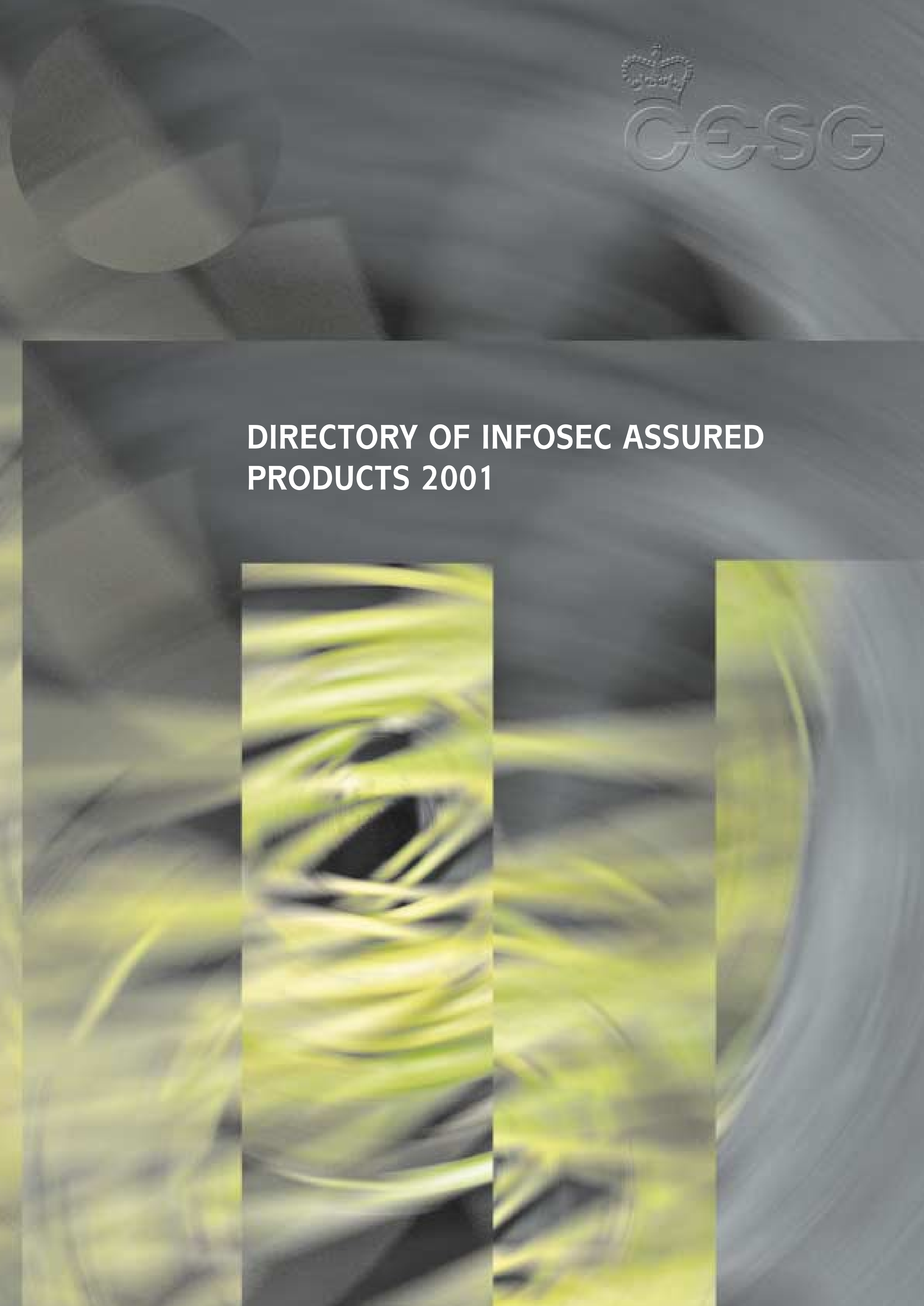


CESG

DIRECTORY OF INFOSEC ASSURED PRODUCTS 2001

CONTENTS

INTRODUCTION

The Communications-Electronics Security Group [CESG] is the UK's National Technical Authority for Information Security. As part of this remit, CESG works closely with IT developers and vendors to provide end users with a choice of products whose security features have been objectively assessed and which meet clear standards of security assurance.

This 'Directory of Infosec Assured Products' is a new publication that replaces the former UKSP-06. It has been produced as a top-level guide for both product developers, vendors and end-users, and gives details of the means by which security products are approved or certified, an overview of the products' features, and the context in which they should be used. The Directory will be updated on an annual basis. However, as new products are regularly being approved and certified, these will be reflected on CESG's websites, accessible via www.cesg.gov.uk, as and when they become available.

The first part of the Directory contains an introduction to CESG's Infosec Assurance and Certification Services [IACS]. IACS has been created to provide a seamless service to customers, and products listed in the sections which follow cover the various aspects of IACS. It is recognised that, in practice, customers will require more specific guidance. The IACS management office has therefore been created to provide advice and guidance to developers, vendors and end-users on the most appropriate solution to their specific assurance requirements.

This is followed by a description of the mechanisms by which products are certified under ITSEC or Common Criteria, a list of certified products, and an explanation of 'protection profiles'. Also contained in the Directory is a brief description of the new 'Fast Track Assessment' (FTA) service which has been designed to assess IT security products at the specific behest of customers in government.

