 9601
Email: sroe@mxisecurity.com
URL: www.mxisecurity.com

SECTION 6

Data Encryption

PGP Desktop

Cryptographic Grade: Baseline IN EVALUATION

PGP Desktop contains a suite of encryption utilities. The CESG evaluation covers PGP Email, which provides encrypted email, and PGP Zip, which provides file encryption. Automatic email encryption is provided, as well as manual creation of an encrypted archive for transfer to removable media. Messages and archives can also be signed to provide source authentication. Policy Management can be provided by use of PGP Universal Server.

Notes: PGP Desktop is supported on Windows 2000 (Service Pack 4), Windows Server 2003 (service Pack 1), Windows XP (Service Pack 1 and 2), Windows Vista (all 32-bit and 64-bit versions) and Windows XP Tablet PC Edition 2005 (requires attached keyboard).

Version: v9.9

350 Brook Drive, Green Park, Reading, Berks RG2 6UH, United Kingdom
Point of Contact: Dave Barnett
Telephone: +44 (0) 208 606 6024
Fax: +44 (0) 208 610 6860
Email: CESG@pgp.com
URL: www.pgp.com

PGP Whole Disk Encryption

Cryptographic Grade: Baseline

PGP Whole Disk Encryption locks down the entire contents of a laptop or desktop hard disk, including boot sectors, system and swap files. Full volume encryption is provided, which allows the encryption of the operating system and all data, in accordance with HMG Standards for data protection. Boot time authentication is provided, once booted, encryption and decryption are transparent to the user. All data written to disk is encrypted using AES.

PGP Whole Disk Encryption protects the confidentiality of data at rest from compromise due to theft or loss of the computer. PGP Whole Disk Encryption software is approved to CESG Baseline Grade for total disk encryption of a hard disk for IBM compatible Personal Computers running the following systems:

- Microsoft Windows XP Professional 32-bit (Service Pack 1, 2, and 3)
- Microsoft Windows XP Professional 64-bit (Service Pack 1 and 2).
- Microsoft Windows XP Professional Tablet PC Edition 2005 (requires attached keyboard)
- Microsoft Windows XP Home
- Microsoft Windows 2000 Professional (Service Pack 4)

Notes

Please note Removable Media Encryption (e.g. encryption of floppies, USB Flash sticks, USB hard disks etc) will not be evaluated or approved as part of this first CAPS certificate. It will be evaluated as part of the second evaluation "PGP Desktop".

Version: Whole Disk Encryption Version 9.9 (build 456) PGP CAPS Activation Package Version 9.9.0

350 Brook Drive, Green Park, Reading, Berks RG2 6UH, United Kingdom
Point of Contact: Dave Barnett
Telephone: +44 (0) 208 606 6024
Fax: +44 (0) 208 610 6860
Email: CESG@pgp.com
URL: www.pgp.com

SECTION 7

Data Erasure

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

ITSEC/CC
Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

CCTM
CESG Claims Tested Mark

Prospective purchasers of CCT Mark approved products or services should read both the ICD and Test Report documents available from the CCT Mark website, to ensure the product or service is appropriate for their needs.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 7

Data Erasure

The guidance for the reuse of disposal of computer storage media is detailed in HMG Infosec Standard No.5, Secure Sanitisation of Protectively Marked Information or Sensitive Information – Issue 2.0, September 2007 (ISS), and CESG Manual S, - Guidance on Secure Sanitisation and Disposal – Issue 2.0, September 2007. These set out the standards for secure data erasure on magnetic, semiconductors and optical media by overwriting and degaussing. All previously approved under SEAP 8500 will now be subject to the IS5 standards.

Also refer to the Common Criteria products section for Data Erasure products that have been certified EAL1/EAL2, refer to IS5 for equivalences to erasure levels.

Secure Overwriting

The secure overwriting of magnetic storage media will either involve clearing, where the media is to be re-used and retains its original highest Protective Marking, or purging where the media is DECLASSIFIED prior to disposal.

Overwriting Products – Lower and High level

Revisions to both IS5 and Manual S have resulted in there being two Overwriting Standard levels, Lower and Higher. Products compliant with these levels offer protection to various degrees, depending on the operational requirements and media type. Readers should refer to IS5 for details. Products will be listed indicating the Overwriting Standard level they are approved to; where these are listed as Baseline or Enhanced, this refers to the previous ISS and Manual S levels.

Degaussing Products

There are two Degaussing Standard levels, Lower and Higher Products listed as approved to Baseline or Enhanced levels, derived from IS5 Issue 1 and Manual S Issue 1, or SEAP 8500 approved, are now retesting to meet the new higher level.

SECTION 7

Data Erasure

Blancco Data Cleaner Version3.3r7 HMG, & Version 3.7r1 HMG

Enhanced | Certificate: January 2003

Blancco Data Cleaner (BDC) is run from a CD or floppy disk so there is no need for installed Windows or DOS operating system. There is auto detection of both ATA/IDE and SCSI hard drives. Individual hard drives and partitions can be selected for data erasure and the user can define 1,3 and 7 overwrites. BDC generates a report that includes:

- Detailed hardware configuration analysis
- Computer name, model and serial number
- Processor (manufacture, model, speed)
- Memory (manufacture, model, speed)
- Hard Drive(s) (manufacture, model, speed, serial number)
- Network device (manufacture, model, speed)

System Requirements:

- IDE or SCSI hard drive
- IBM compatible PC
- 486DX processor (or better)
- 8MB RAM memory, 16 MB recommended
- Booting 1.44 MB diskette drive
- VGA support (running at least 16 colours or better)

Notes

Blancco Data Cleaner v3.3r7 HMG & v3.7r1 HMG are approved at both Baseline and Enhanced Overwriting Standards (refer to HMG Infosec Standard 5).

Blancco Data Cleaner v3.3r7 HMG & v3.7r1 HMG are approved for UK Government use.

Blancco UK
7th Floor, Northway House, 1379 High Road, Whetstone, London, N20 9LP, United Kingdom
Point of Contact Tony Collis
Telephone: +44 (0) 20 8492 3563
Fax: +44 (0) 20 8592 0110
Email: tony.collies@blancco.com
URL: www.blancco.com

Blancco Data Cleaner+ Version 4.5 HMG

Enhanced | Certificate: April 2006

Blancco Data Cleaner+ 4.5 HMG permanently wipes all data from a hard drive up to CONFIDENTIAL, RESTRICTED, SECRET and TOP SECRET level. The software is tailored for desktop, laptop and also for server environments with RAID systems. It will overwrite data from any size of ATA/IDE/SCSI/USB/SATA and FireWire disks. In addition, the software erases all hidden/locked areas on a hard disk such as DCO, HPA and remapped sectors. Enhanced hard disk support guarantees high-speed erasure of 4 HDD per computer. The software can be delivered to the target computer via different media: network, floppy, CD preinstall. Data erased by Blancco Data Cleaner+ HMG cannot be recovered with any existing technology. Once the hard disk(s) are cleaned, the software automatically generates a detailed erasure report with Hardware Asset. Management information that meets and exceeds governmental regulatory requirements. The whole erasure process is digitally protected with MD% protection and a complete verification module for confirming that the data erasure and Hardware Asset Management report is also protected with digital signature in order to prevent report tampering.

Notes

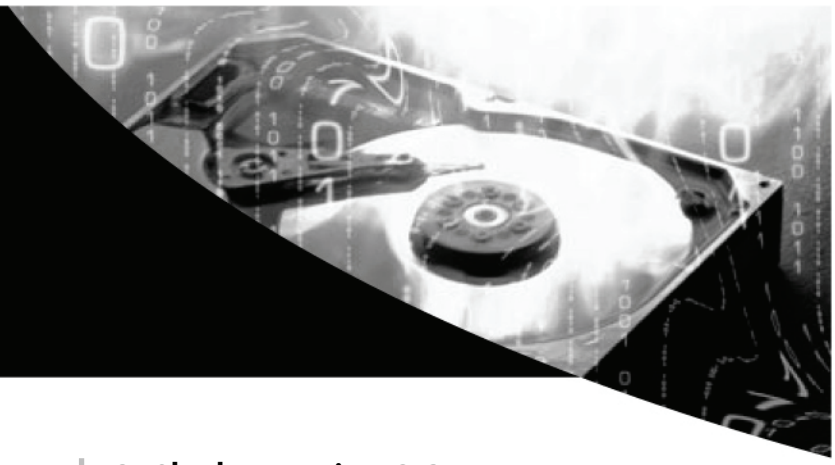
Blancco Data Cleaner+ c4.5 HMG is approved at both Baseline and Enhanced Overwriting Standards (refer to HMG Infosec Standard 5)

Blancco Data Cleaner+ v4.5 HMG is approved to UK Government use.-

Blancco UK
7th Floor, Northway House, 1379 High Road, Whetstone, London, N20 9LP, United Kingdom
Point of Contact Tony Collis
Telephone: +44 (0) 20 8492 3563
Fax: +44 (0) 20 8592 0110
Email: tony.collies@blancco.com
URL: www.blancco.com

SECTION 7

Data Erasure



Blancco Version 4.8 HMG

Enhanced — Certificate: November 2008

Blancco 4.8 HMG permanently wipes all data from a hard disk up to CONFIDENTIAL, RESTRICTED, SECRET and TOP SECRET levels. The software is tailored for desktops, laptops and also for server environments with RAID systems. It will overwrite data from any size of ATA/IDE/SCSI/USB/SATA Fiber Channel and FireWire disks. In addition, the software erases all hidden/locked areas on a hard disk such as DCO, HPA and remapped sectors. Enhanced hard disk support guarantees high-speed simultaneous erasure of 4 HDD per computer via different media: network, floppy, CD, USB and preinstall Data erased by Blancc0 4.8 HMG cannot be recovered with any existing technology. Once the hard disk(s) are cleaned, the software automatically generates a detailed erasure report with Hardware Asset Management information that meets and exceeds government regulatory requirements. The whole erasure process is digitally protected with MD5 protection and a complete verification module for confirming that the data has been securely and fully erased form the hard drive. The data erasure and Hardware Asset Management report is also protected with digital signature in order to prevent report tampering.

Blancco 4.8 HMG is approved at both Lower and Higher Overwriting Standards (refer to HMG Infosec Standard 5) Blancco 4.8 HMG is approved for UK Government.

Blancco UK
7th Floor, Northway House, 1379 High Road, Whetstone, London, N20 9LP, United Kingdom
Point of Contact Tony Collis
Telephone: +44 (0) 20 8492 3563
Fax: +44 (0) 20 8592 0110
Email: tony.collies@blancco.com
URL: www.blancco.com

DESlock+ Version 3.2.7

CCTM — Certificate: 2008/05/0036
Awarded 13th May 2008 — Valid until 12th May 2010

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.

Data Encryption Systems Ltd
Silver St House, Silver St, Taunton, Somerset, TA1 3DL, United Kingdom
Telephone: +44 (0) 1823 352 357
Email: sale@deslock.com
URL: www.deslock.com

SECTION 7

Data Erasure

Hard Disk Magnetic Crusher HC-3000

CCTM	Certificate: 2007/06/0021
Awarded 13th June 2007	Valid until 12th June 2009

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.

Future Technology Industry Limited
Asmec Centre, Eagle House, The Ring Bracknell, Berks, RG12 1HB
United Kingdom
Telephone: +44 (0) 1344 382 100
Email: info@futuretechonogyindustry.com
URL: www.futuretechnologyindustry.com

Hard Disk Magnetic Crusher HC-7800

CCTM	Certificate: 2007/08/0025
Awarded 6th August 2007	Valid until 5th August 2010

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-7800 is a high-power magnetic 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.

Future Technology Industry Limited
Asmec Centre, Eagle House, The Ring Bracknell, Berks, RG12 1HB
United Kingdom
Telephone: +44 (0) 1344 382 100
Email: info@futuretechonogyindustry.com
URL: www.futuretechnologyindustry.com

SECTION 7

Data Erasure

Hard Disk Magnetic Crusher COMBO

CCTM	Certificate: 2007/06/0022
Awarded 13th June 2007	Valid until 12th June 2009

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.

Future Technology Industry Limited
Asmec Centre, Eagle House, The Ring Bracknell, Berks, RG12 1HB
United Kingdom
Telephone: +44 (0) 1344 382 100
Email: info@futuretechonogyindustry.com
URL: www.futuretechnologyindustry.com

IBAS ExpertEraser Version 2.2.0

Enhanced	Certificate: October 2004

IBAS ExpertEraser can be used on any type of hard disk, and is the first approved product that supports ATA6/\LBA48, enabling the secure erasure of hard disks over 137Gb. It also erases SCSI hard drives in a new advanced mode for erasing information added to the grown defect list. A tamper proof erasure certificate is automatically generated the guarantees that all information is securely erased.

- Auto-detection of both ATA.IDE and SCSI hard disk
- Operates directly on the hard disk (bypasses BIOS and OS)
- Menu driven application with context sensitive help
- Refill of erasures through Internet
- Media analysis for erasure verification
- Automatic report generation
- Built in full featured text editor
- Built in system for quality control and traceability
- Sector viewer for visual inspection of overwrites
- Command Line Options
- Display of time remaining

System Requirements:

- IBM compatible PC with i386 processor or better
- 1.44MB floppy or CD-ROM drive
- 640KB RAM

Notes

IBAS ExpertEraser is approved at Baseline and Enhanced Overwriting Standard. (Refer HMG Infosec Standard 5).

IBAS ExpertEraser 2.2.0 is approved for UK Government use.

IBAS UK Limited
Stone Castle, London Road, Greenhithe, Kent, DA9 9JG,
United Kingdom
Point of Contact: IBAS UK Limited
Telephone: +44 (0) 8000 524 173
Fax: +44 (0) 1322 303 033
URL: www.ibasuk.com

SECTION 7

Data Erasure

Kroll Ontrack DataEraser Version 2.0

Enhanced

DataEraser overwrites all data including partitions, folders, directories, files, file tables, dynamic drive overlays and boot record information.

DataEraser creates a self-bootable diskette that runs independently of the operating system allowing use on all IBM compatible PCs and all operating systems.

DataEraser will overwrite both ATA/IDE and SCIS drives either several overwrite options.

Set number of overwrite passes (single overwrite pass, triple overwrite pass and user-defined number (1-99) of overwrite passes).

Select desired overwriting pattern or choose default pattern. DataEraser has either a complete verification or a quick verification, and also produces a Validation Certificate that includes the drive model, serial number and a report of any bad blocks that could not be overwritten.

Kroll Ontrack UK

The Pavillions, 1 Weston Road, Kiln Lane, Epsom, Surrey, KT17 1JG

United Kingdom

Telephone: +44 (0) 1372 741 999

Fax: +44 (0) 1372 741 441

Email: licence@ontrack.co.uk

URL: www.Ontrackdatarecovery.co.uk

Kroll Onrack Eraser Version 3.0

Enhanced Certificate: January 2008

Kroll Ontrack® Eraser is an easy-to-use, highly flexible data erasure software tool that erases all data stored on a targeted media – ensuring that sensitive information does not fall into wrong hands.

- Auto-detection of both IDE/ATA.SATA and SCSI hard disks
- Designed to overwrite USB, FireWire and Solid State media
- Operates directly on the hard disk (bypasses BIOS and OS)
- Menu driven application with context sensitive help
- Overwrites all data on targeted storage devices and platforms detailed in User Guide using proven, customisable overwriting procedures
- Includes flexible reporting features to help you guarantee that all data have been overwritten
- Runs over servers or on individual PCs
- Offer flexible licensing models, fast installation and simple configuration.

Notes:

Kroll Ontrack Eraser Version 3.0 is approved at the lower Level and the Higher Level Overwriting Standards (refer to HMG Infosec Standard 5).

Kroll Ontrack Eraser Version 3.0 is approved for UK Government use (Refer to the CESG Approved statement for further advice.)

Minimum System requirements

- IBM-compatible PC within a Pentium or greater processor
- VGA 800x600 or greater graphics capability (VESA compatibility)
- RAM: CD/DVD boot 64MB, USB, PXE and RIS (WDS) 128MB
- Disk space 200MB of free hard disk space on the Network Server.

Kroll Ontrack UK

The Pavillions, 1 Weston Road, Kiln Lane, Epsom, Surrey, KT17 1JG

United Kingdom

Telephone: +44 (0) 1372 741 999

Fax: +44 (0) 1372 741 441

Email: licence@ontrack.co.uk

URL: www.Ontrackdatarecovery.co.uk

SECTION 7

Data Erasure

Managed Service for Secure Destruction of Data on Magnetic Media Version 1.0

CCTM Certificate: 2008/11/0038

Awarded 28th November 2007 Valid until 27th November 2009

Barron McCann's Secure 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 (IL6) HMG Top Secret. The service offer as data destruction service that ensures data stored on magnetic media such as hard drives and tape is destroyed before the equipment i.e. recycled. Our service allows your organisation to meet both your WEEE and Data Protection Act legal responsibilities.

When carrying out the service we fellow all relevant security standards in data destruction using CESG approved equipment backed by the CESG Claim Tested Mark with full compliance to HMG IS5 and CESG Manual S.

The service is offered off-site at our secure List-X data destruction facility for Media of up to and including 9IL3) Restricted or we can carry out the service at your location anywhere in the UK. All of our data destruction engineers hold at least SC Clearances.

Barron McCann Technology Limited

Bemac House, Fifth Avenue, Letchworth Garden City, Hertfordshire SG6 2HF, United Kingdom

Telephone: +44 (0) 1462 482 333

Email: securedataservices@bemac.com

URL: www.bemac.com

Secure Destruction of Data on Hard Drives and Magnetic Storage Media Version 1.0

CCTM Certificate: 2008/09/0037

Awarded 11th November 2007 Valid until 10th September 2009

Our service helps ensure that your organisation is not at risk from a breach of data classified as HMG RESTRICTED or below.

It helps protect your reputation and reduces the legal and financial risks that could result from an incident of data loss or unauthorised disclosure.

The service is provided on site at your premises. It lets you witness that your sensitive data is eliminated from hard drives and magnetic storage media before any IT equipment leaves your control. It is carried out under your supervision and at a time convenient to you.

The process uses CESG approved degaussing equipment. It is fully auditable and certificates of destruction are issued. It facilitates compliance with UK and EU Data Protection and Environment Recycling regulations (WEEE) and the USA's Sarbanes Oxley Act.

The service is not suitable for material with a protective marking of HMG CONFIDENTIAL or above.

Data Eliminate Limited

53 Balham Grove, London, SW12 8AZ, United Kingdom

Telephone: +44 (0) 845 1234 400

Email: licence@ontrack.co.uk

URL: www.Ontrackdatarecovery.co.uk

SECTION 7

Data Erasure

Ultra Erase Version 1.44 HMG

Enhanced

UltraErase Version 1.44HMG is a platform independent, secure high speed multi interface erasure system running on the ULTRA80 SEEP (Secure-Environment-Erasure-Platform). Designed purely for advanced secure, permanent and auditable sanitisation of CONFIDENTIAL, RESTTICTED, SECRET and TOP SECRET (IL6) data. Once the user data has been erased a certificate of erasure can be printed or stored for archival purpose.

- Easy to use graphical user interface
- Auto – detection of IDE/ATA/PATA/SATA/ SAS and SCSI hard disks
- Erasure at maximum supported data rates.
- Direct "low level" communication with hardware to be erased (Bypass B.I.O.S)
- Complex HPA/DCO detection with unique "End-Stop" algorithm
- Reporting of remapped sectors
- Simultaneous sanitisation of up to 80 disks drives
- Certificates are time stamped and digitally protected.

Notes

UltraErase Version 1.44 HMG is approved at the Lower Level and the Higher Level Overwriting Standards (refer to HMG Infosec Standard 5).

UltraErase Version 1.44 HMG is approved for UK Government use. (Refer to the CESG approved statement for further advice.)

Ultratect Limited

Ultratec House, 3 The Orbital Centre, Icknield Way, Letchworth Garden City, Herts, SG6 1ET, United Kingdom

Point of Contact: Bill Osborne

Telephone: +44 (0) 1462 4900 082 ext x348

Fax: +44 (0) 1462 490 083

Email: Bill.Osbourne@Ultrarec.co.uk

dataerasure@ultratec.co.uk

URL: www.ultratec.co.uk

Verity SV5000 Degausser

Enhanced

For volume erasure of high-density metal tape and cassettes the SV5000's performance will satisfy the requirements. Automatically controlled by an electric eye, the reels, disks or cassettes are placed on the wide conveyor belt where they are transported through the 4000Gauss field.

Up to five thousand diskette or five hundred VHS cassette can be erased per hour. The SV5000 has been specifically designed to meet exacting performance criteria demanded and expected by security operations requiring safe, effective and secure management of their magnetic media.

- Media Erased: Reels ¼", ½" and !" formats
- Maximum diameter 10½"
- Cassette: all formats
- Cartridges: all formats

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Verity SV5000 degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The SV5000 is subject to S(E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The SV5000 may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Verity Systems Limited

Verity House, 2 Eastern Road, Aldershot, Hampshire, GU12 4TD, United Kingdom

Telephone: +44 (0) 1252 317 000

Fax: +44 (0) 1252 316 555

URL: www.veritysystem.com

SECTION 7

Data Erasure

Verity SV90 Degausser

Enhanced

The SV90 is able to perform automatic erasure of high-density magnetic media achieved by applying a highly focused magnetic field.

The Sv90 can cope with a range of media including tapes of up to 16 inches diameter. Up to fifty reels or two hundred cassettes can be efficiently and quietly erased per hour, the Sv90 operates continuously and is quiet, cool and efficient.

- Media Erased: Reels ½" and 1" NAB (16" max), Adapters required for ¼" NAB, ½" IBM and ¼" DIN, for 2" tapes only special SV90/2 is required
- Cassettes: carriages available for Beta SP, digital Betacam, MII, VHS, R-Data 8mm, U-matic, Betcam 3480, TK50, 75, 85, DC600,
- DC1000.

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Verity SV90 degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The SV90 is subject to S(E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The SV90 may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Verity Systems Limited
Verity House, 2 Eastern Road, Aldershot, Hampshire, GU12 4TD,
United Kingdom
Telephone: +44 (0) 1252 317 000
Fax: +44 (0) 1252 316 555
URL: www.veritysystem.com

Verity SV91M Degausser

Enhanced

Designed to erase a range of magnetic media including high-density metal tapes and cassettes, the Verity System SV91M meets the requirements. The SV91M takes ten seconds to completely erase a cassette. It's simple-to-use and compact table top operation provides a thoroughly effective and low cost means of degaussing BETCAM sp, d2, mii, Data, 8mm and other high coercivity tapes

- Media Erased: Broadcast and video cassette –All oxide and metal particle
- Reels: All formats up to 16" diameter including 2" Pancakes up to 16" diameter
- Data: All computer backup cartridges, computer reels, diskettes – single /boxed PC hard drives.

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Verity SV91M degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The SV91M is subject to S(E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The SV91M may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Verity Systems Limited
Verity House, 2 Eastern Road, Aldershot, Hampshire, GU12 4TD,
United Kingdom
Telephone: +44 (0) 1252 317 000
Fax: +44 (0) 1252 316 555
URL: www.veritysystem.com

SECTION 7

Data Erasure

Weircliffe BTE 120M Degausser

Enhanced

The BTE 120M offers fully automatic degaussing for a wide range of tapes used within NATO. The unit uses switched field techniques with media scanning, and in many cases several cassettes can be erased in one operation (depending on size). The BTE 120M can be connected to 230V 50Hz or 115V 60Hz by means of the side entry multi-connector without user adjustment. External lashdown points enable the unit to be securely surface mounted, a rack kit is available as an option. The auto-erasing process facilitates ease of use, whilst interlocks prevent premature removal of the media prior to the degauss cycle being completed.

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Weircliffle BTE 120M degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The BTE 120M is subject to S (E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The BTE 120M may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Weircliffle International Ltd.
Weircliffle Park, St. Andrews Road, Exwick, Exeter, EX4 2AG,
United Kingdom
Telephone: +44 (0) 1392 272 132
Fax: +44 (0) 1392 413 511
Email: sales@weircliffle.com
URL: www.weircliffle.co.uk

Weircliffe BTE 16aM Degausser

Enhanced

The BTE 16aM is a compact table top degaussing designed to erase media with a coercivity of 1000 Oe. The unit is operated by depressing the pneumatic foot pedal, this gives the user control over the degausser whilst leaving both hands free to process media. Cassette formats are slid across the surface of the unit in a procedure clearly printed on the control panel.

Adapters to enable the BTE 16aM to erase DIN, NAB and IBM centred reels are supplied as standard. This versatile degassuer offers SEAP 8500 Type 2 (Higher) erasure on an extensive range of media used in the security, video, computer and data markets.

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Weircliffle BTE 16aM degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The BTE 16aM is subject to S(E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The BTE 16aM may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Weircliffle International Ltd.
Weircliffle Park, St. Andrews Road, Exwick, Exeter, EX4 2AG,
United Kingdom
Telephone: +44 (0) 1392 272 132
Fax: +44 (0) 1392 413 511
Email: sales@weircliffle.com
URL: www.weircliffle.co.uk

SECTION 7

Data Erasure

Weircliffe BTE 220M Degausser

Enhanced

The BTE 220M is operated in the same style as the established BTE 200 range. To ensure compliance with SEAP 8500 standards this unit is fitted with an under-voltage alarm. Should the mains input voltage fall to a level where the erasure specification would not be met, an audible alarm sounds and remains audible on every attempt to use the unit until an acceptable supply is restored.

The BTE 220M also has specific applications in the aircraft industry for erasing flight data charts.

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Weircliffle BTE 220M degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The BTE 220M is subject to S(E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The BTE 220M may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Weircliffle International Ltd.
Weircliffle Park, St. Andrews Road, Exwick, Exeter, EX4 2AG,
United Kingdom
Telephone: +44 (0) 1392 272 132
Fax: +44 (0) 1392 413 511
Email: sales@weircliffle.com
URL: www.weircliffle.co.uk

Weircliffe BTE 29aM Degausser

Enhanced

The BTE 29aM is an "Open Field" degausser designed to erase media with coercivity of 1500 Oe or less. The unit is operated by depressing the pneumatic foot pedal; this gives the user control over the degausser whilst leaving both hands free to process media. Cassette formats are slid across the surface of the unit in a procedure clearly printed on the control panel. Adapters to enable the BTE 29AM to erase DIN, NAB and IBM centred reels are supplied as standard.

Notes:

The SEAP 8500 Degaussing Standard has now been withdrawn and replaced with the CESG Degaussing Standard. This new Standard has two levels of degaussing:

- Lower Level – for RESTRICTED and below
- High Level – for CONFIDENTIAL and above

The Weircliffle BTE 29aM degausser is CESG approved at the Lower Level. This means any magnetic media (holding RESTRICTED or less) may be regarded as NOT PROTECTIVELY MARKED after being degaussed.

The BTE 29aM is subject to S(E)N 06/09. which requires all the SEAP-approved degaussers to be retested against the new CESG Degaussing Standard (at the High Level).

The BTE 29aM may still be used to degauss magnetic media at CONFIDENTIAL and above, but the degauss media is subject to additional handling requirements (detailed in S(E)N 06/09).

Weircliffle International Ltd.
Weircliffle Park, St. Andrews Road, Exwick, Exeter, EX4 2AG,
United Kingdom
Telephone: +44 (0) 1392 272 132
Fax: +44 (0) 1392 413 511
Email: sales@weircliffle.com
URL: www.weircliffle.co.uk

SECTION 8

Firewalls

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 8

Firewalls

AEP Netilla Security Platform Version 6.0.1.4

CCTM	Certificate 2009/06/0047
Awarded: 4th June 2009	Valid until: 3rd June 2011

The AEP Netilla Security Platform (NSP) is an VPN appliance that enables organisations to simply, securely, and cost effectively provide users with browser-based access to corporate applications and files through the security and convenience of a web browser. With computer, telecommunication, branch office employees, business partners and a mobile sales force can quickly and securely reach virtually any resource used in your business.

AEP Network Inc

Focus 31, West Wing, Cleveland Road, Hemel Hempstead, Herts, Hp2 7BW, United Kingdom

Telephone: +44 (0) 1442 458 600

Email: sales@aepnetworks.com

URL: www.aepnetworks.com

3Com© Embedded Firewall

COMMON CRITERIA EAL4	Certificate CRP164 January 2002
CLEF: BT	

The 3Com© Embedded Firewall (EFW) is a distributed firewall and access control security platform for the enterprise. EFW Devices, comprising 3Com NICs together with EFW software developed by Secure Computing Corporation, enforce security policies on all packets transmitted from and received by individual server and workstation machines.

A policy server maintains packet filter policies, which are sent to the EFW Devices using 3-DES encryption. A policy comprises various settings and an ordered list of rules that determine, for each EFW Device associated with that policy, what actions will take place and what events will be logged. A rules consists of various parameters that determine the characteristics for which incoming and outgoing packets will be screened and specifies what action an EFW Device will take if a match occurs.

3Com Business Connectivity Company

Point of Contact Drew Terry

Telephone: +1 801 320 7527

Fax: +1 801 320 6280

Email: drew_terry@3com.com

URL: www.3com.com/secutiry

SECTION 8

Firewalls

Bastion II™

COMMON CRITERIA EAL4 Certificate CRP184 June 2003

CLEF: Logica

Bastion II™ is a high security messaging firewall preferred on environments handling very sensitive information and requiring protection rest of the organisation, CS Bastion II™ allows the controlled and accountable flow of messaging traffic between networks of differing security levels of policies, in environment that would otherwise preclude the direct connection of such networks.

Bastion II™ is optionally available as software or as a pre-packaged system. It provides a two-way application level firewall foe X.400 or SMTP/MIME messaging traffic or for X.525 Directory synchronisation traffic between sensitive private networks or between public and private networks it connects. Bastion II™ prevents any other form of communication between these networks and provides a framework into which a variety of DMZ functions can be pre-configured. Bastion II™ is evaluated to Common CriteriaEAAL4, and builds on the label-based access controls of Sun's Trusted Solaris Operating system, which is itself evaluated to EAL4.

The TOE, Version 2.0.0, running on Trusted Solaris 8 4/01, was certified to EAL4 in June 2003. The TOE is a member of the Common Criteria Assurance Continuity Scheme, under which assurance has been maintained for Version 2.1.0, running on Trusted Solaris 8 12/02 (see Maintenance Report MR1 and Security Target ST1), and Version 2.2.0, running on Trusted Solaris 8 4/01. 12/02, 7/03 and 2/04, (see Maintenance Report MR2 and Security Target ST2).

Deep-Secure,
400 Thames Valley Park Drive, Thames Valley Park, Reading,
Berkshire, RG6 1PT, United Kingdom
Point of Contact: Colin NasH
Telephone: +44 (0) 1684 217 062
Fax: +44 (0) 1189 637 971
Email: colin.nash@deep-secure.com
URL: www.deep-secure.com/

Border Ware Firewall Server Version 6.5

COMMON CRITERIA EAL4 Certificate CRP164 January 2002

CLEF: BT

The Border Ware Firewall includes an integrated operating system and a completed set of services needed to operate a securer and effective Internet connection. The Firewall's operating system (S-Core) is hardened to protect against known vulnerabilities and to provide a secure platform for the extensive set of application proxies that control information flow through the Firewall. The proxies are complemented with an application server for email, FTP, WWW and dual DNS. The integrated Mail server can be configured to provide a complete email system or operate as a relay delivering mail to protected internal servers. Version 6.5 of the Firewall server will be available both packaged on dedicated hardware and as complete software package for easy installation on standard hardware.

BorderWare Technologies Inc
Vista Business Centre, 50 Salisbury Road, Hounslow, Middlesex,
TW4 6JQ United Kingdom
Point of Contact Peter Cox
Telephone: +44 (0) 20 8538 1750
Fax: +44 (0) 02 8572 7708
Email: info@borderware.com
URL: www.borderware.com/

SECTION 8

Firewalls

Border Ware Extreme Mail Firewall Version 3.1

COMMON CRITERIA EAL4 Certificate CRP204 July 2004

CLEF: BT

The Border Ware Extreme Mail Firewall is designed to provide a secure email connection between a corporate network and a public network such as the Internet. Extreme is intended to complement an organisation's Firewall and provides security by:

- Protecting the corporate email servers from attack by preventing direct SMTP connections from public network
- Delivering email through a secure store-and-forward mail relay
- Providing secured message routing functions
- Screening all messages and attachments for malicious content, excluding virus scanning

Extreme is delivered as a pre-load appliance which includes a hardened operating system and all enabled email security functions. The system is managed remotely from a standard Web browser.

The Mxtreme software can be branded by OEM partners and loaded onto the partner hardware. This branding functionality is included within the scope of the evaluation, providing consumers of the branded mail gateway with assurance in the software integrated by the OEM partner.

BorderWare Technologies Inc

Vista Business Centre, 50 Salisbury Road, Hounslow, Middlesex, TW4 6JQ United Kingdom

Point of Contact Peter Cox

Telephone: +44 (0) 20 8538 1750

Fax: +44 (0) 02 8572 7708

Email: info@borderware.com

URL: www.borderware.com/

BorderWare Version 6.1.1 Firewall Server

COMMON CRITERIA EAL4 Certificate CRP136 January 2000

CLEF: BT

The BorderWare Firewall server's EAL4 certification covers the integrated operating system and a completed set of the facilities needed to operate a secure and effective Internet connection. The Firewall operating system (S-CORE) is hardened to protect against known vulnerabilities and to provide a secure platform for the extensive set of application proxies that control information flow through the Firewall. The proxies are complimented with application server for email. FTP, WWW and dual DNS. The integrated Mail server can be configured to provide a complete email system or operate as a relay delivering mail to protected internal servers.

BorderWare Technologies Inc

Vista Business Centre, 50 Salisbury Road, Hounslow, Middlesex, TW4 6JQ United Kingdom

Point of Contact Peter Cox

Telephone: +44 (0) 20 8538 1750

Fax: +44 (0) 02 8572 7708

Email: info@borderware.com

URL: www.borderware.com/

SECTION 8

Firewalls

Check Point VPN-1/Firewall-1 NG on Nokia IPSO (E3)

ITSEC E3 Certificate CRP192 July 2003

CLEF: Logica

This evaluation address the security features of VPN-1/Firewall-1® Next Generation (NG) FP2. including the GUI, Secure Internal, Communication, Remote Management, Authentication, Encryption, an LDAP interface running on Nokia IPSO and a remote access VPN-1 Secure Client allowing remote connection to corporate gateways via Internet connections and secure VPN sessions for access to sensitive network resources running on Microsoft NT. VPN-1/Firewall-1® NG enables enterprise to define and enforce a single Security Policy protecting all corporate network resources with multiple internal systems, and provide secure connective among corporate networks, remote and mobile users, satellite offices and key partners. VPN-1/Firewall-1® NG can be deployed at Internet, Intranet and Extranet access points.

Notes

Only the firewall has been evaluated.

Anyone thinking of using VPN should consult Infosec Manual V and/or CESG for guidance.

Nokia

313 Fairchild Drive, Mountaun View, California, CA 94043-2215, USA

Point of Contact Ed Ingber, Product MAnager

Telephone: +1 650 625 2345

Email: Ed.Ingber@nokia.com

URL: www.nokia.com/securitysolutions/

Check Point VPN-1/Firewall-1 Version 4.1 SP2

ITSEC E3 Certificate CRP149 January 2001

CLEF: Logica

Product description. This evaluation address the core elements of Firewall-1, but also includes the Graphical User Interface, Remote Management, Authentication, Encryption and LDAP interface for Firewall-1 Version 4.1 running on Microsoft NT Version 4.0 SP 5, Solaris 2.6 and AIX Version 4.3. VPN-1/Firewall-1 provides an integrated solution that scales to meet the demands of organisations large and small, securing your enterprise network – LAN, Internet, Intranet and Extranet. VPN-1/Firewall-1 is the center of an extensive policy management framework. The intuitive GUI is used to write the enterprise security policy, which is then applied to all remote or internal gateways.

Notes

Only the Firewall has been evaluated.

Anyone thinking of using VPN should consult Infosec Manual V and/or CESG for guidance.

Check Point Software Technologies Inc

3A Jabotinsky Street, Diamond Tower, Ramat-Gan, 52520, Israel

Telephone: +44 (0) 1223 713 600

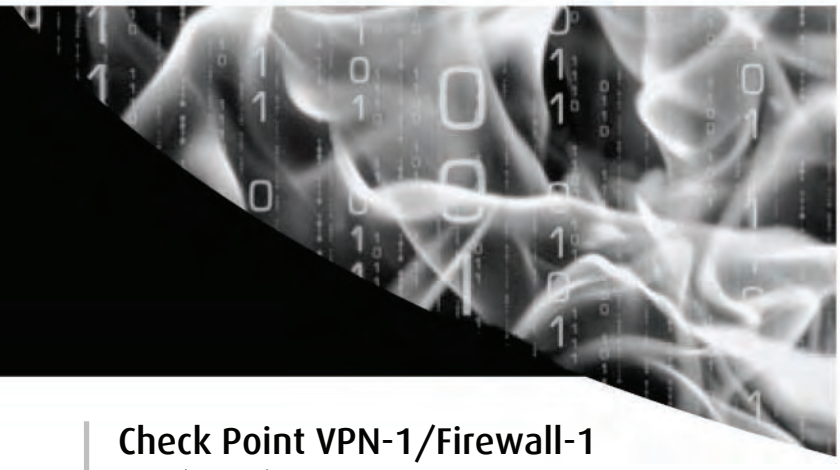
Fax: +44 (0) 1223 713 621

Email: ukinfo@checkpoint.com

URL: www.checkpoint.com

SECTION 8

Firewalls



Check Point VPN-1/Firewall-1 NG (E3)

ITSEC E3 Certificate CRP192 July 2003

CLEF: Logica

This evaluation address the security features of VPN-1/Firewall-1® Next Generation (NG) FP2. including the GUI, Secure Internal, Communication, Remote Management, Authentication, Encryption, an LDAP interface running on Intrusion PDS Pilot 2.4(7) Microsoft NT, Solaris 2.8 and a remote access VPN-1 SecureClient allowing remote connection to corporate gateways via Internet connections and secure VPN sessions for access to sensitive network resources running on Microsoft NT.

VPN-1/Firewall-1® NG enables enterprise to define and enforce a single Security Policy protecting all corporate network resources with multiple internal systems, and provides secure connectivity among corporate networks, remote and mobile users, satellite offices and key partners. VPN-1/Firewall-1® NG can be deployed at Internet, Intranet and Extranet access points.

Notes

Only the firewall has been evaluated.

Anyone thinking of using VPN should consult Infosec Manual V and/or CESG for guidance.

This certificate was amended in July 2003 to include the Intrusion PDS Pilot 2.4 (7) platform. Customers requiring to purchase this configuration should direct enquires to:

Intrusion Inc, Ancells Court, Ancells Business Park, Fleet, Hants, Gu13 8UY

e-mail contact: sales@intrusion.co.uk

Check Point Software Technologies Inc

3A Jabotinsky Street, Diamond Tower, Ramat-Gan, 52520, Israel

Telephone: +44 (0) 1223 713 600

Fax: +44 (0) 1223 713 621

Email: ukinfo@checkpoint.com

URL: www.checkpoint.com

Check Point VPN-1/Firewall-1 NG (EAL4)

COMMON CRITERIA EAL4 Certificate CRP172v2 June 2002

CLEF: EDS

VPN-1/Firewall-1 Next Generation (NG) is a software-based firewall application which provides controlled access between physically connected networks by permitting or denying the flow of IP packets. It also provides IP address translation, IP address hiding and logging of all attempts to communication between physically connected networks. It can operate as a VPN to establish a secure communications channel over an unsecured network using 2 installations of the VPN-1/Firewall-1 firewall. The VPN facility also enables a secure communications channel to be established between a VPN-1/Firewall-1 and a VPN-1 Secure Client to allow remote connection to corporate gateways via Internet connections and secure VPN sessions for access to sensitive network resources Security features of VPN-1/Firewall-1 NG include the GUI, Secure Internal Communication, Remote Management, Authentication, Encryption and an LDAP interface.

This evaluation addressed the firewall functionality and the management of VPN-1/Firewall-1 NG FP1 when running on Microsoft NT SP6a and SUN Solaris 8/0 and the firewall functionality and the management of VPN-1 SecureClient when running Microsoft NT SP6a. The evaluation also addressed the functionality of VPN-1/Firewall-1 NG FP1 which invokes use of both standards-based protocols and cryptographic algorithms to provide Secure Internal Communications and the VPN functionality.

Please note, all product or company names are used for identification purposes only and may be trademarks of their respective owners.

Notes

Only the Firewall has been evaluated.

Anyone thinking of using VPN should consult Infosec Manual V and/or CESG for guidance.

Check Point Software Technologies Inc

3A Jabotinsky Street, Diamond Tower, Ramat-Gan, 52520, Israel

Telephone: +44 (0) 1223 713 600

Fax: +44 (0) 1223 713 621

Email: ukinfo@checkpoint.com

URL: www.checkpoint.com

SECTION 8

Firewalls

Cisco Secure PIX Firewall Software Version 6.2(2)

COMMON CRITERIA EAL4	Certificate CRP180 December 2002
CLEF: BT	

The Cisco Secure PIX Firewall 6.2(2) (Hardware Models 501, 506, 506E, 515, 515E, 520 525 & 535) is a dedicated firewall appliance from Cisco Systems. The product line scales to meet the full range of customer requirements, starting at the SOHO or single user PIX 501 and goes up to the 2Gbps PIX 535. The PIX Firewall is an integrated unit and does not have an underlying operating system such as NT or UNIX, and this increases security and performance as well as keeping management costs down. The certification covers the complete range of firewall models including all network interface combinations, remote management via Telnet from an internal trusted host and Network Address Translation (NAT) functionality.

Cisco Systems

10 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom

Point of Contact: Paul King

Telephone: +44 (0) 20- 8824 8349

Fax: +44 (0) 20 8824 8001

Email: pking@cisco.com

URL: www.cisco/com/bglobal/UK/solutions/ent/avvid_solutions/security_sol_home.shtml

ESafe Version 7.1

CCTM	Certificate 2009/04/0045
Awarded: 28th April 2009	Valid until: 27th April 2011

Founded by pioneers in the anti-malware industry and grounded in onging 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.

eSafe is a:

- Web Security & Productivity Gateway with anti-malware and unauthorized applications filtering.
- Messaging Security Gateway with Spam management.

eSafe uniqueness:

- Proven proactive perimeter threat protection technology.
- Wire speed, deep inspection of web content including HTML.
- Reveals and manages inbound and outbound and other traffic 9e.g.P2P, IM, etc.) in real time.
- Comprehensive protection with Spam management, phishing prevention & IM control.

eSafe benefits:

- Controls spyware proactively at the gateway
- Reduces your risk
- Eli mates security gaps
- Reduces help desk cost
- Frees up IT resources
- Helps enforces security policy
- Helps meet regulatory requirements
- Improves bandwidth

Aladdin Knowledge Systems Ltd

2-3 Fairacres Industrial Estate, Dedworth Road, Windsor, Berkshire, SL4 4LE, United Kingdom

Telephone: +44 (0) 1753 622 266

Email: info@aladdin.com

URL: www.aladdin.com

SECTION 8

Firewalls

MIDASS Firewall Version 1.0

ITSEC E3 Certificate CRP177 January 2003

CLEF: Logica

BAE SYSTEMS' MIDASS Firewall product is a network management firewall for use with the SNMP protocol and a subset of the ICMP protocol. MIDASS filters packets according to their construction (byte level inspection) and also according to the management command which they contain (application level inspection), hence the management information which passes across the firewall can be strictly controlled. The management commands which are permitted by the firewall are hosted such that no packets pass directly between security domains. In addition, MIDASS is a multi-homed firewall, therefore a single installation of the firewall may be used to control access to several security domains.

BAE SYSTEMS
Broad Oak, The Airport, Portsmouth, Hampshire, PO3 5PH, United Kingdom
Point of Contact: Communications Department
Telephone: +44 (0) 1202 408 512
Fax: +44 (0) 23 9222 7594
Email: c4isr@baesystems.com
URL: www.baesystems.com/

Nortel Networks Alteon Switched Firewall
Government Us

COMMON CRITERIA Certificate CRP189 August 2003

CLEF: EDS

Notel Networks Alteon Switched Firewall (ASF) implements a full firewall control plane, based on Check Point Firewall-1 Next Generation. The ASF is a multi-component solution managed as a single system. Jointly designed by Check Point and Nortel, ASF is a tight integration of two key components – an Alteon Switched Firewall Accelerator plus up to six Alteon-Switched Firewall Directors.

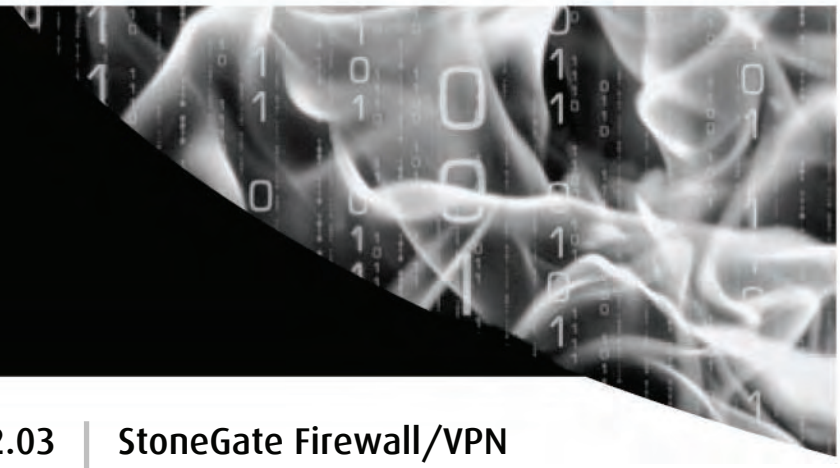
Hardware acceleration allows the offloading to traffic from the firewall inspection engine yielding unmatched performance while still maintaining full security. A full configured ASF can achieve maximum throughput of 4.29Gbps, and support 500,000 simultaneous sessions.

The ASF offers security, ease of management and operational simplicity.

Nortel Network
Maidenhead Office Park, Westacott Way, Maidenhead, Berks, SL6 3QH, United Kingdom
Point of Contact Kianiush Baradaran
Telephone: +1 650 786 9121
Email: kiab@nortelnetworks.com
URL: www.nortelnetworks.com

SECTION 8

Firewalls



Sidewinder G2 Firewall Version6.1.2.03 (sidewinder G2 Security Appliance Model 210D and Sidewinder G2 Software Version 6.1.2.03)

COMMON CRITERIA Certificate CRP239 May 2007

CLEF: BT

The Sidewinder G2™ Security Appliance Model 2150D and Sidewinder G2™ Software Version 6.1.2.03 provide hybrid firewall capability, including application-level proxies, packet filtering, GUI based management, and the hardened SecureOS® UNIX operating system with patented Type Enforcement® technology.

Sidewinder G2™ consolidates many security functions, including strong authentication, intrusion prevention, email-Web-DNS gateway, anti-spam, anti-virus, VPN and SSL termination. (Some of these functions are outside the scope of the evaluation.) The Sidewinder G2™ software is available on a complete appliance line.

Sidewinder G2™ complies with the U.S. DoD Application Level Firewall Protection Profile for Basic Robustness, with assurance increased to EAL4 augmented by ALC_FLR.3

BAE SYSTEMS
Broad Oak, The Airport, Portsmouth, Hampshire, PO3 5PH, United Kingdom
Point of Contact: Communications Department
Telephone: +44 (0) 1202 408 512
Fax: +44 (0) 23 9222 7594
Email: c4isr@baesystems.com
URL: www.baesystems.com/

StoneGate Firewall/VPN

COMMON CRITERIA EAL4 Certificate CRP249 March 2009

CLEF: BT

StoneGate Firewall/VPN provides data and traffic security for the perimeter and segments of a network. StoneGate Firewall/VPN clustering technology ensures continuous secure information flow without any maintenance breaks.

The product is ideally suited to enterprise customers that have geographically dispersed locations but still need to be able to manage all firewalls centrally. StoneGate Firewall/VPN connects remote offices using highly available VPN connections (using several ISP connections). Regulatory needs are satisfied with effective auditing, logging and reporting functionslity StonGate Firewall/VPN appliances rang from small remote office firewalls up to big central firewalls with 10Gbps speed.

Nortel Network
Maidenhead Office Park, Westacott Way, Maidenhead, Berks, SL6 3QH, United Kingdom
Point of Contact Kianiush Baradaran
Telephone: +1 650 786 9121
Email: kiab@nortelnetworks.com
URL: www.nortelnetworks.com

SECTION 8

Firewalls

SWIPSY

ITSEC E3 Certificate CR147 August 2000

CLEF: EDS

The SWIPSY (Switch IP Secuely) Firewall toolkit provides an extensible framework for constructing assured Baston Host firewalls.