The Directory next has a section covering the CESG Assisted Products Scheme [CAPS].

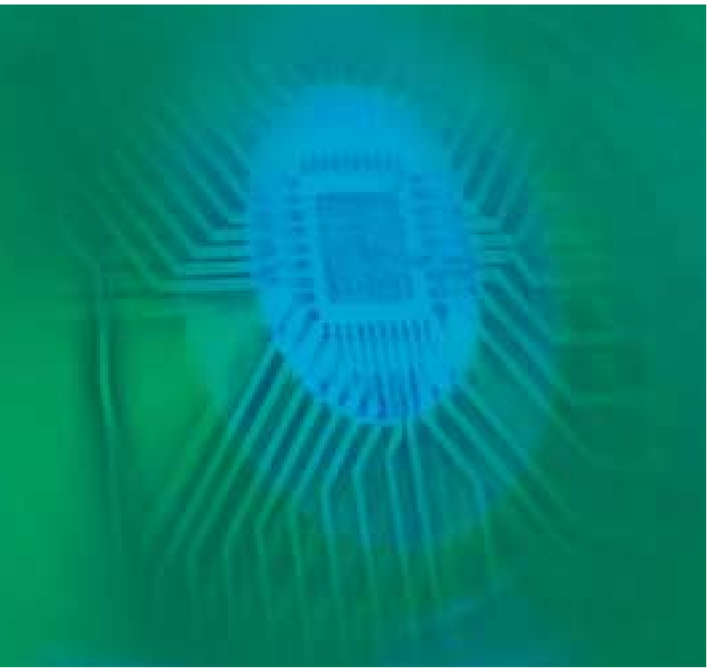
This scheme ensures that government and public sector users have access to a wide range of approved products that employ cryptographic security measures. These products have undergone a thorough investigation of the security offered by the cryptography employed, whether this is through implementation of a CESG algorithm or a public domain algorithm.

Finally, there is a section containing an introduction to TEMPEST services and a list of TEMPEST certified products.

Inevitably, a directory such as this cannot cover all aspects of approved or certified Infosec products and related services. Customers may need more in-depth guidance and advice, and contact details are therefore provided in each of the relevant sections.

For any general queries regarding CESG's wider range of Infosec services, please contact the marketing office, details for which are given on the back page of this directory.

(IACS) Infosec Assurance and Certification Services



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 IACS to offer bespoke solutions to these new security challenges.

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 CC or ITSEC Certification
- Cryptographic approval for HMG and the CNI (usually carried out under CAPS)
- Fast Track assessment of products for HMG and the CNI
- Systems assessments at all levels for HMG and commerce

For End Users...

Products which have been certified by us, or by our partners around the world, offer end users ready-made assurance. Where a Government or CNI customer has a requirement for assurance in an uncertified product, we can perform a Fast Track Assessment. 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 Health Check, is available.

www.cesg.gsi.gov.uk
e-mail: iacs@cesg.gsi.gov.uk

IACS Management Office
PO Box 152 Cheltenham
Gloucestershire GL52 5UF

Tel. +44 (0)1242 238739
Fax: +44 (0)1242 235233

Formal Evaluation and Certification

The products within this section have been certified against either Common Criteria or IT Security Evaluation Criteria (ITSEC). Certificates are awarded 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 purchasers of certified products should read both the ST and the CR to ensure that the product is suitable. STs and CRs are available from the developers and, in addition, can usually be downloaded from the CESG web site.

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.

Certificate Maintenance Scheme

Evaluation results only apply 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. Because the evolution of products is so rapid, the Certificate Maintenance Scheme (CMS) has been devised in response. CMS provides a means of maintaining the same level of assurance in a product after certification without the need for re-evaluation.

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 web site.

Common Criteria	ITSEC
EAL1	–
EAL2	E1
EAL3	E2
EAL4	E3
EAL5	E4
EAL6	E5
EAL7	E6

International Mutual Recognition

Developers whose products are certified against ITSEC or CC enjoy the benefits of an internationally recognised Certificate. In this brochure we detail only those products which have been evaluated in the UK, but end users should access the other relevant national web sites to obtain the most up to date information on products which have been assessed elsewhere. Links are available from the CESG web site and contact details for the other recognised Certification Bodies appear on page 9.

HMG Departments wishing to use foreign certified products in environments where national security is an issue are advised to consult CESG.

Our Certificates are currently recognised as follows:

Assurance Levels Recognised	
Australia & New Zealand	**ITSEC E1-E6** **CC EAL1-4**
Canada Israel USA	**CC EAL1-4**
France Finland Germany Greece Italy Netherlands Norway Spain Sweden Switzerland	**ITSEC E1-E6** **CC EAL 1-7**

Evaluation – CESG working with industry

Formal evaluation in the UK is carried out by independent testing laboratories known as CLEFs which are appointed by the Certification Body in CESG. CLEFs meet rigorous security and ISO/IEC 17025 quality standards. The UK has 5 CLEFs, which can be contracted to carry out both evaluation and preparatory consultancy work. CLEF contact details are on page 9.