SWIPSY is based on a stripped down configuration of Sun's Trusted Solaris (Tsol) 2.5.1 operating system. By relying on the mandatory access controls of Tsol, SWIPSY provides strong separation between networks. Controlled communication between networks can be configured using either a filestore or a TCP/UDP interface.

Third party proxies such as Squid or Message Transfer Agents may be integrated, without the need for re-evaluation, to achieve an E3 firewall. Formal evaluation of the software may be necessary if certain Tsol privileges are needed, as discussed in the Certification Report.

QinetiQ

Cody Technology Park, Ively Road Farnborough, Hampshire, GU14 0LX, United Kingdom

Point of Contact: Sharon Lewis, Customer Contact Team

Telephone: +44 (0) 1684 896 535

Fax: +44 (0) 1684 896 660

Email: Slewis@QinetiQ-TIM.com

URL: www.qinetiq.com/

Symantec Enterprise Firewall Version 8.0

COMMON CRITERIA EAL4 Certificate CRP205 July 2004

CLEF: BT

Symantec Enterprise Firewall provides complete perimeter protection by integrating application proxies, network circuits and packet filtering into its hybrid architecture. Its intuitive management and high-performance characteristics work together comprising the most secure, manageable, flexible firewall for enterprise protection. Integrated components, such as application proxy architecture and a multi-firewall management GUI enable the Symantec Enterprise Firewall to address the broad perimeter security needs to companies connecting to the Internet. Some of the features unique to the Symantec Enterprise Firewall include:

- Initial & continuous system hardening
- DDoS attack protection
- Support for authentication sessions
- Consolidated, non-order-dependent rule setting
- Generic and port-range service proxies supporting legacy, proprietary or emerging protocols.

The product was certified to EEAL4 (augmented with ALC_FLR.1) on Solaris 8, Solaris 9, Windows 2000 Advanced Server and Windows Server 2003 Standard Edition.

Symantec Corporation

380 Ellis Street. Mountain View, CA 94040, USA

Point of Contact Wesley H. Higaki (director, Product Certification)

Telephone: +1 650 527 4701

Fax: +1 650 527 4561

Email: whigaki@symantec.com

URL: www.symantec.com

SECTION 8

Firewalls

Symantec Gateway Security (SGS) Version 3.0 5000 Series (Firewall Engine Only)

COMMON CRITERIA EAL4 Certificate CRP226 April 2006

CLEF: BT

The Symantec Gateway Security addresses the security needs of small and medium-sized offices by integrating seven essential network security applications into a single, easy-to-mange appliance. Its fully integrated, rack-mountable unit protects against today's multi-faceted security threats through a combination of firewall, anti-virus, internet content filtering, intrusion detection and prevention, anti-spam and virtual private networking (VPN) technologies.

SGS Version 3.0 covering 5420, 5440, 5460, 5620, 5640 and 5660 platforms, has been Certified to EAL4 with ALC_FLR.1 for the firewall services only.

The other security applications (i.e. anti-virus, internet content filtering, intrusion detection and prevention, anti-spam, and VPN) have not been evaluated.

Symantec Corporation
380 Ellis Street. Mountain View, CA 94040, USA
Point of Contact Wesley H. Higaki (director, Product Certification)
Telephone: +1 650 527 4701
Fax: +1 650 527 4561
Email: whigaki@symantec.com
URL: www.symantec.com

Symantec Gateway Security Version 2.0 5400 Series (Firewall Engine Only)

COMMON CRITERIA EAL4 Certificate CRP203 April 2004

CLEF: BT

The Symantec Gateway Security is the first comprehensive gateway protection solution that addresses the unique security needs of small and medium-sized offices by integrating seven essential network security applications into a single, easy-to-mange appliance. Its fully integrated, rack-mountable unit protects against today's multi-faceted security threats through a combination of state-of-the-art firewall, anti-virus, internet content filtering, intrusion detection and prevention, anti-spam and virtual private networking (VPN) technologies.

On the Symantec Gateway Security, the certified security application is the firewall; this is an award-winning hybrid firewall that utilises full application inspection technology to provide security against known and unknown threats. The other security applications (i.e. anti-virus, internet content filtering, intrusion detection and prevention, anti-spam, and VPN) are outside the scope of that certification.

The TOE was certified to EAL4 in March 2004. The ALC_FLR.1 augmentation was certified in April 2004.

Symantec Corporation
380 Ellis Street. Mountain View, CA 94040, USA
Point of Contact Wesley H. Higaki (director, Product Certification)
Telephone: +1 650 527 4701
Fax: +1 650 527 4561
Email: whigaki@symantec.com
URL: www.symantec.com

SECTION 8

Firewalls

Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine Only)

COMMON CRITERIA EAL2 Certificate CRP216 May 2005

CLEF: BT

The Symantec Gateway Security 400 Series appliance provides an integrated firewall and live additional security applications, with centralised, flexible, policy-based management for remote/branch office sites with up to 200 nodes. By integrating multiple security functions, networking capabilities, wireless LAN access/security and global security management, the appliance allows enterprise to simplify management and reduce overheads by centrally managing policies and monitoring thousands of remote sites. On the Symantec Gateway Security 400 Series, the scope of the evaluation is the firewall engine. This firewall provides stateful packet inspection for all through traffic and provides firewall rule enforcement. It also provides network address translation to hide internal addresses. All firewall operations are applied to computer groups – a computer in the group is identified by its MAC address, its IP address, its DNS name, or all of these. The other security applications (i.e. anti-virus, internet content filtering, VPN, intrusion detection and prevention) are outside the scope of the evaluation.

Symantec Corporation

380 Ellis Street. Mountain View, CA 94040, USA

Point of Contact Wesley H. Higaki (director, Product Certification)

Telephone: +1 650 527 4701

Fax: +1 650 527 4561

Email: whigaki@symantec.com

URL: www.symantec.com

VCS Firewall Version 3.0

COMMON CRITERIA EAL1 Certificate CRP123 March 1999

CLEF: Logica

The VCS Firewall manages data and communications between trusted and untrusted networks. It supports four independent networks and can manage simultaneously traffic between all pairs of networks. For example, a common implementation is a general office network, a secure internal network, and an internet connection, with the fourth network available for expansion. The VCS Firewall is proxy-based. Proxies for HTTP, Telent, FTP and Mail Exchange, as well as a Generic proxy for all other proxiable protocols, are included. Packet filtering of TCP,UDP and ICMP is also supplied.

All Configuration of the VCS Firewall is by way of a Graphical User Interface. This makes the VCS Firewall easy to configure, as well as providing sanity checking on the configuration.

The VCS Firewall is configured to recognise attacks, and will send alarms in response to these attacks. Furthermore, it can adopt a more secure configuration, providing a fall-back position, if attacked.

The Knowledge Group

6 Mead Court, Copper Road, Thornbury, Avon, BS35 3UW, United Kingdom

Point of Contact Alan Jones

Telephone: +44 (0) 1454 281 265

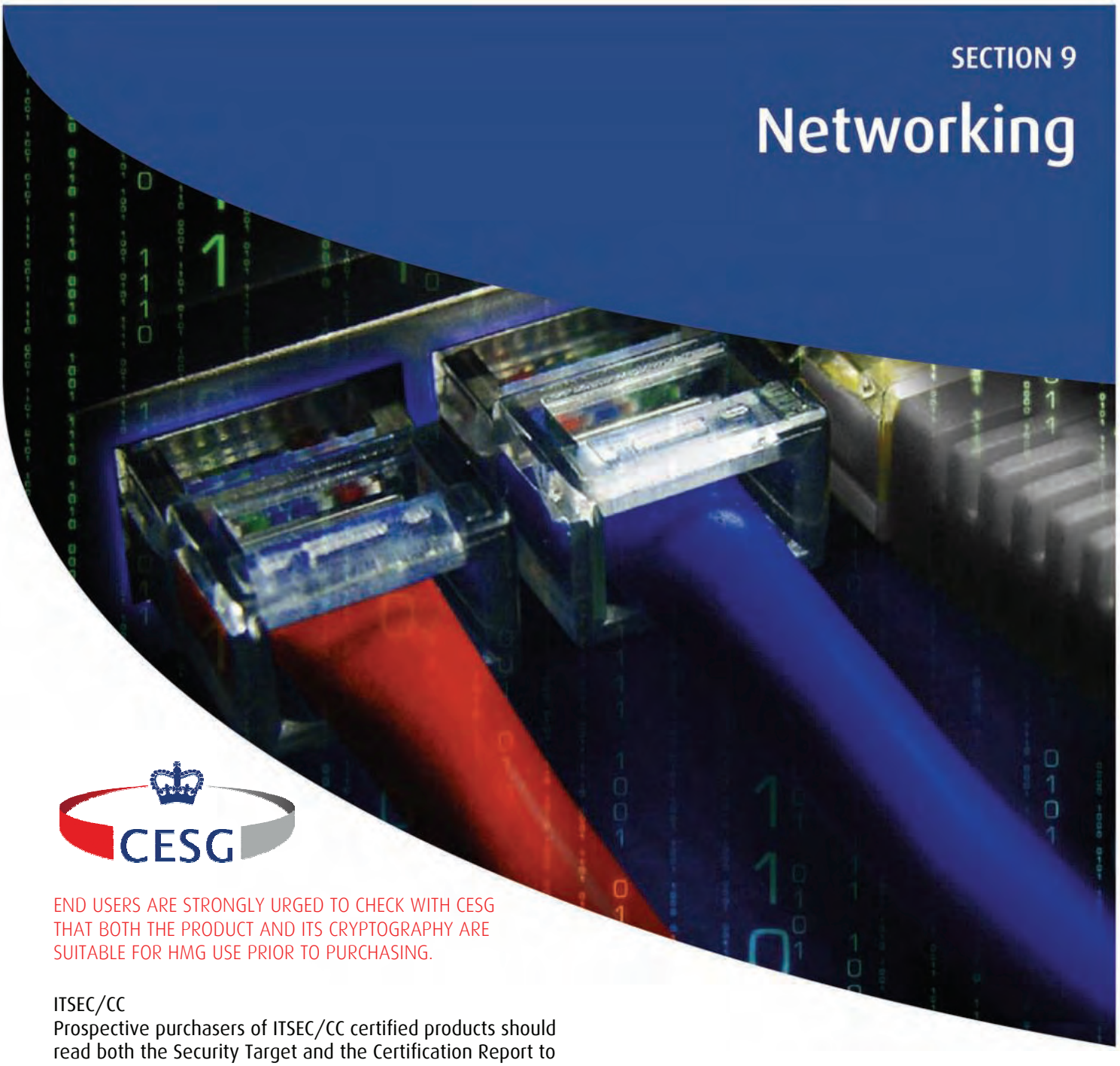
Fax: +44 (0) 1454 281 267

Email: a.jones@ktgroup.co.uk

URL: www.ktgroup.co.uk

SECTION 9

Networking



END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from CESG website.

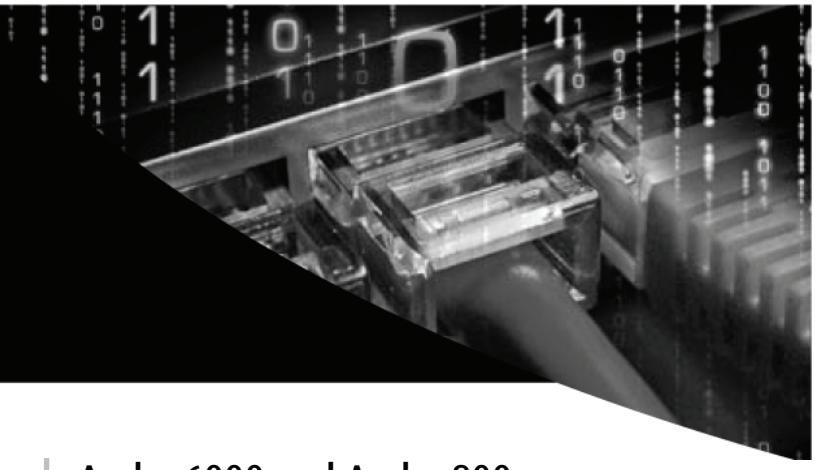
CCTM
CESG Claims Tested Mark

Prospective purchasers of CCT Mark approved products or services should read both the ICD and Test Report documents available from the CCT Mark website, to ensure the product or service is appropriate for their needs.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 9

Networking



AEP SureWare KeyPer 2.1

ITSEC E3 Certificate CR160 October 2001

CLEF: Logica

AEP Keyper is a hardware cryptographic module that provides a highly secure environment for digital signature generation and validation. Further it provides a high degree of safety and integrity of key material (it has been awarded FIPS 1440-1 level 4). AEP Keyper connects to a host computer via standard networking technology in order to provide secure cryptographic services to host computer applications: Key generation Message Authentication Code Signing/Verification. These applications will communicate with SureWare Keyper via the industry standard interface PKC#11. The scope of the evaluation covered those mechanisms that product the cryptographic services that the TOE provides. Triple DES, RSA and SHA-1 contained within the TOE are publicly known. The algorithm implementations have also been independently evaluated within the FIPS programme.

AEP Systems

Focus 31, Wesy Wing, Cleveland Road, Hemel Hempstead, Herts, HP2 7BW, United Kingdom

Point of Contact Steve Lewis

Telephone: +44 (0) 1442 458 600

Mobile +44 (0) 7887 834 016

Fax: +44 (0) 1442 458 601

Email: steve.lewis@aepsystems.com

URL: www.aepnetworks.com

Aruba 6000 and Aruba 800

COMMON CRITERIA EAL2 Certificate CRP246 June 2008

CLEF: Logica

Aruba 6000 and Aruba 800 series Mobility Controllers are wireless LAN (WLAN) switches. A WLAN switch is a gateway device which controls operation of multiple Access Points (APs), processes network data flows between wireless and wired networks, and implements various wired and wireless network and security protocols. Each Aruba Mobility Controller integrates multiple features, such as wireless security protocol processing, policy enforcement firewall. VPN server and wireless intrusion detection/prevention. Aruba Mobility Controllers are hardware devices that run the ArubaOS software suite.

Notes:

The policy enforcement firewall is excluded from the scope of the evaluation.

Aruba 6000 and Aruba 800 series Mobility Controllers are in evaluation to EAL2 and compliance to the Wireless LAN access System PP from the Basic Robustness Environments.

Aruba Networks

Point of Contact Rajeev Shah

Telephone: +1 408 754 1205

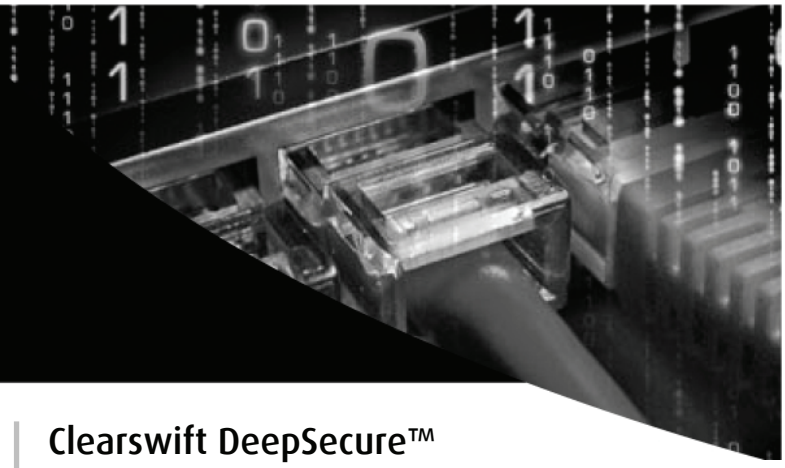
Fax: +1 408 227 4550

Email: rshah@arubanetworks.com

URL: wwwarubanetworks.com/

SECTION 9

Networking



Clearswift DeepSecure™

COMMON CRITERIA EAL4 Certificate CRP213 February 2005

CLEF: Logica

Clearswift Deepsecure™ is a new addition to the Clearswift family of solutions, combining the assured network separation of Clearswift Baston IITM with the advanced content security and management features of ENTERPRISEEsuite™ Clearswift Deepsecure™ is a boundary protection solution for SMTP and X.400 message (including STANAG 4406/ACP123 Military Message) that supports S/MIME signature and encryption, including access to a Directory (X.500 or LDAP) to obtain Certificates and Certificate Revocation Lists. Clearswift Deepsecure™ untilises Trusted Solaris™ Compartmented Mode Workstation labelling and Bastion II™ to provide a Common Criteria EAL4 assured environment, in which signed and encrypted message can be inspected safe from modification and eavesdropping attacks. The evaluation of Clearswift Deepsecure™ Release 2.0.0 E2 was confined to the following aspects of message-flow management:

- Accurate identification and validation of all originator/recipient pairings (relationships) per message
- Invocation of all necessary message-flow mediation checks on message elements
- Release, deletion or queueing for manual inspection of messages
- Incocation of excluded supplementary message handling actions (below).
- Release or deletion of messages resulting from manual inspection
- Logging of associated audit records
- Accurate routing and delivery of released messages and notifications
- Separation, on the DeepSecure™ policy server, of management roles
- Application, on the DeepSecure™ policy server, of security management functions

Functionally excluded form this evaluation includes:

- Message recognition, decomposition and re-composition
- The mediation checks applied to message elements
- The mediation actions (e.g. to remove, replace or annotate message content to generate notification messages and to generate inbound or outbound archives), and
- The management interface running on ClearPoint™ Management Stations.

Clearswift

1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire, RG7 4SA, United Kingdom

Point of Contact Jim Craigie

Telephone: +44 (0) 1635 202 1

Fax: +44 (0) 118 903 9000

Email: Jim.Craigie@clearswift.com

URL: www.clearswift.com

Clearswift DeepSecure™ Release 2.1

COMMON CRITERIA EAL4 Certificate CRP228 August 2006

CLEF: BT

Clearswift Deepsecure™ is a boundary protection device for SMTP and X.400 messages (including STANAG 4406/ACP 123 Military Messages) that provides trusted, policy-based protection against uncontrolled information flow between networks combined with the assured network separation, domain separation and message channel separation of Clearswift Bastion II™. DeepSecure support S/MIME signature and encryption in both SMTP and X.400 messages, including access to a Directory (X.500 or LDAP) to obtain Certificates and Certificate Revocation Lists, and an option for X.841 Security Policies to provide complete compliance with ACP 145 DeepSecure decrypts messages to inspect the content, and can re-sign and re-encrypt messages when required. DeepSecure provides a ClearsPoint™ GUI management station for intuitive configuration of complex policy, and an option for an X.841 Security (Label) Policy Information File (SPIF) Editor, to define and modify X.841 security (Label) policies. The evaluation of DeepSecure Release 2.1 includes the following security functions:

- The ClearPoint management policy definition, modification, selection and activation functions
- The SPIF Editor option
- The policy derivation and execution framework
- The message recognition/de-composition/re-composition function
- The Policy Engine mediation checks and actions for protocol non-conformance
- The Policy Engine actions that can be triggered as a result of policy or policy violations (or other conditions)
- The audit function
- The X.841 (Security) Label Support Library option to support clearance checking and translation of ASN.1 binary encoded security labels
- The PKI data management functions on the Policy Server, ClearPoint and SPIF Editor.
-

Functionality excluded from the DeepSecure Release 2.1 evaluation includes the Policy Engine plug-ins for data type recognition and conformance, de-composition, text extraction, marco detection, re-composition, virus scanning, textual analysis, and spam detection, together with their associated ClearPoint management functions; and the policy Server, Clearpoint and SPIF Editor external library for cryptographic operations.

Clearswift

1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire, RG7 4SA, United Kingdom

Point of Contact Jim Craigie

Telephone: +44 (0) 1635 202 1

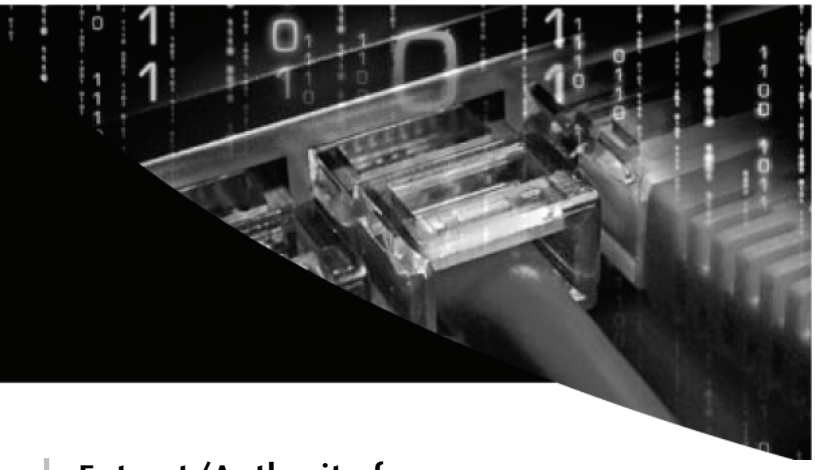
Fax: +44 (0) 118 903 9000

Email: Jim.Craigie@clearswift.com

URL: www.clearswift.com

SECTION 9

Networking



Check Point UTM-1 EDGE W Version 7.5.55

CCTM	Certificate 2009/02/0044
Awarded: 25th February 2009	Valid until: 24th February 2011

Check Point UTM-1 EDGE W Series delivers a tightly integrated set of security and connectivity features to ensure remote sites remain as secure as larger corporate sites, Security features include a stateful inspection firewall, NAT, IPSec, VPN for both site-to-site and remote access. Connectivity features include internal network support with a 4 port switch supporting VLANS and either a DMZ or second Wan port. The integrated Wireless Access Point (802.11b/g) supporting multiple authentication protocols can include up to 4 separate virtual access points. Additionally, the appliance includes an ADSL modem or support for USB Cellular modems for WAN connectivity. For large scale deployments, UTM-1 Edge seamlessly integrates with Check Point's SMART management solutions to greatly simplify security management.

Check Point Software Technologies Ltd
Unit 4 Lindenwood, Crockford Lane, Chineham Business Park,
Basingstoke, RG24 8QY, United Kingdom
Telephone: +44 (0) 1256 374 560
Email: info@checkpoint.com
URL: www.checkpoint.com

Entrust/Authority from Entrust/PKI 5.1

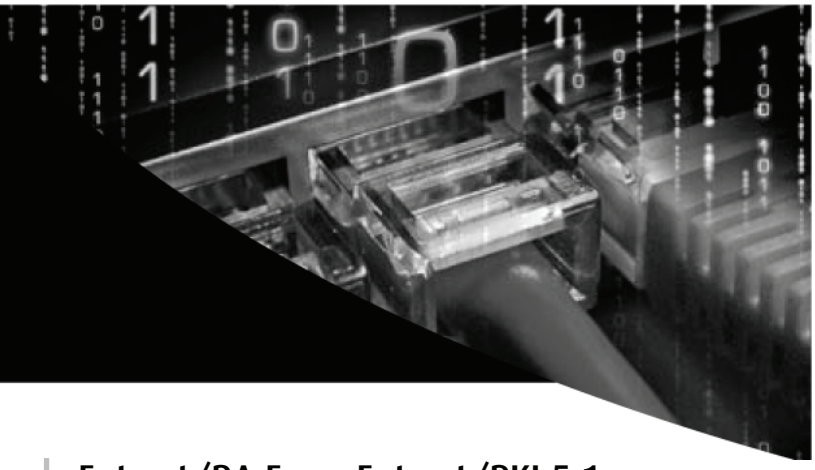
COMMON CRITERIA EAL3	Certificate CRP153 February 2001
CLEF: BT	

Entrust/Authority 5.1 is the core component of an Entrust public-key infrastructure. Acting as the Certification Authority (CA), Entrust/Authority issues X.509 public-key certificates and performs key and certificate management functions. Other Entrust/Authority capabilities include the ability to cross-certify with other CAs, the use of flexible certificates (for including X.509v3 certificate extensions), the use of flexible user password rules, the ability to specify either RSA (1204 or 2048) or DSA 1024 as the CA signing algorithm and CA signing key size, and the ability to renew the CA signing key pair before it expires and to recover from possible CA key compromise.

Entrust
Unit4 (First Floor), Napier Court, Napier Road, Reading, RG1 8BW
United Kingdom
Point of Contact Ian Wills
Telephone: +44 (0) 118 953 3000
Fax: +44 (0) 118 953 3001
URL: www.entrust.com

SECTION 9

Networking



Entrust/RA from Entrust/PKI 5.0

COMMON CRITERIA EAL3 Certificate CRP141 March 2000

CLEF: BT

Entrust/RA is an administrative interface to an Entrust public-key infrastructure. Primary uses for Entrust/RA include: adding and deleting users, revoking certificates and initiating key recovery operations. Security Officers, Administrators, and other Entrust/RA Roles connecting to Entrust/Authority authenticate themselves using digital signatures. Once complete, all messages between Entrust/RA and Entrust/Authority are the secured for confidentiality, integrity and authentication. Cryptographic operations for Entrust/RA and Entrust/Authority are performed on the FIPS 140-1 (Level 2) validated Entrust Security kernel 5.0 cryptographic module or optional hardware cryptographic module, although these are not included in the Common Criteria evaluation.

Entrust

Unit4 (First Floor), Napier Court, Napier Road, Reading, RG1 8BW

United Kingdom

Point of Contact Ian Wills

Telephone: +44 (0) 118 953 3000

Fax: +44 (0) 118 953 3001

URL: www.entrust.com

Entrust/RA From Entrust/PKI 5.1

COMMON CRITERIA EAL3 Certificate CRP153 February 2001

CLEF: BT

Entrust/RA is an administrative interface to Entrust/Authority and allows operations to manage users, set the security policy, and control the PKI. Security Officers and Administrators connecting to Entrust/Authority authenticate themselves using digital signatures. Once complete, all messages between Entrust/RA and Entrust/Authority are then secured for confidentiality, integrity, and authentication. Cryptographic operations for Entrust/RA are performed in the FIPS 140-1 Level 2 validated Entrust cryptographic module. Entrust/RA is currently certified on Microsoft Windows NT 4.0 Service Pack 3.

Entrust

Unit4 (First Floor), Napier Court, Napier Road, Reading, RG1 8BW

United Kingdom

Point of Contact Ian Wills

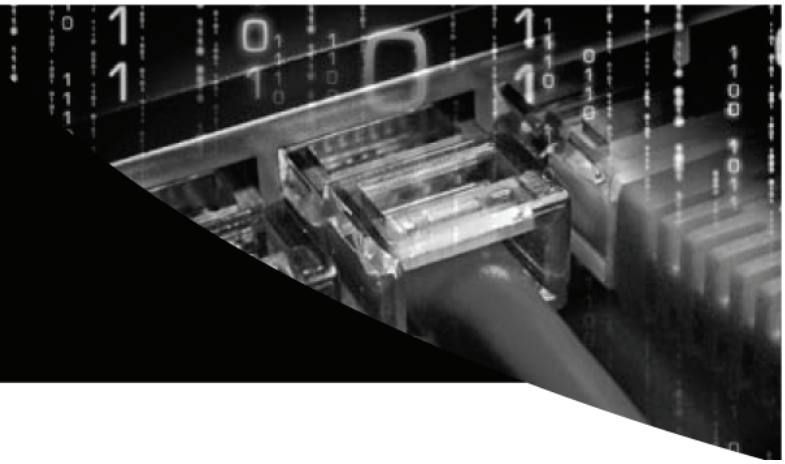
Telephone: +44 (0) 118 953 3000

Fax: +44 (0) 118 953 3001

URL: www.entrust.com

SECTION 9

Networking



IBM Remote Management Centre

ITSEC E1 Certificate CRP115 January 2001

CLEF: Logica

IBM Remote Management Centre provides a focal point for Remote Network Management, Remote Systems Management and Remote Environmental Monitoring. The security of the unit allows multiple customers to be managed form a central location whilst maintaining the integrity of the individual networks and mission critical systems. The service allows RMC staff to integrate with customers networks in a secure manner using a combination of authentication, auditing and accounting incorporated into the secure LAN Several technologies are employed, including firewalls, controlled access lists, user authentication and monitoring. The individual customer's monitoring stations integrate into this secure environment allowing display of individual alarms on a centralised videowall.

IBM

Weybridge Business Park, Addlestone Road, Weybridge, Surrey, KT15 2UF. United Kingdom

Point of Contact David Stacey

Telephone: +44 (0) 1932 851 111

Fax: +44 (0) 1932 814 333

Email: davidstacey@uk.ibm.com

URL: www.uk.ibm.com

Juniper Networks M/T/J series Routers

COMMON CRITERIA EAL3 Certificate CRP237 April 2007

CLEF: BT

Each Juniper Network j-series, M-series routing platform is a complete routing system that supports a variety of high speed interfaces (only Ethernet is within scope of the evaluation) for medium/large networks and network applications. Juniper Networks routers share common JUNOS software, features, and technology for compatability across platforms.

The Juniper platforms are designed as hardware devices, which perform all routing functions internally to the device. All router platforms are powered by the same JUNOS software, which provides both management and control functions as well as all IP Routing.

The Juniper Network M/T/J Series families of Service Routers running JUNOS release 8.1.R1 are certified to EAL3 augmented with ALC_FLR.3 (Systematic Flaw Remediation).

Maintenance Addendum 1

The TOE, Juniper Networks M/T/J Series families of Service Routers running JUNOS release 8.1.R1, was certified to EAL3 in April 2007.. The TOE is a member of the Common Criteria Assurance Continuity Scheme, under which assurance has been maintained for Juniper Networks M/T/J Series Families of Service Routers running JUNO release 8.1R3, covering J2300, J4350 J6350, M7i and M10i (see Maintainance Report MR1 and Security Target ST1 for JUNOS 8.1R3).

Maintenance Addendum 2

The TOE is a member of the Common Criteria Assurance Continuity Scheme, under which assurance has been maintained for Juniper Networks J2300, J2350 J4300, M7i and M10i Service Routers running JUNOS (see Maintainance Report MR2 and Security Target ST2 for JUNOS 8.1R3).

Juniper Networks Inc

1194 North Mathilda Avenue, Sunnyvale, California, 94089, USA

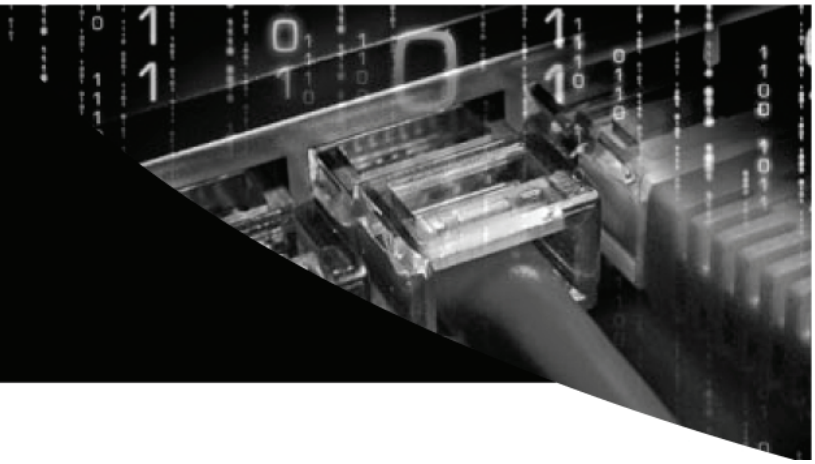
Point of Contact Seyed Safakish

Telephone: +1 408 745 8158

Email:: seyeds@juniper.net

SECTION 9

Networking



Juniper Networks Secure Access Family Version 5.4R2.1

CCTM	Certificate 2007/04/0020
Awarded: 24th April 2007	Valid until: 23rd April 2009

The Juniper Secure Access 4000/6000-FIPS appliance can be deployed to provide secure, anywhere, anytime remote access services to public sector employees from a 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 3and the CCT Mark can be used in the Public Sector for networks carrying information up Protect Level; Business Impact Level 3, Restricted, is outside of the remit of CCTM.

Juniper Networks (UK) Limited

Aviator Park, Addlestone, Surrey, KT15 2PG, United Kingdom

Telephone: +44 (0) 1372 385 500

Email: Thearn@juniper.net

URL: www.juniper.net

Juniper 9.3R1 M/MX/T & EX Family of routers and switches

COMMON CRITERIA EAL3	Certificate CRP248 February 2009
CLEF: BT	

Each Juniper Network MX-series, M-series and T-series routing platform is a complete routing system The EX-series of switches provides high-performance, carrier-class networking solutions. Both the routing platforms and the switches support a variety of high speed interfaces (only Ethernet is within scope of the evaluation) for medium/large networks and network applications. Juniper Networks routers and switches share common JUNOS software, features, and technology for compatibility across platforms.

The Juniper platforms are designed as hardware devices, which perform all routing/switching functions internally to the device. All router/switch platforms are powered by the same JUNOS software, which provides both management and control functions as well as all IP routing.

Juniper Network M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4300 Switches running JUNOS release 9.3R1 are certified to EAL3 augmented with ALC_FLR.3 (Systematic Flaw Remediation).

Maintenance Addendum 1

The TOE is a member of the Common Criteria Assurance Continuity Scheme, under which assurance has been maintained for Juniper Networks EX3200 and EX4200 Switches funning JUNOS release 9.3R2 (see Maintenace Report MR1 and Security Target ST1 for JUNOS 9.3R2).

Juniper Networks Inc

1194 North Mathilda Avenue, Sunnyvale, California, 94089, USA

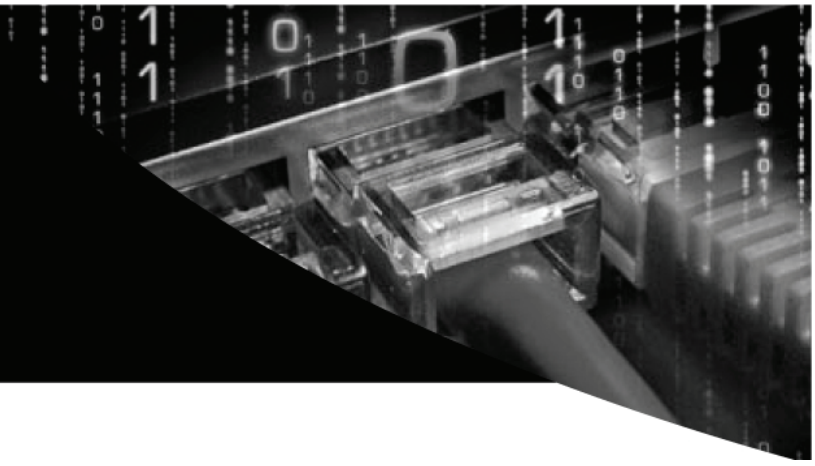
Point of Contact Seyed Safakish

Telephone: +1 408 745 8158

Email:: seyeds@juniper.net

SECTION 9

Networking



JUNOScope IP Service Manager Release 8.2R2

COMMON CRITERIA EAL3 Certificate CRP238 July 2007

CLEF: BT

JUNOScope is a web-based element management system that provides router configuration management. Inventory management, software management, operation status and troubleshooting tools for Juniper Networks J, M, MX, T and TX series routing platforms. JUNOScope is designed to automate and improve efficiency of the day-to-day, network-wide operational tasks of JUNOS devices in a secure, controlled and scalable operating environment.

Four applications modules are available with JUNOScope – Looking Glass, Configuration Manager, Software Manager and Inventory Manager.

JUNOScope IP service Manager release 8.2R2 is certified to EAL3 augmented with ALC FLR.3.

Juniper Networks (UK) Limited

Aviator Park, Addlestone, Surrey, KT15 2PG, United Kingdom

Telephone: +44 (0) 1372 385 500

Email: Thearn@juniper.net

URL: www.juniper.net

Thales SafeMove Version 4.0

CCTM Certificate: 2009/02/0042

Awarded: 25th February 2009 Valid until: 24th February 2011

Thales Safemode is a simple-to-use Model VPN (Virtual Private Network) solution that enables private and public sector organisations to increase the mobility of their workforce, helping them improve efficiency, reduce costs and minimise their carbon footprint. Using SafeMove, workers can securely access information and applications on their office network at any time and place. Robust VPN technology protects the security of all communications, whilst resilient Mobile IP technology maximises availability by providing seamless mobility across a broad range of wired, wireless and mobile networks. Unlike traditional VPN solutions, the SafeMove client transparently switches between networks to maintain the best possible connection without breaking application sessions or requiring re-authentication.

The SafeMove central site gateway is highly scalable and supports multiple serves to ensure optimal performance and resilience in mission-critical environment, whilst a powerful management platform provides complete control over client configuration and simplifies end-user support.

Thales e-Security Limited

Meadow View House, Long Crendon, Aylesbury, Buckinghamshire, HP18 9EQ, United Kingdom

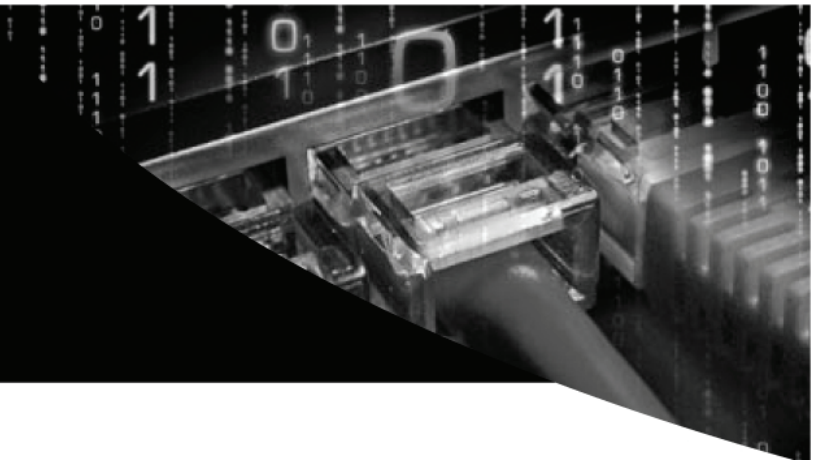
Telephone: +44 (0) 1844 201 800

Email:: emea.sales@thales-esurity.com

URL: www.thales-esurity.com

SECTION 9

Networking



Trucker 2650 Data Collection Unit running ISDX (Realitis Switch) Software 4073 Version 1.05

ITSEC E2 Certificate CRP181 May 2003

CLEF: Logica

Tracker is an intelligent Modem that logs date in 32 Mb of battery memory until polled it receives data on four RS232 ports that can be used for transparent two-way communication with the data source. It will dial out when it detects alarm conditions. When used in a network management system, Tracker prevents subscribers on a switch from gaining access to the remote management system and provides assured separation between subscribers and management traffic. It also protects the switch form unauthorised access when replacing Diagnostic modems. This product was evaluated for the MoD's Defence Fixed Telecommunication Service.

Data Track Technology plc

53 Somerford Road, Christchurch, Dorset, BH23 3TY, United Kingdom

Point of Contact: John Owen, Business Development Manger

Telephone: +44 (0) 1452 270 333

Fax: +44 (0) 1452 270 433

Email: john.owen@dtrack.com.

URL: www.dtrack.com

Tracker 2700 (Data Collection Unit) running Software 10235

ITSEC E2 Certificate CRP220 October 2005

CLEF: Logica

The Tracker 2700 is a secure platform for the management of multi-vendor equipment. IT is designed to utilise IP VPN or modem dial up connectivity, multiple serial, Ethernet and digital contacts, up to 93MB memory and built in UPS. It uses Python scripts to provide advanced alarm filtering, and reporting capability, both SNMP and ASCII, fraud detection, configuration backup, and data buffering.

This product was evaluated for MoD's Defence Fixed Telecommunications Service, and as such, prospective purchasers should read the Certification Report in order to understand the scope of the evaluated product.

Data Track Technology plc

53 Somerford Road, Christchurch, Dorset, BH23 3TY, United Kingdom

Point of Contact: John Owen, Business Development Manger

Telephone: +44 (0) 1452 270 333

Fax: +44 (0) 1452 270 433

Email: john.owen@dtrack.com.

URL: www.dtrack.com

SECTION 10

Operating Systems

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 10

Operating Systems

Hewlett-Packard HP-UX 11i

COMMON CRITERIA EAL4 Certificate: February 2003

CLEF: Logica

HP-UX 11i is Hewlett-Packard's UNIX-based operating environment specifically targeted at internet applications. HP-UX 11i delivers an end-to-end scalable, manageable, and secure infrastructure for developing, deploying and brokering mission-critical e-services.

Hp-UX 11i has been evaluated against the Common Criteria evaluation assurance level EAL4, and the functional requirements in the Controlled Access Protection Profile.

The target environment is for systems that may execute on a single HP 9000Server or be connected to other HP 9000 Servers identically configured to form a local distributed system implementing a unified security policy.

Hewlett-Packard (USA)

19420 Homestead Road, MS 4029, Cupertino, California, 95014, USA

Point of Contact: Mo Mohundro

Telephone: +1 408 447 6186

Email: common_criteria_inquiries@cup.hp.com

URL: www.hp.com/go/security

Hewlett-Packard HP-UX 11i v2

COMMON CRITERIA EAL4 Certificate: CRP225 May 2006

CLEF: Logica

HP-UX 11i is Hewlett-Packard's UNIX-based operating environment specifically targeted at internet applications. HP-UX 11i delivers an end-to-end scalable, manageable, and secure infrastructure for developing, deploying and brokering mission-critical e-services.

HP-UX 11i v1 (HP-UX 11.11) has already been evaluated against the Common Criteria evaluation assurance level EAL4, and the functional requirements in the Controlled Access Protection Profile.

HP-UX 11i v2 (HP-UX 11.23), the latest version of HP-UX 11i, extends the range of platforms available to all HP 9000 (HP PA-RISC based) and HP Integrity (Intel Itanium 2 based) platform. This version has been evaluated against evaluation assurance level EAL4 with ALC_FLR.3 Flaw Remediation and has been evaluated against the functional requirements in the Controlled Access Protection Profile and the Role Based Access Control Protection Profile.

The target environment is for systems that may execute on a single HP platform or be connected to other HP platforms identically configured to form a local distributed system implementing a unified security policy.

Hewlett-Packard (USA)

19420 Homestead Road, MS 4029, Cupertino, California, 95014, USA

Point of Contact: Mo Mohundro

Telephone: +1 408 447 6186

Email: common_criteria_inquiries@cup.hp.com

URL: www.hp.com/go/security

SECTION 10

Operating Systems

Hewlett-Packard HP-UX 11i Version 3 (using CCv2.3)

COMMON CRITERIA EAL4 Certificate: CRP243 March 2008

CLEF: Logica

HP-UX 11i is Hewlett-Packard's UNIX-based operating system that delivers an end-to-end scalable, manageable, and secure infrastructure for developing, deploying and brokering mission-critical e-services. Hp-UX 11i Version 1 executes on (HP PA-RISC based) HP 9000 platforms. HP-UX 11i Version 2 and newer versions of HP-UX 11i execute on (Intel Itanium 2 based) HP Integrity platform as well as on HP 9000 platforms.

HP-UX 11i v1 (HP-UX 11.11) has already been certified to CC EAL4 against the Controlled Access Protection Profile (CAPP).

HP-UX 11i Version 2 (HP-UX 11.23) has been certified to CC EAL4 augmented with Systematic Flaw Remediation (ALC_FLR.3) against CAPP and the Role Based Access Control Protection Profile (RBACPP).

HP-UX 11i Version 3 (HP-UX 11.31) is the latest version of HP-UX 11i and is certified to CC EAL4 augmented with ALC_FLR.3 against CAPP and RBACPP. The evaluated configuration of HP-UX 11i Version 3 supports the hard partitioning (nPars) feature on HP 9000 and HP Integrity platforms.

Hewlett-Packard (USA)

19420 Homestead Road, MS 4029, Cupertino, California, 95014, USA

Point of Contact: Mo Mohundro

Telephone: +1 408 447 6186

Email: common_criteria_inquiries@cup.hp.com

URL: www.hp.com/go/security

Hewlett-Packard HP-UX 11i Version 3 (using CCv3.1)

COMMON CRITERIA EAL4 In Evaluation

CLEF: Logica

HP-UX 11i is Hewlett-Packard's implementation of a UNIX-based operating system that delivers an end-to-end scalable, manageable, and secure infrastructure for developing, deploying and brokering mission-critical e-services.

HP-UX 11i Version 3 (HP-UX 11.31), executing on HP 9000 and HP Integrity platforms, has been certified to CC EAL4, augmented with ALC_FLR.3, and with conformance to CAPP and RBACPP. The evaluated configuration supports hard partitioning (nPars).

HP-UX 11i Version 3 (HP-UX 11.31), the latest version of HP-UX 11i is currently in evaluation to CC EAL4, augmented with ALC_FLR.3 and with conformance to the new COTS Compartmentalized Operations Protection Profile (CCOPP-OS). CCOPP-OS conforms to CC Version 3.1 and is superset of CAPP and RBACPP. The evaluated configuration supports soft partitioning (vPars), as well as nPars.

Hewlett-Packard (USA)

19420 Homestead Road, MS 4029, Cupertino, California, 95014, USA

Point of Contact: Mo Mohundro

Telephone: +1 408 447 6186

Email: common_criteria_inquiries@cup.hp.com

URL: www.hp.com/go/security

SECTION 10

Operating Systems

Hewlett-Packard Tru64 UNIX Version 4.0G

ITSEC E2 Certificate: CR161 October 2001

CLEF: Logica

The Compaq Tru64 UNIX operating system is a 64 bit advanced kernel architecture operating system that provides symmetric multiprocessing, real-time support and numerous features to assist application programmers in developing applications the use shared libraries, multithread support and memory-mapped files. Tru64 UNIX complies with X/OPENTM XPG4 and XTI, POSIX®FIPS and System V Interface definition, amongst many standards and industry specifications It conforms to the OpenGroup Application Environment Specification (AES). The product has been evaluated in a stand-alone configuration against a security target that meets and exceeds ITSEC F-C2 requirements. The following features exceeded F-C2 requirements:

- Password management based on DoD Password Management Guideline.
- Boot authentication
- Access Control Lists based on the POSIX P1003.6 Draft Standard.

Hewlett-Packard

Cain Road, Amen Corner, Bracknell, Berkshire, RG12 1HN,

United Kingdom

Point of Contact: David Suman-Roberts

Telephone: +44 (0) 7831 140 993

Email: david.suman-roberts@hp.com

URL: www.hp.com/uk

Hewlett-Packard Tru64 UNIX Version 5.1A

COMMON CRITERIA EAL4 Certificate: CRP199 February 2004

CLEF: Logica

The HP Tru64 UNIX operating system is a 64 bit advanced kernel architecture operating system that provides symmetric multiprocessing, real-time support and numerous features to assist application programmers in developing applications that use shared libraries, multithread support and memory-mapped files. Tru64 has been certified to Common Criteria evaluation assurance level EAL1, against the functional requirements in the Controlled Access Protection Profile.

Hewlett-Packard

Cain Road, Amen Corner, Bracknell, Berkshire, RG12 1HN,

United Kingdom

Point of Contact: David Suman-Roberts

Telephone: +44 (0) 7831 140 993

Email: david.suman-roberts@hp.com

URL: www.hp.com/uk

SECTION 10

Operating Systems

Microsoft Windows NT Workstation and Windows NT Server Version 4.0

ITSEC E3 Certificate: CR121 March 1999

CLEF: Logica

Windows NT is a multi-tasking operating system for controlling and managing networks of computers and electronic resources in a distributed multi-user environment. Trusted log on for user authentication, DAC of electronic resources, accounting and audit of user activities, and controlling system policies and user profiles in arbitrary network configurations, including interconnection of trusted domains, have been evaluated. The evaluated Windows NT 4.0 SP3 security enforcing functions specified in its Security Target provide the essential evaluating basis on which other specialised security enforcing functions of evaluatable systems such as messaging, electronic business, firewall, virtual private network, and PKI related systems could depend. Microsoft are participating in the development of Common Criteria Protection profiles of such systems. Additional Microsoft products such as Exchange Server, System Management Server, Outlook and Office Clients, Remote Access Services and the clipbook Viewer are excluded from the Target of Evaluation (TOE). Domain based security functionality is included to the transport driver interface; underlying network protocols are also excluded from evaluation.

To obtain an electronic copy of the approved UK ITSEC evaluation installation and configuration for Windows NT4 SP3 document, please go to www.microsoft.com/security/issues/e3fc2summary.asp.

Microsoft Ltd

Point of Contact: Peter Birch

Telephone: +44 (0) 870 60 10 100

Fax: +44 (0) 870 60 20 100

Email: peterbir@Microsoft.com

URL: www.microsoft.com

MONDEX Purse Release 2.0 on MULTOS Version 3 and Hitachi H8/3112 ICC

ITSEC E6 Certificate: CRP129 September 1999

CLEF: Logica

The MONDEX Purse is an electronic purse designed to provide individuals and businesses with an electronic alternative to the use of notes and coins for making cash payments. Mondex electronic cash is stored on Integrated Circuit Cards (ICCs), also known as smartcards. MONDEX Purse Release 2.0, developed by platform seven and Mondex International, has been evaluated when running on MULTOS Version 3, (which has been separately evaluated to ITSEC E6) and the Hitachi H8/3112 ICC. Once value is available in a system of electronic purses, parties can then use purses to make and receive secure payments from one purse to another. Payments may be made to and from banks, between consumers and retailers, or directly between customers. In all cases, value may be transferred in either direction between a pair of purses, but for some classes of purses there may be constraints on the other classes of purse to which payments may be made.