The results of the testing of the product are provided to the Certification Body in an evaluation technical report which forms the basis of the Certification Report. The CB is part of CESG and is itself accredited by UKAS to EN45011 for its ITSEC and CC certifications.

CESG recognises Certificates from other international bodies as follows:

Certification/Validation	Recognised Assurance Levels
AISEP, Australia	Common Criteria EAL1 to EAL4, ITSEC E1 to E6
BSI, Germany	Common Criteria EAL1 to EAL7, ITSEC E1 to E6
CSE, Canada	Common Criteria EAL1 to EAL4
DCSSI, France	Common Criteria EAL1 to EAL7, ITSEC E1 to E6
NIAP, USA	Common Criteria EAL1 to EAL4

Fast Track

Fast Track Assessment (FTA) provides a fast, flexible, cost-effective process for the generation of a CESG endorsed assessment of the extent to which security-enabled products meet the Infosec requirements of Sponsors, in accordance with national Infosec policy. Sponsors would be central and local government, and Critical National Infrastructure (CNI) services, where it is in the national interest. FTA tailors each assessment to the context of the intended use of the product, resulting in a report that provides authoritative guidance on the product’s suitability.

The FTA service provides the assurance required by identified sponsors in products whose market and limited cryptography do not justify formal evaluation and certification, or evaluation under CAPS. The FTA Service is intended to address assurance requirements in the low to medium range.

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 evaluations where only limited functionality is tested and evaluation against an assurance profile (eg E3 for firewall, E2 for authentication, E1 for audit) to meet differing requirements. For Government or CNI users there is also the option of a system IT Health Check.

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, the IACS MO and CESG Listed Advisor Scheme consultants. The need for evaluation consultancy should be discussed with the IACS MO and the CLEFs at the start of the product evaluation lifecycle.

Where cryptography 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 done under the CESG Assisted Products Scheme (CAPS) and as a single package with ITSEC/CC or Fast Track evaluations or assessments.

The IACS Management Office is happy to provide more information on any of the Assurance and Certification Services briefly described here.

CLEF Contact Details

CMG Admiral (CLEF)
King's Court
91-93 High Street
Camberley
Surrey GU15 3RN
Tel. +44 (0) 1276 686678
Fax. +44 (0) 1276 691028
Ralph Worswick
ralph.worswick@cmgplc.com

EDS Ltd (CLEF)
Wavendon Tower
Wavendon
Milton Keynes
Bucks MK17 8LX
Tel. +44 (0) 1908 284234
Fax. +44 (0) 1908 284393
Trevor Hutton
trevor.hutton@edl.uk.eds.com

IBM Global Services (CLEF)
Meudon House
Meudon Avenue
Farnborough
Hants GU14 7NB
Tel. +44 (0) 1252 558081
Fax. +44 (0) 1252 558001
Bob Finlay
bob_finlay@uk.ibm.com

Logica UK Ltd (CLEF)
Chaucer House
The Office Park
Springfield Drive
Leatherhead
Surrey KT22 7LP
Tel. +44 (0) 1372 369831
Fax. +44 (0) 1372 369834
Simon Milford
MilfordS@logica.com

Syntegra (CLEF)
Guidion House
Harvest Crescent
Ancells Park, Fleet
Hants GU13 8UZ
Tel. +44 (0) 1252 778837
Fax. +44 (0) 1252 811635
Janet Scruby
janet.scruby@syntegra.bt.co.uk

Foreign Scheme Contact Details

Australia

www.dsd.gov.au/infosec
The AISEP Manager
Certification & Evaluation Group
Information Security Branch
Defence Signals Directorate
Locked Bag 5076, Kingston ACT 2604
Tel. +61 2 6265 0342
Fax. +62 2 6265 0328

Canada

www.cse.dnd.ca
Communications Security Establishment
Criteria Coordinator
IT Security Standards and Initiatives
PO Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel. +1 613 991 7600
Fax. +1 613 991 7411

France

www.scssi.gouv.fr
Direction Centrale de la Sécurité des
Systèmes d'Information,
18, Rue du Docteur Zamenhof
F-92131, Issy-Les-Moulineaux
Cédex, France
Tel. +33 141 463784
Fax. +33 141 463701

Germany

www.bsi.bund.de
Bundesamt für Sicherheit in der
Informationstechnik
Referat II 2, Godesberger Allee 183
53175 Bonn, Germany
Tel. +49 228 9583 141
Fax. +49 228 9582 455

USA

www.niap.nist.gov/cc-scheme
National Information Assurance
Partnership
100 Bureau Drive (Mailstop 8930)
Gaithersburg, MD 20899-8930, USA
Tel. +1.301.975.2934
Fax. +1.301.948.0279

MONDEX Purse 2.0

ITSEC E6
Certificate Number: P129 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.

SUPPLIER:
MAOSCO Ltd, 47-53 Cannon Street
London EC4M 5SQ
Point of contact: David Meadon
Telephone: +44 20 7557 5420
Facsimile: +44 20 7557 5430
Email: customer.services@multos.com
URL: http://www.multos.com

DEVELOPER:
Platform7, 6th Floor, 1-2 Finsbury Square
London EC2A 1AA
Telephone: +44 (0) 20 7714 8492
Facsimile: +44 (0) 20 7714 8246
URL: http://www.platform7.com

Multos v3 on Hitachi H8/3112 ICC

ITSEC E6
Certificate Number: P130 September 1999
CLEF: Logica

MULTOS is a secure, multi-application operating system for use on an Integrated Circuit Card (ICC) (smartcard), to manage, segregate and execute applications written for MULTOS (such as loyalty, ticketing, credit, debit and electronic purse). 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 ICC's EEPROM. During the production process, each ICC is injected with a unique EEPROM identifier and a unique symmetric 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.

SUPPLIER:
MAOSCO Ltd, 47-53 Cannon Street
London EC4M 5SQ
Point of contact: David Meadon
Telephone: +44 20 7557 5420
Facsimile: +44 20 7557 5430
Email: customer.services@multos.com
URL: http://www.multos.com

DEVELOPER:
Platform7, 6th Floor, 1-2 Finsbury Square
London EC2A 1AA
Telephone: +44 (0) 20 7714 8492
Facsimile: +44 (0) 20 7714 8246
URL: http://www.platform7.com

KILGETTY PLUS NT4 v1.0

Government use only

ITSEC E3
Certificate Number: P112, Issue 2 May 2000
CLEF: EDS

KILGETTY PLUS NT4 is a total hard disk encryption product, which protects government data (protectively marked up to TOP SECRET) against unauthorised access in the event of loss.

KILGETTY PLUS NT4 is for use with IBM compatible computers running Microsoft Windows NT4, with hard disks up to 7.8GB in size. All data that is held on the computer's hard disk is fully encrypted, including data structures, operating system and applications. Access is via a touch memory device (read by a reader attached to the serial port), user identity and password.

KILGETTY PLUS NT4 was evaluated on Microsoft Windows NT4 Server and Workstation versions with Service Packs 3, 4, 5, and 6a.

The Software Box
Green Park Business Centre, Goose Lane
Sutton on the Forest, York YO6 1ET
United Kingdom

Point of Contact: The Security Group
Telephone: +44 (0) 1347 812100
Email: security_group@softbox.co.uk
URL: http://www.softbox.co.uk

KILGETTY PLUS v1.2h

Government use only

ITSEC E3
Certificate Number: p105 November 1998
CLEF: CMG Admiral

KILGETTY PLUS is a total disk encryption product, which protects government data against unauthorised access in the event of loss. For use with IBM compatible computers running Microsoft DOS, Win 3.1 and Win 9x, all data that is held on the computer's hard disk is fully encrypted, including data structures, operating system and applications. Access is via a touch memory device (read by a reader attached to the serial port), user identity and password.

KILGETTY PLUS provides CESG approved protection for data protectively marked up to TOP SECRET and is suitable for hard disks up to 4GB.

The Software Box
Green Park Business Centre, Goose Lane
Sutton on the Forest, York YO6 1ET
United Kingdom

Point of Contact: The Security Group
Telephone: +44 (0) 1347 812100
Email: security_group@softbox.co.uk
URL: http://www.softbox.co.uk

Portcullis Guardian Angel

v5.01D1

ITSEC E2
Certificate Number: 98/93 January 1998
CLEF: Syntegra

The security mechanisms of this pre-DOS loader are designed to enforce PC access control for a hierarchy of users. The security barriers are imposed by:

- Authentication using passwords encrypted by an endorsed implementation of the CESG FIREGUARD algorithm.
- User security profiles, auditing and a File Access Control Matrix managing access to the data.
- Blocking non-authenticated programs to prevent the introduction of malicious code (e.g. Viruses).
- Disk certification preventing the use of floppy disks not formatted by Guardian Angel.
- Encryption of data using an endorsed implementation of the CESG RED PIKE algorithm to protect files being exported or transmitted.

Portcullis Computer Security Ltd
The Grange Barn, Pikes End
Pinner, Middlesex HA5 2EX

Point of contact: Alan Romanis
Telephone: +44 (0) 208 868 0098
Facsimile: +44 (0) 208 868 0017
Email: consult@portcullis-security.com
URL: http://www.portcullis-security.com

Reflex Disknet for NT

v1.20

ITSEC E2
Certificate Number: P125 July 1999
CLEF: Logica

Reflex Disknet for Windows NT Data Security works by creating a “shield” around every system. Disknet denies access to the hard disk if the target PC is booted from a floppy and the system can be configured to prevent any booting from floppy if required. It prohibits users tampering with PC configurations and prevents the introduction of unauthorised/illegal software. PSG module prevents modification or deletion of existing files, and prevents any changes to applications. PSG will also prevent any executable files being installed.

Reflex Magnetics
31-33 Priory Park Road, London NW6 7HP
United Kingdom

Point of contact: Andy Campbell
Telephone: +44 (0) 20 7372 6666
Facsimile: +44 (0) 20 7372 2507
Email: sales@reflex-magnetics.com
URL: http://reflex-magnetics.com

SeNTry 20/20

COMMON CRITERIA EAL1
Certificate Number: P100 July 1998
CLEF: IBM Global Services

SeNTry 2020 enables users to store files securely by generating an encrypted virtual drive on the host PC hard disk, access to which is restricted via a passphrase. The virtual drive can be formatted to either NTFS or FAT file systems and all files are encrypted in real-time. At any time the user can dismount the drive or if required, set an inactivity threshold for automatic dismount.