The Central Bank's role of minting and issuing cash is taken on by an Originator who is responsible for manufacturing electronic value, which is then distributed via the banking system from one purse to another. The process is appropriately regulated, but only the MONDEX Purse has been evaluated.

As with notes and coins, electronic value can be held in any currency. Each purse can hold several currencies at one time, each currency being held separately in a different pocket inside the purse. The value in each currency is always quite distinct from other currencies – no conversion is possible within a purse or as part of a transaction. When payment occurs between purses, the parties involved decide on the currency to be used (and each purse will use this information to select the correct pocket). The total value of each currency in circulation does not change as a result of a successful payment. Should an attempted transfer be unsuccessful, this is recorded in an exception log of the purse allowing such potential losses to be funded.

Mondex International

47-53 Cannon Street, London, EC4M 5SQ, United Kingdom

Point of Contact: Customer Support Team

Telephone: +44 (0) 1925 882 050

Fax: +44 (0) 1925 882 051

Email: kms_support@mastercard.com

URL: www.mondex.com

SECTION 10

Operating Systems

MULTOS 4 on Hitachi H8/3114S ICC

ITSEC E6 Certificate: CRP159 July 2001

CLEF: Logica

MULTOS is a secure, multi-application operating system for smartcards. MULTOS supports application such as EMV (debit/credit), electronic cash, digital identity, GSM and mass transit.

MULTOS implementations are built to an open specification controlled by MAOSCO Ltd. MULTOS is available from a number of vendors. Interoperability ensures that applications developed once will run on all MULTOS implementations.

MULTOS provides a number of key security functions including:

- Card issuer controlled load and delete of applications
- Secure on-card segregation of applications
- Ability to load and authenticate encrypted applications.

Mondex International

47-53 Cannon Street, London, EC4M 5SQ, United Kingdom

Point of Contact: Customer Support Team

Telephone: +44 (0) 1925 882 050

Fax: +44 (0) 1925 882 051

Email: kms_support@mastercard.com

URL: www.mondex.com

MULTOS version 3 on Hitachi H8/3112 ICC

ITSEC E6 Certificate: CRP130 September 1999

CLEF: Logica

MULTOS is a secure, multi-application operating system designed to be used on an Integrated Circuit Card (ICC), also known as a smartcard, to mange, segregate and execute application written for MULTOS (such as loyalty, ticketing, credit and electronic purse).

MULTOS is designed to provide a platform for the common development and operation of applications on ICCs. MULTOS-3 is able to:

- Execute an application written for MULTOS independently of the underlying ICC hardware;
- Load many applications, the applications being able to co-exist on the ICC;
- Enable Application Providers to be confident of the authenticity and integrity of the loaded applications and, where applicable, of the confidentiality of the data held within them; and
- Ensure that the applications are not able to interfere with each other or with MULTOS.

This implementation of the MULTOS-3 specification, developed by platform seven and Mondex International, has been evaluated on an Hitachi H8/3112 ICC. Applications are loaded by MULTOS into the ICCs EEPROM. During the production process, each ICC is injected with a unique EEPROM identifier and a unique symmetic key known only to the MULTOS Security |Manager. Once loaded, MULTOS ensures that the application is segregated from any other applications present on the card.

Mondex International

47-53 Cannon Street, London, EC4M 5SQ, United Kingdom

Point of Contact: Customer Support Team

Telephone: +44 (0) 1925 882 050

Fax: +44 (0) 1925 882 051

Email: kms_support@mastercard.com

URL: www.mondex.com

SECTION 10

Operating Systems

MULTOS Version 4 on Hitachi AE45C ICC

ITSEC E6 Certificate: CRP167 April 2002

CLEF: Logica

MULTOS is a secure, multi-application operating system for smartcards. MULTOS supports application such as EMV (debit/credit), electronic cash, digital identity, GSM and mass transit.

MULTOS implementations are built to an open specification controlled by MAOSCO Ltd. MULTOS is available from a number of vendors. Interoperability ensures that applications developed once will run on all MULTOS implementations.

MULTOS provides a number of key security functions including:

- Card issuer controlled load and delete of applications
- Secure on-card segregation of applications
- Ability to load and authenticate encrypted applications.

This implementation takes advantage of the state-of-the-art AE series smart card technology from Hitachi.

Mondex International

47-53 Cannon Street, London, EC4M 5SQ, United Kingdom

Point of Contact: Customer Support Team

Telephone: +44 (0) 1925 882 050

Fax: +44 (0) 1925 882 051

Email: kms_support@mastercard.com

URL: www.mondex.com

Nokia IPSO 3.5 (E3)

ITSEC E3 Certificate: CRP174 August 2002

CLEF: Logica

IPSO is Nokia's secure appliance operating system that runs on Nokia's IP network security appliances. Derived from FreeBSD, IPSO has evolved into a highly reliable, scalable, easily managed OS for running security critical applications on Nokia platforms. A secure web-based element manager, Voyager, allows administrators to configure and maintain the security appliance. Security applications currently supported include Check Point VPN-1/Firewall-1 and ISS RealSecure intrusion detection system. Software is delivered pre-loaded on the Nokia platform. The E3/EAL4 certified version of IPSO may be downloaded from Nokia Technical Assistance Center (TAC) web site for installation onto the platform.

Nokia

313 Fairchild Drive, Mountain View, California, CA 94043-2215, USA

Point of Contact: Ed Ingbar, Product Manager

Telephone: +1 650 625 2345

Email: Ed.Ingber@nokia.com

URL: www.nokia.com/securitysolutions/

SECTION 10

Operating Systems

Nokia IPSO 3.5, 3.5.1 (E3)

ITSEC E3 Certificate: CRP187 June 2003

CLEF: Logica

IPSO is Nokia's secure appliance operating system that runs on Nokia's IP network security appliances. Derived from FreeBSD, IPSO has evolved into scalable and easily managed OS for running security critical applications on Nokia platforms. A secure web-based element manager, Voyager, allows administrators to configure and maintain the security appliance. Security applications currently supported include Check Point VPN-1/Firewall-1 and ISS RealSecure intrusion detection system. Software is delivered pre-loaded on the Nokia platform. This IPSO version may be downloaded from Nokia Technical Assistance Center (TAC) web site for installation onto the platform. This evaluation is for the purpose-built IP100, 300, 400, 500, 600 and 700 product families.

Nokia

313 Fairchild Drive, Mountain View, California, CA 94043-2215, USA

Point of Contact: Ed Ingbar, Product Manager

Telephone: +1 650 625 2345

Email: Ed.Ingber@nokia.com

URL: www.nokia.com/securitysolutions/

Nokia IPSO 3.5, 3.5.1 (EAL4)

COMMON CRITERIA EAL4 Certificate: CRP191 July 2003

CLEF: Logica

IPSO is Nokia's secure appliance operating system that runs on Nokia's IP network security appliances. Derived from FreeBSD, IPSO has evolved into a highly reliable, scalable, easily managed OS for running security critical applications on Nokia platforms. A secure web-based element manager, Voyager, allows administrators to configure and maintain the security appliance. Security applications currently supported include Check Point VPN-1/Firewall-1 and ISS RealSecure intrusion detection system. Software is delivered pre-loaded on the Nokia platform. IPSO 3.5 has been evaluated to ITSEC E3. The E3 certified version of IPSO may be downloaded from Nokia Technical Assistance Center (TAC) web site for installation onto the platform.

Nokia

313 Fairchild Drive, Mountain View, California, CA 94043-2215, USA

Point of Contact: Ed Ingbar, Product Manager

Telephone: +1 650 625 2345

Email: Ed.Ingber@nokia.com

URL: www.nokia.com/securitysolutions/

SECTION 10

Operating Systems

Red Hat Enterprise Linux 3

COMMON CRITERIA EAL2 Certificate: CRP200 February 2004

CLEF: Logica

Red Hat Enterprise Linux AS/ES/WS 3 running on specified Dell and Hewlett Packard hardware.

Red Hat Enterprise Linux 3 is a commercially supported distribution of the open source Linux operating system, designed for mission-critical enterprise computing. Red Hat Enterprise Linux products provide fully matured and stable technologies specifically designed for commercial usage.

The evaluation covers Red Hat Enterprise Linux AS (for large departmental servers), ES (for medium-scale deployments) and WS (for desktop/client application) running on specified Dell and Hewlett Packard hardware platform.

The Lunix kernel interacts with the hardware platform, providing a common set of services to application programmes. These services include identification/authentication, discretionary access control, audit, object-reuse, process separation and self-testing.

The evaluation is sponsored by Oracle Corporation.

Oracle Corporation

Security Evaluation manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom

Point of Contact: Shaun Leer

Telephone: +44 (0) 118 9423860

Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@oracle.com

URL: otn.oracle.com/deploy/security/seceval/content.html

Sony FeliCa Contactless Smart Card RC-S860

COMMON CRITERIA EAL4 Certificate: CRP165 March 2002

CLEF: Logica

The FeliCa Contactless Smart Card system consists of reader/write devices that communicate with the credit card size smart card FeliCa, suitable for multiple applications such as transit ticketing and electronic purse transactions. The evaluation is applicable to the smart card and operating software as delivered by Sony (reader/writer devices and specific applications are not of scope.

Sony Corporation

International Business Strategy Dept, FeliCa Division, 4-7-35 Kitashinagawa Shinagawa-ku, Tokoy, 140-001, Japan

Point of Contact:....International Marketing Section

Telephone: +81 3 5448 2559

Fax: +81 3 5448 3907

URL: www.sony.co.jp/en/index.html

SECTION 10

Operating Systems

Sony IC with Operating System for Mobile CXD3715GG/GU-x Version 0701

COMMON CRITERIA EAL4 Certificate: CRP240 January 2006

CLEF: Logica

The CXD3715GG/GU-x is an IC with embedded (Mobile FeliCa) operating system, which is intended for transit ticketing and electronic purse transactions. The product is designed to be installed in mobile devices (such as telephones) and has both contactless and contact interfaces. The evaluation is applicable to the combined hardware and software as delivered by Sony (reader/writer devices, host mobile devices and specific applications are out of scope).

Sony Corporation

International Business Strategy Dept, FeliCa Division, 4-7-35

Kitashinagawa Shinagawa-ku, Tokoy, 140-001, Japan

Point of Contact:....International Marketing Section

Telephone: +81 3 5448 2559

Fax: +81 3 5448 3907

URL: www.sony.co.jp/en/index.html

Sun Solaris 8 02/02

COMMON CRITERIA EAL4 Certificate: CRP182 April 2003

CLEF: Logica

Solaris 8 02/02 is a Sun Microsystems Unix-based operating system which can be configured from a number of workstations and servers to form a single distributed system. The Solaris 8 02/02 Operating Environment evaluation includes Sun UltraSPAC III desktop and servers (in 64 bit mode) all sharing information in a distributed network environment. Solaris 8 02/02 has also met the requirements of the Controlled Access Protection Profile.

Sun Microsystem Inc

4150 Network Circle, Santa Clara, California, CA 95054, USA

Point of Contact: Mark Thacker, MS UDF-W04

Telephone: +1 972 992 317

Email: mark.thacker@sun.com

SECTION 10

Operating Systems

Sun Solaris Version 8 with AdminSuite Version 3.0.1

COMMON CRITERIA EAL4 Certificate: CRP148 November 2000

CLEF: Logica

Solaris 8 is a Unix-based operating system which can be configured from a number of workstations and servers to form a single distributed system. AdminSuite 3.0.1 provides tools to configure security aspects of Solaris 8. Both Solaris 8 and AdminSuite 3.0.1 have been developed by Sun Microsystems Inc. Solaris 8, with AdminSuite 3.0.1, has been evaluated under the terms of the UK IT Secuirty Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the specified Sun SPARC and Intel Pentium platforms. It has also met the requirements of the Controlled Access Protection Profile.

Sun Microsystem Inc

4150 Network Circle, Santa Clara, California, CA 95054, USA

Point of Contact: Mark Thacker, MS UDF-W04

Telephone: +1 972 992 317

Email: mark.thacker@sun.com

Sun Trusted Solaris 2.5.1

COMMON CRITERIA EAL4 Certificate: CRP104 September 1998

CLEF: Logica

Trusted Solaris 2.5.1 is a highly configurable trusted operating system based on Sun's Solaris 2.5.1 commercial UNIX operating system. It is designed to meet the specific needs of customers seeking evaluated security systems. Trusted Solaris supports ITSEC E3/F-B1 and ITSEC E3/f-C2 with the following major features, all of which were included in the evaluation:

- MAC. DAC and information labels
- Least privilege
- Full identification and authentication facilities, including password generation
- Separate trusted administration and security roles
- GUI administration tools
- Centralised Trusted Facilities Management
- NIS= Naming Service
- Secure CDE Windowing environment with support for X11R5 and Motif
- Trusted Networking using TCP/IP and TISIX or MASIX protocols
- Trusted NFS
- Auditing
- Multi-level mail

Sun Microsystem Inc

4150 Network Circle, Santa Clara, California, CA 95054, USA

Point of Contact: Mark Thacker, MS UDF-W04

Telephone: +1 972 992 317

Email: mark.thacker@sun.com

SECTION 10

Operating Systems

Sun Trusted Solaris Version 8 4/01

COMMON CRITERIA EAL4 Certificate: CRP148 November 2000

CLEF: Logica

Trusted Solaris 8 4/01 is a highly configurable, multilevel trusted operating environment based on Sun's Solaris 8 4/01 operating environment. It meets and exceeds the specific security requirements of the Labeled Security, Role-based Access Control, and controlled Access protection profiles of the Common Criteria.

Features:

- MAC and DAC – including ACLs;
- Least privilege with fine-grained privileges for all policies;
- Trusted networking and trusted NFS
- Identification and authentication – including password generation;
- Roles for separating user and administration capabilities;
- Rights profiles for grouping commands, applications, and authorisation and assigning to users or roles;
- Multilevel windowing environment with trusted path for invoking trusted commands and applications;
- Centralised administration with easy-to-use graphical tools;
- Auditing actions of users and roles, as well as non-attributable events.

The TOE, Sun Trusted Solaris Version 8 4/01, was certified to EAL4 in June 2002. The ALC_FLR.3 augmentation was certified in March 2004 Assurance has now been maintained using the Common Criteria Assurance Continuity process to fully cover Version 8 2/04; see the Maintenance Report MR1 and updated Security Target ST1 foe details. Assurance in earlier derivatives to Version 8 HW 7/03 was previously maintained using UK Assurance Maintenance process see the Assurance Maintenance Status Summary AMSS for details.

Sun Microsystem Inc

4150 Network Circle, Santa Clara, California, CA 95054, USA

Point of Contact: Mark Thacker, MS UDF-W04

Telephone: +1 972 992 317

Email: mark.thacker@sun.com

XTS-400 STOP Version 6.4 (UKE), running on XTS-400 Model 3200UKE

ITSEC E£ Certificate: CRP104 September 1998

CLEF: Logica

XTS-400/STOP OS Version 6.4 (UKE) is a 32-bit, mutli-tasking, operating system that enforces the Bell LaPadula and Biba models of Mandatory Access Control (MAC) & Mandatory Integrity Control (MIC). The system also supports a Discretionary Access Control (DAC) policy.

XTS-400 associates sensitivity labels with all objects. All subjects have an associated clearance level identifying the maximum security level data they can access. This facilitates Multi-Level Security (MLS) by enabling data sharing across different classifications sensitivities potentially traversing business and system boundaries. The XTS-400 cam also be used to provide the trusted element of a high assurance data guard or application hosting service.

XTS-400/STOP v6.4(UKE) operating system is certified to EAL5 augmented with ACL_FLR.3 and ATE_IND.3, and conformance with LSPP and CAPP protection profiles.

BAE Systems Integrsted Systems Technologies Limited

Grange Road, Christchurch, Dorset, BH23 4JE, United Kingdom

Point of Contact: Kevin Tsang Insyte XTS-400 Project Manager

Telephone: +44 (0) 1202 404 548 or +44 (0) 7793 423 625

Fax +44 (0) 1202 404 090

Email: Kevin.Tsang@baesystems.com

SECTION 11

Protection Profiles

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website

Protection Profiles

A Protection Profile (PP) is a set of requirements Designed for a set of circumstances. It consists of:

- A list of threats
- A list of functions
- A list of assurance activities
- A justification that these address the threat.

PPs can be designed by a group of prospective customers who have similar IT security needs, or by the software developer himself.

A PP is not related to any given product or system, rather it defines a user's needs independent of any specific product

A PP is particularly useful in assisting the formulation of procurement specification.

PPs Certified by the UK Scheme are shown here. Additional PPs can be found at the CC website: www.commoncriteriaportal.org

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 11

Protection Profiles

APACS PIN Entry Device for Protection Profile

COMMON CRITERIA EAL4 Certificate: July 2004

CLEF: Logica

This Protection Public has been developed to identify and describe the basic security requirements needed to protect the PINs, security related critical values and software within PIN Entry Devices where these devices ate to be used to provide offline PIN verification. Such offline verification can be used to provide cardholder identification for smartcard based transactions, and such devices may either supplement or replace existing POS terminals. In addition, this protection profile provides segregation between certain classes of application that may be run on these devices.

The environment for this Protection Profile consists of a device comprising a PIN entry device with integral display, a smartcard interface device (IFD) and a POS terminal. These three components may be combined to form one to three separate physical units where each unit shares a common physical enclosure.

This PP defines a core set of requirements applicable to all such devices and an additional set of requirements, the Local Encryption functional package, applicable to devices where the PIN must be communicated between separate physical units.

Association for Payment Clearing Services
Mercury House, Triton Court, 14 Finsbury Square, London, EC2A 1LQ, United Kingdom
Point of Contact: Association for Payment Clearing Services
Telephone: +44 (0) 20 7711 6200
Fax: +44 (0) 20 7628 0924
Email: corpcomms@apacs.org.uk
URL: www.apacs.org.uk

Controlled Access Protection Profile Version1d

COMMON CRITERIA EAL3 Certificate: October 1999

CLEF: Logica

Controlled Access Protection Profile is designed for use as a Protection Profile under Common Criteria. It is suitable for systems which require individual users and administrators to control access to objects on the basis of user identity or membership of a group. This Protection Profile was developed by the National Security Agency. It is derived from the C2 class of the US Department of Defence's Trusted Computer System Evaluation Criteria (TCSEC). Products evaluated against the Controlled Access Protection Profile must be evaluated to an assurance level of at least EAL3. This protection profile supersedes the UK Controlled Access Protection Profile, which has been withdrawn.

National Security Agency
Point of Contact: H Cohen
Telephone: +1 410 854 4458
Email: www.radium.ncsc.mil/tpep/

SECTION 11

Protection Profiles

COTS Compartmentalised Operation Protection Profile Operating Systems (CCOP)

COMMON CRITERIA EAL4 Certificate: June 2008

CLEF: Logica

The COTS Compartmentalised Protection Profile – Operating Systems (CCOPP-OS).specifies the extensive range of security requirements necessary to solve the security problem that organisations encounter when trying to implement readily available operating systems to handle compartmentalised environments. Developed using guidance from COTS Security Protection Profiles – Operating Systems, CCOPP-OS is conformant with both the Controlled Access Protection Profile (CAPP) and the Role Based Access (RBAC) Protection Profile. COPP-OS also contains requirements for Mandatory Access Control to implement compartmentalisation in real-world environment. CCOPP-OS requires the highest assurance level-EAL4-this mutually recognised under the Common Criteria Recognition Agreement (CCRA).

Hewlett-Parkard

19420 Homestead Road, MS 4029, Cupertino, California, 95014, USA

Point of Contact: Mo Mohundro

Telephone: +1 408 447 6186

Email: common_criteria_inquiries@cup.hp.com

URL: www.hp.com/go./security

Labeled Security Protection Profile Version 1.b

COMMON CRITERIA EAL3 Certificate: October 1999

CLEF: Logica

Labeled Security Protection Profile is designed for use as a Protection Profile under Common Criteria. It is suitable for systems which require a security policy based on a combination of user controlled access to objects and upon the sensitivity or category of labelled information. This Protection Profile was developed by the National Security Agency. It is derived from the B1 class of the US Department of Defence's Trusted Computer System Evaluation Criteria (TCSEC)

Products evaluated against the Labeled Security Protection Profile must be evaluated to an assurance level of at least EAL3 augmented by ADV_SPM.1 (informal security policy model).

This Protection Profile supersedes the UK Labeled Security Protection Profile, which has been withdrawn.

National Security Agency

Point of Contact: H Cohen

Telephone: +1 410 854 4458

Email: hhcohen@missi.ncsc.mil

URL: www.radium.ncsc.mil/tpep/

SECTION 11

Protection Profiles

Microsoft Forefront Client Security

CCTM | Certificate: 2009/04/0046

Awarded: 28th April 2009 | Valid until: 27th April 2011

Microsoft Forefront Client Security is a business security product aimed at providing information assurance at Government Impact Levels 1 and 2, for purchase by central government and the wider public sector, the NHS, education, local authorities, police and criminal justice. Microsoft Forefront Client Security helps provide greater protection and control over the security of network infrastructure through protection from viruses, spyware and Trojans enabling an end-to-end, defense-in-depth security solution.

Benefits

- Protect sensitive data from external threats (malware related compromises and theft by Trojans and sptware, criminal activity, targeted data theft).

Microsoft Ltd

Microsoft Campus, Thames Valley Park, Reading, RG6 1WG, United Kingdom

Telephone: +44 (0) 870 610 0100

Email: kecook@microsoft.com

URL: www.microsoft.com

Oracle DBMS Protection Profile

COMMON CRITERIA EAL3 | Certificate: May 2000

CLEF: Logica

This Protection Profile specifies security requirements for database management systems in organisations where there are requirements for the protection of the confidentiality (on a "need to know"

Oracle Corporation

Security Evaluation Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, United Kingdom

Point of Contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

Fax: +44 (0) 118 924 3171

Email: seceval_us@otracle.com or shaun.lee@oracle.com

URL: ohn.oracle.com/depoly/security/seceval/content.html

SECTION 11

Protection Profiles

PKI Secure Kernel Protection Profile 1.1

COMMON CRITERIA EAL4 Certificate: April 2002

CLEF: Logica

The PKI Secure Kernel Protection Profile is the core specification for a family of PPs that address a complex and distributed PKI with advanced security needs. The PP specifies a protecting layer for the basic usage of asymmetric cryptography. Included within the PP are the software requirements from FIPS 140-2. The PP provides a lot of detail about the environment in which a TOE conforming to the PP is expected to work

Safelayer Communication S.A.

Edif. World Trade Centre, Edif. Sur Planta 4D Moll de Barcelona s/n

08039 Barcelona, Spain

Telephone: +34 93 508 8090

Fax: +34 93 508 8091

Email: pkipp@safelayer.com

URL: www.safelayer.com/

Privilege Directed Content Protection Profile

COMMON CRITERIA EAL2 Certificate: September 2002

CLEF: Logica

This Protection Profile specifies security features and an intended environment of a product designed to protect a website by offering to a web visitor only content consistent with authorisation granted to that visitor, and to protect such a website from subversion.

Authorsizor Ltd

Point of Contact: Richard Atkinson

Telephone: +44 (0) 1423 730 300

Fax: +44 (0) 1423 730 315

SECTION 11

Protection Profiles

Role-Based Access Control Protection Profile Version 1.1

COMMON CRITERIA EAL2 Certificate: September 2002

CLEF: Logica

Role-based access control allows the system administrator to define roles based on job functions within an organisation. The administrator assigns privileges to those roles, which may require finely grained operations to organisation resources. Users are granted membership in the roles based on their job responsibilities. As the user's job responsibilities change, which may be frequent, user membership in roles can be granted and revoked easily. As the organisation inevitably changes, which generally is less frequent, roles can be modified easily through role hierarchies. Role hierarchies allow new roles to inherit most of their definition from existing roles. As the job changes, privileges are changed for the individual roles, which are relatively few, not for individual users, who may number in the hundreds or thousands.

The Role-Based Access Control Protection Profile is meant to define a minimal set of requirements. More advanced functionality can be specified in the security target. Meeting the requirements in this protection profile would significantly enhance the security of many operating systems, database management systems, systems management tools, and other applications.

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD, 20899-8930,USA
Telephone: +1 301 975 2934
Email: inquiries@nist.gov
URL: csrn.nist.gov

SECTION 12

Miscellaneous

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor or CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

ITSEC/CC
Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

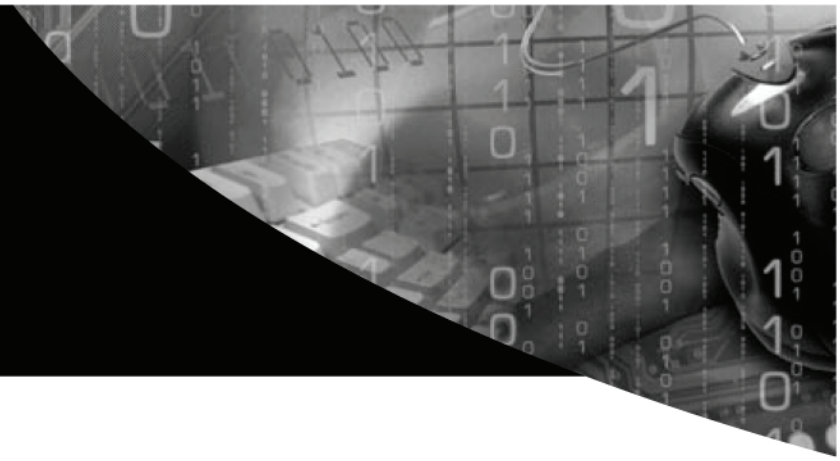
CCTM
CESG Claims Tested Mark

Prospective purchasers of CCT Mark approved products or services should read both the ICD and Test Report documents available from the CCT Mark website, to ensure the product or service is appropriate for their needs.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 12

Miscellaneous



AUDITOR Plus Version 1.4-03 Revision S

ITSEC E1 Certificate: October 1996

CLEF: Logica

AUDITOR Plus is an integrated set of software tool for security auditing and management of Compaq's operating system. OpenVAS contains many security related mechanisms and the product provides a means of automating their use and controlling their effectiveness. Its major areas of functionality are:

- Regular monitoring of system security settings against defined policy Baseline.
- Real-time change detection and response facility
- Multi-level access according to user (System manager, auditor, help desk etc)
- Network wide user authorisation management
- Password synchronisation
- Audit report generation.

IBSL
Ashby House, Derbyshire Road South, Manchester, M33 3JN,
United Kingdom
Point of Contact: Sales
Telephone: +44 (0) 870 121 0990
Fax: +44 (0) 870 121 0995
Email: sales@ibsltech.com
URL: www.ibsltech.com/

BitLocker Drive Encryption™

Cryptographic Grade: See Notes

BitLocker Drive Encryption™ is a full volume data encryption feature of the Ultimate and Enterprise editions of the Microsoft® Windows Vista™ operating system. CESG has examined BitLocker Drive Encryption and have judged that it is suitable for securing IL3 data, when configured to use a Trusted Platform Module (TPM) Version 1.2. a 6 digit PIN and a removable USB dongle, which must be inserted into the computer at power-on. All data saved to a BitLocker Drive Encryption protected volume is reduced to NPM when the computer is shut down or placed in 'hibernation mode'. When used to protect IL3 data, BitLocker must be configured with a CESG-supplied tool, which is provided on the same CD as key material for the product, as described in S(E)N 2007/05. The user PIN must be changed on an annual basis, all other keys do not expire. All data written to the protected volume, the hibernation file, or a crash dump file, is encrypted using 128-bit AES.

Notes: BitLocker Drive Encryption can be used on Windows 7, Windows Vista, Windows Vista SP1 and SP2. The BitLocker Installation Tool, available from CESG, is compatible with the Government Assurance Pack.

Microsoft Ltd
Point of Contact: Stuart Aston
Telephone: +44 (0) 118 909 3418
URL: www.mircosoft.com/uk

SECTION 12

Miscellaneous

BlackBerry Enterprise Solution™

Cryptographic Grade: See Notes

The Research In Motion® (RIM®) BlackBerry® Enterprise Solution™ is a client/server solution including, but not limited to push-email, mobile telephony and Internet services. The BlackBerry Enterprise Solution™ has been assessed as suitable for handling HMG information protectively marked RESTRICTED (impact Level 3), provided that BlackBerry Enterprise Solution Administrators follow the CESG security procedures. Security procedures for BlackBerry® Device Software versions 4.6.1 and earlier, BlackBerry® Enterprise Server 4.1.6 and earlier are provided in Issue 2.1 of Security Procedures for BlackBerry Enterprise Solution Administrators.

The BlackBerry® Smart Card Reader, the PGP® Support Package for BlackBerry® smartphones and the S/MIME Support Package for BlackBerry® smartphones have also been assessed by CESG and found to be suitable for use for handling HMG information protectively marked RESTRICTED (impact level 3). Advice on the use of these products is given in the CESG security procedures.

Notes:

This advice is specific to BlackBerry® Enterprise Solution and should not be construed as being more widely applicable.

Note that some BlackBerry® smartphones contain features such as digital cameras, media card slots and GPS or WiFi® support CESG Security Procedures for BlackBerry Enterprise Solution Administrators Issue 2.1, provides guidance on the configuration and deployment of such smartphones, as part of which CESG typically advises disabling features that effect the overall security of the solution.

CESG has assured the security of the BlackBerry Enterprise Solution™, and provided that administrators and users adhere to the CESG security procedures, CESG has assessed that the BlackBerry Enterprise Solution™ provides an appropriate level of protection for handling RESTRICTED information.

In line with CESG guidance, the GSM phone and SUS functionality on BlackBerry should be for NOT PROTECTIVIELY MARKED use only.

Research in Motion

200 Bath Road, Slough, Berkshire, SL1 3XE. United Kingdom

Point of Contact: Ian Peters

URL: www.blackberry.com

BlackBerry® Device Software Version 4.5

Cryptographic Grade: See Notes IN EVALUATION

The Research in Motion® RIM® Blackberry® Enterprise Solution is a client/server solution including but not limited to push email, mobile telephony and Internet Services. CESG is performing an ongoing assessment of the ability of the Blackberry Enterprise Solution to handle HMG information that is protectivley marked RESTRICTED (Impact Level 3).

CESG is currently assessing Blackberry® Device Software version 4.5.

Interim guidance on the use of Blackberry Device Software version 4.5 is provided in Issue 1.5 of CESG Security Procedures for Blackberry Enterprise Solution Administrators and is available from CESG's IA Bookstore.

Notes:

This advice is specific to the Blackberry Enterprise Solution and should not be construed as being more widely applicable. In line with CESG guidance, the GSM phone functionality on Blackberry smartphones should be for NOT PROTECTIVELY MARKED use only.

Research in Motion

200 Bath Road, Slough, Berkshire, SL1 3XE. United Kingdom

Point of Contact: Graham Baker

URL: www.blackberry.com

SECTION 12

Miscellaneous

DMS Casque

Cryptographic Grade: See Notes — IN EVALUATION

DMS are currently engaged with CESG under CAPS for consultancy and evaluation to enable the design and certification of the next generation of CASQUE to ensure the product meets future demands

Version 2.05

DMS
Stockclough Lane, Feniscowles, Blackburn, Lancs, BB2 5JR,
United Kingdom
Point of Contact: Basil Philipsz
Telephone: +44 (0) 1245 208 419
Fax: +44 (0) 1254 208 418
Email: basil@casque.co.uk
URL: www.dms-soft.com

Entrust/Admin & Entrust/ Authority from Entrust/PKI 4.0a

COMMON CRITERIA EAL3 — Certificate: CRP122 March 1999

CLEF: BT

Entrust/Authority is the core component of an Entrust public-key infrastructure, Acting as the Certification Authority (CA), Entrust/Authority issues X.509 public-key certificates and performs key and certificate management functions, including:

- Creating certificates for all public keys
- Creating encryption key pairs for users
- Managing a secure database of Entrust information
- Enforcing an organisation's security policy.

Entrust/Authority includes other capabilities to ensure the security of an organisation, including.

- Ability to interoperate with other Entrust CAs or with other vendors' CA products
- Use of flexible certificates (to include any extensions in the X.059v3 standard)
- Ability to change the distribution of setup information to users
- Use of flexible password rules
- Ability to specify either RSA or DSA as the CA signing algorithm

Entrust/Admin is an administrative interface to an Entrust public-key infrastructure. Primary users include:

- Adding and deleting users
- Revoking certificates
- Performing key recovery operations

Security Officers and Administrators connecting to Entrust/Authority authenticate themselves using digital signatures. Once complete, all messages between Entrust/Admin and Entrust/Authority are then secured for confidentiality, integrity, and authentication.

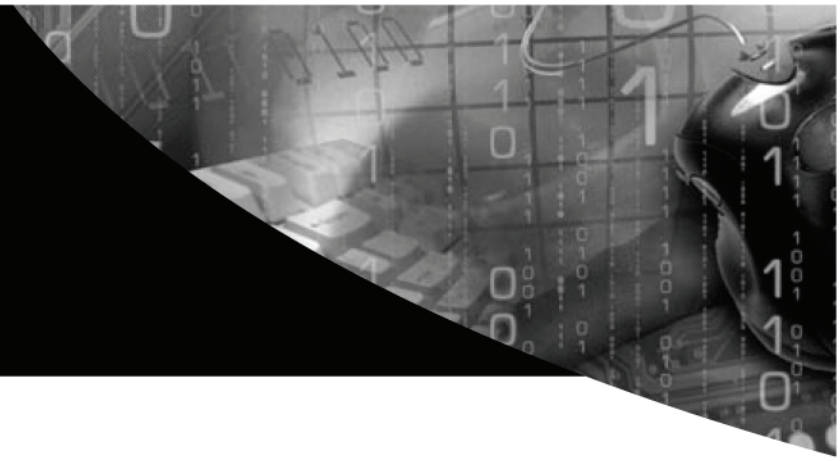
Cryptographic operations for Entrust/Admin and Entrust/Authority are performed on the FIPS140-1 validated Entrust Security Kernel 4.0 cryptographic module or optional hardware cryptographic module.

Entrust/Admin and Entrust/Authority are currently certified on Microsoft Windows NT 4.0 Service Pack 3. Further evaluation work is planned to extend certification to cover a range of operating systems platforms.

Entrust
Unit 4 (First Floor), Napier Court, Napier Road, Reading, RG1 8BW
United Kingdom
Point of Contact: Ian Wills
Telephone: +44 (0) 118 953 3000
Fax: +44 (0) 118 953 3001
URL: www.entrust.com

SECTION 12

Miscellaneous



GlassLock "EM Shield" RF attenuating paint

Cryptographic Grade: See Notes

EM Shield has been developed to specifically address FR, EMI and EMP transmission/intrusions in military, government and commercial environments. This unique, water-based material is extremely conductive and provides a safe and effective EM barrier for many non-metallic surfaces. It is non-toxic, extremely lightweight, durable and manufactured exclusively for GlassLock.

EM shield can target desired attenuation levels throughout a wide frequency spectrum without extensive, heavy and expensive metal shielding techniques.

Retrofitting or repairs to existing enclosures of facilities are easily accomplished with spray, brush or roll-on applications.

A single coat of EM shield can yield in excess of 55dB attenuation at frequencies up to 6GHz. It is a neutral beige colour and can be easily over painted or wallpapered in order to cosmetically enhance secure facilities.

GlassLock Ltd
Morgan's Farm, Swanwick Lane, Swanwick, Southampton, SO31 7HF, United Kingdom
Point of Contact: John Hall
Telephone: +44 (0) 1489 577 233
Fax: +44 (0) 1489 565 155
Email: jhall@glasslock.com
URL: www.glasslock.co.uk

GlassLock "SpyGuard" Window Film

Cryptographic Grade: See Notes

The SpyGuard™ range of products has been developed to mitigate against RF and Optical transmissions/intrusions through windows. The use of these materials now enables the construction or refurbishment of secure facilities without the need to remove windows or block out natural light.

SpyGuard™ is as an attenuator for RF (up to_6GHz) and IR (<1600nm)). It is a virtually clear, transparent film or laminated glass. It reduces intrusion from laser microphones, optical recorders, WiFi, IR and RF hacking through window apertures as well as giving protection from EMI and EMP attack.

SpyGuard™ also provides benefits as a certified safety film or glass laminate for blast protection. Additionally, it has over 50% solar energy reduction, thus producing a substantial return on investment through energy savings.

Products evaluated to date are:

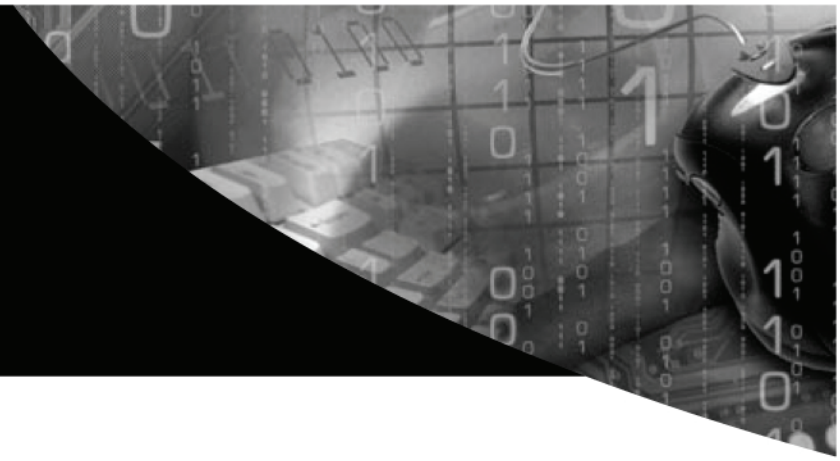
- SpyGuard level 1
- Level 1
- Level 2 Lite

SpyGuard level 2i has only been evaluated for RF attenuation properties only.

GlassLock Ltd
Morgan's Farm, Swanwick Lane, Swanwick, Southampton, SO31 7HF, United Kingdom
Point of Contact: John Hall
Telephone: +44 (0) 1489 577 233
Fax: +44 (0) 1489 565 155
Email: jhall@glasslock.com
URL: www.glasslock.co.uk

SECTION 12

Miscellaneous



LiveState Delivery Version 6.0.1

COMMON CRITERIA EAL2 Certificate: CRP229 August 2006

CLEF: BT

Symantec LiveState Delivery is an enterprise-class system for remotely delivering operating systems, applications, and programs, across network to desktops and servers. Symantec LiveState Delivery uses scheduled push and pull technology to deliver software from centralised servers to multiple PCs or servers simultaneously. Symantec LiveState Delivery provides a suite of administrative tools that allow identified and authorised administrators (with a variety of roles) to manage the untended deployment of business-critical software from centralised Windows servers to multiple PCs or servers simultaneously.

Symantec Corporation

380 Ellis Street, Mountain View, CA 94040, USA

Point of Contact: Wesley H. Higaki (Director, Product Certification)

Telephone: +1 650 527 4701

Fax: +1 650 527 4561

Email: whigaki@symantec.com

URL: www.symantec.com/

Multiple Logical Processor Facility Version 3.3.0

ITSEC E3 Certificate: March 1999

CLEF: Logica

The Hitachi Data Systems MLPF Version 3.3.0 logically partitions a single hardware platform with respect to several operating systems. This allows the definition and allocation of hardware system resources to named partitions. Each partition is capable of being independently operated as if it were a physical processor complex. An operating system in a logical partition can function simultaneously with those in other logical partitions. Information in logical partition is not directly or indirectly accessible to other logical partitions unless sharing is deliberately set. This means that a user on the operating system of a logical partition is not aware of other operating systems on other logical partitions.

Hitachi Data Systems

Office of the CTO, 750 Central Expressway, MS 3407, Santa Cara, California, CA 95050-2627, USA

Point of Contact: Nelson King

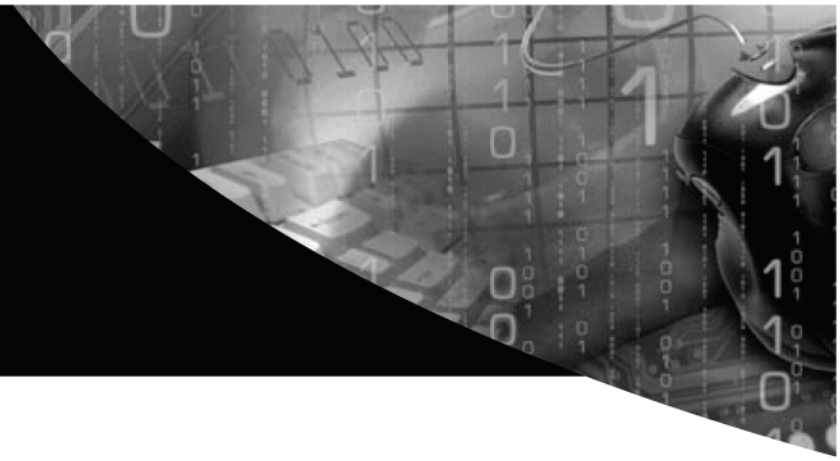
Telephone: +1 408 970 7979

Fax: +1 408 562 5477

URL: www.hds.com

SECTION 12

Miscellaneous



Oracle Business Intelligence Enterprise Edition Release 10.1.3

COMMON CRITERIS EAL3 Certificate CRP 250 June 2009

CLEF: Logica

Oracle Business Intelligence Enterprise Edition (Oracle BIEE) is a suite of products comprising a BI server and BI presentation tools, that allows enterprise to manage, report on the present access to their data via a single common business model. It contains features that ensure data confidentiality, integrity and system availability.

Oracle BIEE provides users with secure, fine-grained access to enterprise resources and assets, enabling them to obtain, view, analyse and report on enterprise data.

Oracle BIEE is used with Oracle Database and Oracle Internet Directory, and is also capable of interfacing with other enterprise data repositories and directory servers.

Oracle Corporation

Security Evaluations Manager, Server Technologies, 520 Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA United Kingdom

Point of Contact: Shaun Lee

Telephone: +44 (0) 118 924 3860

Fax: +44 (0) 118 924 3171

Email: seceval_us@oracle.com or shaun.lee@oracle.com

URL: otn.oracle.com/deploy/security/seceval/content.html

Sectra Radio Blocker Pouch

Cryptographic Grade: Notes

The Radio Blocker Pouch has been developed by Sectra in conjunction with CESG to allow mobile phones, PDAs and laptops to be carried on sensitive sites without the fear of compromise from unwanted radio signalling. The Radio Blocker Pouch is made from a unique radio suppression material that stops all signals to and from a mobile phone making it completely inoperable whilst in the pouch. The Radio Blocker Pouch has a removable inner lining to allow the waterproof outer cover to be cleaned without damage to the protection elements of the design. The Sectra Radio Blocker Pouch is the only product of its kind that meets the requirements of UK Government. The Sectra Radio Blocker Pouch is available in three sizes – Small (for mobile phones), Medium (for PDAs) and Large (for laptops).

Sectra Communications AB

Teknikringen 20, SE-583 30 Linkoping, Sweden

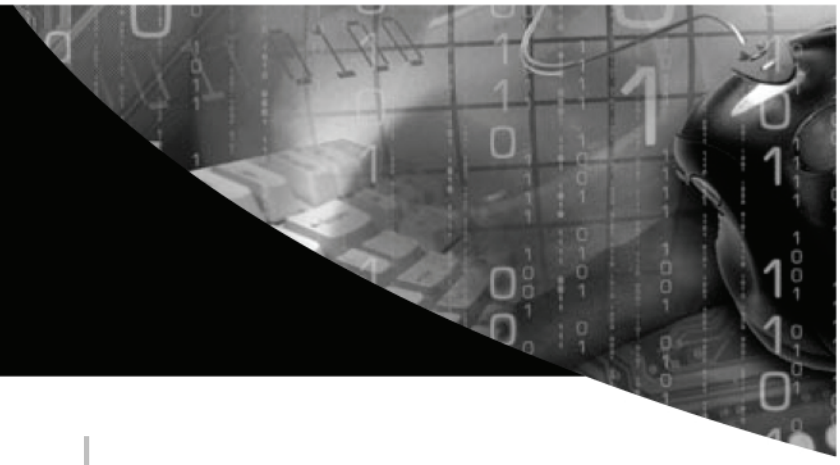
Point of Contact: Karin Carlsson

Telephone: +46 13 23 56 19

Fax: +46 13 22 21 85

Email: info@sectra.se

URL: www.sectra.com



Tamper Respondent Technology

Cryptographic Grade: See Notes

Gore D3 Tamper Respondent Technology provides a respondent barrier to physical intrusion in security hardware.

The D3 sensor is an organic, flexible sheet sensor which folds around an electronic package to create an envelope with no direct entry points. Once coated, entry without circuit damage and detection is very improbable. Electrically, the sensor consists of a resistive network which is continually monitored by a detector circuit inside the package. When detection occurs it is fast and permanent. The sensor is low power and being non metallic is also very difficult to analyse by x-ray. D3 is designed to detect penetration by conducting and non conducting drills and probes as well as by erosive and chemical attacks.

The D3 system has successfully undergone a number of validations to FIPS140-1 level 4 and ZKA criteria.

Notes:

CAPS approved for incorporation in up to Enhanced Grade applications.

W L Gore and Associates (UK) Ltd
Dundee Technology Park, Dundee, DD2 1JA, United Kingdom
Point of Contact: Keith Cuthbert
Telephone: +44 (0) 1382 569 239
Fax: +44 (0) 1382 561 007
Email: kcuther@wlgore.com
URL: www.wlgore.com

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

THIS SECTION IS CURRENTLY UNDER REVIEW.

For further details see address opposite

CONTACT DETAILS

Customer Support Office
A2j
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Telephone: +44 (0)1242 709 141
Fax: +44 (0)1242 709 193
Email: enquiries@cesg.gsi.gov.uk
URL: www.cesg.gov.uK

Section 13

TEMPEST

The security of information may be compromised by electromagnetic phenomena. Communications and IT equipment and systems can produce electromagnetic emanations which may compromise the confidentiality of information. This aspect of information security is known as TEMPEST. CESG has developed an understanding of the current threat to information integrity and availability from electromagnetic phenomena and ensures that cost-effective measures are provided.

CESG provides the following unique specialist TEMPEST services:

- Equipment and installation design guidance
- Certification standards
- Certification for compliance with HMG standards
- Background and installation-design training
- Testing training. Leading to formal internationally recognised accreditation
- Specialist signals processing and analysis.

To find out about the products available, please consult the following lists, which are arranged alphabetically by equipment category. Please note that these products are available only to HMG, UK Critical National Infrastructure (CNI) and NATO customers. There are two lists: SDIP Level A/ AMSG-720B is the Compromising Emanations Laboratory Test Standard, SDIP Level B/ AMSG-788A is the Laboratory Test Standard for Protected Facility Equipment. Contact details for the manufacturers of the products are given at the end of this section. For more details on a specific approved product, please refer in the first instance to the company point of contact for that product. For more general enquires regarding approval of TEMPEST products, please contact the CESG Customer Support Office on:

Telephone: +44 (0) 1242 709 141
Fax: +44 (0) 1242 709 193
Email: enquiries@cesg.gsi.gov.uk

For policy on TEMPEST please consult CESG Good Practice Guide 14 and the Security Policy Framework.