The software can be installed on either a Windows NT Server or NT Workstation (Version 4.0 SP3). The size of the virtual drive is limited by the OS and can utilise the following encryption algorithms:

- MDC/SHS
- DC/RIPM
- Cast
- Square
- DES
- MDC/SHA1
- Blowfish
- Triple DES
- Safer

MIS Corporate Defence Solutions
MIS House, Hermitage Court
Hermitage Lane, Maidstone
Kent ME16 9NT, United Kingdom

Telephone: +44 (0) 1622 723400
Facsimile: +44 (0) 1622 728580
Email: uk.sales@mis-cds.com
URL: http://mis-cds.com

STOPLOCK V v2.23a
STOPLOCK V\SC v2.23
STOPLOCK V SCenSOS v2.23a

ITSEC E3
Certificate Number: 96/65a September 1996
CLEF: Logica

Stoplock V is a software based access control package for use on IBM PCs and compatibles running MS-DOS or Windows 3.x. It provides tools for the controlling, monitoring and protection of data. Stoplock V/Sc includes an additional smartcard for user authentication and user management, and Stoplock V SCenSOS provides integration with the SCenSOS operating system for networked control and system management.

The evaluated functions include:

- Identification and Authentication;
- Access Control:
  - enhanced boot protection
  - access restrictions to files and directories
  - rights defined by administrators only
- Trusted Processes defined by a privileged user.
- Accountability and Audit:
  - Audit trail of various events
  - audit trail may only be accessed by privileged users.

Conclusive Logic Ltd
Babbage House, 55 King Street,
Maidenhead, Berkshire SL6 1DU
United Kingdom
Point of contact: Steve Mathews
Telephone: +44 (0) 1628 470900
Facsimile: +44 (0) 1628 470901
URL: http://www.conclusive.com

Argus B1/CMW

v1.2 for Solaris 2.4

Argus C2/TMW

v1.2 for Solaris 2.4

ITSEC E3 F-B1 CMW ITSEC E3 F-C2 TMW
Certificate Number:
96/73a (B1/CMW, x86 platform)
December 1996
96/73b (C2/TMW, x86 and SPARC platforms)
December 1996
CLEF: CMG Admiral

The Argus TMW and CMW products are workstation/server enhancements that bring an off-the-shelf Solaris 2.4 system up to labeled-C2 and B1 level respectively. Each provides full floating information label functionality. The CMW product also provides mandatory access control (MAC) based on sensitivity labels. Both support labelled printing and a complete labelled X-windows subsystem for system-high (TMW) and multilevel (CMW) operations. Each can operate in either X-window or command-line mode for desktop or server applications. The evaluation included trusted networking, trusted path, least privilege, audit, and other functionality.

Argus Systems Group, Inc.
1809 Woodfield Drive, Savoy, IL 61874, USA
Point of contact: Paul A. McNabb
Telephone: +1 217 355 6308
Facsimile: +1 217 355 1433
Email: info@argus-systems.com
URL: http://www.argus-systems.com

Argus B1/CMW

v1.3.2 for Solaris 2.4

Argus C2/TMW

v1.3.2 for Solaris 2.4

ITSEC E3 F-B1 CMW ITSEC E3 F-C2 TMW
Certificate Number:
99/89a (B1/CMW, x86 platform)
September 1999
99/89b (C2/TMW, x86 and SPARC platforms)
September 1999
CLEF: CMG Admiral

The Argus TMW and CMW products are workstation/server enhancements that bring an off-the-shelf Solaris 2.4 system up to labeled-C2 and B1 level respectively. Each provides full floating information label functionality. The CMW product also provides mandatory access control (MAC) based on sensitivity labels. Both support labelled printing and a complete labelled X-windows subsystem for system-high (TMW) and multilevel (CMW) operations. Each can operate in either X-window or command-line mode for desktop or server applications. The evaluation included trusted networking, trusted networked access, trusted path, least privilege, superuser emulation, audit, and other functionality.

Argus Systems Group, Inc.
1809 Woodfield Drive, Savoy, IL 61874, USA
Point of contact: Paul A. McNabb
Telephone: +1 217 355 6308
Facsimile: +1 217 355 1433
Email: info@argus-systems.com
URL: http://www.argus-systems.com

Hewlett Packard HP-UX 10.20

ITSEC E3 /CESG ASSISTED PRODUCTS SCHEME
Certificate Number: P111 February 1999
CLEF: CMG ADMIRAL

Hewlett-Packard's HP-UX version 10.20 is an X/Open UNIX 95 branded product, meaning that it conforms with X/Open's Single UNIX Specification (SPEC1170). In addition HP-UX 10.20 complies with such standards as X/Open Portability Guide Issue IV Base Profile (XPG4), OSF AES, IEEE POSIX 1003.1 and 1003.2, SVID 3 level 1 APIs, as well as all major de facto APIs such as BSD 4.3.