SDIP 27 Level A or AMSG-720B

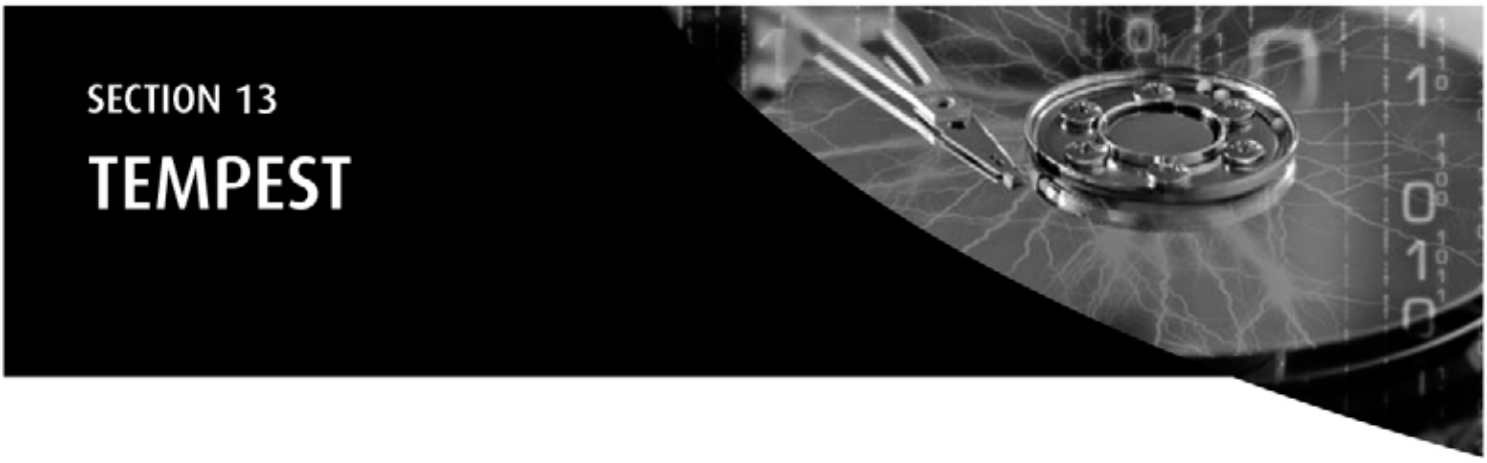
CATEGORY	MANUFACTURER	EQUIPMENT
COMPUTER		
NOTEBOOK	Secure Systems and Technologies Ltd.	SN770TF
NOTEBOOK	Secure Systems and Technologies Ltd.	SC1000TF-8321
PERSONAL	Secure Systems and Technologies Ltd.	SC2000BT-P
PERSONAL	Secure Systems and Technologies Ltd.	SC2000TF-8354
PERSONAL	Secure Systems and Technologies Ltd.	SN6700TF-200
PERSONAL	Secure Systems and Technologies Ltd.	SC7000TF-327/400
PERSONAL	Secure Systems and Technologies Ltd.	SC7550TF-100
FACSIMILE INTERFACE	Secure Systems and Technologies Ltd.	SSG 933T
FASCIMILE	Secure Systems and Technologies Ltd.	SF5780TF
MONITOR COLOUR	Secure Systems and Technologies Ltd.	SL17BT-001/004
COLOUR	Secure Systems and Technologies Ltd.	SL19TF-8347
PRINTER LASER	Secure Systems and Technologies Ltd.	SP460TF-100
LASER	Secure Systems and Technologies Ltd.	SP1006TF-100
LASER	Secure Systems and Technologies Ltd.	SP3000TF-124
LASER	Secure Systems and Technologies Ltd.	SP3525TF
LASER	Secure Systems and Technologies Ltd.	SP4700TF-101
HUB 4-PORT USB	Secure Systems and Technologies Ltd	SB404TF-8378
ROUTER	Secure Systems and Technologies Ltd	SR1605BT
SCANNER MOBILE SCANNER	Secure Systems and Technologies Ltd	SS65TF-8373
MOBILE SCANNER	Secure Systems and Technologies Ltd	SS100TF-8240

SDIP 27 Level B or AMSG-788A

CATEGORY	MANUFACTURER	EQUIPMENT
COMPUTER LAPTOP, RUGGED	GRID Defence Systems Ltd	1587B
NOTEBOOK	Secure Systems and Technologies Ltd.	SN51TI-100
NOTEBOOK	Secure Systems and Technologies Ltd.	SN73TI-004
NOTEBOOK	Secure Systems and Technologies Ltd.	SN500AT
PERSONAL	Secure Systems and Technologies Ltd.	SC2800TI-950
PERSONAL	Secure Systems and Technologies Ltd.	SC6000AT
PERSONAL	Secure Systems and Technologies Ltd.	SC6865AT
PERSONAL	Secure Systems and Technologies Ltd.	SC7000TI
PERSONAL	Secure Systems and Technologies Ltd.	SC7550TI-100
PERSONAL	Secure Systems and Technologies Ltd.	SC7600TI-900
FACSIMILE	Secure Systems and Technologies Ltd.	SF5780TI
FIBRE OPTIC HUB	Secure Systems and Technologies Ltd.	SB8000AT-001
HUB	Secure Systems and Technologies Ltd.	SB8100AT-001
MODEM	Secure Systems and Technologies Ltd.	LD-7132
MONITOR COLOUR	Secure Systems and Technologies Ltd.	SL17TI-004
COLOUR	Secure Systems and Technologies Ltd.	SL19TI-001/8346
COLOUR	Secure Systems and Technologies Ltd.	SL21TI-100
MISCELLANEOUS DISTRIBUTION SWITCH	SELEX Communications	LDS101
PRINTER	Blazepoint Ltd.	200i
LASER	Blazepoint Ltd.	T162
DOT MATRIX, RUGGED	Secure Systems and Technologies Ltd	PD-121B
LASER	Secure Systems and Technologies Ltd.	SP3000TI
LASER	Secure Systems and Technologies Ltd.	SP4650TI-900
LASER	Secure Systems and Technologies Ltd.	SP5100AT-100
SCANNER	Secure Systems and Technologies Ltd.	SS5400AT

SECTION 13

TEMPEST



Company	Address	Content
Blazepoint Ltd	2 Tower Estate, Warpsgrove Lane, Chalgrove, Oxfordshire. OX44 7XZ	Telephone: +44 (0) 1865 892 030 Contact: Mr D Selwood
GRID Defence Systems Ltd	Highbridge House, 93-96 Oxford Rd, Uxbridge, Middlesex. UB8 1LU	Telephone: +44 (0) 1895 230 650 Contact: Mr P Rushton (Piers)
Secure Systems and Technologies Ltd	Brunel Court, Waterwells, Gloucester. GL2 2AL.	Telephone: +44 (0) 1452 371 999 Contact: Mr N Minett-Smith (Nick)
Selex Communications	Signal House – Grange Road, Christchurch, Dorset BH23 4JE	Telephone: +44 (0) 1202 506004 Contact: Mr G Chant

SECTION 14

Mobile Solutions

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

The predominant feature of products in this section is their mobile usability. They will however contain features that would otherwise be represented in other sections, e.g. Access Control or Data Encryption.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor of CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

CCTM
CESG Claims Tested Mark

Prospective purchasers of CCT Mark approved products or services should read both the ICD and Test Report documents available from the CCT Mark website, to ensure the product or service is appropriate for their needs.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 14

Mobile Solutions

CREDANT Mobile Guardian Enterprise Edition Version 5.2.1.(SP4)

CCTM	Certificate: 2008/02/0034
Awarded 18th February 2008	Valid until: 17th February 2010

CREDANT Mobile Guardian (CMG) Enterprise Edition is a scalable mobile security and management software platform threat enables organisations 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, organisations can easily increase the speed of business execution by enabling business processes to reduce the risk of going mobile safely "go mobile".

Credant Technologies, Inc

88 Kingsway. London, WC2B 6AA, United Kingdom

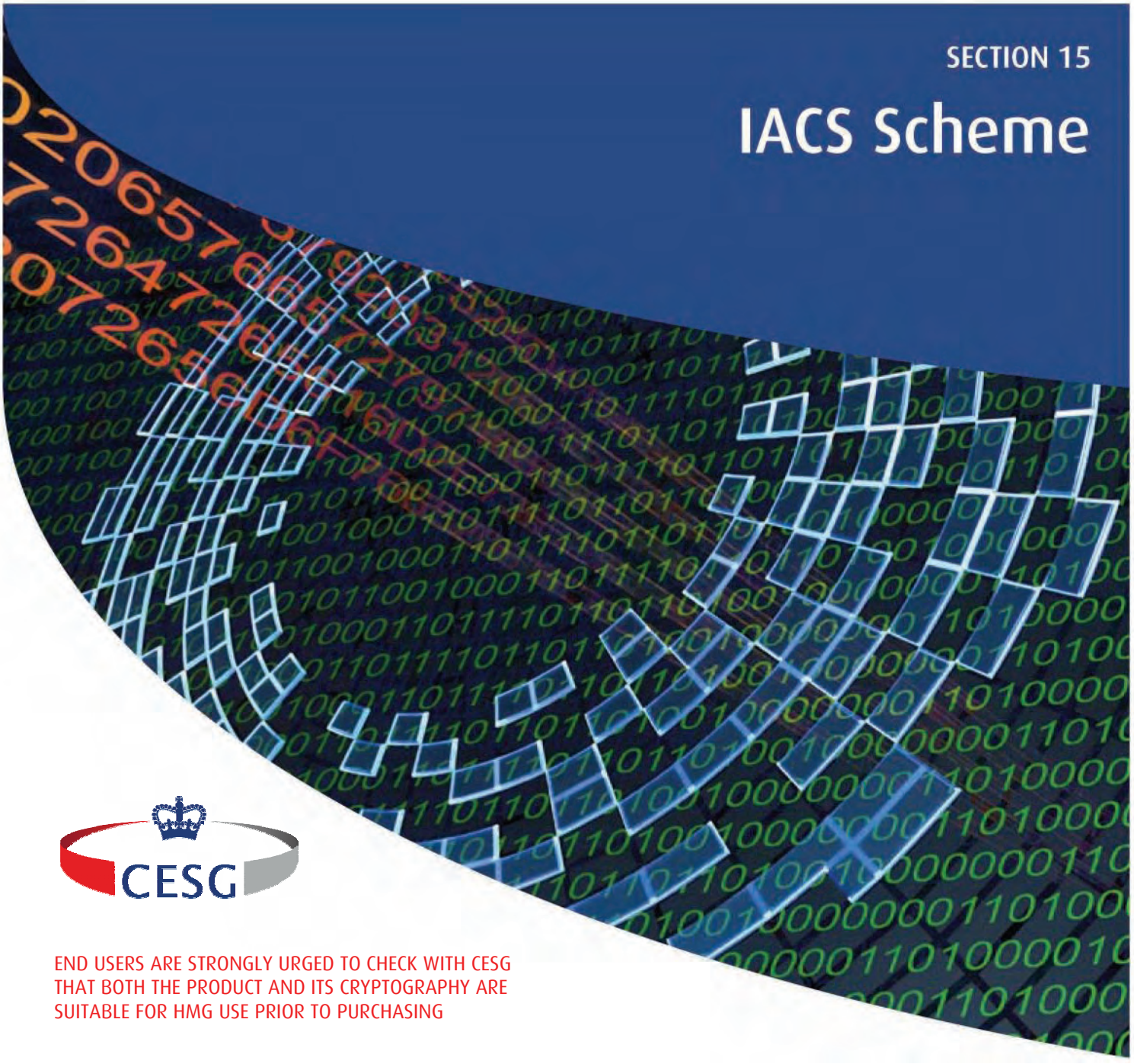
Telephone: +44 (0) 207 7267 440

Email: emeasales@credant.com

URL: www.credant.com

SECTION 15

IACS Scheme



CESG

END USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 15

IACS Scheme

Below you will find a brief description of the IACS schemes.

IT Security Evaluation Criteria (ITSEC)

ItSEC is the set of criteria used for the past decade by Europe and Australasia for the evaluation of products and systems. ITSEC was a major building block in the formulation of the Common Criteria.

Common Criteria

CC represents the outcome of international efforts to align and develop the existing European and North American criteria and has been ratified as ISO standard 15408. The approximate assurance correspondence between ITSEC and CC is shown below. A fuller description of the testing carried out at each assurance level is contained on the CESG's web site. http://www.cesg.gov.uk/

Common Criteria	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Itsec		E1	E2	E3	E4	E5	E6

Certificate Maintenance Scheme

Evaluation results only appear to a specific version of a product, and any subsequent changes (including patches, hot fixes and service packs) to that product may invalidate those results and, therefore, the Certificate. Due to the evolution of products being so rapid, the Certificate Maintenance Scheme (CMS) has been devised in response to this, CMS provides a means of maintaining the same level of assurance in a product after certification without the need for re-evaluation.

International Mutual Recognition

Developers whose products are certified against ITSEC or CC enjoy the benefits of an internationally recognised Certificate. In this Directory we detail only those products which have been evaluated in the UK. However, CESG recognises products evaluated outside the UK against Common Criteria by recognised foreign Certification Bodies. A list of all products evaluated (or in Evaluation) against Common Criteria is available in the External Common Criteria appendix (page 15.1), together with a list of recognised foreign Certification Bodies' websites to obtain more detailed information on products. Links are available from CESG web site. The Common Criteria website www.commoncriteriasportal.org also provides a list of products Certified or in Evaluation against Common Criteria HMG Departments wishing to use foreign certified products in environments where national security is an issue are advised to consult CESG.

Evaluation – CESG working with Industry

Formal evaluation, except for cryptographic evaluation, in the UK is carried out by independent testing laboratories known as Commercial Evaluation Facilities (CLEFs) which are appointed by the Certification Body in CESG. CLEFs meet rigorous security and ISO/ITIEC 17025 quality standards. The UK has 3 CLEFs, which can be contracted to carry out both evaluation and preparatory consultancy work. CLEF contact details are on page 14.5.

The results of the testing of the product are provided a to the Certification Body in an evaluation technical report which forms the basis of the Certification Report. The Certification Body is part of CESG and is itself accredited by UKAS to EN45011 for its ITSEC and CC Certification.

CTAS

The CESG Tailored Assurance Service (CTAS) is intended for a wide range of IT products and systems ranging from simple software components to national infrastructure networks. Therefore, a toolbox of activities is provided the enables each evaluation to be tailored as appropriate. A summary of these components is provided in the table below.

- Assurance Activities
- Development Procedures Review
- Product Functionality and Design Assessment
- System Architecture and Design Review
- Security Functional Testing
- Installation and Operational Procedures
- Vulnerability Analysis and Testing
- Source Code Analysis
- Assurance Maintenance Review.

The Accreditors will decide which of those activities are most appropriate for their system. Furthermore, it will be possible to trade-off the effort required between the various activities depending on the risk.

Note that it is not the intention to evaluate a whole system, just the key barriers and interfaces.

SECTION 15

IACS Scheme

Evaluation will be carried out by contractors approved by CESG to a specification detailed in the Security Target and Evaluation Work Programme. CESG will agree the scope and technical approach of the evaluation and will review the work of the contractor. CESG will also make recommendations on the significance of any issues that are discovered.

The deliverables will be an Evaluation Report from the contactor and an Assessment Statement from CESG.

The Evaluation report summarises the results, list any security vulnerabilities or major functionality errors, and highlights any additional residual risks and (where known) their business impact. Statements in the report regarding risks will make clear their relevance in the context of use of the product or system and identify whether they are generic to the product or due to s specific system configuration.

The CESG Assessment Statement will confirm the extent to which the evaluation achieved the desired aims and summarise the significance of the main findings, highlighting any security risks or (where known) business impacts. It will describe the connection of the results to IS1 and any additional information that may be required. At this point the Tailored Assurance evaluation of the system or product is completed.

KPMG LLP

8th Floor, I Canada Square , Canary Wharf, London E14 5AG
Point of Contact: Martin Jordan
Telephone +44 (0) 207 311 5386
Mobile: 07790 904 245
Fax: +44 (0) 207 311 5836
Email: martin.Jordan@kpmg.co.uk
URL: www.kpmg.co,uk

NCC Group PLC

The Manchester Technology Centre, Oxford Road, Manchester M1 7ED.
Point of Contact: Andy Hague
Telephone: +44 (0) 161 209 5321
Mobile: 07773 315 293
Fax: +44 (0) 161 209 5222
Email: andy.hague@nccgroup.com
URL: www.nccgroup.com

NGS Software Ltd.

52 Throwley Road, Sutton, Surrey SM1 4BF

Telephone: +44 (0) 208 401 0070
Mobile: 07881 813792
Fax: +44 (0) 208 401 0076
Email: dave@ngssoftware.com
URL: www.ngssoftware.com

For the latest information on this scheme, please refer to CESG website.

System Evaluations

System evaluation is highly relevant as a means of minimising risk and as a confidence hallmark for trading partners, especially as systems typically comprise a combination of certified and uncertified products. Important benefits of such evaluations are demonstrable compliance with the provisions of the Data Protection Act (1998), and supporting evidence that will enhance existing ISO17799 accreditation and assist in demonstrating compliance with BS7799 Part 2. CESG offers a number of flexible options including evaluation against an assurance profile (e,g, E3 for firewall, E2 for authentication, E1 for audit) to meet differing requirements. For Government or Critical National Infrastructure users there is also the option of a system IT Security Health Check or FTA. For further information, contact CESG.

For the latest information on this scheme, please refer to CESG website.

Cryptographic Evaluations

Where cryptographic is a key function of the security functionality offered by the product and the intended end users include HMG clients, then this must be assessed by CESG. This can be started under the CESG Assisted Products Service (CAPS) before undergoing evaluation and as a single package with ITSEC/CC evaluations or assessments.

The CESG Assisted Products Service (CAPS)

CAPS has been established to provide design consultancy for developers and vendors of products utilising cryptographic security measures. The service also

SECTION 15

IACS Scheme

Provides cryptographic verification of these products to Government standards by:

- Investigating the correct implementation of an approved cryptographic algorithm
- Identifying and removing any vulnerabilities in the cryptographic implementation
- Assessing other functions supporting the cryptographic mechanisms.

The outcome of participation in CAPS is a cryptographic evaluation and the formal approval for a product's use by HMG and other organisations processing sensitive information.

CAPS has been very successful in ensuring that a wide range of approved cryptographic products is available for use by HMG and public sector customers. The latest cryptographic product approvals can be found on the CESG web site at www.cesg.gov.uk. This site also provides a list of those products currently undergoing the approval process.

CESG carries out an annual review to ensure cryptographic products are still countering identified threats in the light of technological developments and other factors. If a cryptographic product is considered to be no longer countering the identified threat then further sales approvals will be refused and the product will be withdrawn from the Directory.

What do we mean by cryptographic products?

A cryptographic product uses a hardware, software or firmware implementation of any form of cryptography to enforce a security function, whether the design of the cryptography is published in the public domain or not. HMG policy determines the standards required in the design and implementation of cryptography for the product to be approved for the protection of sensitive Government data. These standards are:

HMG Cryptographic Standards

Cryptographic products are graded in terms of three different Cryptographic Protection Levels:

Baseline: These products use CESG-approved public domain cryptographic algorithm. Within the UK Baseline products are suitable for the protection of data up to the RESRTICTED Protective Marking. This is also minimum grade of encryption required to protect communications of RESTRICTED material to or from places outside the United Kingdom.

The transmission of RESTRICTED material over the Internet requires Baseline Grade encryption, regardless of the geographical location of the user. It is Departments to decide, on the basis of a risk assessment, whether additional measures, including Enhanced Grade encryption, may be needed in particular circumstances.

Enhanced: These products generally use CESG designed cryptographic algorithms but can sometimes use or include CESG-approved public domain algorithms. Enhanced grade products can protect data up to and including the CONFIDENTIAL Protective Marking and can also be used to protect material marked SECRET with a life of less than one year. Certain Enhanced grade products contain a CESG designed High Grade algorithm that permits them to be used for long term SECRET data with specific CESG approval.

High Grade: This level of cryptographic protection is for material Protectively Marked SECRET and above.

FIPS 140 Security Requirements for Cryptographic Modules

FIPS 140 validations are conducted by Cryptographic Module Testing laboratories who are accredited by NIST and CSE under the Cryptographic Module Variation Programme www.nist.gov/cmvp. If cryptographic is used to protect PRIVATE data at level 2 of the e-Government Security Framework www.govtalk.gov.uk then a FIPS 140 validated product should be used. Validated products are listed at http://csrc.nist.gov/groups/STM/cmvp/validation.html/

Access Control – Password Handling products

Where a product employs a CESG developed password Hasking and Generation algorithm, CESG retains the right to check that the implementation of the algorithm in those products has been done accurately and to an acceptable standard. It should be remembered that this does not constitute a full Cryptographic evaluation.

Entering into evaluation within IACS

Developers need to contact both a CLEF and the IACS Management Office in order to determine what sort of evaluation is to be carried out and how much the service will cost. It may be advisable to obtain some technical consultancy services prior to the commitment to evaluation, and guidance and advice is available from the CLEFs.

SECTION 15

IACS Scheme

The IACS Management Office and CESG Listed Advisor Scheme consultants. The need for evaluation consultancy should be discussed with the IACS Management Office and the CLEFs at the start of the product evaluation lifecycle.

The IACS Management Office is happy to provide more information on any of the Assurance and Certification Services briefly described here.

CCTM

The CESG Claims Tested Mark (CCTM) scheme provides a testing and certification process for products and services that will deliver assurance at impact Levels 1 and 2. For information on products and services already certified under the scheme and details of the CCTM scheme, visit www.cctmark.gov.uk

UK Commercial Evaluation Facility (CLEF) Contact Details

Vistorm

Vistorm UK Information Security, Bartley Wood Business Park, 1-3 Bartley Way, Hook Hampshire, RG27 9XA, United Kingdom

Point of Contact:	Tony Gallagher
Telephone:	+44 (0) 1256 742 357
Fax:	+44 (0) 1256 742 060
Email:	Tony.Gallagher@vistrorm.com
URL:	www.vistorm.com

CTA.
LogicaCMG

250 Brook Drive, Green Park, Reading, RG2 6UA, United Kingdom

Point of Contact:	Patrick Wandsworth
Telephone:	+44 (0) 118 965 0627
Email:	clef@logica.com
URL:	www.logica.com

Siventure

Unit 6, Clivemont Road, Cordwallis Park, Maidenhead, Berkshire, SL6 7BU, United Kingdom

Point of Contact:	Simon Milford
Telephone:	+44 (0) 1628 651 366
Fax:	+44 (0) 1628 551 365
Email:	simon.milford@siventure.com
URL:	www.siventure.com

SECTION 16

External Common Criteria Scheme

ND USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING

Potential users of products contained in this annex should ensure that they have checked the entry at www.commoncriteriaportal.org to determine which CCRA member certified it. To ensure that CESG recognises the certificate, please make direct contact with the IACS Management Office.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor or CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

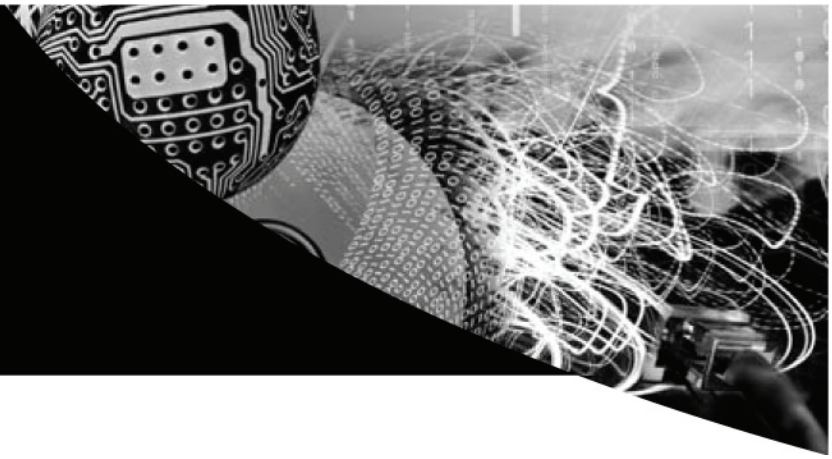
ITSEC/CC

Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from the CESG website.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 16

External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Access Control Devices and Systems			
Citrix® Presentation Server™ 4.5	Citrix Systems Inc.	EAL2+	01 July 2007
RedCastle Version 2.0 for Windows	REDGATE	EAL3+	21-DEC-08
Passlogix v-GO Access Accelerator Suite	Passlogix Inc.	EAL3+	16-DEC-08
ExaProtect Security Management Solutions (SMS)	Exaprotect	EAL1	27-NOV-08
Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8	Citrix Systems Inc.	EAL2+	28-AUG-08
OfficeServ 7400 GWIMC	SAMSUNG ELECTRONICS INC.	EAL3+	16-JUL-08
Symantec™ Networking Access Control Version 11.0	Symantec Corporation	EAL2+	15-JUL-08
IronPort Messaging Gateway Version 5.1.2	IronPort Systems	EAL2	28-JUL-08
Oracle Identity and Access Management 10g Release 10.1.4.0.1	Oracle Corporation UK Limited	EAL4+	27-JUL-08
EXshield V1.0.1.R	SAMSUNG NETWORKS INC.	EAL4	13-JUN-08
Cisco Systems (1100, 1200, 1300, 1400 series Wireless Devices running IOS 12.3 (8)A2; 3200 series Wireless Router running IOS 12.4(6) XE3; A55350, 5400,5850 Universal Gateway running IOS 12.4(17); IAD2430 Integrated Access Device running IOS 12.4(17) with Cisco Secure Access Control Server (ACS) version 4.12.4.13 for Microsoft Windows Server	Cisco Systems Inc	EAL3+	09-JUL-08
Hitachi ID Management Suite Version 3.2	Hitachi ID Systems, Inc.	EAL2	16-MAY-08
RedCastle v3.0 for Asianux	REDGATE	EAL4	30-APR-08
SNIPER IPS Version 6.0e	NOWCOM co., Ltd	EAL4	11-APR-08
Citrix Presentation Server 4.5	Citrix Systems Inc.	EAL2+	01-JUL-07
SANRISE Universal Storage Platform CHA/DKA Program, TagmaStore \Universal Storage Platform CHA/DKA Program. SANRISE Network Storage Controller CHA/DKA Program SANRISE H12000CHA/DKA Program SANRISE H10000 CHA/DKA Program 50-04-34-00/00	Hitachi. Ltd	EAL2	27-JUL-078

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Access Control Devices and Systems (Continued)			
CA Access Control for Windows r8	CA.Inc.	EAL3	20-JUN-07
Citrix Password Manager, Enterprise Edition, Version 4.5	Citrix Systems Inc,.	EAL2+	01-JUN-07
HiCommand Suite Common Component Version 05-51-01	Hitachi, Ltd	EAL2+	30-MAY-07
Boeing Secure Network Server (SNS-3010 and SNS-3210)	The Boeing Company	EAL4+	10-MAY-07
Xceedium GateKeeper Version 4.0	Xceedium	EAL3	05-APR-07
UCosminexus Application Server 07-00	Hitachi Ltd.	EAL2+	27-MAR-07
IBM Tivoli Access Manager for e-Business Version 6.0 with Fixpack 3	IBM Corporation	EAL3+	12-MAR-07
Voiceldent Unit 1.0	Deutsche Telekon AG/T-COM	EAL2+	10-JAN-07
REDOWL secuOS Version 4.0 for RHEL4	TsonNet Co, Ltd	EAL3+	05-JAN-07
RedCastle Version 2.0 for Asianux	REDGATE	EAL3+	22-DEC-06
RedCastle Version 2.0 for RedHat	REDGATE	EAL3+	22-DEC-06
SNIPER IPS Version 5.0(E2000)	WINS Technet Co, Ltd.	EAL4	27-OCT-06
SNIPER IPS Version 5.0(E4000)	WINS Technet Co, Ltd.	EAL4	27-OCT-06
3eTI 3e-525A-3 Access System	3e Technologies International, Inc	EAL2+	15-SEP-06
Citrix Presentation Server 4.5	Citrix Systems Inc.	EAL2+	01-JUL-07
IBM Tivoli Access Manager for Operating Systems Version 5.1 and Fixpack 17	IBM Corporation	EAL3+	24-MAR-06
IBM Tivoli Identity Manager, Version 4.6	IBM Corporation	EAL3+	16-FEB-06
Siebel eBusiness Platform Version 7.8.2	Siebel Systems. Inc	EAL2	01-JAN-06
Computer Associates eTrust Single Sign-On Version 7.0 patch Q067747	Computer Associates	EAL2	18-OCT-05
Secutor Systems Inc. Data Vault X4 version 1.0	Secutor Systems Inc	EAL4	23-SEP-05
Sun java™ System Identity Manager	Sun Microsystems Inc.	EAL2	24-AUG-05

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Access Control Devices and Systems (Continued)			
Citrix MetaFrame Presentation Server 4.0	Citrix Systems Inc	EAL2	01-AUG-05
IBM Tivoli Access Manager for e-Business Version 5.1 with Fixpack 6	IBM Corporation	EAL3+	27-JUL-05
Tarantella Enterprise 3 Version 3.40.911 with Tarantella Security Pack, Version 3.41.211	Tarantella Ltd	EAL2	13-MAY-05
Reflex Disknet Pro	Reflex Magnetics Ltd	EAL2	28-APR-05
SafeGuard Easy 3.20 für Windows 2000	Utimarco Safeware AG	EAL3	24-SEP-04
IBM WebSphere Portal Version 5.0.2	IBM Corporation, New York, USA	EAL2	23-AUG-04
Citrix MetaFrame XP Presentation Server with Feature Release 3	Citrix Systems Inc	EAL2	01-APR-04
Sentinel Model III	Delta Security Technologies	EAL4	01-SEP-02
Biometric Systems and Devices			
PalmSecure SDK Version 24 Premium	Fujitsu Limited	EAL2	30-DEC-08
FortGate™-50B, 200A, 300A, 310B, 500A, 800, 1000A, 3016B, 3600, 3600A, 3810A-E4, 5001SX, 5001FA2, 5001A-DW and FortiWiFi-50B Unified Threat Management Solutions and FortiSO™ 3.0 CC Compliant Firmware	Fortnet, Incorporated	EAL4+	28-Nov-08
Proofpoint Protection Server® Version 5.0.4	Proofpoint, Inc	EAL2+	29-SEP-08
SonicOS Version 5.0.1 on NSA Series and TZ Series appliance	SonicWALL, Inc	EAL4+	16–MAY-08
APPGate Security Server	APPGate Network Security AB	EAL2+	05-MAY-08
Tutus Farist 2.5.2 and 2.5.2-R	Tutus Data AB	EAL4+ALC_F	LR.1 28-FEB-08
Cybex SwitchView SC Series Switches	Avocnet Corporation	EAL4+	30-JAN-08
Sidewinder 7.0.0.02	Secure Computing Corporation	EAL4+	09-NOV-07
Fortress Wireless Secure Gateway Version 1.0	Fortress Technologies, Inc	EAL3	23-OCT-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

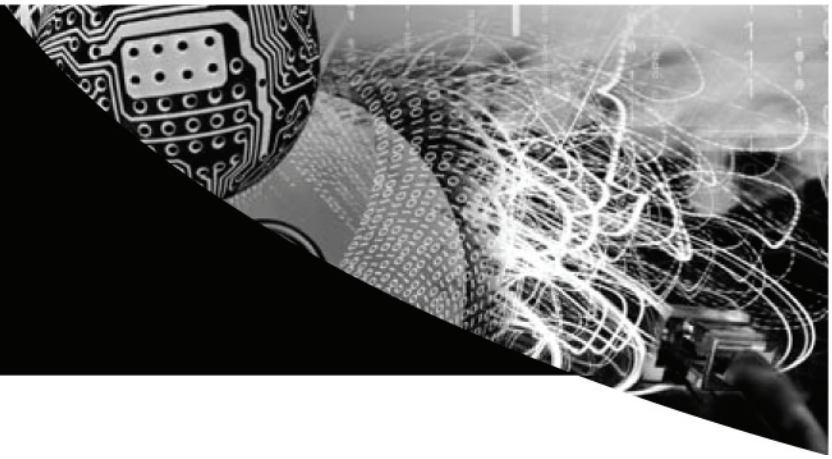
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Biometric Systems and Devices (Continued)			
Symantec Mail Security 8300 Series Appliances Version 5.0	Symantec Corporation	EAL2	22-AUG-07
GeNUScreen 1.0	GeNUA Gesellschaft für Netzwerk-und UNIX-Administration mbH	EAL4+	04-JUL-07
Outbound Downgrade Filter of ASDE Link-1 Forward Filter Version 1.5	NATO C3 Agency	EAL4	14-JUN-07
Senforce Endpoint Secuirty Suite Version 3.1.175	Senforce Technologies, Inc	EAL4+	07-JUN-07
WEBS-RAY 2.0	TrinitySoft Co, Ltd	EAL4	11-MAY-07
Sidewinder G2 Firewall Version 6.1.2.03 (Sidewinder G2 Security Appliance Model 2150D and Sidewinder G2 Software Version 6.1.2.03)	Secure Computing Corporation	EAL4+	01-MAY-07
IPCOM EX Series Firmware Secuirty Component Version1.0.00, Microsoft Internet Security and Acceleration Server 2004 – Enterprise Edition – Service Pack 2 – Version 4.0.3443.594	Microsoft Corporation	EAL4+	21-MAR-07
Cisco ASA 5510, 5520, and 5540 Adaptive Secuirty Appliances and Cisco PIX 515, 515E, 525, 535 Security Appliances, Version 7.0(6)	Cisco Systems, Inc	EAL4+	09-Mar-07
Netfence firewall Version 3.0-2	Phion information technologies GmbH	EAL4+	08-MAR-07
Cisco Firewall Services Module (FWSM) Version 3.1 (3.17) for: Cisco Catalyst 6500 Switches and Cisco 7600 Series routers	Cisco Systems, Inc	EAL4+	05-MAR-07
Cryptek Inc. DaimondTEK (DiamondCentral (NSC Application S/W Version 2.4.0.5, NSD-Prime F/W Version 2.4.0.3) and NSD (DiamondLink, DiamondPak, DiamondVPN, DiamondSAT, DiamondUTC) F/W Version 2.4.0.3) 04, CP 106), Diamond VPN (also sold as CV100); Diamond SAT	Cryptek Inc	EAL4+	20-FEB-07
Cisco IOS Firewall Version 12.3(14)T and 12.4(4)T	Cisco Systems	EAL4=	27-Nov-06
Vforce 1700 Version 1.0	NexG Co, Ltd	EAL3+	27-OCT-06
Vforce 2200 Version 1.0	NexG Co, Ltd	EAL3+	27-OCT-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



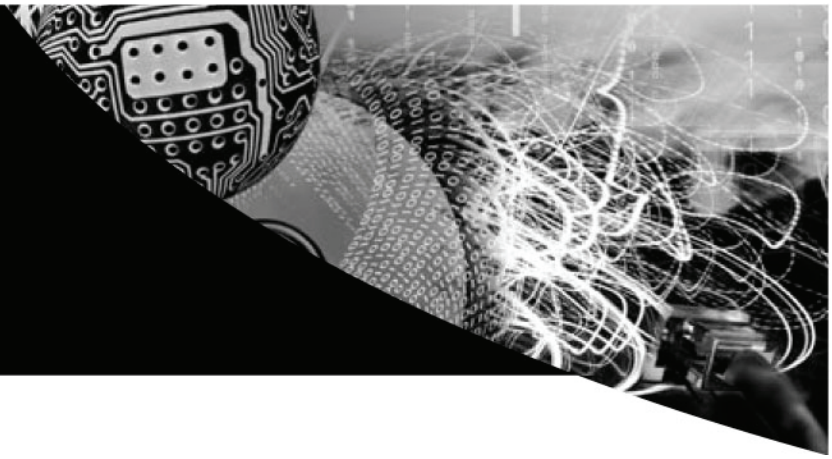
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Biometric Systems and Devices (Continued)			
Astaro Security Gateway (ASG) Version 6.300	Astro AG	EAL2+	25-SEP-06
GeNUGate Firewall 6.0 1.0	GeNUA Gesellschaft für Netzwerk- und UNIX-Administration mbH	EAL4+	12-SEP-06
SafezoneIPS V3.0(SZ-4000)	LG N-Sys	EAL4	30-AUG-06
SECUREWORKS IPSWall 1000 Version 4.0	Oullim Inc,	EAL4	30-AUG-06
Check Point VPN-1/Firewall-1 NGX	Check Point Technologies Ltd	EAL4+	25-AUG-06
DeepSecure Release 2.1	Clearswift	EAL4	01-AUG-06
CyberGuard Firewall/VPN 6.2.1	Secure Computing Corporation	EAL4+	31-MAY-06
Siderwinder G2 Security Appliance Model 2150C with Sidewinder G2 Software Version 6.1.0.05.E51	Secure Computing Corporation	EAL4+	16-FEB-06
Lucent VPN Firewall Version 7.2 (Patch 292)	Lucent Technologies Inc.	EAL4	19-JAN-06
Juniper Networks Security Appliance Evaluation Platform: Juniper Networks NetScreen-5GT, -5XT, -25, -50, -204, -208, -500; Juniper Networks ISG 1000 and 2000; Juniper Networks NetScreen 5200 and 5400 5GT runs ScreenOS 5.0.0r9.r; ISG 1000 and 2000	Juniper Networks	EAL4+	25-DEC-05
CyberGuard Firewall/VPN Version 6.2.1	CyberGuard Corporation	EAL4+	06-DEC-05
CyberGuard Firewall/VPN Version 6.2.1 Models 1150, 1250, 3100, 3400, 3600, 5100, 7100	CyberGuard Corporation	EAL4+	06-DEC-05
SecureLogix Corporation™ ETM™ (Enterprise Telephony Management) System Version 5.0.1	SecureLogix Corporation®	EAL2+	04-NOV-05
Siderwinder G2 Security Appliance Model 410 with Sidewinder G2 Software Version 6.1.0.05.E51	Secure Computing Corporation	EAL4+	27-OCT-05
Microsoft Internet Security and Acceleration Server 2004 – Standard Edition – Version 4.0.2161.50	Microsoft Corporation	EAL4+	20-SEP-05
SurfControl E-mail Filter for SMTP Version 5.0, Service Pack2	SurfControl plc	EAL2	16-SEP-05
Nokia IP130, IP350, and IP380 Firewall/VPN Appliance with Check Point VPN-1/Firewall-1 NG FP2	Nokia Corporation	EAL4	16-SEP-05

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



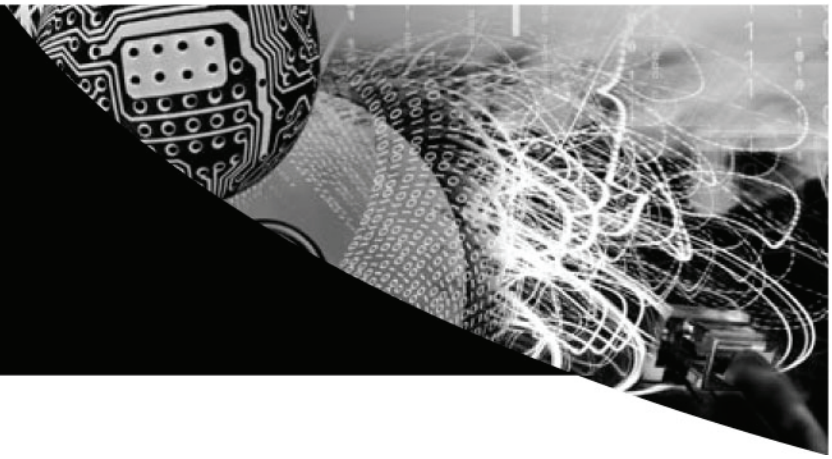
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Biometric Systems and Devices (Continued)			
Alteon Switched Firewall Version 2.0.3 with Hotfix 315/NG_FP3_HFA_315	Nortel	EAL4	12-SEP05
Check Point Software Technologies Incorporated VPN-1/Firewall-1 Next Generation Feature Pack 1	Check Point Software Technologies Incorporated	EAL4	12-SEP-05
Firebox® X Family: Core™ and Peak™ Series with Firewall™ Version 8.0	WatchGuard Technologies, Inc.	EAL4	08-JUL-05
CyberGuard Firewall/VPN Version 6.1.2	CyberGuard Corporation	EAL4+	10-MAY-05
Siderwinder G2 Security Appliance Model 2150 with Sidewinder G2 Software Version 6.1.0.05.E51	Secure Computing Corporation	EAL4+	10-MAY-05
Symantec Gateway Security 400 Series Version 2.1 (Firewall Engine Only)	Symantec Corporation	EAL2	01-MAY-05
Suite Logicielle IPS-Firewall Netasq Version 5	Netasq	EAL2+	01-MAR-05
Fortinet FortiGate™ -50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS™ 2.80 Firmware	Fortinet, Incorporated	EAL4+	28-FEB-05
Clearswift Deep Secure	Clearswift	EAL4	01-JAN-05
Arkoon Fast Firewall v3.0/11 (configurations A200, A500, A2000 et A5000)	Arkoon Network Security	EAL2+	23-NOV-04
BorderWare Mxtreme Mail Firewall Version 8.0	BorderWare	EAL4+	01-AUG-04
Symantec Enterprise Firewall Version 8.0	Symantec Corporation	EAL4	01-JUL-04
Siderwinder G2 Security Appliance Model 210, 310, 315, 410, 415, 510, 515, 1100, 1150, 2150, 4150 and Sidewinder G2 Software Version 6.1	Secure Computing Corporation	EAL4+	01-JUL-04
Symantec Gateway Security Version 2.0 5400 Series (firewall Engine Only)	Symantec Corporation	EAL4	01-APR-04
SecureLogix Corporation™ ETM™ (Enterprise Telephony Management) System Version 4.1	SecureLogix Corporation	EAL2+	01-MAR-04
NetScreen Appliance Models 25, 50, 5XP and 5XT with ScreenOS 4.0.2r7.0	NetScreen Technologies, Inc.	EAL4+	01-JAN-04

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



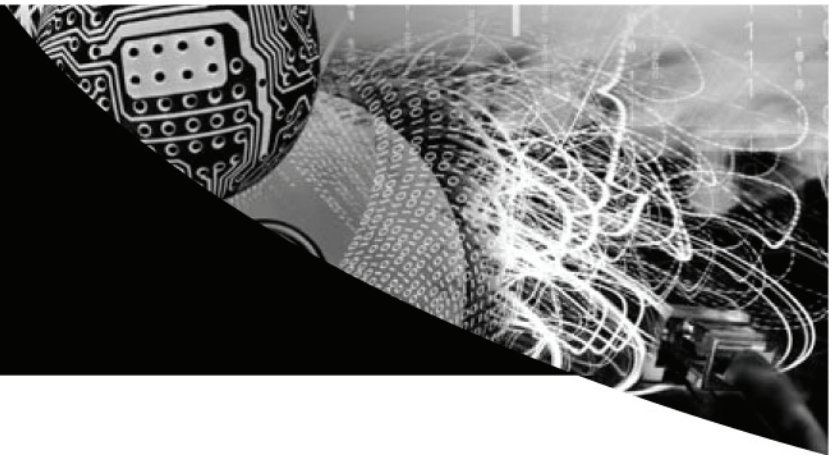
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Biometric Systems and Devices (Continued)			
NetScreen Appliance Model 500, 208, 204 with Screens 4.0.2r7.0	NetScreen Technologies, Inc	EAL4+	01-DEC-03
Lucent Technologies Lucent VPN Firewall Version 7.0 (Patch 531)	Lucent Technologies, Inc	EAL2	01-OCT-03
NetScreen Appliance Model 5200 with Screens 4.0.2r7.0	NetScreen Technologies, Inc	EAL2	01-OCT-03
Stonesoft StoneGate Firewall Version 2.0.5	Stonesoft Corporation	EAL4+	01-SEP-03
Symantec Enterprise Firewall, Version 7.0.4 running on Windows 2000 SP3 and on Solaris 7 & 8	Symantec Corporation	EAL4	01-SEP-03
Check Point VPN-1/Firewall-1© NG on Nokia IPSO	Nokia	EAL4	01-SEP-03
ISA Server 2000 with Service Pack 1 and Feature Pack 1, Firewall	Microsoft Corporation	EAL2	01-SEP-03
Nortel Networks Alteon Switched Firewall Version 2.0.3	Nortel Networks	EAL4	01-AUG-03
Cybex SwitchView SC, Model 520-147-004/Model 520-319-003	Avocent Huntsville Corp	EAL4	01-JUL-03
CS Bastion II	Clearswift	EAL4	01-JUN-03
3Com© Enbedded Firewall Version 1.5.1	Secure Computing Corporation	EAL2	01-JUN-03
NetScreen Appliances includes models, 5XP, 5XT, 25, 50, 204, 208, 500, and 2500 each with Screen 4.0.2r6	NetScreen Technologies, Inc.	EAL4	01-JUN-03
Siderwinder© G2 Firewall, Version 6.0	Secure Computing Corporation	EAL4+	01-MAY-03
SecureLogix Corporation™ ETM™ (Enterprise Telephony Management) System Version 4.0.1	SecureLogix Corporation	EAL2+	01-APR-03
Cisco Secure PIX Firewall Version 6.2(2)	Cisco Systems, Inc	EAL4	01-DEC-02
Owl Computing Technologies Data Diode Version 1 and Owl Computing Technologies Data Diode Version 2	Owl Computing Technologies, Inc	EAL2	01-NOV-02
NetScreen Appliance Models 5XP, 5XT, 25, 50, 100, 204, 208, 500, and 5200 each with ScreenOS 4.0.0r7.0	NetScreen Technologies, Inc.	EAL2	01-NOV-02

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



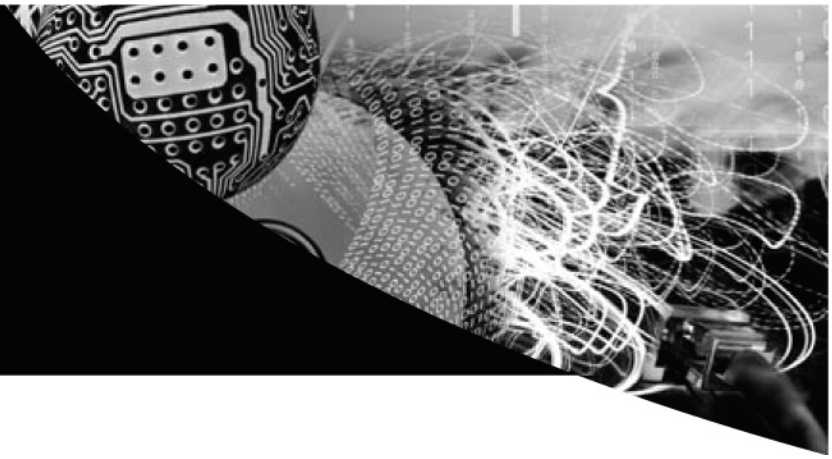
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Biometric Systems and Devices (Continued)			
Siderwinder Firewall, Version 5.2.1	Secure Computing Corporation	EAL2+	01-SEP-02
Check Point VPN-1/Firewall-1© NG	Check Point Software Technologies Ltd	EAL4	01-JUN-02
Symantec Enterprise Firewall, Version 7.0			
Gauntlet Firewall Version 6.0 on Sun Solaris, Version 2.8	Secure Computing Corporation Australia Pty Ltd	EAL4	01-APR-02
SecureLogix Corporation™ Enterprise Telephony Management (ETM™) Platform Version 3.0.1	SecureLogix Corporation®	EAL2+	01-FEB-02
BorderWare Firewall Server Version 6.5	BorderWare Technologies Inc	EAL4+	01-JAN-02
SecureSwitch Dual Network Switch Model #5000600l	Market Central, Inc	EAL4	01-OCT-01
Cisco Secure PIX Firewall Version 5.2(3)	Cisco Systems, Inc.	EAL4	01-JAN-01
CyberGuard Firewall for Unix Ware Release 4.3/KnightStar Premium Appliance firewall 4.3	Secure Corporation formerly CyberGuard Corporation	EAL4+	01-DEC-00
SecureLogix Corporation™ TeleWall™ System Version 2.0	SecureLogix Corporation®	EAL2+	01-OCT-00
Watchguard LiveSecurity System w/Firebox II	Watchguard Technologies	EAL2	01-AUG-00
BorderWare Version 6.1.1 Firewall Server	BorderWare Technologies Inc	EAL4+	01-JAN-00
Safeguard Firewall, Version 2.0.2	Fujitsu Limited	EAL3	01-JAN-00
DragonFly Companion, Version 3.02, Build 129	ITT Industries	EAL2	01-OCT-99
ConSeal Private Desktop Version 1.4	Signal9 Solutions	EAL1	01-MAY-99
VCS Firewall Version 3.0	The Knowledge Group	EAL1	01-MAR-99
DragonFly Guard Model G1.2	ITT Industries	EAL2	01-OCT-98
Milkyway Networks Black Hole Firewall Version 3.01E2	SLM (Milkway) Networks Corporation	EAL3+	01-AUG-97