HP-UX 10.20 is designed to exceed the ITSEC F-C2 functionality class, with the following notable extensions:

- Terminal-based User Authentication
- Time-based User Authentication
- Boot Authentication
- Access Control Lists
- 'Green Book' compliant Password Management - generation & encryption

HP-UX 10.20 is supported across the full range of HP9000 Workstations and Servers

Hewlett-Packard Ltd
Nine Mile Ride, Wokingham,
Berkshire RG40 3LL, United Kingdom

Point of contact: Christopher Simpson
Telephone: 01344-365029
Facsimile: 01344-763747
Email: christopher_simpson@hp.com
URL: http://www.hp.com/uk

IBM DYNIX/ptx Unix

v4.1 SLS and 4.1a SLS on Symmetry 5000 Systems (models SE30 and SE40)

ITSEC E3
Certificate Number: 97/74 February 1997
CLEF: Logica

DYNIX/ptx is a secure Operating System certified to E3 F-C2, and is IBM's enhanced version of UNIX for the Symmetry series of symmetric multiprocessing systems. DYNIX/ptx conforms to all the leading industry operating systems standards, including IEEE POSIX 1003.1-1990, FIPS, X-Open, XPG4, Intel ABI+, OSF AES and USLSVID3. DYNIX/ptx includes specific support for operations with concurrent user populations in excess of 1000 and disk volumes in excess of 1000GB. The hardware may be extended by adding more processors with true linear performance scalability.

Three additional CESG modules are available for use in HMG systems and may be applied for, namely FIRESTONE, THUNDERBOLT and THUNDERFLASH password encryption and generation packages.

Point of contact: Valerie Ashton
Telephone: +44 (0) 1932 851111
Facsimile: +44 (0) 1932 850011
Email: val_ashton@uk.ibm.com
URL:

IBM DYNIX/ptx

v4.4.2 running on Symmetry 5000 systems and NUMA-Q 2000

ITSEC E3
Certificate Number: P108V2 January 2000
CLEF: Logica

DYNIX/ptx Version 4.4.2 (with CESG algorithms) is IBM's enhanced version of UNIX running on Symmetry 5000 systems (Model SE40) and NUMA-Q (Non Uniform Memory Access) 2000 (with EMC≈ Symmetrix 3430/3700 disk arrays) and is evaluated to E3 F-C2.

DYNIX/ptx is a robust and reliable implementation of UNIX for secure commercial projects running enterprise level applications. DYNIX/ptx conforms to all the leading industry operating systems standards, including IEEE POSIX 1003.1-1990, FIPS, X-Open, XPG4, Intel ABI+, OSF AES and USLSVID3.

Four optional CESG modules will be available for use in HMG systems, namely FIREGUARD, FIRESTONE, THUNDERBOLT and THUNDERFLASH password encryption and generation packages.

Point of contact: Valerie Ashton
Telephone: +44 (0) 1932 851111
Facsimile: +44 (0) 1932 850011
Email: val_ashton@uk.ibm.com
URL:

Microsoft Windows NT Workstations and Win NT Server 4.0

ITSEC E3
Certificate Number: P121 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 basis on which other specialised security enforcing functions of evaluatable systems such as messaging, firewall, virtual private network, and PKI related systems could depend. Microsoft are participating in the development of Common Criteria Protection Profiles of such systems.

Microsoft Ltd
Microsoft Campus, Thames Valley Park,
Reading, Berks RG1 1WG, United Kingdom

Point of contact: Peter Birch
Telephone: +44 (0) 870 6010 100
Facsimile: +44 (0) 870 6020 100
Email: peterbir@microsoft.com
URL: http://www.microsoft.com/uk

Sun Solaris 2.6

Certificate Maintenance Scheme

ITSEC E3
Certificate Number: P101 January 1999
CLEF: Logica

Solaris 2.6 is the latest version of Sun's commercial Solaris operating system evaluated to ITSEC E3/F-C2. The product was initially evaluated on the Sun UltraSPARC-1 Workstation and servers sharing information in a distributed networking environment. The evaluation includes the following features in addition to the ITSEC Functionality Class F-C2:

- CDE window system
- Networking utilising the TCP/IP protocol
- NIS+ Distributed Naming Service
- NFS

In February 1999, Sun entered into the Certificate Maintenance Scheme and evaluation is extended to a wide range of Sun platforms, from uni-processor MicroSPARC workstations to multi-processor UltraSPARC Enterprise servers.

Sun Microsystems Inc
MPK 18-211 rm 2295, 901 San Antonio Road,
Palo Alto, CA 94303, USA

Point of contact :
Telephone:
Facsimile: +1 650 786 5731
Email: Solaris-Security-Target@Eng.Sun.Com
URL: http://www.sun.com/security

Sun Solaris

v8 with AdminSuite v 3.0.1

COMMON CRITERIA EAL4
Certificate Number: P148 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 certified as meeting the Common Criteria Part 3 conformant requirements of 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 Microsystems Inc
MPK 18-211 rm 2295, 901 San Antonio Road,
Palo Alto, CA 94303, USA

Point of contact :
Telephone:
Facsimile: +1 650 786 5731
Email: Solaris-Security-Target@Eng.Sun.Com
URL: http://www.sun.com/security

Trusted Solaris 2.5.1

Certificate Maintenance Scheme

ITSEC E3
Certificate Number: P104 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 security needs of customer 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;
- Graphical User Interface 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 TSIX or MASIX protocols;
- Trusted NFS;
- Auditing;
- Multi-level mail.