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Data protection			
ZoneCentral Version 3.1, build 533	PrimX Technologies	EAL2+	18-DEC-08
PGP Universal Server with Gateway and Key Management Version 2.9 running on Fedora Core 6	PGP Corporation	EAL2	21-NOV-08
Applied Identity ID-Enforce Hardware Appliance (models 5000, 7000, and 1000) with ID-Enforce Gateway, Version 3.3 including the ID-Enforce Client D-Mark Version 3.3 and the Identisphere Manager (ID-Policy Version 3.3)	Applied Identity	EAL2	06-OCT-08
Safend Protector Version 3.0	Safend Ltd	EAL2	13-AUG-08
SafeNet Protect Drive Enterprise Version 8.1.1	SafeNet Inc	EAL4	11-AUG-08
Cisco Security MARS 110 and 110R, Cisco Security MARS 210, and Cisco MARS GC2, with software Version 5.2.4.2487	Cisco Systems Inc.	EAL2	07-AUG-09
AquaLogic Interaction 6.1 with AquaLogic Interaction Development Kit	BEA Systems, Inc.	EAL2+	23-MAY-08
Lanscope StealthWatch NC Appliance (Model numbers M45, M250, M250X, G1 G1C, G1X, G1XC, and G1CFX) and StealthWatch Xe	Lanscope. Inc	EAL2+	12-MAY-08
CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1.SP4	CREDANT Technologies, Inc	EAL3	05-MAY-08
Tutus Filkrypto 1.0.2	Tutus Data AB	EAL3	25-FEB-08
FDRERASE/OPEN, Version 02, Level 05	Innovation Data Processing	EAL2+	29-JAN-08
Microsoft Windows Rights Management Services (RMS) 1.0 SP2	Microsoft Corporation	EAL4+	08-AUG-07
SecureDoc Disk Encryption, Version 4.3C	WinMagic Inc.	EAL4	04-JUL-07
Senforce Endpoint Security Suite Version 3.1.175	Senforce Technologies, Inc	EAL4+	07-JUN-07
Connect: Direct® with Secure+ Option v4.5 running on IBM OS/390 and z/OS	Sterling Commerce Inc.	EAL2+	03-OCT06
Connect: Direct® with Secure+ Option Version 3.7 running on UNIX and v4.2 on Windows	Sterling Commerce Inc.	EAL2+	15-SEP-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

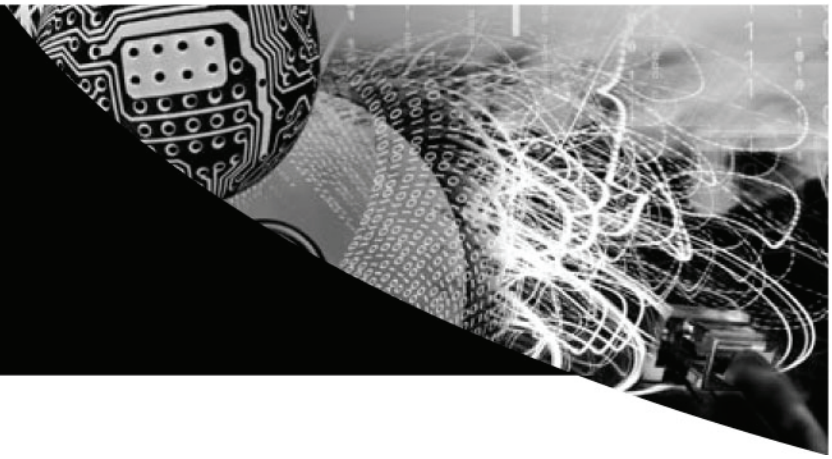
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Data protection (Continued)			
SafeBoot Version 5	Control Break International	EAL4	01-MAY-06
Data Overwrite Security Unit Type D Software Version 0.03	Ricoh Company, Ltd	EAL2	29-MAR-06
Documentum Content Server™ Version 5.3 and Documentum Administrator™ Version 5.3	EMC Documentum	EAL2	21-DEC-05
Silicon Data Vault Desktop Version SDV201B03-0003 and Silicon Data Vault Laptop Version SDV18A03-A2-0003	Secure Systems Limited	EAL2	15-OCT-05
ProtectDrive Version 7.0.3	SafeNet Inc	EAL2	20-SEP-05
FDRERASE/OPEN, Version 5.4, Level 50	Innovation Data Processing	EAL2+	15-AUG-05
Access Control Library 2.0.1 and eSNACC 1.3	Getronics Government Solutions	EAL3+	22-APR-05
Trusted Platform Module Atmel AT975SC3201	Atmel Corporation	EAL3+	08-APR-05
BULL Trustway PCI 2400 (PCA2 Version 76675628-115A S302)	BULL S.A.	EAL2+	21-SEP-04
Security BOX Crypto 6.0 library	MSI S.A.	EAL4+	10-MAY-04
Pointsec PC Version 4.3	Pointsec Mobile Technologies, Inc	EAL4	01-JAN-04
Groove Workspace, Groove Enterprise Management Server, and Groove Enterprise Relay Server, Version 2.5	Groove Networks, Inc	EAL2+	01-SEP-03
Destroy & Destroy Lite 2.01	The Australian Software Company Pty Limited.	EAL2+	01-AUG-03
Encryption Plus© Hard Disk 7.0	PC Guardian	EAL1	01-APR-03
PC Guardian Encryption Plus Hard Disk Version 7.0	PC Guardian	EAL1	01-APR-03
Tripwire Manager 3.0 with Tripwire for Servers 3.0, Tripwire Manager 3.0 with Tripwire for Servers Check point Edition 3.0	Tripwire, Inc.	EAL1	01-Mar-03
UniShred Pro Version 3.3.1	Los Altos Technologies	EAL1	01-DEC-02
Data-Defender 1.0	Fachhochschule Aachen Fachbereich Elektrorechnik und Informationstechnik und IBH-IMPEX Elektronik GmbH	EAL1	01-MAY-02

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



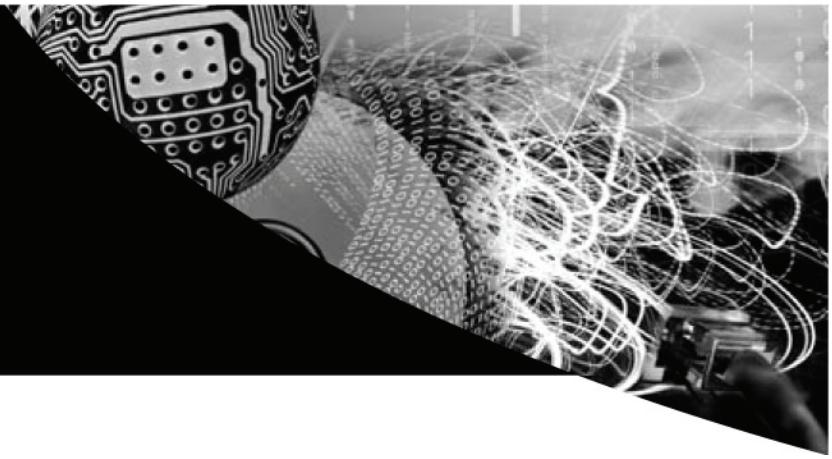
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Data protection (Continued)			
SafeGuard Easy for Windows 2000, Version 1.0	Utimaco Safeware AG	EAL1	01-APR-02
Cryptographic Security Chip for PC Clients, Manufactured by ATMEL (AT90SP0801)	IBM Corporation	EAL3+	01-OCT-01
Electronic Engineering Systems, Inc (EESI) SuperNet 2000 EAL4/r1	Electronic Engineering Systems, Inc	EAL4	01-OCT-00
SuperNet 2000	Electronic Engineering Systems, Inc	EAL4	01-OCT-00
SecureDoc Disk Encryption Version 2.0	WinMagic Inc.	EAL1	01-JUL-99
TrueDelete Version 4.0	Entrust Technologies	EAL1	01-MAR-99
Databases			
Database Engine of Microsoft SQL Server 2005 SP2, Enterprise Edition (English) Version 9.00.3068.00	Microsoft Corporation	EAL4+	24-OCT-08
Oracle Internet Directory 10g (10.1.4.0.1)	Oracle Corporation	EAL4+	27-JUN-08
TeraText DBS 4.3.13	Science Applications International Corporation (SACIC)	EAL2	20-JUN-08
IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6)	International Business Machines Corporation (IBM)	EAL3+ADV_S	29-JAN-08
Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition with Critical Patch Update July 2007	Oracle Corporation	EAL4+	24-JAN-08
Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1 with Critical Patch Update July 2007	Oracle Corporation	EAL4+	24-JAN-08
Sybase Adaptive Server Enterprise 15.0.1	Sybase, Inc	EAL4+	21-SEP-07
Netezza Performance Server Version 3.0	Netezza Corporation	EAL3+	17-SEP-07
IBM WebSphere Federation Server Version 9.1	IBM Corporation	EAL4+	25-MAY-07
PostgreSQL Certified Version Version 8.1.5 for Linux	NTT DATA Corporation	EAL1	22-MAR-07
TeraData Database Version 2R6.1	NCR Teradata	EAL4+	15-FEB-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



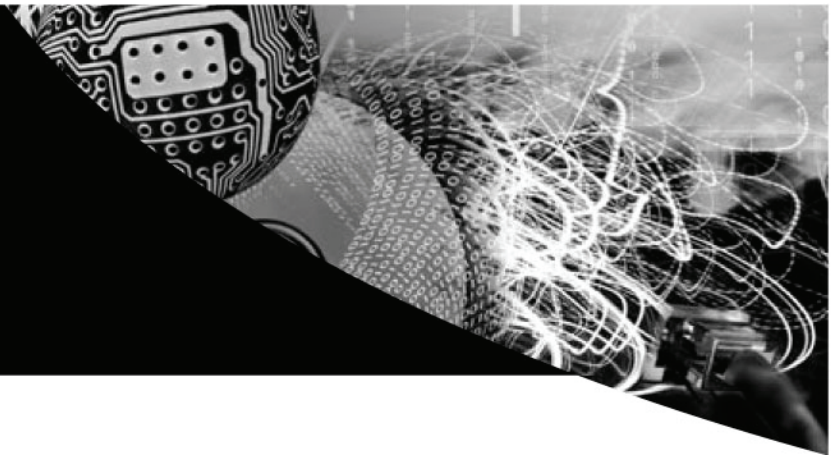
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Database (Continued)			
InterSystems Cache 5.1	InterStstems Corporation	EAL3	15-FEB-07
IBM DB2 Enterprise Server Edition for Linux, Unix, and Windows	International Business Machines Corporation	EAL4+	26-JAN-07
Oracle HTTP Server (OHS) 10g (10.1.2)	Oracle Corporation	EAL4	01-JAN-07
HIRDB/Single Server Version 7 07-03	Hitachi, Ltd	EAL1	22-NOV-06
Symfoware Server Enterprise Extended Edition 8.0.1 (with patch T000132QP-01 and T000133QP-01)	Fujitus Limited	EAL1	22-NOV-06
HIRDB/Parallel Server Version 7 07-03	Hitachi, Ltd	EAL1	22-Nov-06
Symfoware Server Enterprise Extended Edition 7.0.2	Fujitus Limited	EAL1	31-OCT-06
Oracle Application Server 10g	Oracle Corporation	EAL4	01-MAY-06
Adaptive Server Anywhere 9.0.1/9.0.2 Component of SQL Anywhere Studio 9	iAnywhere Solutions Inc	EAL3+	24-APR-06
Oracle Label Security 10g	Oracle Corporation	EAL4+	01-SEP-05
Oracle Database 10g Enterprise Edition	Oracle Corporation	EAL4+	01-SEP-05
Sybase IQ User Administration Version 12.6	Sybase, Inc	EAL3+	11-FEB-05
Oracle9i Label Security on SUSE Linux	Oracle Corporation	EAL4+	01-FEB-05
Oracle9i Release 9.2.0.1.0 on SUSE Linux	Oracle Corporation	EAL4+	01-FEB-05
Adaptive Server Enterprise Version 12.5.2	Sybase, Inc.	EAL4+	20-JAN-05
IBM DB2 Content Manager for Multiplatforms Version 8.2	IBM Corporation	EAL3+	22-DEC-04
IBM WebSphere Application Server Version 5.0.2.8	IBM Corporation	EAL2+	02-DEC-04
Trusted RUBIX Version 5.0 Multilevel Security Relational Database Management System	Infosystems Technology, Inc	EAL4	15-OCT-04
Teradata Database Version 2 R5.0.2	NCR Corporation	EAL2	11-OCT-04
DB2 Universal Database Version 8.2 Workgroup Server edition for Windows, Linux, AIX and Solaris	IBM Corporation	EAL4+	17-SEP-04
Symfoware Server Enterprise Extended Edition	Fujitsu Ltd	EAL4	26-NOV03

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



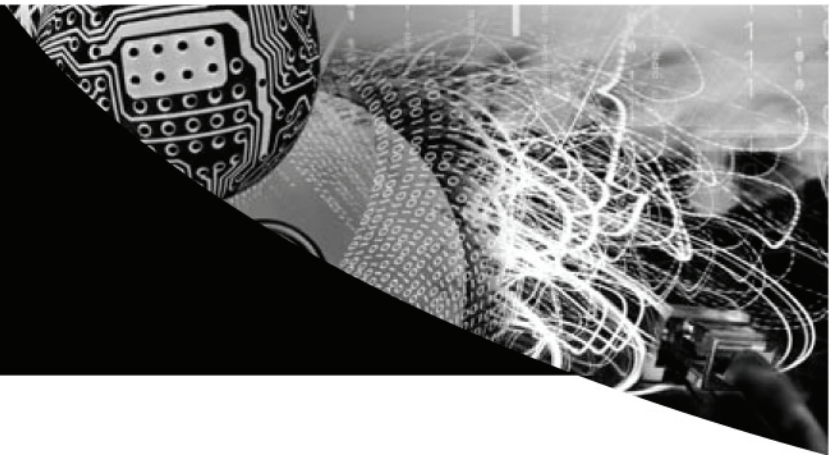
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Database (Continued)			
Oracle9i Release 9.2.0.1.0	Oracle Corporation	EAL4+	01-SEP-03
Oracle9i Label Security	Oracle Corporation	EAL4+	01-SEP-03
Oracle8i Label Security	Oracle Corporation	EAL4	01-MAY-02
Oracle8i Release 8.1.7.0.0	Oracle Corporation	EAL4	01-JUL-01
Oracle8 Release 8.0.5.0.0	Oracle Corporation	EAL4	01-OCT-00
Oracle7 Release 7.2.2.4.13	Oracle Corporation	EAL4	01-SEP-98
Detection devices and systems			
TippingPoint Intrusion Protection System (IPS) E-Series (5000E, 2400E, 1200E, 600E, 210E), software Version 2.5.3.6933	TippingPoint Technologies, Inc	EAL2+	05-SEP-08
Symantec™ Endpoint Protection Version 11.0	Symantec Corporation	EAL2+	25-JUN-08
Third Brigade Deep Security 5.0	Third Brigade, Inc	EAL3+ALC_F	
AirDefence Enterprise 7.2	AirDefence Inc.	EAL2	10-MAR-08
Cisco Intrusion Prevention System (IPS) Version 6.0 Cisco 4200 Series Sensors (IPS 4255,IDS4250, IPS4240, IDS4215, IPS4260); Cisco AIP-SSm-10 and AIP-SSM-20 for the ASA; NM-CIDS; IDSM-2	Cisco Systems, Inc.	EAL2+	31-MAY-07
McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 patch 1	McAfee, Inc.	EAL3	17-MAY-07
RFprotect™ Distributed Version 6.1.2, RFprotect™ Sensor Version 6.1.22, and RFprotect™ Mobile Version 6.1.2	Network Chemistry, Inc.	EAL2	15-MAY-07
Vanguard Enforcer Version 7 Release 1	Vanguard Integrity Professionals, Inc.	EAL3+	08-MAR-07
Cryptek Inc. DiamondTEK (DiamondCentral (NSC Application S/W Version 2.4.0.5, NSD-Prime F/W Version 2.4.0.3) and NSD (DiamondLink, DiamondPak, DiamondVPN, DiamondSAT, DaimondUTC) F/W Version 2.4.0.3) 04, CP 106), Diamond VPN (also sold as CV100); DiamondSAT	Cryptek Inc.	EAL4+	20-FEB-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



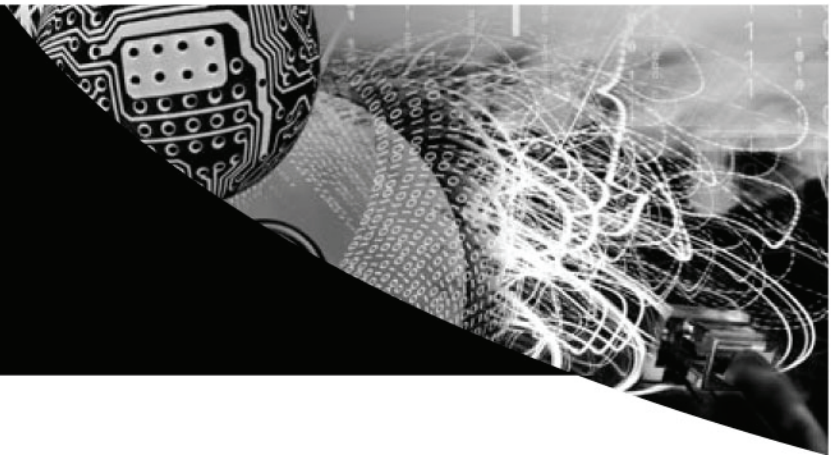
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Detection devices and systems (Continued)			
Qradar Version 5.1.2	Q1 Labs, Inc.	EAL2	26-JAN-07
TESS TMS Version 4.5	INFOSEC Technologies	EAL4	23-DEC-06
Symantec™ Critical System Protection Version 5.0.5	Symantec Corporation	EAL2+	27-NOV-06
ArcSight Version	ArcSight, Inc	EAL3+	29 SEP-06
AirDefence Guard Version 3.5	AirDefence Inc,	EAL2	28-JUL-05
ForeScout ActiveScout V3.05/ConterACT Version 4.1.0	ForeScout Technologies, Inc	EAL4	11-JUL-05
Sourcfire Intrusion Detection System (NS 500, NS 1000, NS 2000, NS 2100, NS 3000, MC 1000,MC 3000)	Sourcefire Inc.	EAL2	03-JUN-05
NFR SentivistT Version 4.0.2 – Updated to Version 4.0.6 and Sentivist Sensor Models 310C, 320C and 320F	NFR Security, Inc	EAL2	22 APR 05
Symantec Manhunt Version 2.11	Symantec Corporation	EAL3	01-DEC-03
TippingPoint UnityOne Version 1.2	TippingPoint Technologies, Inc	EAL2	01-AUG-03
Intrusion, Inc. SecureNet Pro Intrusion Detection System Version 4.1	Intrusion, Inc SecureNet Pro	EAL2	01-DEC-02
ICs Smart Cards and Smart Card related Devices and Systems			
JCLX80jTOP201ID smart Card: java Trusted Open Platform on SLE66CLX800PE microcontroller	Trusted Logic	EAL5	19-DEC-08
eTravel EAC Version 1.1 (Version 01 02) embedded on P5CD080 and P5CD144 microcontrollers	Gemalto	EAL4+	18-DEC-08
TCOS Passport Version 2.0 Release 2-ID1/P5CD080V0B	T-Systems Enterprise Services GmbH	EAL5+	16-DEC-08
S3CC924/S3CC928 16-bit RISC Microcontroller for Smart Card, Revision 1	Samsung Electronics Co, Ltd	EAL5+	11-DEC-08
TCOS Passport Version 2.0 Release 2-ID1/SLE66CLX800PE	T-Systems Enterprise Services GmbH	EAL4+	08-DEC-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



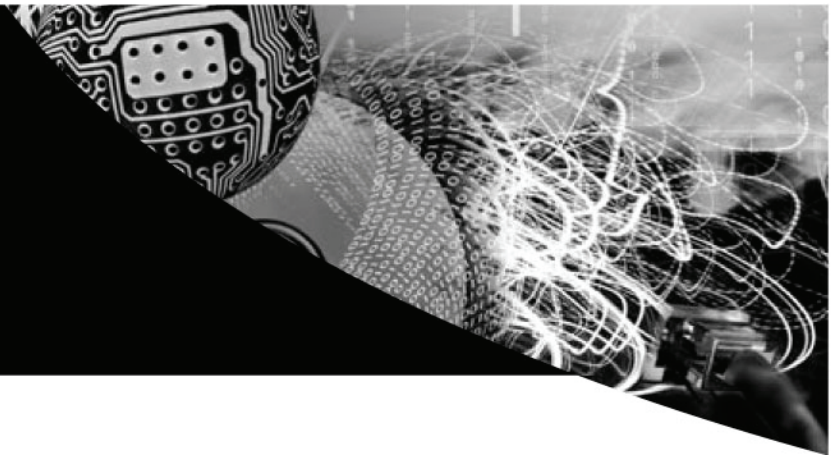
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Atmel Smartcard ICs AT905SC28872RCU/ AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00. or 00.03.13.00	Atmel Corporation	EAL5+	04-DEC-08
NXP Smart Card Controller P5CC052V0A with IC dedicated software: Secured Crypto Library Release 2.0	NXP Semiconductors Germany GmbH	EAL5+	02-DEC-08
NXP Smart Card Controller P5CC037V0A with IC dedicated software: Secured Crypto Library Release 2.0	NXP Semiconductors Germany GmbH	EAL5+	27-NOV-08
NXP Smart Card Controller P5CC024V0A, P5CC020V0A, P5C020V0A, P5CC012V0A all with IC dedicated software: Secured Crypto Library Release 2.0	NXP Semiconductors Germany GmbH	EAL5+	26-NOV-08
Infineon Smart Card IC (Security Controller) SLE66CL187PEM/m2984-a11, SLE66CL187PE/m2985-a11, SLE66CL187PES/ m2986-a11, SLE66CL88PEM/ m2995-a11, SLE66CL88PE/m2994-a11, SLE66CL87PEM/m2992-a11, SLE66CL879PES/m2993-a11, SLE66CL87PE/m2991-a11 and SLE66CL48PE/ m2983-a11 all with specific IC dedicated software	Infineon Technologies AG	EAL5+	25-NOV-08
Infineon Smart Card IC (Security Controller) SLE66CLX1600PEM/m1590-a12, SLE66CLX1600PE/ m1596-a12, SLE66CLX1600PES/ m1597-a12, SLE66CX1600PE/m1598-a12, SLE66CLX1440PEM/ m2090-a12, SLE66CLX1440PE/ m2091-a12, SLE66CLX1440PES/m2092-a12, SLE66CLX1440PE/ m2093-a12, SLE66CLX1280PEM/m2094-a12, SLE66CLX1280PE/m2095-a12, SLE66CLX1280PES/ m2096-a12, SLE66CLX1280PE/m2097-a12 all optional with RSA2048 V1.5 and ECC V1.1 and all with specific IC Dedicated Software	Infineon Technologies AG	EAL4+	06-NOV-08
MTCOS Pro 2.0 ICAO/ST19NR66	MaskTech International GmbH	EAL4+	04-NOV-08
LINQUS USIM 128K Smartcard: ESIGN PKI signature application loaded on GemXplore Generations GT152B-EP38 platform embedded on SLE88CFX400/m8834b17, Version 1.0	Gemalto/Infineon Technologies AG	EAL4+	03-NOV-08
ChipKartenterminal SmartTerminal ST-2xxx Firmware Version 5.11	Cherry GmbH	EAL3+	15-OCT-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

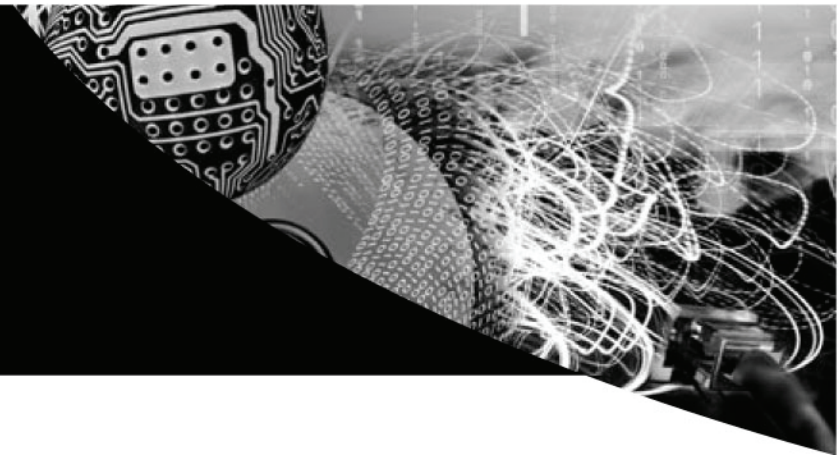
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
STARCOS 3.3 Passport Edition Version 2.0b	Giesecke & Devrient GmbH	EAL4+	10-OCT08
S3FS91J/S3FS91H/S3FS91V	Samsung Electronics	EAL4+	29-SEP-08
STARCOS 3.3 Passport Edition Version 2.0a	Giesecke & Devrient GmbH	EAL4+	18-SEP-08
Renesas HD65256D smartcard integrated circuit V0.1	Renesas Technology Corp.	EAL4+	16-SEP-08
Renesas AE57C1 (HD65257C1) smartcard integrated circuit V01	Renesas Technology Corp	EAL4+	16-NOV-08
Secure Microcontroller ST23YL18A	STMicroelectronics	EAL5+	16-SEP-08
Secure Microcontroller ST23YL18A with Cryptographic Library NesLib SA rev 1.0	STMcroelectronics	EAL5+	16-SEP-08
BAROC/FISC Terminal Security Access Module, Version 1.0	Finacial Information Service Co. Ltd (FISC)	EAL4+	15-SEP-08
ChipKartenterminal SmartTerminal ST-2xxx Firmware Version 5.11	Cherry GmbH	EAL3+	15-OCT-08
Infineon Smart Card IC (Security Controller) SLE66CL180PE/m1585-a14, SLE66CL180PEM/m1584-a14, SLE66CL180PES/ m1586-a14, SLE66CL81PE/ M1594-a14, SLE66CL81PEM/m1595-a14, SLE66CL80PE/m1591-a14, SLE66CL80PEM/m1592-a14, SLE66CL81PES/m1593-a14, SLE66CL41PE/ m1583-a14 all with specific dedicated software	Infineon Technologies AG	EAL5+	22-AUG-08
Secure Microcontroller ST23YL80B	STMcroelectronics	EAL5+	16-AUG-08
Secure Microcontroller ST23YL80B with Cryptographic Library NesLib SA rev 1.0	STMcroelectronics	EAL5+	16-AUG-08
ETravel EAC Version1.1 embedded on secure microcontroller P5CD080 and P5CD144	Gemalto	EAL4+	14-AUG-08
TCOS Passport Version 2.0 Release 2-EAC/ SLE66CLX800PE	T-Systems Enterprise Services GmbH	EAL4+	12-AUG-08
TCOS Passport Version 2.0 Release 2-EAC/ P5CD080V0B	T-Systems Enterprise Services GmbH	EAL4+	08-AUG-08
Infineon Smart Card IC (Security Controller) SLE66CX162PE/m1531-a24 and SLE66CX80PE/m1533-a24 both optional with RSA2048 V1.5 and ECC V1.1 and both with specific IC dedicated software	Infineon Technologies AG	EAL5+	08-AUG08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

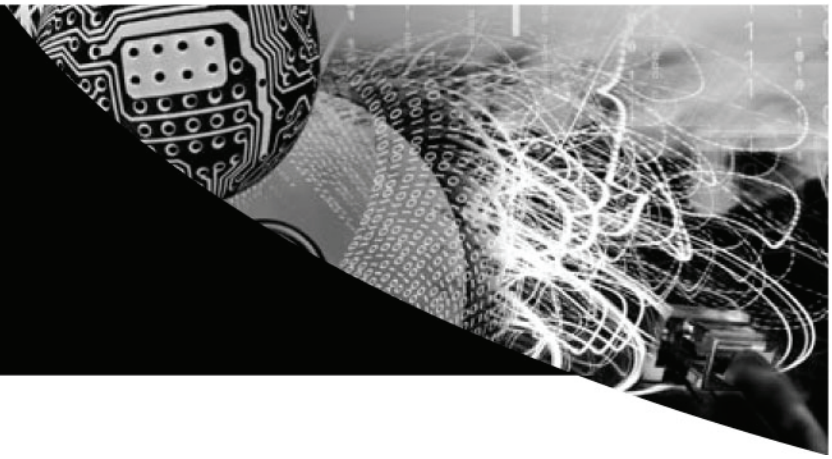


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
E-Passport Morpho-ePass V3 with BAC, AA and EAC RSA/EAC ECC embedded on secure microcontroller STMicroelectronics	Sagem Défence Sécurité/ATMEL Smart Card ICs	EAL4+	28-JUL-08
ASEPcos-CNS/CIE with Digital Signature Application embedded on secure microcontroller AT90SC12872RCFT	Athena Smartcard Solutions Ltd	EAL4+	28-JUL-08
MTCOS Pro 2.1 EAC on P5CD080V08	MaskTech GmbH	EAL4+	08-JUL-08
NXP Smart Card Controller P5CD144V0B with IC Dedicated Software, Secured Crypto Library Release 2.0	NXP Semiconductors Germany GmbH	EAL5+	03-JUL-08
S3CC9LC 16-bit RISC Microcontroller for Smart Card, Revision 2	Samsung Electronics Co., Ltd	EAL5+	01-JUL-08
S3CC91A 16-bit RISC Microcontroller for Smart Card, Revision 3	Samsung Electronics Co., Ltd	EAL4	01-JUL-08
Secure Microcontroller RISC S3FS9CI 32-bit for S-SIM applications	Samsung Electronics Co., Ltd	EAL4+	28-JUN-08
Starcos 3.3 Passport Edition, Version 1.0	Giesecke & Devrient GmbH	EAL4+	27-JUN-08
Sony FeliCa Contactless Smart Card IC Chip RC-S962/1	Sony Corporation	EAL4	27-JUN-08
NXP Smart Card Controller P5CD040V0B with IC dedicated Software, Secured Crypto Library Release 2.0 to EAL5+	NXP Semiconductors Germany GmbH	EAL5+	26-JUN-08
NXP Smart Card Controller P5CC052V0A with specific IC Dedicated Software	NXP Semiconductors Germany GmbH	EAL5+	24-JUN-08
NXP Smart Card Controller P5CD080V0B with Dedicated Software Secured Crypto Library Release 2.0	NXP Semiconductors Germany GmbH Business Line Identification	EAL5+	13-JUN=08
NXP Smart Card Controller P5CCC024V0A, P5CC020V0A, P5C020V0a and P5CC012V0A each with Dedicated Software: Secured Crypto Library Release 2.0 to CC EALS5+	NXP Semiconductors Germany GmbH	EAL5+	13-JUN-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
ID-One ePass 64 Version 1 with BAC and AA embedded on secure microcontroller Atmel	Oberthur Card System	EAL4+	11-JUL-08
TCOS Passport Version 2.0 Release 2-BAC/P5CD080V0B	T-Systems Enterprise Services GmbH	EAL4+	30-MAY-08
TCOS Passport Version 2.0 Release 2-BAC/SLE66CLX800PE	T-Systems Enterprise Services GmbH	EAL4+	30-MAY-08
Secure Microcontroller CXD9916H3/MB94RS403 & HAL Library for contactless smart-card FeliCa	Fujitsu Limited	EAL4+	28-MAY-08
Infineon Smart Card IC (Security Controller), SL66CX680PE/m1534-a14, SLE66CX360PE/m1536-a14, SLE66CX482PE/m1577-a14, SLE66CX480PE/m1565-a14, SLE66CX182PE/m1564-a14, all optional with RSA 2048 Version 1.5 and all with specific IC Dedicated Software	Infineon Technologies AG	EAL5+	27-MAY-08
Infineon Smart Card IC (Security Controller), SL66CLX800PE/m1581-e13/a14, SLE66CLX800PEM/m1536-e13/a14, SLE66CLX800PES/m1582-e13/a14, SLE66CX800PE/m1599-e13/a14, SLE66CLX360PE/m1587-e13/a14, SLE66CLX360PES/m1589-e13/a14, SLE66CLX180PE/m2080-a14, SLE66CLX180PEM/m2081-a14 SLE66CLX120PE/m2028-a14, SLE66CLX120PEM/m2083-a14, all optional with RSA 2048 V1.5 and ECC V1,1 and all with specific IC dedicated software	Infineon Technologies AG	EAL5+	27-MAY-08
ID-One EPass 64 Version 2.0 with BAC and AA	Oberthur Card System	EAL4+	26-MAY-08
Secure Microcontroller ATMEL AT90SC1281RCU rev. B	ATMEL Secure Products Division	EAL4+	20-MAY-08
ID-One EPass 64 Version 2.0 with EAC and ECC	Oberthur Card System	EAL4+	16-MAY-08
ID-One EPass 64 Version 2.0 with EAC and RSA	Oberthur Card System	EAL4+	16-MAY-08
Infineon Smart Card IC (Security Controller), SL66CLX800PE/m1581-e12, SLE66CLX800PEM/m1580-e12, SLE66CLX800PES/m1582-e12, SLE66CLX360PE/m1587-e12, SLE66CLX360PEM/m1588-e12, SLE66CLX360PES/m1589-e12, SLE66CLX800PE/m1599-e12, all with RSA 2048 V1.5 and ECC V1,1 and all with specific Dedicated Software	Infineon Technologies AG	EAL5+	15-MAY-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
TCOS Passport Version 2.0 Release 1.1/P5CD080V0B	T-Systems Enterprise Services GmbH SSC Testfactory & Security	EAL4+ADV_1	04-APR-08
Secure Microcontroller ATMEL AT90SC256144RCT/AT90SC25672RCFT rev. E	AMTEL Secure Products Division	EAL4=	25-MAR-08
Secure Microcontroller ATMEL AT90SC9604RU rev. E	AMTEL Secure Products Division	EAL4+	14-MAR-08
STARCO 3.3 Passport Edition Version 1.0	Giesecke & Devrient GmbH	EAL4+ADV_I	
Secure Microcontroller ATMEL AT90SC12872RCFT/AT90SC12836RCFT rev. M	AMTEL Secure Products Division	EAL5+	27-FEB-08
ATMEL Toolbox 00.03.02.07 on the AT90SC family of devices	AMTEL Secure Products Division	EAL5+	20-FEB-08
MultiApp ID SSCD – MultiApp ID v1.0 patch Version 3.1 embedded on Secure Microcontroller SLE66CX680PE-A13	Gemalto/Infineon Technologies AG	EAL4+	13-FEB-08
MultiApp ID Java Card Platform – MultiApp ID Version 1.0 and patch Version 3.1 embedded on the secure Microcontroller SLE66CX680PE-A13	Gemalto/Infineon Technologies AG	EAL4+	11-FEB-08
TCOS Passport Version 2.0 Release 1/SLE66CLX800PE	T-Systems Enterprise Services GmbH SSC Testfactory & Security	EAL4+ADV_I	06-FEB-08
STARCO 3.01 PE Version 1.2	Giesecke & Devrient GmbH	EAL4+ADV_I	31-JAN-08
STARCO 3.2 PE Version 1.0	Giesecke & Devrient GmbH	EAL4+ADV_I	18-DEC-07
E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I Secure Microcontroller	NTTDATA Corporation	EAL4+	14-DEC-07
ST19NR66-A Secure Microcontroller	STMicroelectronics SA	EAL5+	13-DEC-07
CardOS Version 4.2B FIPS with Application for Digital Signature, running on Infineon Chips SLE66CX322P and SLE66CX642P	Siemens AG	EAL4+	29-NOV-07
MultiApp ID Tacograph 36K card: GEOS platform and Tachograph V1.1 application masked on SLE66CX360PE; Ref. T1002264 A7/version 1.1	Gemalto	EAL4+	16-NOV-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Card ASEPcos-CNS/CIE: At90SC144144CT microcontroller embedded the software ASEPcos-CNS/CIE with Digital Signature Application	Athena Smartcard Solutions Inc	EAL4+	08-NOV-07
TCOS Passport Version 2.0Release 1/P5CD080V0B	T-Systems Enterprise Services GmbH SSC Testfactory & Security	EAL4+	29-OCT-07
Application Morpho-Citiz 32 embedded on PHILIPS/NXP P5CC036V1-D microcontroller (ref: MC32/P5CC036V1D/1.0.1)	Sagem Défence Sécurité/NXP Semiconductors	EAL4+	24-SEP-07
Application Morpho-Citiz 32 embedded on ATMEL microcontroller AT90SC12836RCT-E microcontroller (ref: MC32/AT58819E/1.0.1)	Sagem Défence Sécurité/NXP Semiconductors	EAL4+	24-SEP-07
Java Card System of Usimera Protect Version 1.0 card on SLE88CFX4000P	Gemalto	EAL4+	17-SEP-07
S3CC91C 16-Bit RISC Microcontroller for Smart Card Version 0	Samsung Electronics	EAL4+	10-SEP-07
S3CC9LC 16-Bit RISC Microcontroller for Smart Card Version 2	Samsung Electronics Co., Ltd	EAL4+	10-SEP-07
Infineon Smart Card IC (Security Controller), SL66CL180PE/m1585-e12, SLE66CL180PEM/m1584-e12, SLE66CL180PES/m1586-e12 SLE66CL81PE/m1594-e12, SLE66CL81PEM/m1595-e12, SLE66C80PE/m1591-e12, SLE66CL80PEM/m1592-e12, SLE66CL80PES/m1593-e12, SLE66CL41PE/m1583-e12, with IC dedicated software	Infineon Technologies AG	EAL5+ALC_D	30-AUG-07
Certification Report			
COSMOS V1.1 Card: ID One IAS applet Version 1.01(SSD configuration) loaded on COSMOS 64 RSA D Version 5.4 embedded on P5CT072V0P	Oberthur Card Systems	EAL5+	29-AUG-07
NXP P541G072V0P (JC0P 41 Version 2.3.1)	IBM Deutschland Entwicklung GmbH	EAL4+	10-Aug-07
MICARDO Version 3.0 R1.0	Sagem Orga GmbH	EAL4+	31-JUL-07
TCOS Passport Version 1.0 Release 2/P5CD072V0Q and TCOS Passport Version 1.0 Release 3/SLE66CLX651P/m1522-a14	T-Systems Enterprise Services GmbH SSC Testfactory & Security	EAL4+	31JUL-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Starco 3.01 PE Version 1.1	Giesecke & Devrient GmbH	EAL4+	17-JUL-07
NXP Smart Card Controller P5CD040V0B, P5CC040V0**B**, P5CD020V0B and P5CC021V0A each with specific IC Dedicated Software	NXP Semiconductors Germany GmbH Business line Identification	EAL5+	05-JUL-07
NXP Smart Card Controller P5CD080V0B, P5CN080V0**B**, and P5CC080V0B each with specific IC Dedicated Software	NXP Semiconductors Germany GmbH Business Line Identification	EAL5+	05-JUL-07
NXP Smart Card Controller P5CD144V0B, P5CN144V0**B**, and P5CC144V0B each with specific IC Dedicated Software	NXP Semiconductors Germany GmbH Business Line Identification	EAL5+	05-JUL-07
SM4148 LSI module for Smart Card	Sharp Corporation	EAL4+	04-JUL-07
Renesas AE55C1 (HD65255C1) smartcard integrated circuit Version 03 with ACL Version 2.22	Renesas Technology Corporation	EAL4+	04-JUL-07
Sony FeliCa Contactless Smart Card IC Chip RC-S960/1	Sony Corporation/Fujitsu	EAL4+	28-JUL-07
NXP Smart Card Controller P5CT072V0N, P5CD071V0N, P5CD036V0N, including specific Inlay Packages OM95xx, each with specific IC Dedicated Software	NXP Semiconductors Germany GmbH Business line Identification	EAL5+	26-JUL-07
Renesas HD65256D Version 01 smartcard integrated circuit	Renesas Technology Corporation	EAL4+	30-MAY-07
MICARDO V3.0 R1.0 HPC Version 1.0	Sagem Orga GmbH	EAL4+	25-MAY-07
DNIe Version 1.13	FNMT-RCM	EAL4+	16-MAY-07
Sdu ICAO eMRTD Version 1.0	Sdu Identification bv	EAL4+	02-MAY07
Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18, SLE88CFX2921P/m8859b18, each with PSL V2.00.07 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	27-APR-07
Card Usimera Protect: SLE88CFX4000P microcontroller embedded SIM, USIM and OTA applications on java card open platform (Version 2.1)	Gemalto/Infineon Technologies AG	EAL4+	30-MAR-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

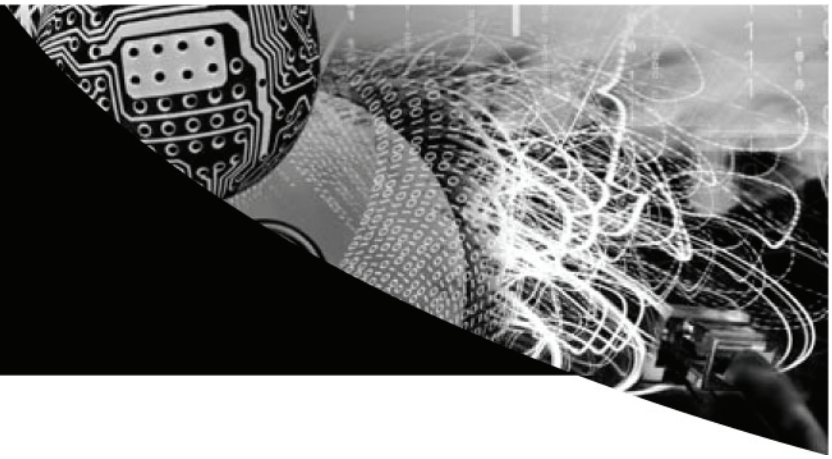
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
ST19NA18C secure microcontroller	STMcroelectronics	EAL5+	28-MAR-07
Oberthur Card ID-One ePass 64K: application ID-One ePass 64K embedded on Philips (NXP) P5CD072/V0P and P5CD072.V0Q components	Oberthur Card System/Philips (NXP)	EAL4+	23-MAR-07
PhenoStor® Kartenlesegerat GRE100010	Bayer Innovation GmbH	EAL3	09-MAR-07
Renesas HD65256D Version 01, smartcard integrated circuit	Renesas Technologies Corporation	EAL4+	08-MAR-07
S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11	Samsung Electronics Co., Ltd	EAL4+	01-MAR-07
S3CC9GW 16-Bit RISC Microcontroller for Smart Card, Version 5	Samsung Electronics Co., Ltd	EAL4+	21-FEB-07
ATMEL Secure Microcontroller AT90SC1287RCFT/AT90SC12836RCFT rev. I&J	ATMEL Secure Products Division	EAL5+	16-FEB-07
MTCOS Pro 2.0 ICACO	MaskTech GmbH	EAL4+	14-FEB-07
ATMEL Secure Microcontroller AT90SC6404RT rev. B	Atmel SmartCard ICs	EAL5+	09-FEB-07
Infineon Smart Card IC (Security Controller) SLE66CLX800PE/m1581-s12, SLE66CLX800PEM/m1580-e12, SLE66CLX800PES/m1582-e12, SLE66CLX360PE/m1587-e12, SLE66CLX360PEM/m1588-e12 ands SLE66CLX360PES/m1589-e12 with specific IC Dedicated Software	Infineon Technologies AG	EAL5+	29-JAN-07
IDOneClassIC Card: ID-One Cosmos 64 RSA Version 5.4 and applet IDOneClassIC Version embedded on P5CT072V0P	Oberthur Card Systems	EAL4+	29-JAN-07
ATMEL Secure Microcontroller AT90SC6408RFT rev. E	Atmel SmartCard ICs	EAL4+	15-JAN-07
Infineon Smart Card IC (Security Controller) SLE66C166PE/m1532-a24	Infineon Technologies AG	EAL5+	01 JAN 07
Infineon Smart Card IC (Security Controller) SLE66CL80P/m1457-a14 and SLE66CL81P/m1436-a14 with specific IC Dedicated Software	Infineon Technologies AG	EAL5+	01-JAN-07
JavaCard Platform GXP3.2-E64PK-CC with GenSAFE V2 Version 1.0	Gemplus SA	EAL4+	01-JAN-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
TCOS Passport Version 1.o Release2/P5CD072V0Q and TCOS Passport Version 1.0 Release 2/SLE66CLX641P/m1522-a12	T-Systems Enterprise Services GmbH, SSC Testfactory & Security	EAL4+	01-JAN-07
Tachograph Card Version 1.1 128/64 R1.0	ORGA Kartensysteme GmbH	EAL4+	01-JAN-07
MN67S140, RV3, FV12 – EAST JAPAN RAILWAY COMPANY Suicall Contactless Smart Card IC Chip	Matsushita Electric Industrial Co.Ltd	EAL4	01-JAN-07
Philips Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with specific IC Dedicated Software	Philips Semiconductors GmbH	EAL5+	01-JAN-07
Philips Secure Smart Card Controller P5CT072V0Q, P5CD072V0Q, P5CD036V0Q including specific Inlay Packages OM95xx, each with specific IC Dedicated Software	Philips Semiconductors GmbH	EAL5+	01-JAN-07
ATMEL Secure Microcontroller AT90SC25672RCT-USB rev. D	Atmel SmartCard ICs	EAL4+	19 DEC-06
IC Platform of FeliCa Contactless Smartcard CXD9861/MB94RS402 with HAL-API & DRNG Library	Fujitsu Limited	EAL4+	14-DEC-06
ATMEL Secure Microcontroller AT90SC9618RCT rev. D	Atmel SmartCard ICs	EAL4+	14-DEC-06
AXSEAL CC V2 72K e-Passport application embedded on Philips P5CD072V0Q Microcontroller	Gemalto/Philips Semiconductors	EAL4+	12-DEC-06
ST19NR66B secure microcontroller	STMicroelectronics	EAL5+	08-DEC-06
Application e-Passport AXSEAL CC V2 36K embedded on Philips P5CD036V0Q microcontroller	Gemalto/Philips Semiconductors	EAL4+	28-NOV-06
ATMEL Secure Microcontroller AT90SC12836RCT rev. K	Atmel SmartCard ICs	EAL4+	27-Nov-06
ATMEL Secure Microcontroller AT90SC320288RCT/AT90SC144144CT rev. G	Atmel SmartCard ICs	EAL4+	16-NOV-06
ST19WR66I secure Microcontroller	STMicroelectronics	EAL5+	07-NOV-06
MULTOS SM10 R2 Version 1.0	Samsung SDS	EAL4+	29-SEP-06
Sharp passport booklet module Version 1.1	Sharp Corporation	EAL4+	29-SEP-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Carta Nazionale dei Servici \(CNS) based on component P5CT072V0P Masked by GOP ID MX 64 with CNS 1.0.7 application	Oberthur Card System	EAL4+	15-SEP-06
Renesas AE4SX1-C (HD65145X1) smartcard integrated circuit Version 2	Renesas Technology Corporation	EAL4	13-SEP-06
Infineon Smart Card IC (Security Controller), SLE66CL80P/m1457a14 and SLE66CL81P/m1436a14 with specific IC Dedicated Software	Infineon Technologies AG	EAL5+	13-SEP-06
Renesas AE57C1 (HD65257C1) smartcard integrated circuit Version 01	Renesas Technology Corporation	EAL4+	13-SEP-06
ATMEL Secure Microcontroller AT90SC6404RT rev. I	Atmel SmartCard ICs	EAL5+	08-SEP-06
MICARDO Tachograph Version 1.0 R1.0	Sage Orga GmbH	EAL4+	06-SEP-06
ATMEL Secure Microcontroller AT90SC12872RCFT rev. E	Atmel SmartCard ICs	EAL5+	01-SEP-06
Philips P541G072V0P (JCOP 41 Version 2.2)	Philips Semiconductors GmbH	EAL4+	31-AUG-06
Starco 3.01 PE	Giesecke & Devrient GmbH	EAL4+	03-AUG-6
Infineon Smart Card IC (Security Controller) SLE88CFX4000P/m8830b17, SLE88CFX4002P/m8834b17, SLE88CFX3520P/m8847b17, SLE88CFX2920P/m8849b17, SLE88CF4000P/m8845b17, SLE88CF4002P/m8846b17, SLE88CF3520P/m8848b17, SLE88CF2920P/m8850b17 each with PSL Vo.50.23_E107 or PSL Vo.50.23_E10 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	21-JUN-06
Philips Secure Smart Card Controller P5CD009V2A and P5CC009V2A each	Philips Semiconductors GmbH	EAL5+	23-MAY-06
Philips Secure Smart Card Controller P5CD009V2B with specific IC Dedicated Software	Philips Semiconductors GmbH	EAL5+	23-MAY-06
Renesas AE55C1 (HD65255C1) smartcard integrated circuit Version 02 with ACL Version 1.43 and additional SHA-256 function	Renesas Technology Corporation	EAL4+	15-MAY-06
Java Card Open Platform	Axalto	EAL4+	10-May-06
ST19WR08C secure microcontroller	STMicroelectronics	EAL5+	20-APR-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Renesas AE55C1 (HD65255C1) smartcard integrated circuit Version 02 with ACL Version 1.43	Renesas	EAL4+	28-MAR-06
Infineon Smart Card IC (Security Controller) SLE88CFX4000P/m8830b17, SLE88CFX4002P/m8834b17, SLE88CFX3520P/m8847b17, and SLE88CFX2920P/m8849b17 each with PSL Vo.50.23 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	23-MAR-06
Philips P5CD036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software	Philips Semiconductors GmbH	EAL4+	13-MAR-06
Philips P5CD036V1D Secure Smart Card Controller with Cryptographic Library IC Dedicated Support Software	Philips Semiconductors GmbH	EAL4+	10-MAR-06
TEMD Version 1.0 (2004-3)	Microelectrónica Española S.A	EAL4+	23-JAN-06
Tarjeta Electrónica Del Ministerio de Defensa TEMD 1.0	Microelectrónica Española S.A	EAL4+	23-JAN-06
ACOS EMV-AV03V1 Configuration B	Austria Card Plastikkarten und Ausweissysteme GmbH	EAL4+	20-JAN-06
ACOS EMV-AV03V1 Configuration A	Austria Card Plastikkarten und Ausweissysteme GmbH	EAL4+	20-Jan-06
ATMEL Secure Microcontroller AT90SC12872RCFT rev. E	Atmel Smart Card ICs	EAL4+	22-DEC-06
JTOP e-Passport – Composant SLE66CLX641P masqué par l'application jTOP e-Passport Version 8.05	Trusted Logic/Infineon	EAL4+	19-DEC-06
ATMEL AT90SC6404RT rev. I microcontroller	Atmel Smart Card ICs	EAL4+	15-DEC-06
Infineon Smart Card IC (Security Controller) SLE66CLX320P/m1559b19, SLE66CLX321P/m1359b19, both with RSA2048 V1.3 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	12-DEC-06
ATMEL AT90SC6404RT rev. B microcontroller	Atmel Smart Card ICs	EAL4+	08-DEC-06
Applet CryptoSmart Version 2.0 on platform Oberthur COSMOS64RSA D V5.2	ERCOM S.A.	EAL2+	01-DEC-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
TCOS Passport Version 1.01/PSCT072 and TCOS Passport Version 1.01/SLE66CLX641P	T-Systems International GmbH	EAL4+	30-NOV-05
ITSO SAM (reference 00_06_13) embedded on microcontroller ATMEL AT90SC3232CS (reference AT568D9 revision K)	ECEBS, Atmel	EAL4+	24-NOV-05
Infineon Smart Card IC (Security Controller) SLE66CLX1162PE/m1531-a24, and SLE66CLX80PE/m1533-a24, both with RSA2048 V1.4 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	11-NOV-05
Java Card Mokard Safe 2.2 Version 2.4.0	ST Incard S.R.L	EAL4+	11-NOV-05
Infineon Smart Card IC (Security Controller) SLE66CLX640P/m1523-a11, and SLE66CLX641P/m1522-a11, both with RSA2048 V1.3 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	08-NOV-05
Micro-circuit S3CJ9QD (reference S3CL9QDX01 rev. 6)	Samsung	EAL4+	27-OCT-05
Philips Secure Smart Card Controller P5CT072V0N including OM9500/1 and OM9501/2, P5CD072V0N and P5CD036V0N with specific IC Dedicated Software	Philips Semiconductors GmbH	EAL5+	07-OCT-05
Infineon Smart Card IC (Security Controller) SLE66C168PE/m1530-a25, SLE66C84PE/m1538-a25, SLE66C44PE/m1539-a25 and SLE66C24PE/m1563-a25 both with specific IC Dedicated Software	Infineon Technologies AG	EAL5+	30-SEP-05
SM4128 (V3) A5-step module	Sharp Corporation	EAL4+	20-SEP-05
Infineon Smart Card IC (Security Controller) SLE66CX680PE/m1534a13, and SLE66CX360PE/m1563a13 both with RSA 2048 V1.4 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	14-SEP-05
Philips Secure Smart Card Controller P5CC036V1C with specific IC Dedicated Software Secure Smart Card Controller	Philips Semiconductors GmbH	EAL5+	12-SEP-05
IC Chip for the reader/writer RC-S940 (CXD9768GG), Version 4	Sony Corporation	EAL4	01-SEP-05
ATMEL AT90SC19272RC rev. E Microcontroller f	Atmel Smart Card ICs	EAL4+	25-AUG-05