Sun Microsystems Inc
MPK 18-211 rm 2295, 901 San Antonio Road,
Palo Alto, CA 94303, USA

Point of contact:
Telephone:
Facsimile: +1 650 786 5731
Email: Solaris-Security-Target@Eng.Sun.Com
URL: http://www.sun.com/security

Authoriszor Secure Extranet Access Management System

IN EVALUATION COMMON CRITERIA EAL4
Projected Certification Date: July 2001
CLEF: IBM Global Services

Authoriszor been developed to provide a secure HTTP page delivery system which publishes WWW pages via Microsoft Internet Information Server. Content is protected from attack by storing it in a location that is inaccessible from the Internet whilst webroot is constantly monitored to protect against file deposition or modification attacks.

The optional client support allows web content to be delivered, on demand, in strict accordance with a client's pre-defined security profile.

It provides a Management System that will allow:

- Multiple site support;
- Positive Identification of clients;
- Definition of security profiles for clients and content;
- Activity logging.

Authoriszor Ltd
Windsor House, Cornwall Rd
Harrogate HG1 2PN, United Kingdom

Point of contact: Richard Atkinson
Telephone: +44 (0) 1423 730300
Facsimile: +44 (0) 1423 730315
Email: richard.atkinson@authoriszor.com
URL: http://www.authoriszor.com

Entrust/Admin & Entrust/Authority from Entrust/PKI 4.0a

COMMON CRITERIA EAL3
Certificate Number: P122 March 1999
CLEF: Syntegra

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. Other Entrust/Authority capabilities include the ability to cross-certify with other CAs, the use of flexible certificates (for including X.509v3 certificate extensions), and the use of flexible user password rules.

Entrust/Admin is an administrative interface to Entrust/Authority and allows operators to manage users, set the security policy, and control the PKI. All messages between Entrust/Admin and Entrust/Authority are secured for confidentiality, integrity, and authentication.

Entrust Technologies Ltd.
1000 Innovation Drive, Ottawa, Ontario, Canada,
K2K 3E7

Point of contact: Darryl Stal
Telephone: (613) 270-3483
Facsimile: (613) 270-2503
E-mail: entrust@entrust.com
URL: http://www.entrust.com

Entrust/RA from Entrust/PKI 5.0

COMMON CRITERIA EAL3
Certificate Number: P141 March 2000
CLEF: Syntegra

Entrust/RA 5.0 is an administrative interface to Entrust/Authority and allows operators 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 Technologies Ltd.
1000 Innovation Drive, Ottawa, Ontario, Canada,
K2K 3E7

Point of contact: Darryl Stal
Telephone: (613) 270-3483
Facsimile: (613) 270-2503
E-mail: entrust@entrust.com
URL: http://www.entrust.com

Entrust/RA from Entrust/PKI 5.1

COMMON CRITERIA EAL3
Certificate Number: P153 February 2001
CLEF: Syntegra

Entrust/RA 5.1 is an administrative interface to Entrust/Authority and allows operators 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 being evaluated on Microsoft Windows NT 4.0 Service Pack 6a.

Entrust Technologies Ltd.
1000 Innovation Drive, Ottawa, Ontario, Canada,
K2K 3E7

Point of contact: Darryl Stal
Telephone: (613) 270-3483
Facsimile: (613) 270-2503
E-mail: entrust@entrust.com
URL: http://www.entrust.com

Entrust/Authority from Entrust/PKI 5.0

COMMON CRITERIA EAL3
Certificate Number: P141 March 2000
CLEF: Syntegra

Entrust/Authority 5.0 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 (1024 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 Technologies Ltd.
1000 Innovation Drive, Ottawa, Ontario, Canada,
K2K 3E7

Point of contact: Darryl Stal
Telephone: (613) 270-3483
Facsimile: (613) 270-2503
E-mail: entrust@entrust.com
URL: http://www.entrust.com

Entrust/Authority from Entrust/PKI 5.1

COMMON CRITERIA EAL3
Certificate Number: P153 February 2001
CLEF: Syntegra

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 (1024 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 Technologies Ltd.
1000 Innovation Drive, Ottawa, Ontario, Canada,
K2K 3E7

Point of contact: Darryl Stal
Telephone: (613) 270-3483
Facsimile: (613) 270-2503
E-mail: entrust@entrust.com
URL: http://www.entrust.com

Remote Management Centre

ITSEC E1
Certificate Number: S115 January 2001
CLEF: CMG Admiral

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 from 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 customers 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 851111
Facsimile: +44 (0) 1932 814333
Email: davidstacey@uk.ibm.com
URL: http://www.uk.ibm.com

Luna® CA^3 Token

IN EVALUATION COMMON CRITERIA EAL4
Projected Certification Date: 1 July 2001
CLEF: SYNTEGRA

The Luna® CA3 Token, Luna® Dock Card Reader, and Luna® PIN Entry Device combine to provide a robust hardware security module for Certification Authorities, Certification Service Providers and Validation Authorities within Public Key Infrastructures. The product provides secure generation, storage, access control and backup of the private signing key of the Authority.
It provides advanced security features such as trusted path for entry of authentication data, M of N activation for multi-person control of critical operations and Luna® Key Cloning for secure backup of private keys and other sensitive data.