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

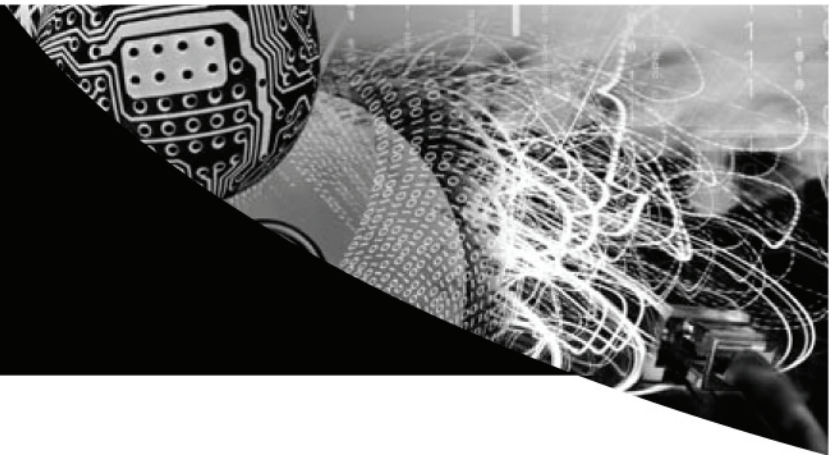
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Philips P5CC036V1D and P5CC009V1D with specific IC Dedicated Software Secure Smart Card Controller	Philips Semiconductors GmbH	EAL5+	19-AUG-05
Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16, with RSA 2048 V1.30 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	12-AUG-05
ATMEL AT90SC12836RCT rev Microcontroller	Atmel Smart Card ICs	EAL4+	09-AUG-05
Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14, and m1484f18 with RSA 2048 V1.30 and specific IC Dedicated Software	Infineon Technologies AG	EAL5+	22-APR-05
ST22L128-A rev. L microcontroller	STMicroelectronics	EAL5+	05-APR-05
ST19XL18P microcontroller	STMicroelectronics	EAL4+	05-APR-05
ATMEL AT90SC7272C rev. D microcontroller	Atmel Smart Card ICs	EAL4+	11-mar-05
Plate-forme Xaica-alpha Version V150i_alpha7rs3_SMO32 sur micro-circuit ST19Xr34F	NTTDATA Corporation/STMicroelectronics	EAL4+	08-MAR-05
ATMEL AT90SC6404RT rev. F microcontroller	Atmel Smart Card ICs	EAL4+	14-FEB-05
Chipkartenterminalfamilie KBPC CX/CX Top	Fujitsu Siemens Computers GmbH	EAL3+	16-DEC-04
ST19WK08G microcontroller	STMicroelectronics	EAL4+	15-DEC-04
ATMEL AT90SC9608RC rev. I microcontroller	Atmel Smart Card ICs	EAL4+	15-DEC-04
ATMEL AT90SC96404R rev. I microcontroller	Atmel Smart Card ICs	EAL4+	15-DEC-04
SmartBord xx44	Cherry GmbH	EAL3+	10-DEC-04
ATMEL AT055SC1604R rev. K microcontroller	Atmel Smart Card ICs	EAL4+	O6-DEC-04
Infineon Smart Card IC (Security Controller) SLE66C82P/m1474a15, and SLE66C42P/m1495a15	Infineon Technologies AG	EAL5	16-NOV-04
Philips P5CC036V1C and P5CC009V1C Secure Smart Card Controller	Philips Semiconductors GmbH	EAL5+	11-NOV-04
ST19XR34F Microcontroller	STMicroelectronics	EAL4+	08-OCT-04
NEC V-WAT 64 V3.0 (UPDt9216000) Microcontroller	NES SCAC/NEC	EAL4+	19-SEP-04

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

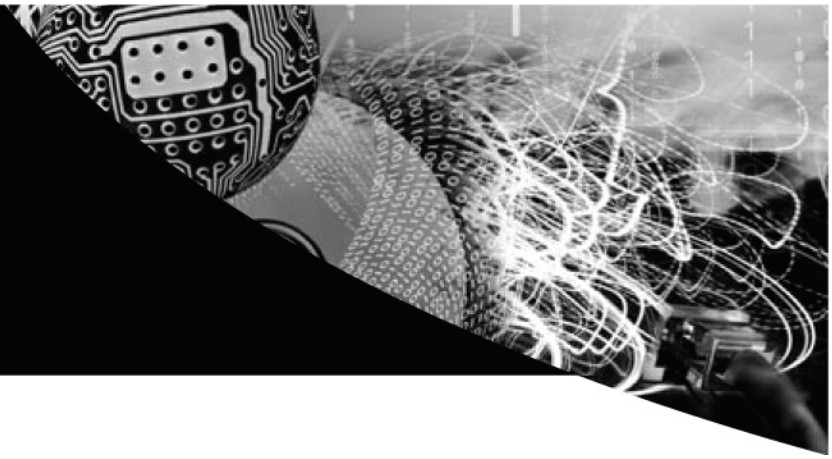


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Philips P5CT072V0M and P5CC0720VoM Secure Smart Card Controller	Philips Semiconductors GmbH	EAL5+	16-SEP-04
Philips P5CC036V0M Secure Smart Card Controller	Philips Semiconductors GmbH	EAL5+	08SEP-04
Philips P5CC009V0M Secure Smart Card Controller	Philips Semiconductors GmbH	EAL5+	06-SEP-04
ST19WL66B microcontroller	STMicroelectronics	EAL4+	20-AUG0-04
ST19XL34P microcontroller	STMicroelectronics	EAL4+	20-AUG-04
Samsung S3CC9RB microcontroller	Samsung Electronics	EAL4+	11-MAY-04
Samsung S3CC9P9 microcontroller	Samsung Electronic	EAl4+	11-MAY-04
Samsung S3CC9FB microcontroller	Samsung Electronic	EAL4+	11-MAY-04
TCOS Tachograph Card Version 1.0	T-Systems International GmbH Service Line SI, T-Telesec	EAL4+	01-MAY-04
Tachograph Card Version 1.1 128/64 R1.1	ORGA Kartensysteme GmbH	EAL4+	01-MAY-04
ATMEL AT90SC9608R rev. F microcontroller	Atmel Smart Card ICs	EAL4+	02-APR-04
Renesas AE45C1 (HD65145C1) smartcard Integrated circuit, Version 01	Renesas Technology Corporation	EAAL4+	01-JAN-04
ATMEL AT90SC9608R rev. E microcontroller	Atmel Smart Card ICs	EAL4+	19-DEC-03
MULTOS 14C (1-1-1) platform with patch AMD0029v002 on component SLE66CX322P/m1484a24	Keycorp Limited/Infineon Technologies AG	EAL4+	04-DEC-03
ATMEL AT90SC3232CS microcontroller	Atmel Smart Card IC	EAL4+	18-NOV-03
Infineon Smart Card IC (Security Controller) SLE66CX322P/ with RSA 2048/m1484a24/m1484a27 and m1484b14	Infineon Technologies AG	EAL5+	01-OCT-03
ATMEL AT90SC9608RC microcontroller	Atmel Smart Card ICs	EAL4+	22-SEP-03
Icitizen Tachograph Version 0.9.0 (reference M256LFCHRON_SI_A5_05_01)	Schlumberger Ststemes, Infineon Technologies	EAL4+	08-SEP-03
Application M/Chip 4 Version 1.0.1.1 for MULTOS	Mondex International Ltd	EAL4+	08-SEP-03

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

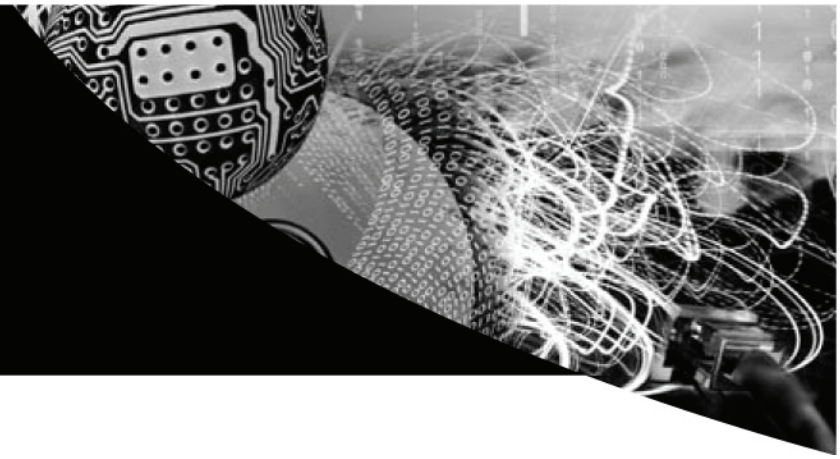
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Tachograph Card Version 1.0 128/64 R1.0	ORGA Kartensysteme GmbH	EAL4+	01-AUG-03
Philips Smart Card Controller P16WX064V0C	Philips Semiconductors GmbH Business Unit Identification	EAL5+	01-JUN-03
Renesas AE43C (HD65143C) Smartcard Integrated Circuit Version 01	Renesas Technology Corp.	EAL4+	01-MAY-03
Philips Smart Card Controller P8WE6017V1J	Philips Semiconductors GmbH Business Unit Identification	EAL5+	01-JAN03
ATMEL A05SC3208R microcontroller (AT568D6 Rev. E)	Atmel Smart Card ICs	EAL4+	01-JAN-03
Hitachi AE450 (HD651450) Smartcard Integrated Circuit Version 01	Hitachi Ltd	EAL4+	01-DEC-02
Philips Smart Card Controller P8WE5033V0G	Philips Semiconductors GmbH Business Unit Identification	EAL5+	01-AUG-02
Philips Smart Card Controller P8WE5033V0F	Philips Semiconductors GmbH Business Unit Identification	EAL5+	01-AUG-02
GemXpresso Pro E64 PK – Java Card Platform Embedded Software V3 (Core)	Gemplus S.A.	EAL4	01-JUL-02
GemXpresso Pro E64 PK – Java Card Platform Embedded Software V3 (Core)	Gemplus S.A.	EAL5+	01-JUL-02
Smart Card IC (Security Controller) SLE66CX322P with RSA 2048/m1484a23	Infineon Technologies AG	EAL5+	01-MAY-02
Hitachi AE45C (HD65145C) Smartcard Integrated Circuit Version 01	Hitachi Ltd	EAL4+	01-MAY-02
GemXplore Xpresso V3 Java Card Platform Embedded Software V3 (Core)	Gemplus S.A.	EAL4	01-APR-02
Sony FeliCa Contactless Smart Card RC-S860	Sony Corporation	EAL4	01-MAR-02
Philips Smart Card Controller P8WE6004V0D	Philips Semiconductors GmbH Business Unit Identification	EAL5+	01-MAR-02
GemXplore Xpresso V3 Java Card Platform Embedded Software V3 (Core)	Gemplus S.A.	EAL5+	01-FEB-02

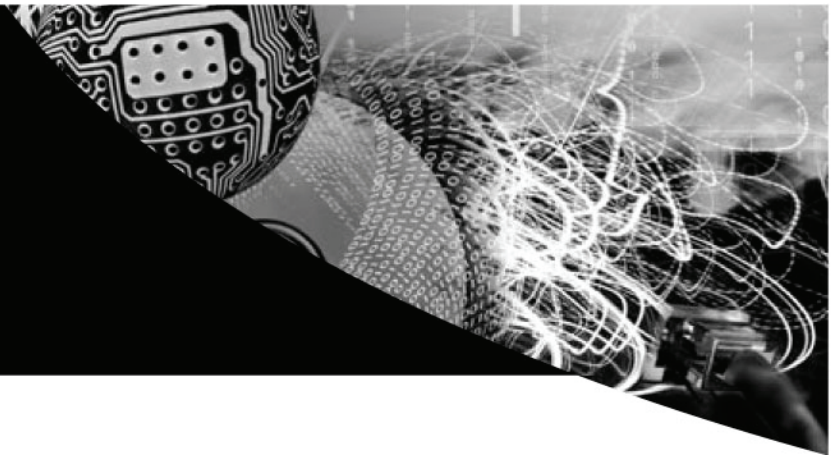
HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
JavaCard 32K CRISTAL (reference M256LCAC2)	SchlumbergerSena, Infineon Technologies SA	EAL4+	01-JAN-02
JavaCard 32K CRISTAL (reference M256LCAC2)	SchlumbergerSena, Infineon Technologies SA	EAL4	01-JAN-02
Gemplus CB-BO'/EMV: P8WE6004V0D Component embedded by MPH021 application (reference P8WE6004V0D/C017D)	Philips, Gemplus	EAL4+	01-JAN-02
ATMEL AT90SC19264RC microcontroller (AT568D5 rev. F)	Atmel Smart Card ICs	EAL4+	01-JAN-02
ATMEL AT05SC1604R microcontroller (AT568C6 rev. H)	Atmel Smart Card ICs	EAL4+	01-JAN-02
ST19SF02AD Component embedded by O.C.S. BO' V3 application (reference ST19SF02AD/RRR)	STMicroelectronics, Oberthur Card Systems	EAL4+	01-JAN-02
Samsung S3CC9PB Microcontroller (reference S3CC9BX01)	Samsung Electronics	EAL4+	01-JAN-02
ATMEL ATE05SC1604R Integrated circuit (AT568C6 rev. I)	Atmel Smart Card ICs	EAL4+	01-JAN-02
COSMOSPOLIC 2.1 V4 JavaCard Open Platform Embedded Software Version 1	Oberthur Card Systems	EAL4+	01-JAN-02
Philips Smart Card Controller P8WE6017V1I	Philips Semiconductors GmbH Business Unit Identification	EAL5+	01-JUL-01
ST19 platform (0.6æ technology): ST19SF16Ccxyz Integrated circuit	STMicroelectronics	EAL4+	01-JAN-01
VOP 2.0.1/JavaCard 2.1.1 JPH33V2 Operating system Version 1 installed on Integrated circuit Philips P8WE5033	Oberthur Card System m	EAL1+	01-JAN-01
ATMEL AT05SC3208R Integrated circuit (reference AT55898 r,v. Q)	Atmel Smart Card ICs	EAL4+	01-JAN-01
ATMEL AT90SC3208R Integrated circuit (reference AT568A9 rev. F)	Atmel Smart Card ICs	EAL1+	01-JAN-01
CT2000 embedded Component (reference ST16RFHD50/RSG-A)	ASK	EAL1+	01-JAN-01

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



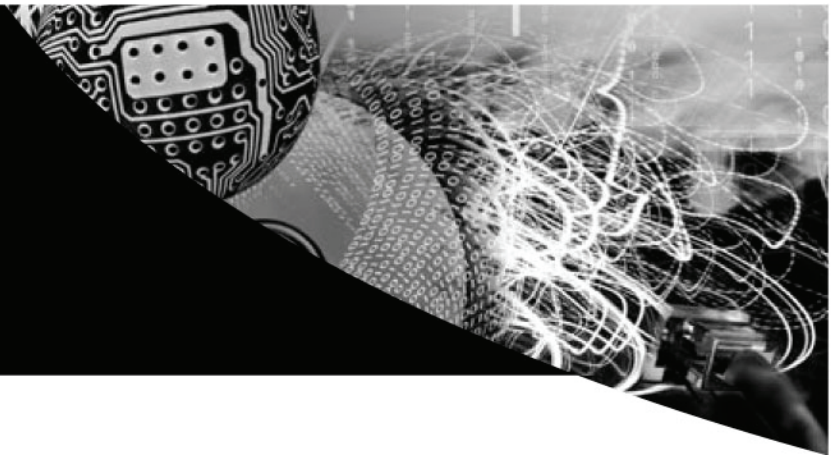
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
M/Chip Select Version 2.0.5.2 Application	Mondex International Ltd	EAL1+	01-JAN-01
MODEUS electronic purse: MODEUS carrier card Version1.1 (reference: ST16RF58/RSE+) and SAM TC/C Version 1.1 retailer security module (reference: ST19SF16FF/RVN)	ASK, CP8, STMicroelectronics	EAL1+	01-JAN-01
Mondex Purse 2 Version 0203 Applet for Multos 4	Mondex International	EAL4+	01-JAN-01
MONEO/CB hybrid card: MONEUS electronic purse application and B4/BO' V3 bank application (reference ST19SF16CC/RCQ Version B312/B023) and SAM retailer security module (reference ST19SF16CC/RCQ Version C112)	IBM, STMicroelectronics	EAL4+	01-JAN-01
MONEO/CB hybrid card: MONEUS electronic purse application and B4/BO' V3 bank application (reference ST19SF04AB/RCU Version B312/B024) and trader SAM security module (reference ST19SF16CC/RCQ Version C112)	IBM, STMicroelectronics	EAL4+	01-JAN-01
Oberthur BO' application Version 1.0.1 and GemClub Version 1.3 loaded on JavaCrad/V0P GemXpresso Platform 211 Version 2	Oberthur Card Systems, Gemplus, Trusted Logic	EAL1+	01-JAN-01
Oberthur B4-BO' V3 Version 1.0 Applet for Multos 4	Oberhtur Card Systems	EAL4+	01-JAN-01
Palmera Protect platform Version 2.0 JavaCard (SLE66CX320P/SB62 embedded component)	SchlumbergerSema, Infineon Technologies	EAL1+	01-JAN-01
ST19 platform (0.6æ technology): ST19SF04A Integrated circuit	STMicroelectronics	EAL4+	01-JAN-01
S3C8975 for smart cards Integrated circuit	Samsung Electronics	EAL1+	01-JAN-00
ST19 platform (0.6æ technology): ST19SF02ADxyz Integrated circuit	STMicroelectronics	EAL4+	01-JAN-00
ST19 platform (0.6æ technology): ST19SF04ABxyz Integrated circuit	STMicroelectronics	EAL4+	01-JAN-00
ST19 platform (0.6æ technology): ST19SF08CExyz Integrated circuit	STMicroelectronics	EAL4+	01-JAN-00
ST19 platform (0.6æ technology): ST19SF16FFxyz Integrated circuit	STMicroelectronics	EAL4+	01-JAN-00

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

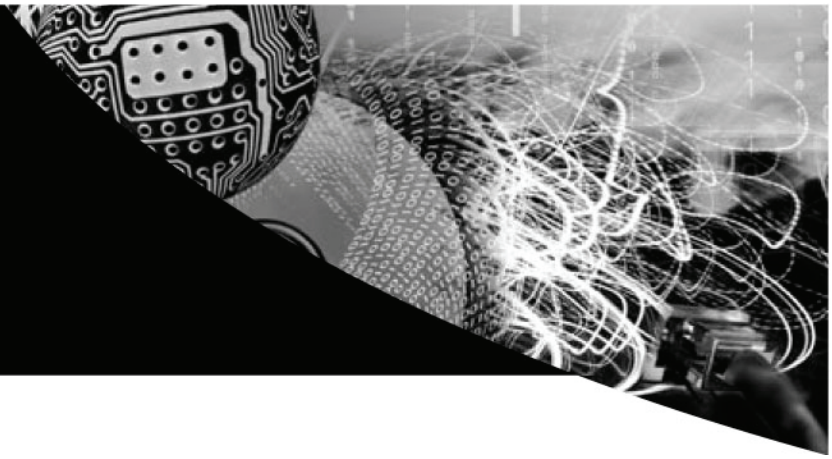


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
ICs, Smart Cards and Smart Card related Devices and Systems (Continued)			
Oberthur BO' application Version 1.0 and Router Version 1.0 designed for Multos Version 4.2	Oberthur Card Systems	EAL4+	01-JAN-00
GemVision SmartID/C application embedded on ST19SF08AC/RMY component	Gemplus	EAL4	01-JAN-00
GemVision SmartID/C application embedded on ST19SF08AC/RMY component	Gemplus	WAL4+	01-JAN-00
JavaCard/V0P GemXpresso 211 platform (Philips Integrated circuit P8WE5032/MPH02)	Philips Semiconductors, Gemplus	EAL1+	01-JAN-00
JavaCard/V0P GemXpresso 211 platform V2 (Philips P8WE5032/MPH04 embedded component, A00000018434D Card Manager)	Philips Semiconductors, Gemplus	EAL1+	01-JAN-00
ST19 platform (0.6æ technology): ST19SF088Dxyz Integrated circuit	STMicroelectronics	EAL4+	01-JAN-00
Philips Smart Card Controller P8WE5032V0B	Philips Semiconductors Hamburg Unternehmensbereichder Philips GmbH	EAL3	01-NOV-99
JavaCard/V0P GemXpresso 211 platform (Philips P8WE5032/MPH02 integrated circuit) with Oberthur BO' v0.32 and Visa VSDC v1.08 applets	Philips Semiconductors Gemplus, Oberthur Card Systems, Visa International Groupement Carte Bleue	EAL1+	01-Jan-99
'Mondex Purse 2@ electronic purse Version 0203 component SLE66CX160S, MULTOS V4.1N operating System	Mondex International	EAL1+	01-JAN-99
B4/B)' bank application of the MONEO/CB hybrid card (reference: ST19SF16BRCL Version B303/B002)	Société Européenne de Monnaie Electronique	EAL1+	01-JAN-99
MONEO electronic wallet card carrier (ST19SF16BRCL v.B303) and PSAM retailer security module (ST19SF16BRCL v.C103)	Société Européenne de Monnaie Electronique	EAL1+	01-Jan-99
Key Management Systems			
BigFix Enterprise Suite Version 7.1.1.315	BigFix, Inc	EAL3	16-Jan09
EnCase Enterprise Version 6.8	Guidance Software, Inc	EAL2	20-NOV-08
Fidelis Extrusion Prevention System 5.0.3	Fidelis Security Systems, Inc	EAL2+	29-OCT-08
Ingrian Networks DataSecure Appliance i416, i426, and i116 Release 4.5.2	Ingrian Networks	EAL2+	10-MAY-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme

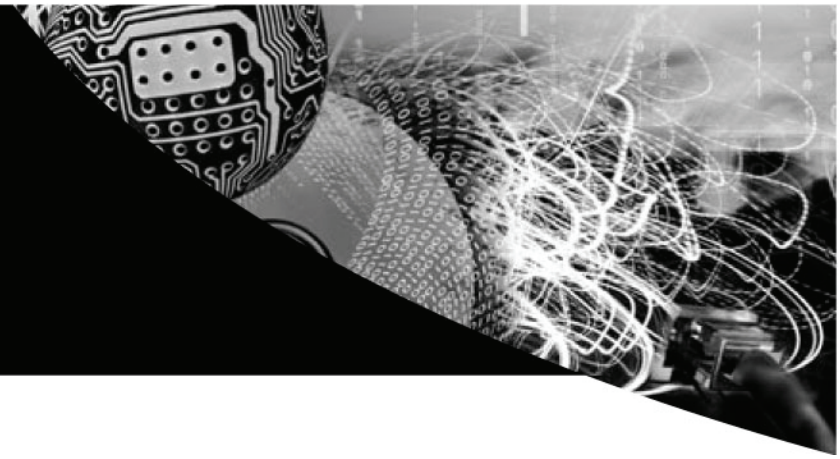


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Key Management Systems (Continued)			
IBM Tivoli Directory Server Version 6	IBM Deutschland	EAL4+	22-APR-08
NetIQ Secure Configuration Manager Version 5.6 and Solaris executable of the NetIQ Security Agent for Unix Version 5.6	NetIQ, Incorporated	EAL2	31-Mar-08
Public Key Infrastructure Framework Version 2.1	United States Marine Corps	EAL4+	08-JAN-08
Public Key Infrastructure Framework (PKIF) Version 1.2	United States Marine Corps	EAL4+	08-AUG-08
Tumbleweed Valicert Validation Authority Version 4.8, Hot Fix 3 (build 388)	Tumbleweed Communications Corp.	EAL3	08-JUN-06
IBM Tivoli Directory Server Version 6.0 Fix Pack 1, Interim Fix 5	IBM Corporation	EAL4+	02-MAR-06
KEYONE 3.0	Safelayer Secure Communications, S.A.	EAL4+	23-JAN-06
Entrust Authority Security Manager 7.0	Entrust Incorporated	EAL4+	15-NOV-04
CoreStreet Real Time Credential Validation Authority Version 4.0	CoreStreet	EAL3+	01-SEP-04
IBM Directory Server 5.2	IBM Corporation	EAL3	01-MAR-04
Alacris OCSP Server Professional Version 3.0.0	Alacris Corporation	EAL2	01-FEB-04
Alacris OCSP Server Professional Version 4.0.0	Alacris Corporation	EAL2	01-JAN-04
IBM Directory Server 5.1	IBM Corporation	EAL2	01-AUG-03
TrustedNet Connect, Version 2.0	SecureNet Limited	EAL4	01-MAY-03
Timestamp Server Version 2.0.2 Patch 1	Baltimore Technologies Pty Limited	EAL3	01-MAY-03
Netscape Certificate Management System 6.1 Service Pack 1	America Online, Inc	EAL4+	01-MAR-03
RSA Keon CA System, Version 6.5	RSA Keon CA System	EAL4+	01-DEC-02
Luna® CA3 v3.97	SafeNet Inc	EAL4+	01-NOV-02
Passport Certificate Server® Version 4.1.1	Diversinet	EAL2+	01-MAY-02

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme

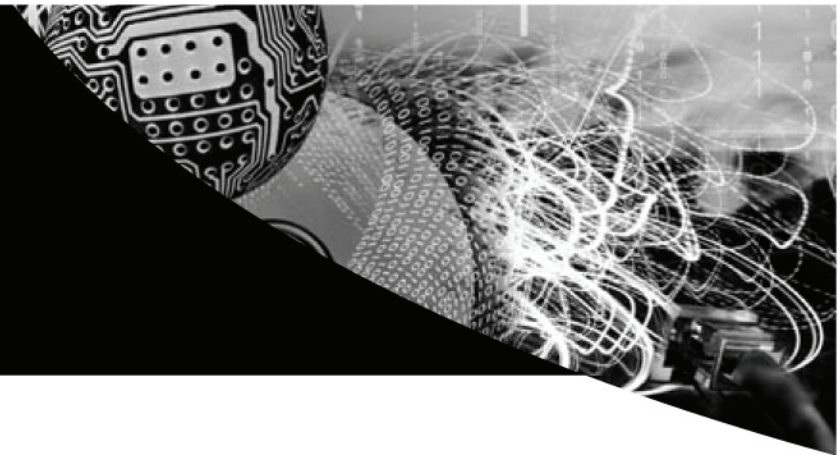


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Key Management Systems (Continued)			
Entrust/Authority from Entrust/PKI 5.1	Entrust Technologies, Inc	EAL3	01-FEB-01
Entrust/RA from Entrust/PKI 5.1	Entrust Technologies, Inc	EAL3	01-FEB-01
Entrust Authority from Entrust/PKI 5.0	Entrust	EAL3	01-MAR-00
Entrust/Admin & Entrust/Authority from Entrust/PKI 4.0a	Entrust	EAL3	01-MAR-99
Network and Network related Devices and Systems			
Cisco Network Admission Control (NAC) solution including the NAC Appliance, NAC Network Module for Cisco Integrated Services Routers (ISRs), NAC Agent, NAC Profiler, and Cisco Secure Access Control Server (ACS)	Cisco Systems	EAL2=	16-FEB-09
Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product	General Dynamics Canada	EAL2+	10-FEB-09
JUNOS 9.3R1 M/MX/T & EX Family of routers and switches	Juniper Networks Inc	EAL3	02-JAN-09
Cisco MDS 9000Family SAN-OS Release 3.2(2c)	Cisco Systems	EAL3+	25-SEP-08
Juniper Networks Odyssey Access Client (FIPS Edition), Version4.56	Juniper Networks, Inc	EAL3+	23-SEP-08
Nortel VPN Router Version 7.05 and Client Workstation Version 7.11	Nortel Networks	EAL4+	27-AUG-08
Cisco ACE XML Gateway and Manager Version 5.0.3	Cisco Systems. Inc	Eal3+	12-Aug-08
Configuresoft Enterprise Configuration Manager 4.0	Configuresoft	EAL3	31-JUL-08
Cisco Info Center v7.1 with Cisco WebTop Version 2.0	Cisco Systems, Inc	EAL2	31-JUL-08
IBM Tivoli Netcool OMNIbus Version 7.1 with Tivoli Netcool Webtop Version 2.0	IBM Corporation	EAL2	31-JUL-08
Check Point Integrity Agent, Version 6.5.063.145	Check Point Software Technologies Ltd	EAL4+	23-Jul-08
Foundry Networks IronSheild (BigIron, NetIron, and FastIron) Switches and Routers	Foundry Networks, Inc	EAL2+	11-JUL-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

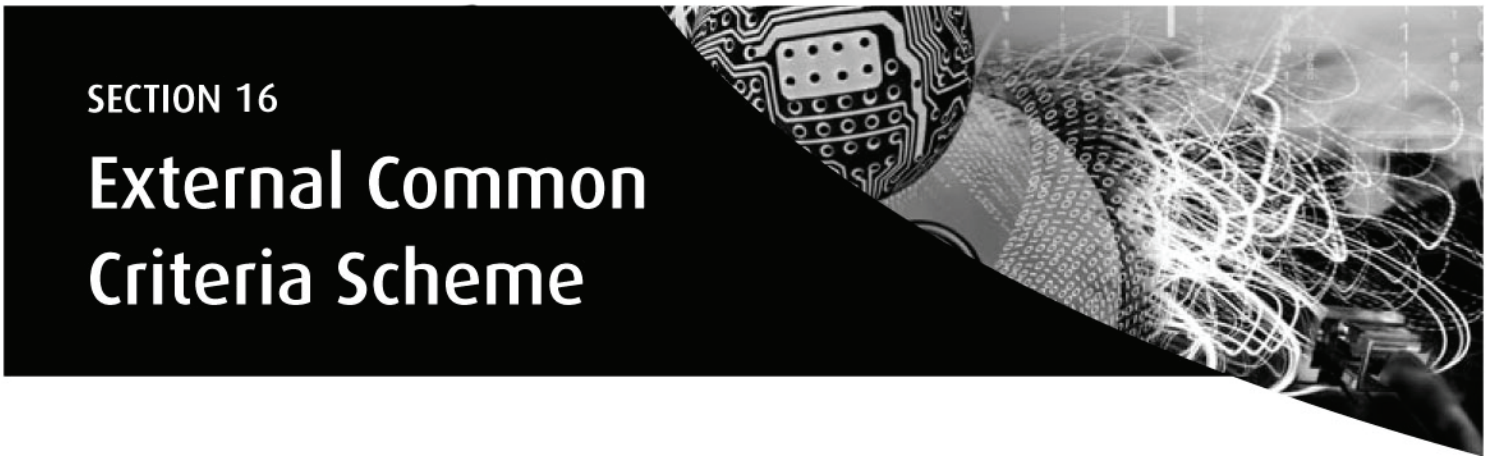
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Network and Network related Devices and Systems (Continued)			
Equant IPVPN system	France Telecom R&D, IIex	EAL2+	08-JUL-08
CypherNET Multi-Protocol Encryptor	Senetas Corporation Ltd	EAL2	06-JUN-08
Cisco IOS IPSec on the Integrated Services Routers, VPN Services Module (VPNSM) and IPSec VPN Shared Port Adapted (SPA), Including VLAN Separation	Cisco Systems	EAL4+	31-MAY-08
Cisco Systems Catalyst Switches and Cisco Secure ACS for Windows Server Version 4.1.4.13	Cisco Systems	EAL3+	27_MAY-08
CA Unicenter Systems Management INSM) r11.1	CA,Inc	EAL2	16-MAY-08
McAfee Hercules Policy Auditor and McAfee Hercules Remediation Manager Version 4.5	McAfee Inc	EAL3	11-APR-08
Appliance MISTRAL TRC 7535 Version4.6.1	Thales Communications S.A.	EAL3+	10-MAR-08
Cisco Systems Routers (800, 1700, 1800, 2600Xm. 2800, 3700, and 7200 running Cisco IOS Release 12.4(11) T2, 7300, 7400, and 7600 running Cisco IOS Release 12.2(18) SXF8; 1000 and 12000 running 12.0(32)s7) and Cisco Secure ACS Version 4.1.2.12	Cisco Systems	EAL3	29-FEB-08
FirePass 4100 Version 5.5.2 + Hotfix HF-522-10	F5 Networks, Inc	EAL2+	19-DEC-07
Blue Coat ProxySG Operating System Version 4.2.5.1	Blue Coat Systems, Inc	EAL2+	14-NOV-07
Fortress Wireless Secure Gateway Version 1.0	Fortress Technologies, Inc	EAL3	23-OCT-07
StillSecure Safe Access Version 5.0	Still Secure	EAL2	04-OCT-07
Symantec™ Security Information Manager Version 4.5	Symantec Corporation	EAL2	12-SEP-07
EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) management Suite 6.5.1	EMC Corporation	EAL2	03-AUG-07.
JUNOScope IP service Manager 8.2R2	Juniper Networks Inc	EAL3+	01-JUL-07
Marimba Client and Server Management from BMC Software Release 6.0.3	BCM Software, Inc	EAL3	21-JUN-07
Senforce endpoint Security Suite Version 3.1.175	Senforce Technologies, Inc	EAL4+	07-Jun-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



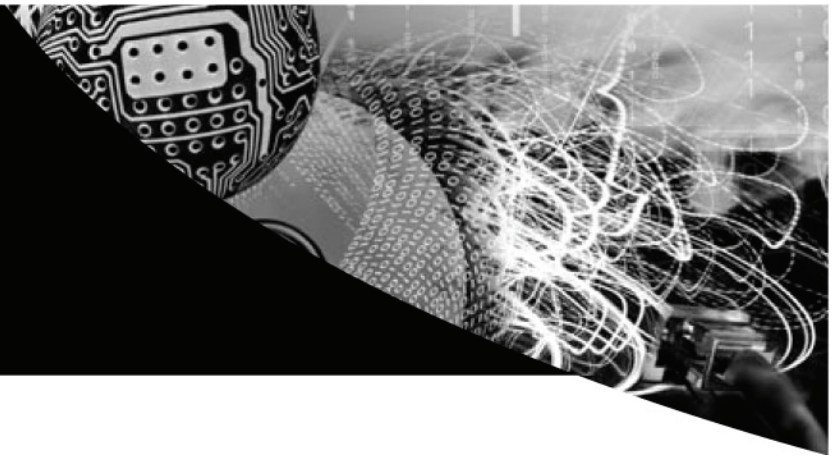
SECTION 16

External Common Criteria Scheme

Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Network and Network related Devices and Systems (Continued)			
Cisco Remote Access VPN	Cisco Systems Inc	EAL2	25-MAY-07
Datacryptor 2000 V3.41 & Datacryptor Advanced Performance V3.511	Thales e-Security Ltd	EAL4	04-MAY-07
CA Directory r8.1 0608 (build 942)	CA, Inc	EAL3	30-APR-07
BIG-IP Local Traffic Manager 6400 High Availability Pair (Qty 2) HardwarePN: 200-0153-05 Rev. C Software Version 9.2.3 + Hotfix CR69440	F% Networks, Inc	EAL2+	16-APR-07
BMC Remedy Action Request System 6.3	BMC Software, Inc	EAL3	10-APR-07
SafezoneIPS@v1.0(sz240U)	LG N-Sys	EAL4	05-APR-07
SafezoneIPS@v1.0(sz5XU)	LG N-Sys	EAL4	05-APR-07
BEA WebLogic Portal V8.1 SP% with BEA06-81/02 and BEA07-107.02 security advisory patches	BEA Systems, Inc	EAL2+	02-APR-07
Juniper Networks M/T/J Series Routers	Juniper Networks Inc	EAL3+	01-APR-07
Security Threat Exclusion System SHEILD/ExLink-IA 1.0	Hitachi Information Systems, Ltd	EAL1	22-MAR-07
CISCO IOS/IPSec release 12.4(6)T3, 12.4(7) & 12.2(33)SRA	Cisco Systems	EAL2	21-MAR-07
Sniffer InfiniStream Enterprise (Sniffer InfiniStream 3.0 SP1 (MR7) Console Software, Sniffer InfiniStream 3.0 SP1 (MR7) Capture Engine Software, Sniffer Enterprise Administrator 4.1 (MR2) Software, Sniffer Enterprise Visualizer 4.1 (MR2) Software)	Network General	EAL3+	09-FEB-07
StillSecure VAM V5.5	StillSecure	EAL2	26-JAN-07
HP Network Node Manager Advanced Edition Software Version 7.51 with patch PHSS_35278	Hewlett-Packard Development Company, L.P.	EAL2	26-JAN-07
Vforce 1700 V1.0	NexG Co, Ltd	EAL3+	27-OCT-06
Vforce 2200 V1.0	NexG Co, Ltd	EAL3+	27-OCT-06
Citadel Hercules® Enterprise Vulnerability Management (EVM) Version 4.1	McAfee, Inc	EAL3	23-OCT-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Network and Network related Devices and Systems (Continued)			
Juniper Network IDP 4.0 & NSM 2006.1	Juniper Networks, Inc	EAL2	23-OCT-06
CISCO IOS/IPSec release 12.3(6a)	www.cisco.com	EAL4	29-SEP-06
LANDesk Management Suite 8	LANDesk Software, Inc	EAL2	28-SEP-06
Remote Communication Gate Application Software 3.34	Ricoh Company, Ltd	EAL3	28-JUN-06
STAT Guardian™ Vulnerability Management Suite (VSM) 6.4.0	Harris Corporation	EAL2+	23-MAY-06
Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14	Juniper Networks	EAL2	24-APR-06
HP OpenView Select Access Version 5.2	Hewlett-Packard Company	EAL2	13-APR-06
Marconi Service Edge Routers (BXR-1000/BXR-5000)	Marconi Corporation plc	EAL3	29-MAR-06
Securify SecurVantage Version 5.0	Securify Inc	EAL3	24-FEB-06
ETrust Admin V8.0 with CAM Version 1.11 patch	Computer Associates	EAL2	03-FEB-06
BEA WebLogic Server 7.0 SP6 with BEA05-107.00 Advisory Patch	BEA Systems Inc	EAL2+	27-Jan-06
Opsware System 4.5 Patch 1	Opsware	EAL2	12-DEC-05
Arbor Networks PeakFlow X Version 3.1.4	Arbor Network Inc	EAL2	02-NOV-05
Cisco ONS 15454 SONET Multiservice Provisioning Platform (MSPP)	Cisco Systems Inc	EAL2	21-OCT-05
CipherOptics™ SG-Series Network Security Appliance Version 3.1 – Models SG 100 and SG 1002	CipherOptics Inc	EAL2	21-OCT-05
Secure Remote Access (SRA) Client Version 3.7.1 Server Version 4.2.1	ActivCard Developments Pty Ltd	EAL2	01-OCT-05
Owl Computing Technologies, Inc Data Diode Network Interface Card Version 3	Owl Computing Technologies, Inc	EAL4	02-SEP-05
Hewlett-Packard OpenView Operations for UNIX V A.08.10	Hewlett-Packard Company	EAL2	19-AUG-05
Boitier MISTRAL TRC 7535 Version 4.5.2.2	Thalès Communications	EAL23+	30-MAY-05

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

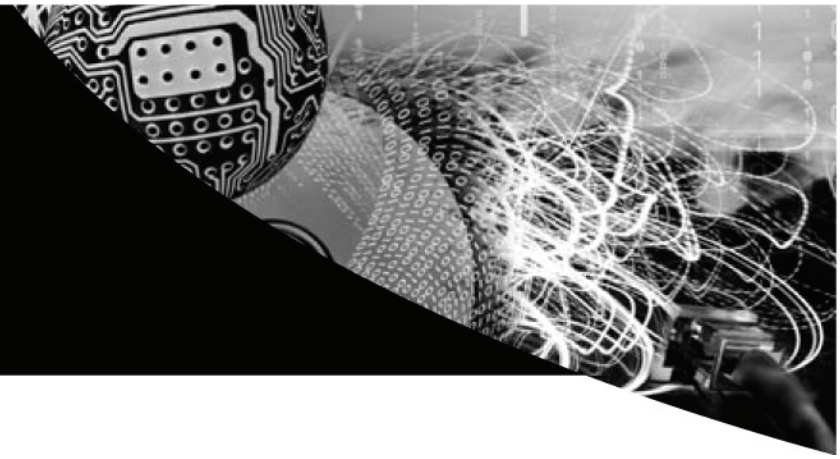
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Network and Network related Devices and Systems (Continued)			
NCircle™ IP360TM Vulnerability Management System Version 6.3.4	NCircle Inc	EAL3	16-MSY-05
SQ-Phoenix Digital Encryptor Version2.7	CES Communications Ltd	EAL2	27-APR-05
Marconi ASX/TNX and BXR Family of Multiservice Switch/Routers	Marconi Corporation plc	EAL3	13-APR-05
NIKSUN®, Inc NetDetector®/NetVCR® 2005	NIKSUN® Incorporated	EAL2	03-MAR-05
Market Central SecureSwitch Fiber Optic A/B/C Switch Revision A	Market Central, Inc	EAL4+	13-JAN-05
Network Security Manager™ (NSMTM) Version 4.1	Intelliactics Inc.	EAL2	01-DEC-04
BULL Trustway VPN Appliance Version 3.01.06	BULL S.A.	EAL4+	26-NOV-04
Marconi Selenia Communications MPS	Marconi Selenia Secure Systems	EAL4	01-JUL-04
Citadel Hercules® Automated Vulnerability Remediation Version 2.2.0	McAfee Inc	EAL3	01-MAR-04
Foundry Networks, Management Module IV: J-BxGNR4 and J-FxGMR4	Foundry Networks Inc	EAL2	01-JAN-04
Juniper Networks M & T Family of Internet Routers running JUNOS 6.0r1. Model numbers M5. M10, M20, M40e, M7i, M160, T320, T640	Juniper Networks	EAL2	01-JAN-04
Securify SecurVantage Version 3.1	Securify, Inc	EAL2	01-JAN-04
Secureworks Version 3.0	Oullim Information Technology, Inc	EAL3	01-SEP-03
STAT® Scanner Professional Version 5.08	Harris Corporation	EAL2+	01-APR-03
BMC Software PATROL, Version 3.4.11	BMC Software	EAL2	01-SEP-02
Cisco IPSec Crypto System	Cisco Systems Inc	EAL4	01-SEP-02
DiamondTEK	Cryptek Secure Communications, LLC	EAL4	01-JUN-02
BMC PATROL Perform/Predict, Version 6.5.30	BMC Software	EAL2	01-APR-02
M>Tunnel 2.5 (MT25-B34-08)	EADS Telecom	EAL2+	01-JAN-02
CTAM Cyphercell ATM Encryptor Version 1.2.1	Senetas Corporation Ltd	EAL4	01-APR-01
Secure Session VPN Version 4.1.1	KyberPass	EAL1	01-OCT-00

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



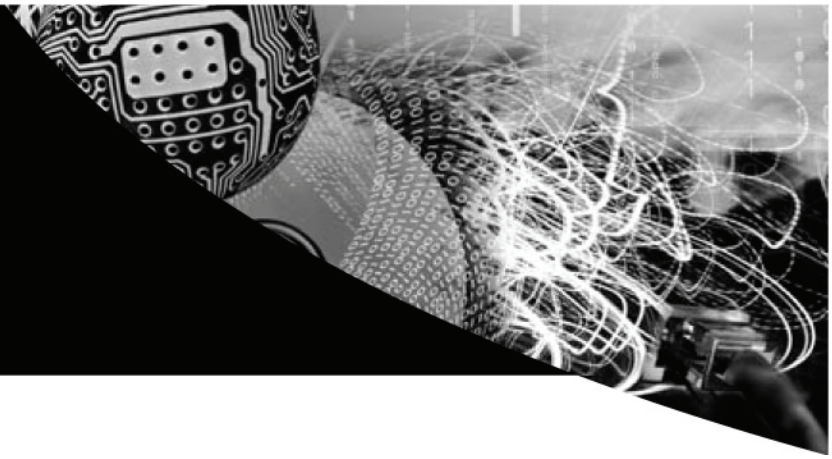
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Operating systems			
Cray UNICOS/Ic Operating System 2	Crai Incorporated	EAL3+	12-DEC-08
SECUWARE OPERATING SYSTEMS version 4.1.0.276	Secuware	EAL2	10-NOV-08
SECUWARE VIRTUAL SYSTEMS version 4.1.0.276	Secuware	EAL2	10-NOV-08
PR/SM for IBM System z10 EC GA1	International Business Machines Corporation (IBM)	EAL5	29-OCT-08
Oracle Enterprise Linux Version 5 Update 1	Oracle Corporation	EAL4+	15-OCT-08
Microsoft Windows Vista and Windows Server 2008	Microsoft Corporation	EAL1	17-SEP-08
Green Hills Software INTEGRITY-178B Separation Kernel, comprising: INTEGRITY-178B Real Time Operating System (RTOS), VersionIN-ICR750-0101-GH01_Rel running on Compact PCI card Version CPN 944-2021-021 with PowerPC, Version 750Cxe	Green Hills Software, Inc	EAL6+	01-SEP-08
Microsoft Windows Mobile 6.1	Microsoft Corporation	EAL2+	06-AUG-08
IBM z/VM Version 5 Release 3	IBM Deutschland Entwicklung GmbH	EAL4+	28-JUL-08
XTS-400/STOP 6.4 U4	BAE Systems, Inc	EAL5+	03-JUL-08
Aruba 6000 and Aruba 800 Series Mobility Controller running ArubaOS Version 2.4.8.14-FIPS	Aruba Networks	EAL2+	27-JUN-08
Solaris 10 Release 11/06 Trusted Extensions	Sun Microsystems, Inc	EAL4+	11-JUN-08
AIX 6 Version 6100-00-02 with optional Virtual IO Server (VIOS) Version 1.5	International Business Machines Corporation (IBM)	EAL4+	15-MAY-08
Red Hat Enterprise Linux Version 5.1	Silicon Graphics, Inc	Eal4+	21-APR-08
Hewlett Packard HP UX-11i	Hewlett-Packard Company	EAL4+	26-MAR-08
Windows Mobile 6	Microsoft Corporation	EAL2+ALC_F	
Microsoft Windows Mobile 5.0 MSFP	Microsoft Corporation	EAL2+ALC_F	
IMB z/)S Version 1, Release 9	Microsoft Corporation	EAL2+ALC_F	
Microsoft Windows Server 2003 SP2 including R2, Standard, Enterprise, Datacenter, x64, and Itanium Editions; Windows XP Professional SP2 and x64 SP2; Windows XP Embedded SP2	Microsoft Corporation	EAL4+	07 FEB-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



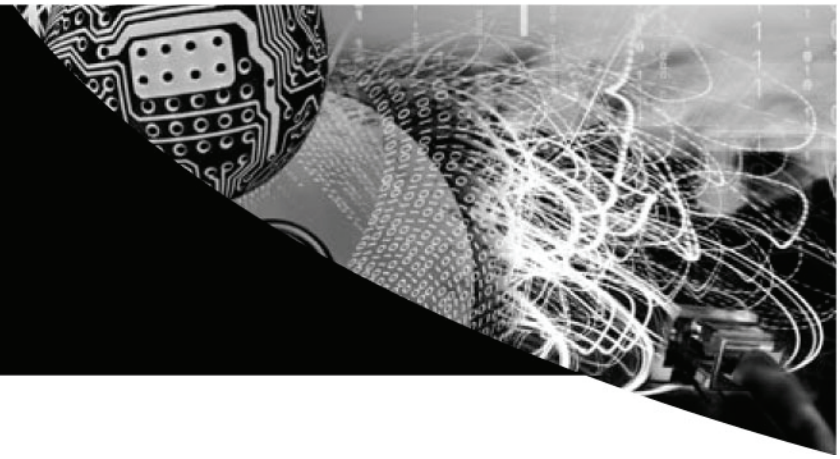
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Operating systems (Continued)			
Solaris™ 10 Release 11/06	Sun Microsystems inc	EAL4+	06-NOV-07
SUSE Linux Enterprise Server 10 SP1	IBM Corporation	EAL4+	08-OCT-07
Oracle Enterprise Linux Version 4 Update 4	Oracle Corporation UK Limited	EAL4+	19-JUL-07
Oracle Enterprise Linux Version 4 Update 5	Oracle Corporation	EAL4+	18-JUL-07
Red Hat Enterprise Linux Version 5	Hewlett Packard Company	EAL4+	26-JUN-07
Airtight Networks SpectraGuard Enterprise Version 5.0 and SpectraGuard SAFE Enterprise Edition Version 2.0	AirTight Networks, Inc	EAL2	08-JUN-07
Re Hat Enterprise Linux Version 5 running on IBM Hardware	IBM Corporation	EAL4+	07-JUN-07
eEye Retina Enterprise Suite, Comprising the following eEye components: Retina Network Security Scanner Version 5.4.21.53, REM Version 3.0.2.571.	eEye Digital Security Corporation	EAL 2	25-MAY-07
IBM z/OS Version 1, Release 8	IBM Corporation	EAL4+	16-May-07
OSIV/MSP Version 1, Release 8	Fujitsu Limited	EAL1	27-ARP-07
Network Appliance Data ONTAP Versions 7.0.3 and 7.0.4	Network Appliance, Inc	EAL2	03-APR-07
Microsoft Windows 2003 and Microsoft Windows XP	Microsoft Corporation	EAL4+	01-APR-07
Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 4 Running on Unisys ES7000 Hardware models405, 410, 420, 430, 440, 505, 510, 520, 530, 540, and one	Unisys Corporation	EAL3+	29-JUN-07
Red Hat Enterprise Linux (RHEL) Advanced Server (AS) Version 3 Update 5 Running on Unisys ES7000 Hardware models405, 410, 420, 430, and 440	Unisys Corporation	EAL3+	29-JAN-07
MIRACLE LINUX Version 4.0/MIRACLE LINUX Version 4.0 One/MIRACLE LINUX Version x86-64 One Operating system Version 4.0	MIRACLE LINUX CORPORATION	EAL1	24-JAN-07
IBM AIX 5L for POWER V5.3, Technology Level 5300-05-02 with Argus Systems Group PitBull Foundation Suite 45.0 and optional IBM Virtual 10 Server (VIOS) Version 1.3	Innovative Security Systems, Inc	EAL4+	16-JAN-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

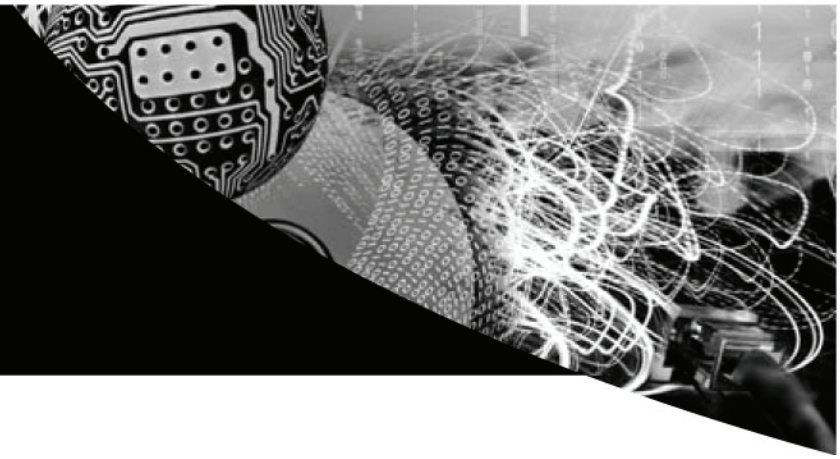


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Operating systems (Continued)			
PR/SM LPAR for the IBM System z9 109	IBM Corporation	EAL5	01-JAN-07
IBM AIX 5L for POWER V5.2 Maintenance Level 5200-6 Program Number 5765-E62	IBM Corporation	EAL4+	01-JAN-07
PR/SMTM LPAR for the IBM System z9™ Enterprise Class and the IBM System z9™ Business Class	IBM Corporation	EAL5	01-JAN-07
IBM AIX 5L for POWER V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3	IBM Corporation	EAL4+	22-DEC-06
Solaris™ 10 Release 03/05	Sun Microsystems, Inc	EAL4+	15-DEC-06
Red Hat Enterprise Linux AS, Version 4 Update 4	RED Hat, Inc	EAL3+	22-SEP-06
Microsoft Windows 2003/XP with x64 Hardware Support Manufacture: Microsoft Corporation Conformance: EAL4 Augmented with ALC_FLR.3	Microsoft Corporation	EAL4+	18-SEP-06
SUSE Linux Enterprise Server Version 8 with Service Pack 3	Suse Linux Products GmbH	EAL3+	06-JUN-06
Red Hat Enterprise Linux Version 4 Update 2 AS & Red Hat Enterprise Linux Version 4 Update 2 WS	Red Hat, Inc	EAL3+	31-MAY-06
IBM AIX 5L for POWER V5.2 Maintenance Level 5200-5 with Innovative Security Systems PitBull Foundations 5.0	IBM Corporation	EAL4+	02-MAY-06
HP-UX 11i v2	Hewlett-Packard Company	EAL4+	01-May-06
Vmware ESX Server 2.5.0 & VirtualCenter 1.2.0	Vmware, Inc	EAL2	27-MAR-06
IBM z/OS, Version 1, Release &	IBM Corporation	EAL4+	02-MAR-06
Red Hat Enterprise Linux (RHEL) Version4 Update 1 AS and Red Hat Enterprise Linux (RHEL) Version 4 Update 1 WS	Red Hat, Inc	EAL4+	26-JAN-06
Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021	Microsoft Corporation	EAL$=	09-NOV-05
Microsoft Windows Server 2003 and Microsoft Windows XP	Microsoft Corporation	EAL4+	06-NOV-05

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme



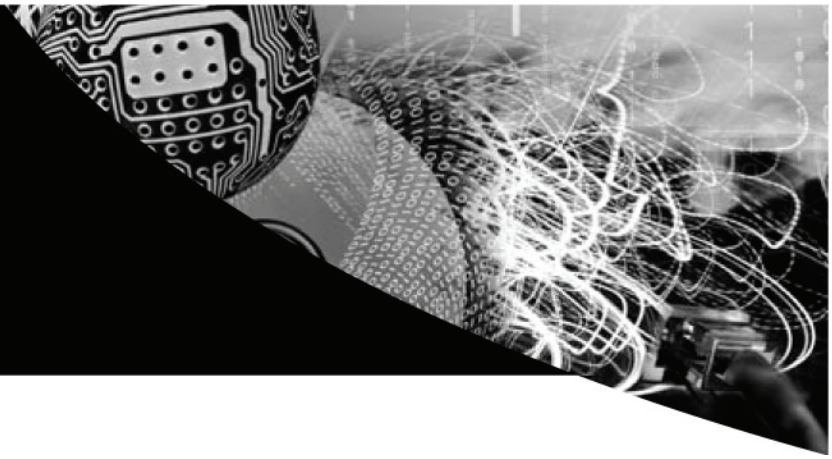
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Operating systems (Continued)			
SUSE Linux Enterprise Server Version 9 with Service Pack 2, ProPack 4 for Service Pack 2 and certification-sles-sgi-eal3 package	Novell® SUSE LINEX Products GmbH	EAL3+	13-OCT-05
Network Appliance Data ONTAP 6.5.2R1	Network Appliance	EAL2	29-SEP-05
SUSE Linux Enterprise Server 8 with service pack 3 to CC EAL3+	Suse Linux Products GmbH	EAL3+	12-AUG-05
IBM i5/OS V5R3MO running on IBM eServer models 520, 550, and 570 with Software Feature Code 1930	IBM Corporation	EAL4+	10-AUG-05
Blue Coat ProxySG Operating System Version 3.2.4.8	Blue Coat Systems Inc	EAL2	08-AUG-05
IBM z/VM Version 5, Release 1 with RSU1	IBM Corporation	EAL3+	27-JUL-05
SUSE Linux Enterprise Server Version 9 with certification-sles-ibm-eal4 package	Novell-SUSE LUNIX AG	EAL4+	09-MAR-05
IBM z/VM Version 1, Release 6	IBM Corporation	EAL3+	09-MAR-05
XTS-4009(tm)/STOP(tm) 6.1.E	BAE Systems Information Technology	EAL5+	01-MAR-05
Solaris™ 9 Release 08/03	Sun Microsystems, Incorporated	EAL4+	25-JAN-05
Apple Mac OS X Version 10.3.6 and Apple Mac OS X Server Version 10.3.6	Apple Computer, Inc.	EAL3	13-JAN-05
Red Hat Enterprise Linux WS, Version 3 Update 3	Hewlett Packard Company	EAL3+	23-SEP-04
SUSE Linux Enterprise Server 8 with service pack 3	SUSE LINUX AG	EAL3+	23-SEP-04
Red Hat Enterprise Linux AS, Version 3 Update 3	Hewlett Packard Company	EAL3+	23-SEP-04
Cray UNICOS/mp Operating System Version 2.4.15	Cray Incorporated	EAL2+	30-AUG-04
Red Hat Enterprise Linux AS, Version 3 Update 2	Red Hat Incorporated	EAL3+	02-AUG-04
Red Hat Enterprise Linux WS, Version 3 Update 2	Red Hat Incorporated	EAL3+	02-AUF-04
PR/SM on IBM zSeries 990	IBM Corporation	EAL	01-MAY04
Sun Trusted Solaris Version 8 4/01	Sun Microsystems Inc	EAL4	01-MAR-04

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



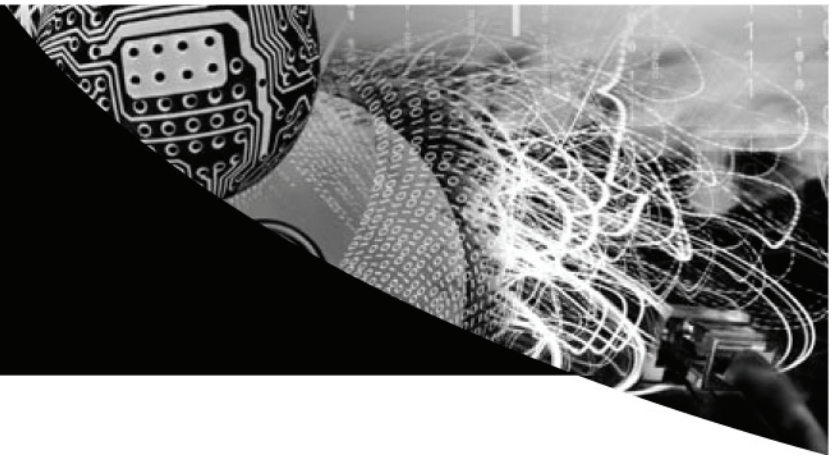
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Operating systems (Continued)			
XTS-400/STOP 6.0.E	BAE Systems Information Technology	EAL4+	01-MAR-04
Hewlett-Packard Tru64 UNIX V5.1A	Hewlett Packard Company	EAL1	01-FEB-04
Red Hat Enterprise Linux 3	Oracle Corporation	EAL2	01-FEB-04
SuSE Linux Enterprise Server V8, Service Pack 3, RC4, with certification-sles-eal3 package	SUSE LINUX AG	EAL3+	01-JAN-04
IBM LPAR for POWER 4 for the IBM pSeries Firmware Releases 3R031021 (p630), 3K031021 (p650) and 3H031021 (p690)	IBM Corporation	EAL4+	01-JAN-04
IBM AIX SL for POWER V5.2 with Recommended Maintenance Package 5200-01, Program Number 5765-E62	IBM Deutschland	EAL4+	01-SEP-03
Nokia IPSO 3.5, 3.5.1 (EAL4)	Nokia	EAL4	01-JUL-03
Processor Resource/System Manager (PR/SM) on IBM zSeries 800 and 900	IBM Corporation	EAL4	01-JUN-03
Processor Resource/System Manager (PR/SM) on IBM zSeries 800 and 900	IBM Corporation	EAL5	01-JUN-03
Sun Solaris 8 02/02	Sun Microsystems Inc	EAL4	01-APR-03
Processor Resource/System Manager (PR/SM) on IBM for the IBM eServer zSeries 900	IBM Corporation	EAL5	01-FEB-03
Hewlett-Packard HP-UX 11i	Hewlett-Packard Company	EAL4	01-FEB-03
Processor Resource/System Manager (PR/SM) on IBM for the IBM eServer zSeries 900	IBM Corporation	EAL4	01-FEB-03
AIX 5L for POWER Version 5.2, Program Number 5765-E62	IBM Informationssysteme Deutschland GmbH	EAL4+	01-NOV-02
Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886	Microsoft Corporation	EAL4+	01-OCT-2
Trusted IRIX/CMW v6.5.13, with patches 4354, 4451, 4452, 4373, 4473	Silicon Graphics, Inc	EAL3	01-MAY-02

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme

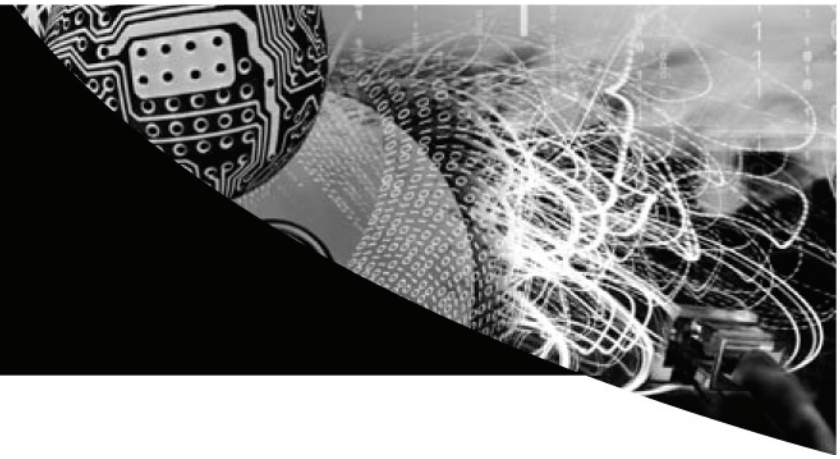


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Operating systems (Continued)			
IRIX v6.5.13, with patches 4354, 4451, 4452	Silicon Graphics, Inc	EAL3	01-APR-02
SuSE Linux Enterprise Server Version 8	SUSE LINUX AG	EAL2+	01-FEB-02
Sun Solaris Version 8 with AdminSuite Version 3.0.1	Sun Microsystems Inc	EAL4	01-NOV-02
B1/EST-X Version 2.0.1 with AIX, Version 4.3.1	Bull S.A. and IBM Informationssysteme Deutschland GmbH	EAL4	01-MAR-99
Other devices and systems			
Belkin OmniView Secure DVI Dual-Link 2-port (F1DN102D) or 4-port (F1DN104D) KVM Switch	Belkin	EAL4+	11-FEB-09
XFER Service Version 2.0.1	Norwegian Defence Communication and Information Services Division	EAL4	01-FEB-09
IBM BD2 Document Manager Version 8.4 Fix Pack 1	IBM, Inc	EAL3+	30-JAN-09
BITACORA Version 4.0.2	S21SEC	EAL2	29-DEC-08
Fuji Xerox ApeosPort-II 7000/6000 Series Contr0ller Software for Asia Pacific Version: Controller ROM Version 1.180.7	Fuji Xerox co., Ltd	EAL3	28-NOV-08
IBM Logical Partition Architecture for Power 6 operating on IBM Power Systems hardware (models E8A, MMA, and FHA)	IBM Internet Security Systems, Inc	EAL4+	26-NOV-08
Data Security Kit DA-SC06 Version: Version 1.01	Panasonic Communications Co., Ltd	EAL2	30-OCT08
bizhub 501/bizhub 421/bizhub 361/ineo 501/ineo 421/ineo 361 Control Software Version: A0R50Y0-0100-G00-11 (System Controller), A0R50Y0-1D00-G00-10 (BIOS Controller)	Konic Minolta Business Technologies, Inc	EAL3	30-OCT-08
Enterasys Dragon Intrusion Defence System Version 7.2.3 Running on Dragon Appliances	Enterasys Networks, Inc	EAL2+	17-OCT-08
IBM Proventia Network Enterprise Scanner and IBM SiteProtector	IBM Internet Security Systems, Inc	EAL2	10-OCT-08
Canon MFP Security Chip Version 1.50	Canon Inc	EAAL3	24-SEP-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

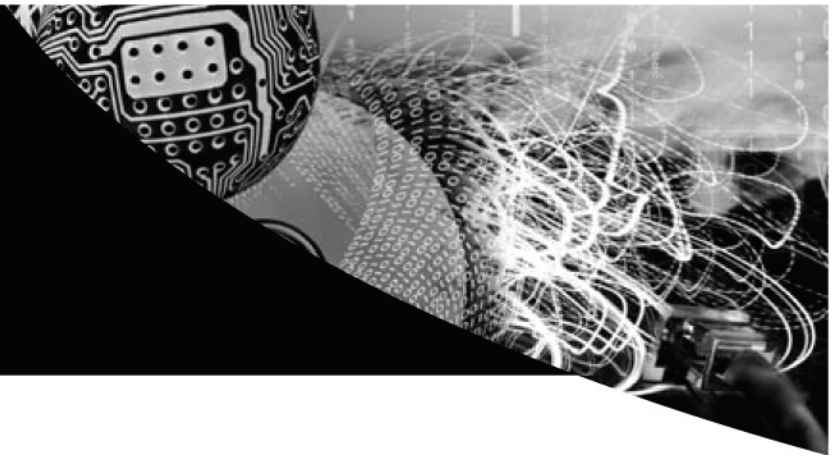
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Xerox WorkCentre 5222/5252/5230 Version: Controller+PS ROM Version 1.204.4 IOT ROM Version 11.21.0, IIT ROM Version 3.7.0, ADF ROM Version 20.0.0	Fuji Xerox Co Ltd	EAL2	11-SEP-08
Xerox WorkCentre 5225A/5230A Version: Controller+PS ROM Version 1.224.0 IOT ROM Version 11.21.0, IIT ROM Version 23.7.0, ADF ROM Version 20.0.0	Fuji Xerox Co Ltd	EAL2	11-SEP-08
Oce Smart Imager 10.3.5.68 as used in the Oce VarioPrint 21x0 Release 4.1	OCE Technologies B.V.	EAL2+	19-AUG-08
Xerox WorkCentre 5030/5050 Multifunction Systems, System Software Version 5.003.07.000	Xerox Corporation	EAL2+	19-AUG-08
EpsonNet ID Print Authentication Print Module Version 1.5bE	SEIKO EPSON CORPORATION	EAL2	12-AUG-08
Voiceldent Unit 2.0	Deutsche Telekom AG/T-Com	EAL2+	08-JUL-08
Digitaler Tachograph EFAS-3 V01	Efkon	EAL4+	19-JUN-08
IBM WebSphere Message Broker Version 6.0.0.3	IBM Deutschland	EAL4+	13-JUN-08
Xerox WorkCentre 7346 Version: Controller+PS ROM Version 1.223.4, IOT ROM Version 3.2.0, IIT ROM Version 20.4.3, ADF ROM Version 11.6.5	Fuji Xerox Co., Ltd	EAL2	13-JUN-08
Fuji Xerox ApeoPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software Version Controller ROM Version 1.0.10	Fuji Xerox Co., Ltd	EAL3	30-MAY-08
Fuji Xerox ApeoPort-III C4400 DocuCentre-III C4400 Series Controller Software Version Controller ROM Version 1.0.8	Fuji Xerox Co., Ltd	EAL3	30-MAY-08
Data Security Kit DA-SC04 V1.00	Panasonic Communications Co., Ltd	EAL2	30-MAY-08
Vmware ESX Server 3.0.2 and Virtual Center 2.0.2	Vmware, Inc	EAL4+	20- MAY 08
MAWIS Rev 3.0	MOBA Mobile Automation AG	EAL1	16-MAY-08
Secure Mail (IronMail) Software Version 6.7HF2	Secure Computing Corporation	EAL2+	29-APR-08
NEC Group Secure Information Exchange Site Version 1.0	NEC Corporation	EAL1+	25-APR-08

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

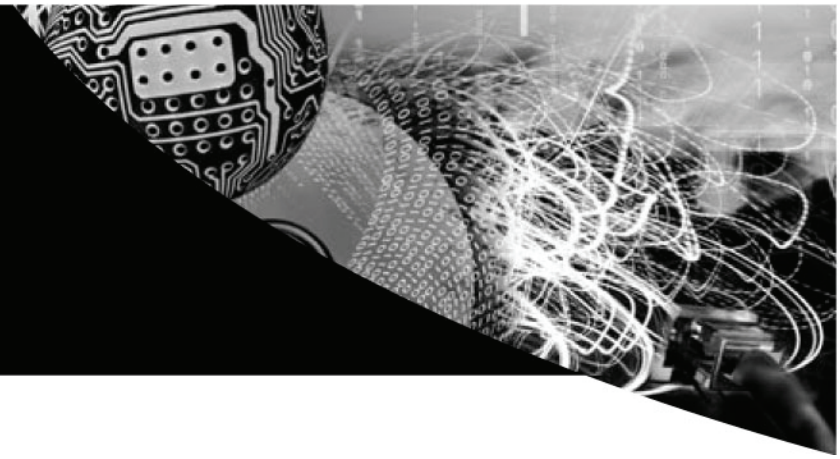


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Essentris Clinical Information System Release 1.4	CliniComp International, Inc	EAL3	11-APR-08
Magicolor 8650 Control Software Version A02E0Y0-0100-GP0-12	Konica Minolta Business Technologies, Inc	EAL3	26-MAR-08
bizhub C353P/ineo+ 353P Control Software Version A02E0Y0-100_GN012	Konica Minolta Business Technologies, Inc	EAL3	26-MAR-08
Xerox WorkCentre 7232/7242 Version Controller+PS ROM Ver.1.203.0, IOT ROM Version 4.7.0, IIT ROM Ver.20.4.1, ADF ROM Version 20.0.0	Fuji Xerox Co., Ltd.	EAL2	28-FEB-08
DataOverwriteSucurity Unit Type I software Version 1.01m	Ricoh Company, Ltd	EAL3	28-FEB-08
DataOverwriteSucurity Unit Type H software Version 1.01x	Ricoh Company, Ltd	EAL3	28-FEB-08
Fuji Xerox DocuCentre-II C3000 Series Controller Software for Asia Pacific Version: Controller ROM Version 1.121.4	Fuji Xerox Co., Ltd	EAL2	25-JAN-08
Fuji Xerox DocuCentre-II 3005/2055/2005 Series Controller Software for Asia Pacific Version: Controller ROM Version 1.130.1	Fuji Xerox Co., Ltd	EAL2	25-JAN-08
Fuji Xerox ApeosPort-II 5010/4000/3000 Series Controller Software for Asia Pacific Version: Controller ROM Version 1.180.0	Fuji Xerox Co., Ltd	EAL2	25-JAN-08
Fuji Xerox ApeosPort-II C7500/C6500/C5400, DocuCentre-II C7500/C6500/C5400 Series Controller Software for Asia Pacific Version: Controller ROM Version 2.100.0	Fuji Xerox Co., Ltd	EAL2	25-JAN-08
Veridat Ident, Volumen, Verweigung 4,0	Veridat Eurotech GmbH	EAL1	25-JAN-08
EMC® Disk Library Version 3.1	EMC Corporation	EAL2	22-JAN-08
NEC Groups Information Leakage Prevention System Version: 1.0	NEC Corporation	EAL1+	26-DEC-07
Canon iR3025/iR3030/iR3035/iR3045 Series HDD Data Erase Kit-B1 Version: 1.00	Canon Inc	EAL3	26-DEC-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

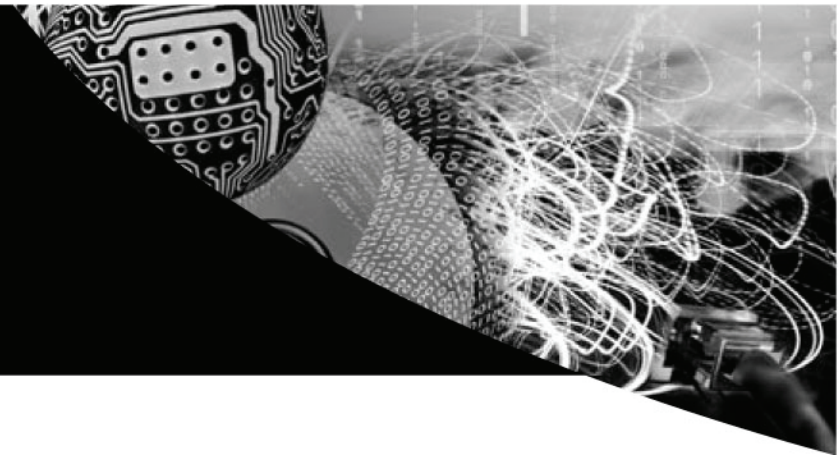
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Xerox WorkCentre 73282/7335/7345 Version: Controller +PS ROM Version 1.221.100 IOT ROM Version 3.4.0 IIT ROM Version 20.4.1 ADF ROM Version 11.6.5	Fuji Xerox Co., Ltd	EAL2	26-DEC-07
Knowledge Center Suite Version 6.5 with Service Pack 4	Supportsoft, Inc	EAL2	21-DEC-07
McAfee Foundstone 5.0.4	McAfee Inc	EAL2	07-DEC-07
bizhub C253/bizhub C203/ineo+253/ineo+203 Control Software	Konica Minolta Business Technologies, Inc	EAL3	26-NOV-07
bizhub C353/ineo+353 Control Software	Konica Minolta Business Technologies, Inc	EAL3	26-NOV-07
EMC ControlCenter® 5.2 Service Pack 5	EMC Corporation	EAL2+	13-NOV-07
EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC® Solutions Enabler 6.3	EMC Corporation	EAL2+	13-NOV-07
IBM Logical Partition Architecture for Power6	IBM Corporation	EAL4+	07-NOV-07
Trusted Security Filter – TSF 101	Thales Norway AS	EAL5	01-NOV-07
bizhub C650.ineo+650 Control Software v A00J0y0-0100-GM0-00	Konica Minolta Business Technologies, Inc	EAL3	29-OCT-07
bizhub C550/bizhub C451/ineo+550/ineo+451 Control Software V A00H0Y0-0100-GM0-00	Konica Minolta Business Technologies, Inc	EAL3	29-OCT-07
c-ident, Version 1.0	c-trace GmbH	EAL1	23-OCT-07
Fortress Wireless Secure Gateway Version 1.0	Fortress Technologies, Inc	EAL3	23-OCT-07
BEA WebLogic Integration Version 8.1 SP6 with BEA07-169-00 Security Advisory Patch	BEA Systems, Inc	EAL2+	19-OCT-07
BEA WebLogic Platform Version 8.1 SP6 with BEA07-169-00 Security Advisory Patch	BEA Systems, Inc	EAL2+	19-OCT-07
EMC® Celerra® Network Server v5.5 funning on EMC® Celerra® NSX and EMC® Celerra® NS Series	EMC Corporation	EAL2+	15OCT-07
bizhub PRO C550/ineo+5500 Image Control Program A0E70Y0-0100-G00-10	Konica Minolta Business Technologies, Inc	EAL3	27-SEP-07
EMC® CLARiiON® FLARE v3.24 with Navisphere Version 6.24 running on CX3 Series Storage Systems	EMC Corporation	EAL2+	25-SEP-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

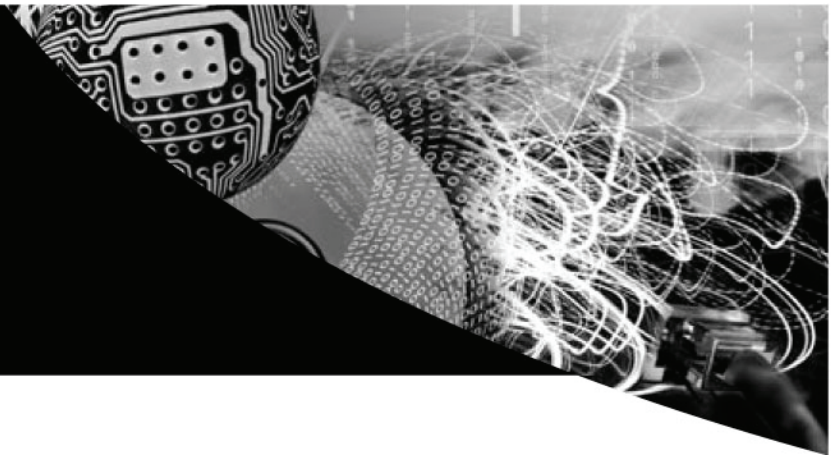


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs)	Exmark International, Inc	EAL2	21-SEP-07
Lexmark X646dte (firmware revision LC2.MC.P239b), X646e (Firmware revision LC.MC.P239b), X646ef (firmware revision LC2.TI.P239b), X772e (firmware revision LC2.TR.P275), X850e (firmware revision LC2.BE.P238b), X852e (firmware revision LC2.BE P238b), X254e (firmware revision LC BE P238b), X940e (firmware revision LC BR P060) and X945e (firmware revision LC BR P060) Multifunction Printers	Lexmark International, Inc	EAL2	21-SEP-07
V3Pro2004 and AhnLab Policy Center 3.0	AhnLab. Inc	EAL4	17-SEP-07
V3Net for Windows server 6,0 and AhnLAb Policy Center 3.0	AhnLab. Inc	EAL4	17-SEP-07
Blackberry® Enterprise Server Version 4.1.3	Research in Motion	EAL2+	12-SEP-07
Blackberry® Wireless Handheld Software Version 4.1.0	Research in Motion	EAL2+	12-SEP-07
EOS Original Data Security System Version 1.0	Canon Inc	EAL2	30-AUG-07
NetIQ Security Manager 5.5	NetIQ, Incorporated	EAL2	09-AUG-07
IBM Global Security Kit Version 7.0.4.11	IBM Corporation	EAL4	02-AUG-07
Crypto Token USB TKO1S147	Datatech Sistemas Digitales Avanzados S.L.	EAL3	19-JUL-07
Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275	Xerox Corporation	EAL2+	30-JUN-07
bizhub C250P/ineo+250P/magicolor 7460CK Control Software 4038-0100-GM0-11-000	Konica Minolta Business Technologies, Inc	EAL3	27-JUN-07
bizhub C450P/ineo+450P Control Software 4037-0100-GM0-11-000	Konica Minolta Business Technologies, Inc	EAL3	27-JUN-07
bizhub C352P/ineo+351P/magicolor 8460CK Control Software 9J06-0100 GM0-11-000	Konica Minolta Business Technologies, Inc	EAL3	27-JUN-07
bizhub C252P/ineo+251P/magicolor 7465CK Control Software 4038-0100-GN0-03-000	Konica Minolta Business Technologies, Inc	EAL3	27-JUN-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme

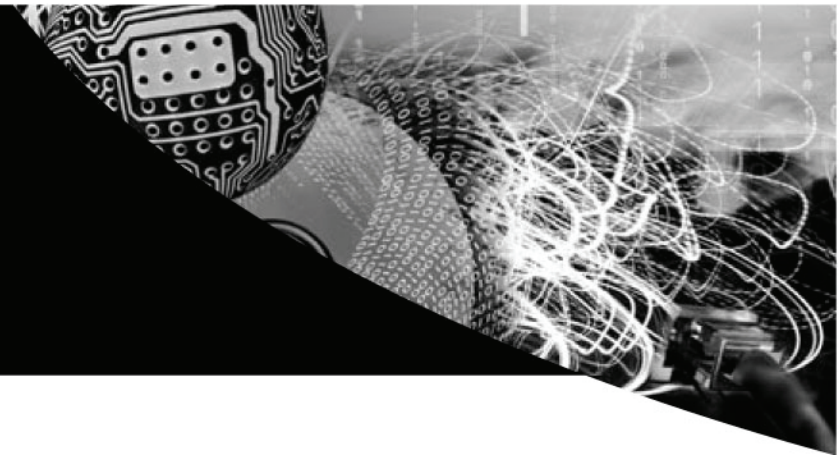


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
HP Laser Jet M4345 MFP System Firmware Version 40.021.7, HP LaserJet M3027 MFP System Firmware Version 40.021.7A, HP LaserJet M3035 MFP system Firmware Version 48.021.07a, HP LaserJet M5025 MFP System Firmware Version 48.021.7A, HP LaserJet M5035 MFP System Firmware Version 40.021.7A, HP Color LaserJet 4730 MFP System Firmware 46.151.8	Hewlett-Packard Development Company, L.P.	EAL3	22-JUN07
McAfee VirusScan Enterprise Version 8.51 and McAfee ePolicy Orchestrator Version 3.6	McAfee, Inc	EAL2+	22-JUN-07
Xerox WorkCentre 7655/7665 Multifunction Systems	Xerox Corporation	EAL2+	18-UN-07
NitoSecurity Intrusion Prevention System Version 7.1.3	NitoSecurity, Inc	EAL3+	11-JUN-07
CA Integrated Threat Management r.8.0.445	CA, Inc	EAL3	10-JUN-07
Belkin Omniview Secure KVM Models F1DN102U, F1DN104U, F1DN108U	Belkin International, Inc	EAL4	08-JUN-07
bizhub C252/ineo+251 Control Software	Konica Minolta Business Technologies, Inc	EAL3	30-MAY-07
Voltage SecureMail Suite 2.0	Voltage Security	EAL2	29-MAY-07
eEye Retina Network Security Scanner Version 5.4.21.53	eEye Digital Security Corporation	EAL2	25-MAY-07
McAfee Secure Content Management Appliance Version 4.0	McAfee Inc	EAL2	18-MAY-07
Océ SRA Controller, Version 3, Bundle 8.02	OCE Printing Systems	EAL3+	16-MAY-07
Ricoh Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B	Ricoh Company Ltd	EAL3	16-MAY-07
Gentran Integration Suite (GIS) 4.2	Sterling Commerce Incorporated	EAL2+	15-MAY-07
OKI Color Page Printer C8800 Security Module DS 01.00	Oki Data Corporation	EAL3	27-APR-07
bizhub 500/bizhub 420/bizhub 360/ineo500/ineo420/ineo360 Control Software 50GA-0100-G00-30-000	Konica Minolta Business Technologies, Inc	EAL3	27-APR-07

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

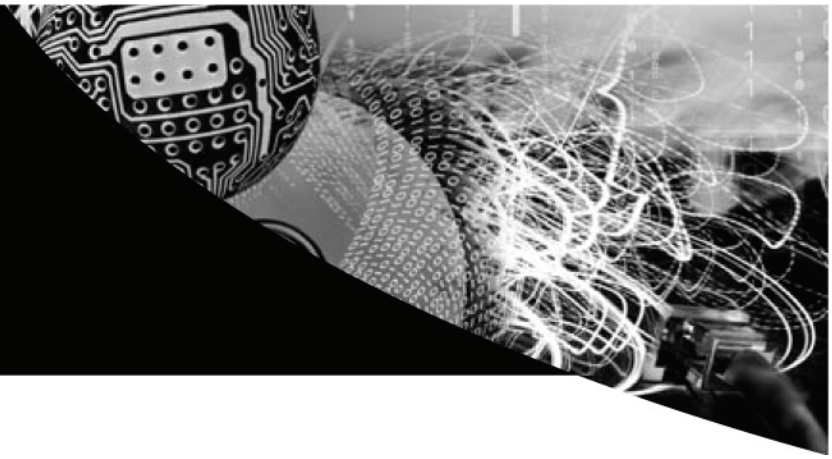
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Microsoft Certificate Server 2003	Microsoft Corporation	EAL4+	10-APR-07
bizhub 500/bizhub 420/ineo 500/ineo 420 Control Software 50GA-0100G00-21-000	Konica Minolta Business Technologies, Inc	EAL3	22-MAR-07
Japan: bizhub PRO C6500 Gazou Seigyo Program Overseas: bizhub PRO C6500 Image Control Program A03U0Y0-0011-G00-15	Konica Minolta Business Technologies, Inc	EAL3	22-MAR-07
Bizhub 750/bizhub 600/ineo 750/ineo 600 Control Software MFP system controller program: 57AA-00100-G00-21-000 MFP image controller program: 57 AA - 1000-G00-21-000	Konica Minolta Business Technologies, Inc	EAL3	22-MAR-07
Database Engine of Microsoft EQL Server 2003Enterprise Edition (English) SP1, Version/Build.00.2047.00	Microsoft Corporation	EAL1	21-MAR-07
IBM Websphere Application Server Version 6.1.0.2	IBM Corporation	EAL4+	16-MAR-07
IBM Websphere Application Server Network Deployment Version 6.1.0.2	IBM Corporation	EAL4+	16-MAR-07
SecureWave Sanctuary Device Control Version 3.2	Secure Wave	EAL2	16-MAR-07
Hewlett Packard HP LaserJet 9040 MFP System Firmware Version 08.09.1.3, HP LaserJet 9050 MFP System Firmware Version 08.09.1.3, HP LaserJet 4345 MFP System Firmware Version 09.091.1.4, HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4	Hewlett-Packard Company	EAL3	28-FEB-07
Fuji Xerox DocuCentre-II 4000/3000 Series Data Security Kit Controller ROM Version 1.0.17	Fuji Xerox Co., Ltd	EAL2	22-FEB-07
Fuji Xerox ApeosPort-II C7500.C6500/C5400 DocuCentre-II C7500/C6500/C5400 Series Data Security Kit Controller ROM Version 2.0.1	Fuji Xerox Co., Ltd	EAL2	22-FEB-07
Fuji Xerox ApeosPort-II 4000/3000 Series Data Security Kit Controller ROM Version 1.40.17	Fuji Xerox Co., Ltd	EAL2	22-FEB-07
Xerox WorkCentre 7228/7235/7245 Series Security Kit Controller+PS Ver1.220.2	Fuji Xerox Co., Ltd	EAL2	22-FEB-07

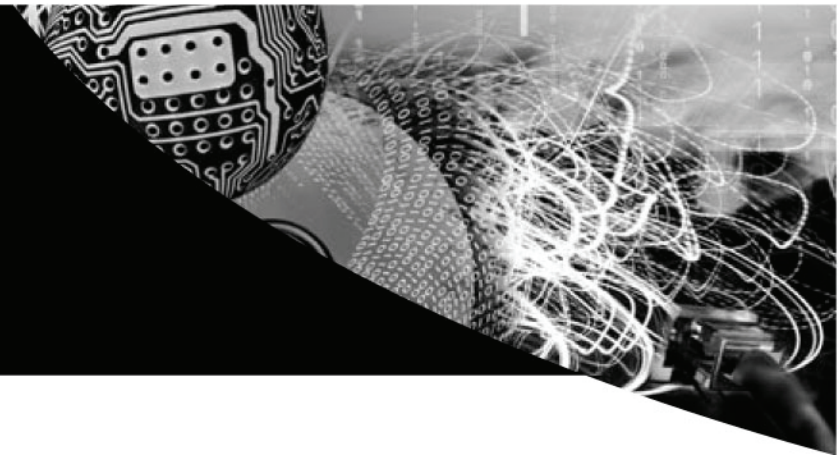
HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Data OverWriteSecurity Unit F Software 1.05	Ricoh Company, Ltd	EAL3	22-Feb-07
IBM WebSphere Application Server for z/OS V6.1.0.2	IBM Corporation	EAL4+	16-FEB-07
IBM Tivoli Licence Compliance Manager Version 2.2, Fix Pack 1	IBM Corporation	EAL2+	14-FEB-07
Owl Computing Technologies Data Diode Network Interface Card Version 4	IBM Corporation	EAL4	01-FEB-07
ETrust Security Command Center r8 SP1 with CR2 patch	Computer Associates International, Inc.	EAL2	26 JAN-07
Data Overwrite Security Unit Type D Software Version 0.03	Ricoh Company Ltd	EAL3	24-JAN-07
Data Overwrite Security Unit Type C Software Version 0.04	Ricoh company, Ltd	EAL3	24-AN-07
bizhub 350/bizhub 250/bizhub 200/ineo 350/ineo 250 (Ver.2) Control Software 4040-01000-G20-52-000	Konica Minolta Business Technologies, Inc		
Check Point Integrity Agent, Version 6.5.063.145	Check Point Software Technologies, Ltd	EAL4+	11-JAN-07
ImageNow v5.42 SP3 and WebNOW v3.42	Perceptive Software, INC.	EAL2+	10-JAN-07
PR/SM LPAP for the IBM eServer zSeries z890 and z990	IBM Corporation	EAL5	01-JAN-07
Océ Smart Imager 8.3.3.39 as used in the Océ VP 2090 R3.3	OCE Technologies B.V.	EAL2+	01-JAN-07
System Software for e-STUDIO520/600/720/850 Version 1.0	TOSHIBA TEC CORPORATION	EAL3	01-JAN-07
System Software for e0STUDIO202L/232/282 Version 1.0	TOSHIBA TEC CORPORATION	EAL3	01-JAN-07
EOS-1D Mark II firmware Version 1.0.1	Canon Inc	EAL2+	01-JAN-07
TIBCO Enterprise Message Service Version 4.3.0	TIBCO Software	EAL2	31-DEC-06
Sentinel from Novell Version 5.1.1	Novell Inc (Formerly e-Security Inc)	EAL2	30-DEC-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

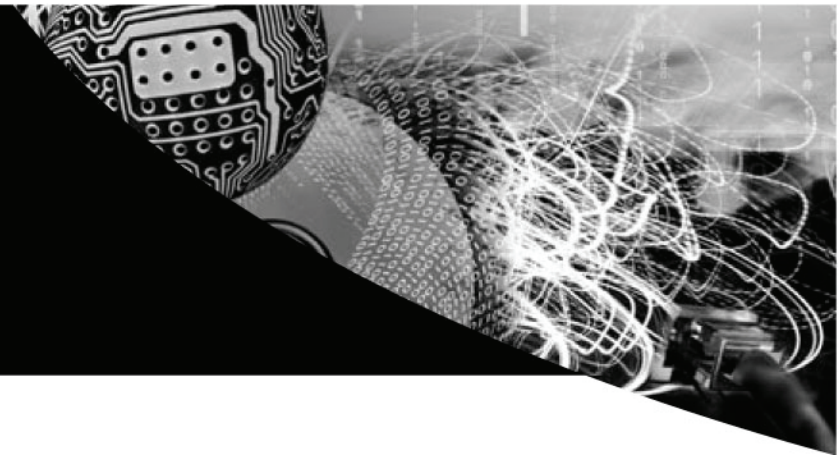


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
MX-FRX3 Version M.10	Sharp Corporation	EAL3+	15-DEC-06
Fuji Xerox DocuCentre-II C4300/C3300/C2200 Series Security Kit for Asia Pacific Controller ROM Version 1.101.7	Fuji Xerox Co., Ltd	EAL2	15-DEC-06
Data Security Kit DA-SC02 Version 1.00	Panasonic Communications Co, Ltd	EAL2	15-DEC-06
Fuji Xerox DocuCentre-II C4300/C3300/C2200 Series Data Security Kit Controller ROM Version 1.1.16	Fuji Xerox Co., Ltd	EAL2	15-DEC-06
Fuji Xerox DocuCentre-II C4300/C3300/C2200 Series Security Kit for Asia Pacific Controller ROM Version 1.121.7	Fuji Xerox Co., Ltd	EAL2	15-DEC-06
EUR Form Client 05-07	Hitachi	EAL2+	15-DEC-06
Fuji Xerox ApeosPorter-II C4300/C3300/C2200 Series Data Security Kit Controller ROM Version 1.141.16	Fuji Xerox Co., Ltd	EAL2	15-DEC-06
bizhub c450/bizhub C351/ineo+ 450/ineo+ 350 Control Software 4037-0100-GM0-05-000	Konica Minolta Business Technologies, Inc	EAL3	22-NOV-06
bizhub C250/ineo+ 250 Control Software 4038-0100-GM0-05-000	Konica Minolta Business Technologies, Inc	EAL3	22-NOV-06
bizhub C352/Bizhub C300/ineo+ 351/ineo+ 300 Control Software 9J06-0100-GM0-05-000	Konica Minolta Business Technologies, Inc	EAL3	22-NOV-06
Los Altos Technologies Unishred Pro Version 3.3.2	Los Altos Technologies	EAL2	22-NOV-06
Tenix Interactive Link Data Diode Device, Gigabit Variant, Version 3.0	Tenix Datagate	EAL7+	16-NOV-06
SecureWave Sanctuary Application Control Desktop Version 2.8	SecureWave	EAL2	08-NOV-06
Data Security Kit(D) Software Version 1.00E	KYOCERA MITA Corporation	EAL3	31-OCT-06
Data Security Kit DA-SC03 Version 1.01	Panasonic Communications Co, Ltd	EAL2	31-OCT-06
Data Security Kit DA-SC01 Version 1.01	Panasonic Communications Co, Ltd	EAL2	31-OCT-06
MX-FRX2 Version M.10	Sharp Corporation	EAL3+	31-OCT-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme

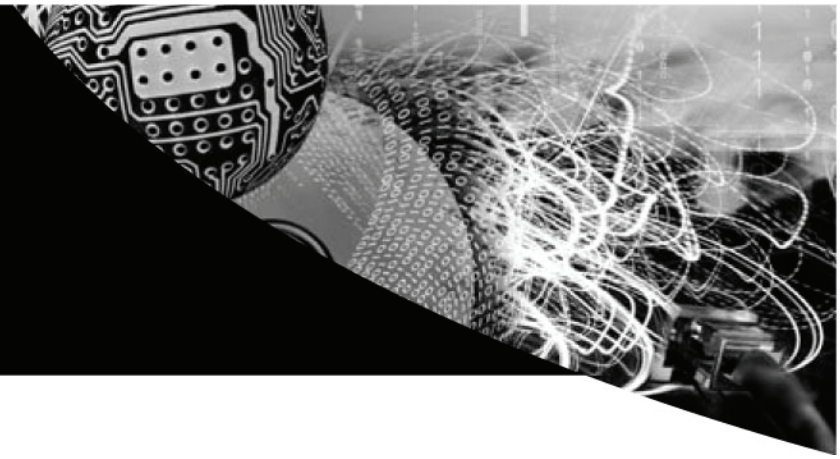


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
bizhub 350/bizhub 250/bizhub 200/ineo+ 350/ineo 250 (ver.1) Control Software 4040-0100-G10-25-000	Konica Minolta Business Technologies, Inc	EAL3	31-OCT-06
Xceedium GateKeeper	Xceedium, Inc	EAL2	31-OCT-06
Data Security Kit(D) Software V1.00J	KYOCERA MITA Corporation	EAL3	31-OCT-06
Active TSM V3.0	Oullim Inc	EAL4	27-OCT-06
OCE Digital Access Controller (DAC) R9.1.6	OCE Technologies B.V.	EAL2+	26-OCT-06
Metastorm e-work 6.6.1	Metastorm, Inc	EAL2	24-OCT-06
HDD SecureD Version 1.6	High Desity Devices AS	EAL4+	18-OCT-06
EFI Foery System 6 or 6e Secure Erase Options and EFI Fiery System 7 or 7e Secure Erase Option	Electronics for Imaging, Inc	EAL3+	10-OCT-06
IBM WebSphere MQ 6.0.1.1	IBM United Kingdom Limited	EAL4+	02-OCT-06
3eTI Client CryptoClient Software (3e-10F-C-2 or 3e-10F-A-2)	3e Technologies International, Inc	EAL2+	15-SEP-06
MX-FRX1 Version M.10	Sharp Corporation	EAL3+	14-SEP-06
SecureWave Sanctuary Application Control Custom Edition Version 2.8	SecureWave	EAL2	11-SEP-06
Fuji Xerox ApeosPort 750 I/650 I, DocuCentre 750 I/650 I Series Security Kit for Asia Pacific Controller ROM Version 1.101.2	Fuji Xerox Co., Ltd	EAL2	07-SEP-06
Fuji Xerox ApeosPort C7550 I/C6550 I/C5540 I, Docucentre C7550 I/C6550 I/C5540 I Series Security Kit for Asia Pacific Controller ROM Version 1.102.2	Fuji Xerox Co., Ltd	EAL2	07-SEP-06
Fuji Xerox ApeosPort 550 I/450 I/350 I, Docucentre 550 I/450 I Series Security Kit for Asia Pacific Controller ROM Version 1.100.3	Fuji Xerox Co., Ltd	EAL2	07-SEP-06
Gefäßidentifikationssystem BiTech bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern	Deister electronic GmbH	EAL1	24-AUG-06
ABox 1.0	T-Systems International GmbH	EAL3	14-AUG-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

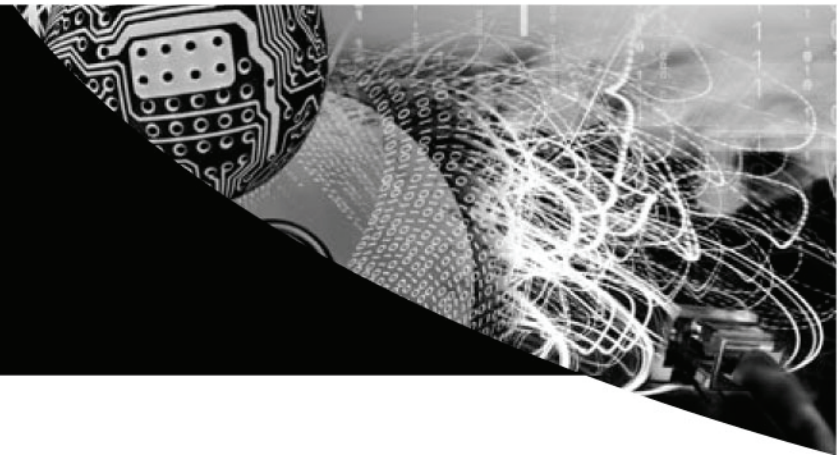
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
LiveState Delivery Version 6.0.1	Symantec	EAL2	01-AUG-06
Canon MFP Security Chip 1.00	Canon Inc	EAL3	07-JUL-06
System Software for e-STUDIO2500c/3500c/3510c Version 1.0	TOSHIBA TEA CORPORATION	EAL3	28-JUN-06
Carrier Access Broadmore 500, 1700, and 1750 Release 4.1.1	Carrier Access Corporation	EAL3	26-JUN-06
SecureInfo Risk Management System 3.2.06.12	SecureInfo Corporation	EAL2	26-JUN-06
Promia Intelligent Agent Security Manager, Version 1.2 (IASM)	Promia Incorporated	EAL3+	09-JUN-06
IBM WebSphere Application Server Version 6.0.2.3	IBM Corporation	EAL4+	22-MAY-06
ISS SiteProtector, Proventia A, Proventia G, and Network Sensor	Internet Security Systems, Inc	EAL2	16-MAY-06
WebSphere Application Server 6.0	IBM Corporation	EAL4+	12-MAY-06
CipherTrust IronMail Secure Email Gateway Software Version 4.0.0	CipherTrust, Inc	EAL2	01-MAY-06
BEA WebLogic Server 8.1 SP%	BEA Systems, Inc	EAL2+	28-APR-06
BAE Military Message Handling System (MMHS) Filters Version 1.1.1	BAE Systems Information Technology	EAL4	24-APR-06
DEP/PCI Version 3.1 Host Security Module (Hardware & Software)	Banksys N.V.	EAL3+	10-APR-06
Xerox WorkCentre/WorkCenter Pro 232/238/245/255/265/275	Xerox Corporation	EAL2	06-APR-06
Platform LSP® HPC 6.2	Platform Computing Inc	EAL2	04-APR-06
System Software for e-STUDIO281c/351c/451c Version 1.0	TOSHIBA CORPORATION	EAL3	29-MAR-06
System Software for e-STUDIO352/452 Version 1.0	TOSHIBA CORPORATION	EAL3	29-MAR-06
Data Overwrite Security Unit Type C Software Version 0.04	Ricoh Company, Ltd	EAL2	29-MAR-06
Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b	Lexmark	EAL2	23-FEB-06

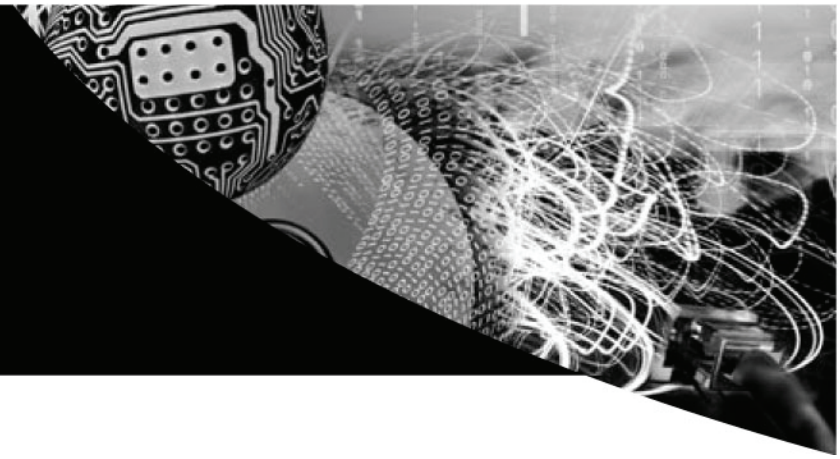
HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
VPNConnect Version 1.2.650	I_MOTION GmbH	EAL2	14-FEB-06
Fuji Xerox ApeosPort 750 I/650 I/550 I DocuCentre 750 I/650 I/550 I Series Data Security Kit Controller ROM Version 1.1.1	Fuji Xerox Co., Ltd	EAL2	08FEB-06
Fuji Xerox ApeosPort C7550 I/C6550 I/C5540 I, Docucentre C7550 I/C6550 I/C5540 I Series Data Security Kit Controller ROM Version 1.1.4	Fuji Xerox Co., Ltd	EAL2	08-FEB-06
SigabaNet 2.2	Secure Data In Motion, Inc.dba Sigaba	EAL2+	07-FEB-06
Radware APSolute OS	Radware	EAL3	03-FEB-06
ETrust Audit r8	Computer Associates	EAL2	03-FEB-06
OCE Digital Access Controller R8.1.10	OCE Technologies B.V.	EAL2+	27-JAN-06
WebMethods Fabric 6.5	WebMethods Inc	EAL2	23-DEC-05
IBM WebSphere Business Integration Message Broker, Version 5.0, Fix Pack 4	IBM Corporation	EAL3+	15-DEC-05
Juniper Networks Secure Access Family Release 5.1R2	Juniper Networks Inc	EAL2	01-DEC-05
DiamondTEK (DiamondCentral NSC (also sold as CC200) Application S/W Version 2.4.0.5, NSD-Prime F/W Version 2.4.0.3; and NSD (DiamondLink (also sold as CL100), DiamondPak (also sold as CP102, CP104, CP106), Diamond VPN (also sold as CV1000); DiamondSAT	Cryptek, Inc, Sterling VA, USA	EAL4	01-DEC-05
Microsoft Windows Server 2003 Certificate Server	Microsoft Corporation	EAL4+	15-NOC-05
AR-FR22 Version S.10	Sharp Corporation	EAL3+	20-OCT-05
Canon iR6570/iR5570 Series iR Security Kit-B3 Version 1.03	Canon Inc	EAL3	20-OCT-05
Mazu Profiler Blade System Version 5.0	Mazu Networks Inc	Eal2	10-OCT-05
Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C218/C2636/C3545 Advanced Multifunction System including image Overwrite Security	Xerox Corporation	EAL2	30-SEP 05

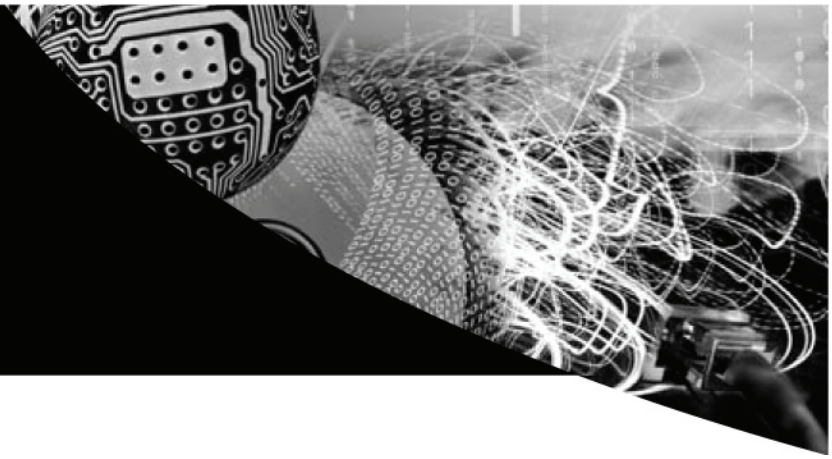
HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03	Canon Inc	EAL3	09-SEP-05
Data Security Kit(B) Software Version 1.10E	KYOCERA MITA Corporation	EAL3	09-SEP-05
Data Security Kit(B) Software Version 1.10J	KYOCERA MITA Corporation	EAL3	09-SEP-05
AR_FR21 Version M.10	Sharp Corporation	EAL3	07 SEP-05
Tenix Interactive Link Data Diode Version 2.1	Tenix Datagate Pty Ltd	EAL7	30-AUG-05
Tenix Interactive Link Version 5.1	Tenix Datagate Pty Ltd	EAL5	19-AUG-05
Fuji Xerox ApeosPort C4535 I/C3636 I/C2521 I DocuCentre C4535 I/C3636 I/ C2521 I Series	Fuji Xerox Co., Ltd	EAL2	07-JUL-05
Trust-CANP V8.0i	Nippon Telegraph and Telephone Corporation	EAL2	07-JUL-05
bizhub PRO 920 control software image control program (image control I1); 10-0000 Controller control program (IP control); 10-0000	Konica Minolta Business Technologies, Inc	EAL3	07-JUL-05
MBC CONTROL-SA	BMC Software Inc	EAL2	24-JUN-05
Digital Tachograph SMARTACH STANDARD (reference 912435 Ind D, 921439 Ind D, 921463 Ind D, 921459 Ind A)	ACTIA	EAL4+	24-JUN-05
Tumbleweed MMS and IME Version 5.5.3	Tumbleweed Communications Corp	EAL2	23-JUN-05
Marimba Desktop/Mobile Management and Server Change Management	Marimba Inc	EAL3	10-JUN-05
Canon iR5570/iR6570 Series Encrytped Printing Software-B1 Version 1.01	Canon Inc	EAL2	03-JUN-05
AR_FR11 Version M.20	Sharp Corporation	EAL3	03-JUN-05
ACTIA IS2000 SRES (reference 921441 indice A), ACTIA IS2000 SRES FIAT (reference 921492 indice A)	ACTIA	EAL4+	26-MAY-05
PR/SM LPAP for the IBM eServer zSeries Z890 and z990	International Business Machines Corporation (IBM)	EAL4	13-MAY-05

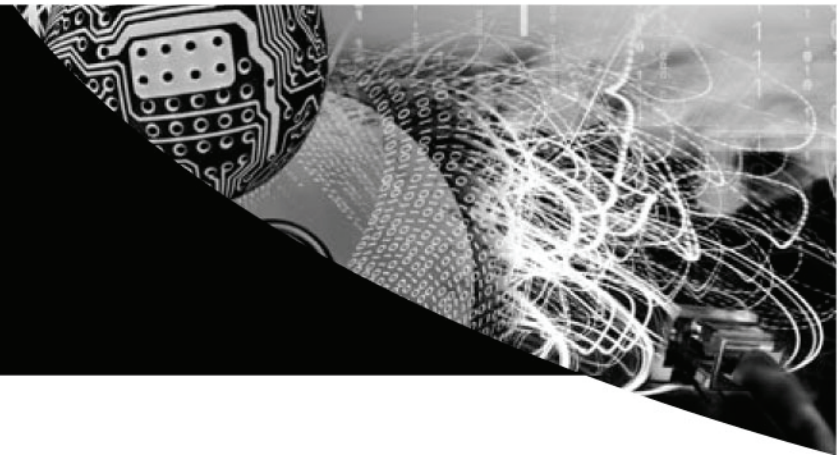
HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Cisco VoIP Telephony Solution	Ciso Systems Inc	EAL1	12-MAY-05
Appliporter Security Kitt 01-00	Hitachi, Ltd	EAL2	28-APR-05
NetForensics 3.1.1 with Point Update 45149	NetForensics, Inc	EAL2	07-APR-05
Nexor MMHS Security	Nexor Ltd	EAL2	14-Mar-05
Scramble Board GP-1031 Version 2.0	TOSHIBA TEC CORPORATION	EAL2	11-MAR-05
AR-FR12M Version M.20	Sharp Corporation	EAL3+	11-MAR-05
CBB Business Application unit Version 1.0	The Bank Of Tokyo-Mitsubishi/MITSUBISHI ELECTRIC INFORMATION SYSTEMS CORPORATION	EAL21	11-MAR-05
bizhub PRO 1050 control software Image control program (Image control I1): 11-0000 Controller control program (IP control P1): 10-0000	Konica Minolta Business Technologies, Inc	EAL3	21-FEB-05
bizhub PRO 1050P zentai seigyo software Overseas: bizhub PRO 1050P control software	Konica Minolta Business Technologies, Inc	EAL3	21-FEB-05
Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 1.04	Canon Inc	EAL2	21-FEB-05
OCE Digital Access Controller Version 7.3.6	OCE Technologies B.V.	EAL2+	11-FEB-05
Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 34/45/55 Advanced Multifunction System with Image Overwrite Security Service Maintenance Pack 2	Xerox Corporation	EAL2	11-FEB-05
Xerox WorkCentre C65/C75/C90 and WorkCentre Pro 65/75/90 Advanced Multifunction System with Image Overwrite	Xerox Corporation	EAL2	11-FEB-05
InCrypto34v2	ST INCARD S.r.I	EAL4+	02-FEB-05
Oracle Internet Directory 10g	Oracle Corporation	EAL4+	01-FEB-05
ACTIA IS2000 Motion Senor – SNARTACH LxRy (reference 921442 indice A, 921443 indice A, 921444 indice A, 921445 indice A, 921446 indice A, 921447 indice A, 921448 indice A, 921449 indice A, 921450 indice A, 921451 indice A, 921460 indice A)	ACTIA	EAL4+	25-JAN-05

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

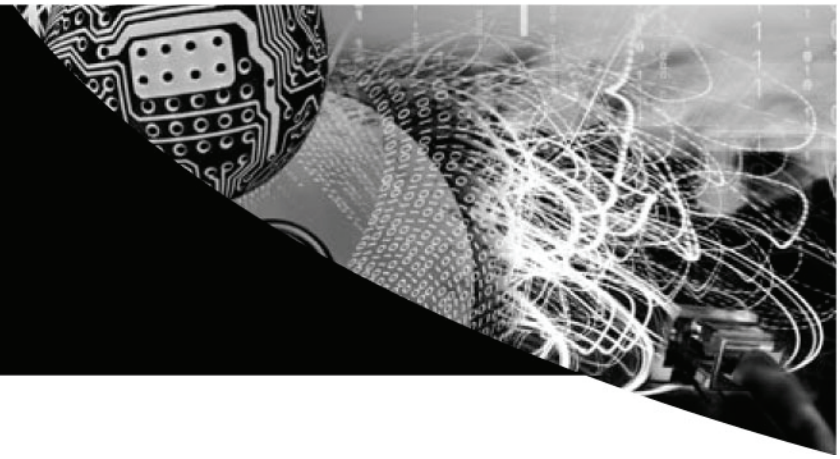


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Java Intelligent Agent Componentware IV, Version 4,3,11	DAI Labor Technische Unicersität Berlin	EAL3	19-JAN-05
ACTIA L2000 Digital Tachograph – SMARTACH Famlie Standard 9reference 921435 Indice B, 921439 Indice B et 921463 Indice B)	ACTIA	EAL4+	18-JAN-05
Xacita IA Manager Enterprise Edition Version 4.0 SP2, Build 485	Xacta Corporation	EAL2	14-JAN-05
Actional Security Gateway Version 3.1.2.5	Actional Corporation	EAL2+	11-JAN-05
ACOS EMV_A03V0, Konfiguration A	Austria Card GmbH	EAL4+	24-NOV-04
HOBLink Secure, Version 3.1	HOB GmbH & Co. KG	EAL2	27-OCT-04
4036 Multi Function Peripheral Control Software (for bizhub c350/CF2203/8022) Macro System Controller: 4036-10G0-18-00 Network Module: 4036-A0G0-04-00	Konica Minolta Business Technologies Inc	EAL3	17-SEP-04
Data Security Kit AR-FR4, Data Security Kit AR-FR5 AR-FR4: Version M.20 AR-FR5: Version E.20	Sharp Corporation	EAL4	17-SEP-04
Fuji Xerox DocCentre 719/659/559 Series Data Security Kit, DC System ROM Version V512, PESS ROM Version V3.0.4	Fuji Xerox Co., Ltd	EAL2	17-SEP-04
IDS Balancer Version 2.2 Appliance (IDSB3531-CCV1.0, ISDSB3532-CCV1.0, IDSB4508-CCV1.0)	Top Layer Networks	EAL2	03-SEP-04
McAfee IntruShield Intrusion Detection System	McAfee Incorporated	EAL3	31-AUG-04
Internal Communications Management System (ICMS) Version 3.7.1.0	Thales Communications SA	EAL3	19-AUG-04
External Communications Management System (ECMS) Version 4.1	Thales Communications SA	EAL3	19-AUG-04
Di3510 Series.Di3510f Series Multi Function Peripheral Security Kit User Interface: 4030-20G0-05-00 Network Module: 4030-A0G0-03-00	Konica Minolta Business Technologies Inc	EAL3	03-AUG-04
SeL Version 1 rev o1	Canon Sales Co., Inc	EAL1	03-AUG-04
7222/7228/7235 control software version 10.0000	Konica Minolta Business Technologies Inc	EAL3	29-JUN-04

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme

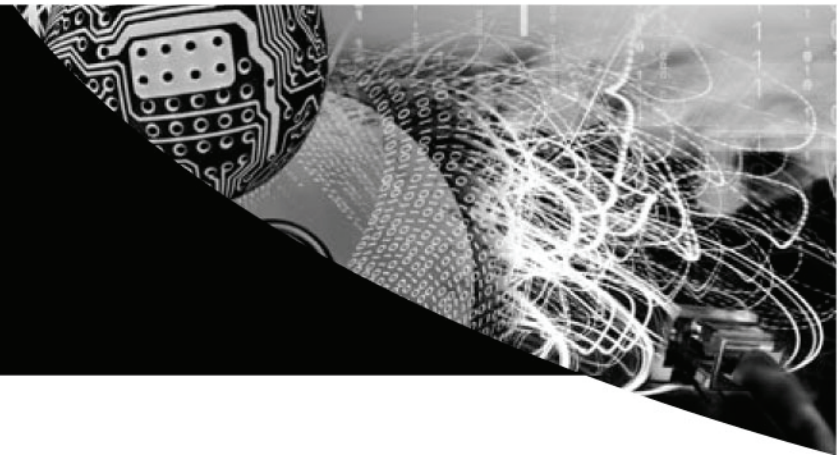


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Canon ImageRUNNER 2200/2800/3300 Series Software Version iR200N-Usen50.06 with Security Kit B1	Canon USA Inc	EAL3	16-JUN-04
Symantec CyberWolf v2.0	Symantec Corporation	EAL2	04-JUN-04
Thales operator Terminal Adapter (OTA)	Thales Norway AS	EALS5	19-MAY-04
IBM WebSphere MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6	IBM Corporation	EAL2	27-APR-04
Thales Message Handling System (MHS)	Thales Systems Canada	EAL3	01-APR-04
Data security kit for digital MFD; AR-FR10 Version S.10	Sharp Corporation	EAL3+	16-Mar-04
Scrambler-board GP-1010 Version 2.0	TOSHIBA TEC CORPORATION	EAL2	01-MAR-04
7145 control software 25.000	Konica Minolta Business Technologies, Inc	EAL3	16-MAR-04
KnoWho Authentication Server Version 1.2.2. and Private ID Version 2.1.15	Iridian Technologies, Inc	EAL2	01-OCT-03
IBM Tivoli Access Manager for e-business 4.1 with Fixpaxk 5	IBM Corporation	EAL3+	01-OCT-03
G-Server Version 2.5	Gilian Technologies Inc	EAL1	01-AUG-03
California Microwave Mail List Agent and Profiling User Agent (MLA/PUA) Version 3.1.0 with Patch A	Northrop Grumman Systems Corporation, California Microwave Systems	EAL2	01-AUG-03
DEP/PCI Version 3.0 Host Security Module (Hardware & Software)	Banksys N.V.	EAL3+	01-AUG-03
Trend Micro InterScan VirusWall 3.52 for NT Trend Micro InterAScan Viruswall 3.6 for Solaris, HP-UX, and Linux	Bodacion Technologies	EAL1	01-FEB-01
Persona 5.0	Esker, Incorporated	EAL3	01-DEC-02
Sharp Corporation Multifunction Device with Data Security Kit (AR-FR$ V.M.10, AR-FR5 V.E.10, AR-FR6 Version J.10)	Sharp Electronics Corporation	EAL2	01-DEC-02

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

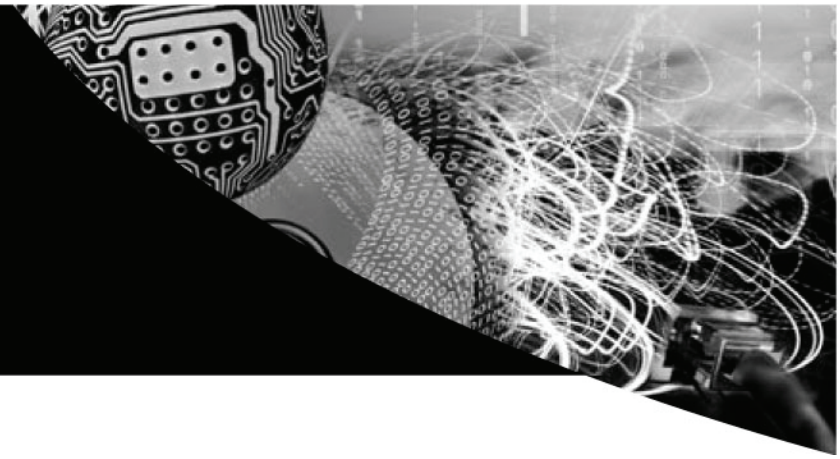
External Common Criteria Scheme



Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Other devices and systems (Continued)			
Messaging Management System, Version 4.6	Tumbleweed Communications Pty. Ltd	EAL2	01-MAR-02
VPN IPSec administration service, Netselo	Netcelo	EAL1+	01-JAN-02
Smart Card IC Development flow, Smart Card IC Development section in Kumamoto, NEC-Japan	NEC Smart Card IC development Section, Kumamoto (Japan)	WAL3	01-JAN-02
SurfinGate, Version 5.6	Finjan Software, Inc	EAL3	01-OCT-01
Bioscrypt™ Enterprise for NT Logon Version 2.1.3	Biocrypt, Inc	EAL2	01-JUN-01
Sharp Data Security Kit (AR-FR1/AR-FR2/AR-FR3 for Sharp Imager Family (FR-287, AR-337, AR-407, and AR-507)	Sharp Electronics Corporation	EAL2	01-APR-01
Partitioning of virtual private networks as part of the Equant IP VPN service (Version 1.0)	Equant, France Telecom Transpac	EAL1+	01-JAN-01
CZ6 production line on the NEC site in Yamaguchi, Japan	NEC Yamaguchi Ltd, NEC SCAC	EAL1+	01-JAN-01
Products for digital signature			
EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03. Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN Tri@nk (Artikel-Nr. HCPNCKS/C05 Firmware Version 68.17)	KOBIL Systems GmbH	EAL3+	12-JAN-09
FAST Signature application, Version 1	Dictao	EAL2+	17-Dec-08
Virtuelle Poststelle des Bundes (Verifikationsmodul) Version 2.2.3.2	Bremen online services GmbH and Co. KG	EAL3+	24-OCT-08
Virtuelle Poststelle des Bundes (OSCI) Version 2.2.3.2	Bremen online services GmbH and Co. KG	EAL3+	24-OCT-08
Sign Live! CC Version 3.2.3	Intarsys consulting GmbH	EAL3+	29-AUG-08
S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1	OPENLiMit Holding AG	EAL4+	26-JUN-08
ASF Advanced Signature Framework Version 4.1	TB-Solutions Advanced Technologies, S.L.	EAL3+	09-APR0-8
Touch & Sign 2048 Version 1.00	ST Incard S>R>L>	EAL4+AVA_M	

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

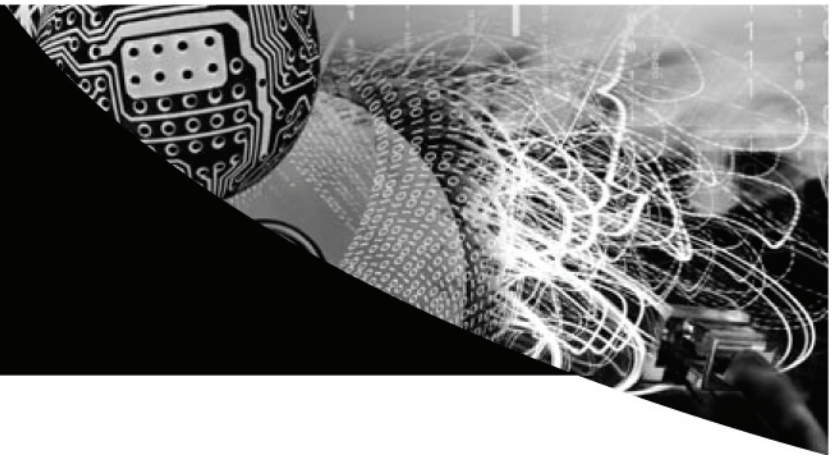


Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Products for digital signature (Continued)			
STARCO 3.2 QES Version 1.0	Giesecke & Devrient GmbH	EAL4+AVA_M	
Openlimit SignCubes BasisKomponenten 2.1 Version 2.1.6.3	OPENLiMiT SignCubes AG	EAL4+AVA_M	
Openlimit SignCubes BasisKomponenten 2.1 Version 2.1.1.1 with OPEMLiMiT PDF Plugin version 2.0.1.1 for Adobe	OPENLiMiT SignCubes AG	EAL4+	18-DEC-07
BKK OPENLiMiT base components 2.1, Version 2.1.2.1.	OPENLiMiT SignCubes AG	EAL4+	11-DEC-07
Virtual Poststelle des Bundes (Verifikationsmodul), Version 2.2.2.6	Bremen online services GmbH and Co KG	EAL3+	23-NOV-07
Virtual Poststelle des Bundes (OSCI), Version 2.2.2.6	Bremen online services GmbH and Co KG	EAL3+	23-NOV-07
Virtual Poststelle des Bundes (Basis), Version 2.2.2.6	Bremen online services GmbH and Co KG	EAL3+	23-NOV-07
Dictao Validation Server DVS Version 4.0.6	Dictao	EAL3+	24-OCT-07
S-TRUST Sign-it base components 2.1, Version 2.1.4.1	OPENLiMiT SignCubes AG	EAL4+	18-SEP-07IAIK-JCE CC Core 3.15
IAIK-JCE CC Core 3.15	Stiftung Secure Information and Communication Technologies SIC	EAL3	23-JUN-07
Openlimit SignCubes base components 2.1, version 2.1.6.1	OPENLiMiT SignCubes AG	EAL4+	16-MAY-07
Openlimit SignCubes base components 2.1, version 2.1.1.1	OPENLiMiT SignCubes AG	EAL4+	28-FEB-07
S-TRUST Sign-it base components 2.1, Version 2.1.5.1	OPENLiMiT SignCubes AG	EAL4+	28-FEB-07
Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS: 01, Firmware Version 1.06	Fujitsu Siemens Computers GmbH	EAL3+	16-JAN-07
BKK OPENLiMiT bas components 2.0 Version 2.0.2.1	OPENLiMiT SignCubes AG	EAL4+	01-JAN-07
S-TRUST Sign-it base components 2.0, Version 2.0.0.1	OPENLiMiT SignCubes AG	EAL4+	01-JAN-07
Smart card reader SPR532 Firmware Version 5.10	SCM Microsystems GmbH	EAL3+	22-DEC-06
Smart card reader SPR532 Firmware Version 5.09	SCM Microsystems GmbH	EAL3+	22-DEC-06
Chipkartenterminal KAAN Advanced Hardware Version K104R3, Firmware Version 1.02	KOBIL Systems GmbH	EAL3+	20-DEC-06
RSA Certificate Manager Version 6.7	RSA Security Inc	EAL4+	11-DEC-06

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

External Common Criteria Scheme



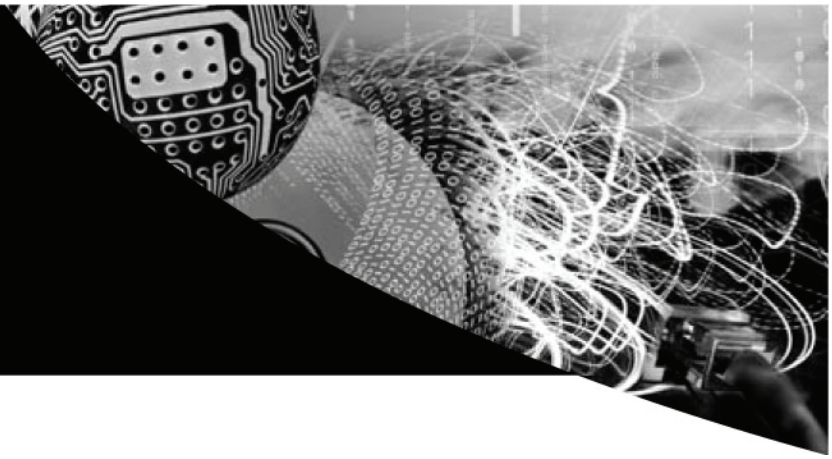
Consumers – List of evaluated products

Product	Supplier	Assurance Level	Certification Date
Products for digital signature (Continued)			
Cybertrust UniCERT Version 5.2.1	Cybertrust	EAL4+	25-OCT-06
ZKA SECCOS Sig Version 1.5.3	Sagem Orga GmbH	EAL4+	08-SEP-06
S-TRUST Sign-it base components 2.0, Version 2.0.3.1	OPENLiMiT SignCubes AG	EAL4+	22-JUN-06
ZKA SECCOS Sig Version 1.5.2	Sagem Orga GmbH	EAL4+	13-JUN-06
AdSignerWeb Version 3.1.800/Signature Creation Application	Dictao	EAL3+	28-APR-06
Smart Terminal ST-2xxx Firmware Version 5.08	Cherry GmbH	EAL3+	09-FEB-06
Openlimit SignCubes base components 2.0, version 2.0.1.1 with Openlimit SignCubes PDF Plugin Version 2.0.1.1 for Adobe Openlimit SignCubes base components 2,o Version 2.0.1.1 DBsign for Client/Server Applications Version 3.0	Gradkell Systems Inc	EAL2	30-SEP-05
Dbsign for HTML Applications Version 3.0	Gradkell Systems Inc	EAL2	30-SEP-05
Dbsign for Oracle Web Forms Applications Version 3.0	Gradkell Systems Inc	EAL2	30-SEP-05
Chipkartenterminal der Familie CardMan Trust CM3621/CM3821	OMNIKEY GmbH	EAL3+	05-SEP-05
Applatoo Version 1.2.4	France Telecom R&D, Iiex	EAL2+	25-APR-05
Openlimit SignCubes 1.6, Version 1.6.0.5	OPENLiMiT Holding AG	EAL3+	19-Nov-04
IKey 2032	SafeNet Inc	EAL2	01-AUG-04
SignCubes Professional, Version 1.5	SignCubes GmbH	EAL3+	22-JUL-04
T-TeleSec Signet, Version 1.6.0.4	T-Systems International GmbH	EAL3+	22-JUL-04
BKK SignCubes, Version 1.5	Bundesverband der Betriebskrankenkassen	EAL3	22-JUL-04
Openlimit SignCubes, Version 1.5	OPENLiMiT SignCubes AG	EAL3+	22-JUL-04
T-TeleSec Signet, Version 1.5	T-Systems International GmbH	EAL3+	22-JUL-04
E.sqia SignCubes, Version 1.5	e-Siqua Informationstechnologien GmbH	EAL3	22-JUL_04

HMG Departments wishing to use foreign certified products in environment where national security is an issue are advised to consult CESG

SECTION 16

External Common Criteria Scheme



Foreign Certification Bodies – Contact Details

Australia and New Zealand (Certificate Authorising)

Defence Signals Directorate (representing the federal Government of Australia) and Government Communications Security Bureau (representing the Governmant of New Zealand0 jointly operate the Australasian Information Security Evalyuation Program (AISEP).

Defence Signals Directorate, AISEP Manager, Information Security Group Locked Bag 5076, Kinston ACT 2604

Telephone: +61 2 6265 0342
Fax: +61 2 6265 0328
URL: www.dsd.gov.au/infosec

Austria (Certificate Authorising)

Federal Chancellery, Federal Ministry of Public Servic and Sports

URL: www.cio.gv.at/

Canada (Certificate Authorising)

The Communication Security Establishment (CSE) operates the Canadian Common Evaluation and Cerification Criteria Scheme.

Canadian Common Criteria Evaluation and Certification Scheme Communications Security Establishment

Telephone: +1 631 991 7956
Fax: +1 613 991 7902
URL: http://www.cse-cst.gc.ca/services./common-criteria/common-criteria-e.html

Czech Republic (Certificate Consuming)

National Security Authority of the Czech Republic P.O. Box 49, CZ-150 06 Praha 56, Czech Republic

Telephone: +420 257 283 333
Fax: +420 257 283 200

Demark (Certificate Consuming)

National IT and Telecom Agency IT-Security Office, Holsteinsgade 63, 2100 Copenhagen, Denmark

Telephone: +45 3545 0000/+45 3545 0365
Fax: +45 3545 0012

Finland (Certificate Consuming)

Ministry of Finance
P.O. Box 28, 00023 Valtioneuvosto, Finland

France (Certificate Authorising)

Direction Centrale de la Securite des Systems d'Information (DCSSI) operates the French Evaluation and Certification Scheme

Direction Centrale de la Securite des Systems d'Information (DCSSI) Centre de Certification, 51 Boulvard de Latour=Maubourg

Telephone: +33 1 71758265
Fax: +33 1 71758260
URL: www.ssi.gouv.fr

Germany (Certificate Authorising)

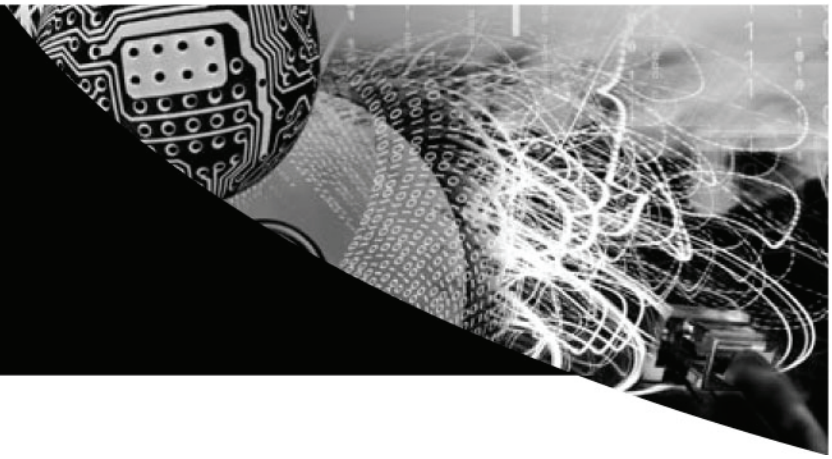
The Bundesamt for Sicherheit in der Informationstechnik (BSI) operates the German Evaluation and Certification Scheme

Bundsamt für Sicherheit in der Informationstecnik
Referat III 2.2, Godsberger Allee 185-189,
53175 Bonn, Germany

Telephone: +49 228 9582 111
Fax: +49 228 9582 455
URL: www,bsi.bund.de

SECTION 16

External Common Criteria Scheme



Foreign Certification Bodies – Contact Details

Greece (Certificate Authorising)

Ministry of Interior
Pan. Hanellopoulou 4, Athens 10177. Greece

Hungary (Certificate Consuming)

Ministry of IT and Telecommunication
H-1077 Budapest, Dob utca 75081

URL: www.ihm.hu

India (Certificate Consuming)

Government of India Department of Information Technology
TSQC IT Services
ERTL (East), DN Block, Sector-V, Salt Lake, Kolkata-700091

Telephone: +91 33 23674693
Fax: +91 33 23679472

Israel (Certificate Consuming)

Standards Institution of Israel
42 Lebanon St. 69977 Tel-Aviv, Israel

Telephone: 972 646 7668

Japan (Certificate Authorising)

Japan Information Technology Security Evaluation and Certificate Scheme (JISEC) operates the Japanese Evaluation and Certification Schemme.

Information Security Certification Office
Information Technology Promotion Agency (IPA)
Bunkyo Green Court Center Office, 2-28-8 Hon-Komagome,
Bunkyo-ku, Tokyo 113-6591, Japan

Telephone: +81 3 5978 7538
Fax: +81 3 5978 7538
URL: www.ipa.go.jp/security.jisec/jisec_e/index.html

The Republic of Korea (Certificate Authorising)

The National Intelligence Service (NIS) operates the Korean IT Security Evaluation and Certification Scheme (KECS)

Telephone: +82 2 3412 3380
Fax: +82 2 557 1129
URL: www.kecs.go.kr

The Netherlands (Certificate Authorising)

TNO-Certification operates the Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

TNO Certification, P.O. Box 541, 7300 AM Apeldoorn
The Netherlands

Telephone: +31 55 549 34 68
Fax: +31 55 549 32 88
URL: www.tno-certification.nl

Norway (Certificate Authorising)

The Norwegian National Security Authoruty operates the Morwegian Certification Authority for IT Security (SERTIT)

SERTIT

Telephone: +47 67 86 40 00
Fax: +47 67 86 40 09
URL: www.sertit.no/

Singapore (Certificate Consuming)

Infocomm Development Authority of Singapore (IDA)
Technology Standards, Technology Direction
8 Temasek Boulvard #14-00 Suntec Tower 3
S038988 Republic of Singapore

Telephone: +65 6211 1233
Fax: +65 6211 2211

Spain (Certificate Authorising)

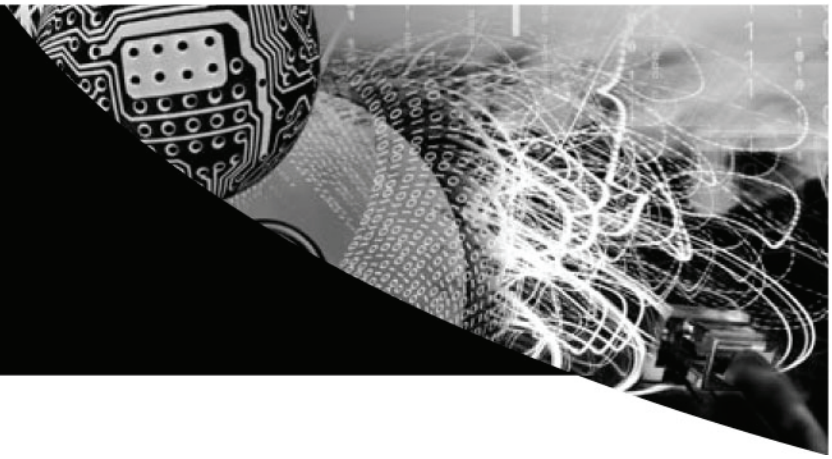
The-Certification Body (CB) of the Spanish Evaluation and Certification Scheme operates under the scope of the National Cryptologic Cneter.

Centro Criprològico Nacional
Centro Nacional de Intelligencia, Ministerio de Defensa
Avda. Parde Huidobro, s/n 28032 MADRID, Spain

URL: www.oc.ccn.cni.es

SECTION 16

External Common Criteria Scheme



Foreign Certification Bodies – Contact Details

Sweden (Certificate Consuming)

The Swedish Conmmon Criteria Evaluation and Certification Scheme is maintained and operated by the Swedish Certification Body fir IT-Security (CSEC), a unit within the Swedish Defence Materiel Adminstration (FMV)

Swedish Certification Body for IT Security FMV/CSEC,
S-115 88 Stockholm, Sweden

Telephone: +91 33 23674693
Fax: +91 33 23679472

Turkey (Certificate Consuming)

TSE (Turkish Standards Institution)
Necatibey Cad No. 112, Bakanliklar 06100. Ankara

Telephone: +90 312 418 48 84
Fax: +90 312 418 01 16
URL: www.tse.org.tr

United Kingdom (Certificate Authorising)

CESG and the Department of Trade and Industry (DTI) operate the UK IT Security Evaluation and Certification Scheme

Certification Body SECREtariat
UK IT Security Evaluation and Certification Scheme
Po Box 152 Cheltenham GL52 %UF, United Kingdom

Telephone: +44 (0) 1242 238739
Fax: +44 (0) 1242 235233
URL: www.cesg.gov.uk

The United States (Certificate Authorising)

The National Institute of Standards and Technolgy (NIST) and the National Security Agency (NSA) operate the Common Criteria Evaluation and Validation Scheme (CCEVS) under the National Information Assurance Partnership (NIAP).

National Information Assurance Partnership
Department of Defence, 9800 Savage Road, Suite 6740
Ft. George Meade, ND 20755-6740, USA

Telephone: +1 410 854 4458
Fax: +1 410 854 6615
URL: www.niap-ccevs.org

SECTION 17

Index

NB USERS ARE STRONGLY URGED TO CHECK WITH CESG THAT BOTH THE PRODUCT AND ITS CRYPTOGRAPHY ARE SUITABLE FOR HMG USE PRIOR TO PURCHASING.

CAPS
CESG Assisted Products Service

Prospective purchasers of CAPS approved products are reminded that the product descriptions in the Directory are a guide only, and that they should consult the product's Security Target and Handling Instructions before purchasing to check the product's suitability. Security Targets for CAPS products are available from the vendor and the Handling Instructions are available from either the vendor of CESG. Please note that these documents are often Protectively Marked and therefore available only to recipients with a valid need to know and appropriate storage and handling facilities.

ITSEC/CC
Prospective purchasers of ITSEC/CC certified products should read both the Security Target and the Certification Report to ensure the product is suitable. These are available from the vendor and in addition can usually be downloaded from CESG website.

CTAS
CESG Tailored Assurance Service

The CESG Tailored Assurance Service CTAS has been established to provide its customers with a mechanism for utilising CESG authorised suppliers to undertake Information Assurance activities in a flexible, agile and efficient manner tailored to accreditors needs. CTAS offers an improved approach to evaluation over existing schemes, its central feature being a thorough search for IA vulnerabilities.

For further information about other aspects of CESG's work, please contact: Customer Support Office, CESG, A2j, Hubble Road, Cheltenham, Gloucestershire, GL510EX. Telephone: +44 (0) 1242 709141 Fax: +44 (0) 1242 709193 .Email: enquiries@cesg.gsi.gov.uk

SECTION 17

Index

Products listed alphabetically by name

SECTION 17

Index

Products listed alphabetically by name

SECTION 17

Index

Products listed alphabetically by name

SECTION 17

Index

Products listed alphabetically by name

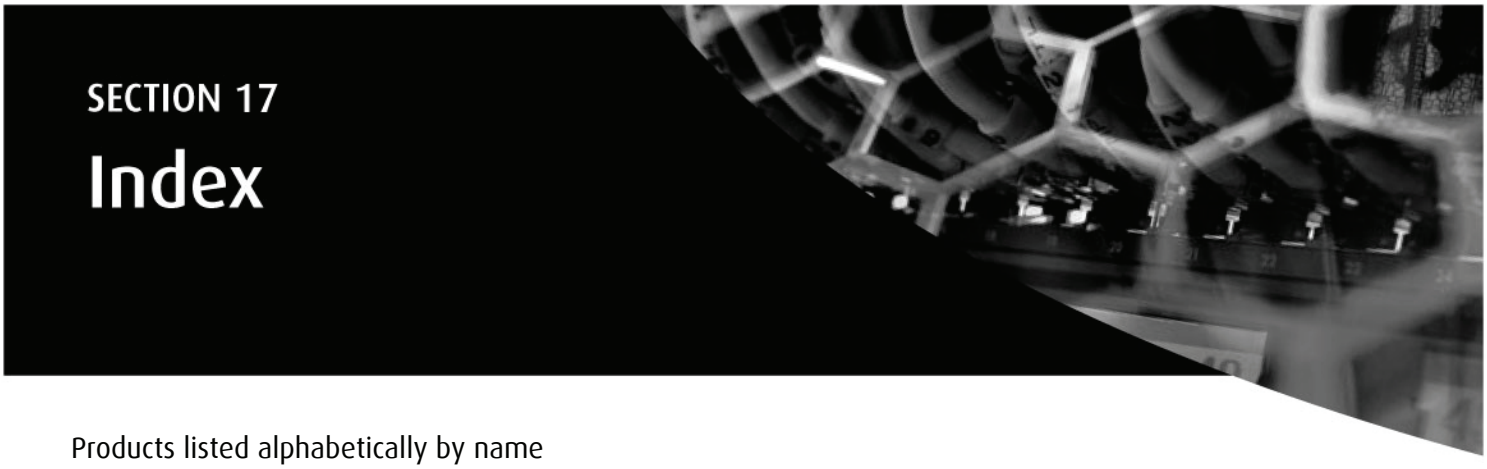
SECTION 17

Index

Products listed alphabetically by name

SECTION 17

Index



Products listed alphabetically by name

SECTION 17

Index

Products listed alphabetically by name

SECTION 17

Index

Products listed alphabetically by name

SECTION 17

Index

Products listed by category

SECTION 17

Index

Products listed by category

SECTION 17

Index

Products listed by category

SECTION 17

Index

Products listed by category

SECTION 17

Index

Products listed by category

SECTION 17

Index

Products listed by category

SECTION 17

Index

Products listed by category

SECTION 17

Index

Information Assurance – related abbreviations

CAPS	CESG Assisted Products Service
CB	Certification Body
CC	Common Criteria
CCTM	CESG Claims Tested Mark
CLEF	Commercial Evaluation Facility
CMS	Certificate Maintenance Scheme
CNI	Critical National Infrastructure
COTS	Commercial-off-the-self
CR	Certification Report
CTAS	CESG Tailored Assurance Service
EAL	Evaluation Assurance Level
IACS	Information Assurance and Consultancy Services
IEC	International Electro-technical Commission
IS	Infosec Standard
ISO	International Standardisation Organisation
ITSEC	IT Security Evaluation Criteria
MO	Management Office
PP	Protection Profile
SEAP	Security Equipment Assessment Panel
ST	Security Target
UKAS	United Kingdom Accreditation Service