Chrysalis-ITS
One Chrysalis Way, Ottawa, ON
K2G 6P9, Canada

Point of contact: Terry Fletcher, VP Trusted
Systems Engineering
Telephone: 613 723-5076
Facsimile: 6I3 723 5078
Email: sales@chrysalis-its.com
tfletcher@chrysalis-its.com
URL: http://www.chrysalis-its.com

SureWare KeyPer v1.0

ITSEC E3
Certificate Number: P154 March 2001
CLEF: IBM Global Services

SureWare Keyper is a hardware cryptographic module that guarantees the safety and integrity of key material. SureWare Keyper has been awarded FIPS 140-1 level 4. It connects to a host computer via standard networking technology in order to provide secure cryptographic services to host computer applications:

- Key Generation
- Encryption
- Message Authentication Code
- Signing

These applications will communicate with SureWare Keyper via the industry standard interface PKCS#11.

The scope of the evaluation covered those mechanisms that protect the cryptographic services that the TOE provides. Triple DES and SHA-1 contained within the TOE are publicly known. Other cryptographic services provided such as RSA and Diffie Hellman, were outside the scope of the evaluation.

Baltimore Technologies Ltd
39/41 Parkgate Street, Dublin 8, Ireland
Point of contact:
Telephone: +61 2 9409 0300
Facsimile: +61 2 9409 0301
Email: info@baltimore.com
URL: http://www.baltimore.com

SureWare Net ED20M

IN EVALUATION ITSEC E3 and CAPS
Projected Certification Date: December 2001
CLEF: IBM Global Services

The SureWare Net ED20M is an Ethernet VPN encryptor that allows users to communicate protectively marked material across untrusted networks by using cryptographic mechanisms to lower the marking of the actual network traffic.

Features:

- Transfer of encrypted user data IP datagrams between pairs of encryptors
- Configurable security policy for authorising IP addresses and protocols
- Automated key management
- Audit trail of events
- Local and remote management options
- Security enforcing remote management communications protected cryptographically
- Authenticated local management
- Operational and standby modes
- Tamper resistant crypto-kernel
- Operation with Ethernet V2.0 and IEEE 802.3 with SNAP headers

Baltimore Technologies Ltd
39/41 Parkgate Street, Dublin 8, Ireland
Point of contact:
Telephone: +61 2 9409 0300
Facsimile: +61 2 9409 0301
Email: info@baltimore.com
URL: http://www.baltimore.com

Tracker 2650 Data Collection Unit

ITSEC E2
Certificate Number: P133 March 2000
CLEF: Logica

Tracker is an intelligent modem that reliably logs data in 32 Megabytes of battery backed memory until polled. It receives data on four RS232 ports that can also 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 from unauthorised access when replacing diagnostic modems.

This product was evaluated for the MOD's Defence Fixed Telecommunications Service.

Data Track Technology plc
153 Somerford Road
Christchurch
Dorset BH23 3TY
United Kingdom

Point of contact: Mike Terry, Business Development Manager
Telephone: +44 (0) 1425 282022
Facsimile: +44 (0) 1425 271978
Email: mterry@dtrack.com
URL: http://dtrack.com

BorderWare Firewall Server v6.1.2

COMMON CRITERIA EAL4
Certificate Number: P136 January 2000
CLEF: Syntegra

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'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 complimented with application server for E-mail, FTP, WWW and dual DNS. The integrated Mail server can be configured to provide a complete e-mail system or operate as a relay delivering mail to protected internal servers.

BorderWare Technologies Inc
1 The Harlequin Centre, Southall Lane,
Southall, Middlesex UB2 5NH, United Kingdom
Point of contact:
Telephone: +44 (0) 20 8893 6066
Facsimile: +44 (0) 20 8574 8384
Email: info@borderware.com
URL: http://www.borderware.com

BorderWare Firewall Server

v6.5

IN EVALUATION COMMON CRITERIA EAL4
PROJECTED CERTIFICATION DATE: 3Q 2001
CLEF: Syntegra

The BorderWare Firewall includes an integrated operating system and a completed set of services needed to operate a secure 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 complimented with application server for E-mail, FTP, WWW and dual DNS. The integrated Mail server can be configured to provide a complete e-mail system or operate as a relay delivering mail to protected internal servers. V6.5 of the Firewall server will be available both packaged on dedicated hardware and as a complete software package for easy installation on standard hardware.

BorderWare Technologies Inc
1 The Harlequin Centre, Southall Lane,
Southall, Middlesex UB2 5NH, United Kingdom
Point of contact:
Telephone: +44 (0) 20 8893 6066
Facsimile: +44 (0) 20 8574 8384
Email: info@borderware.com
URL: http://www.borderware.com

Check Point Firewall-1

v4.0 Stateful Inspection

ITSEC E3
Certificate Number: P107 March 1999
CLEF: CMG Admiral

This evaluation addresses the core elements of Firewall-1 i.e. the Stateful Inspection engine, auditing, address translation and the command-line user interface for Microsoft NT Version 4.0 SP 3, Solaris 2.6, AIX version 4.2.1 and HP-UX Version 10.10.

The Firewall-1 product suite delivers an integrated solution that scales to meet the demands of organizations large and small, securing your enterprise network – LAN, Internet, intranet and extranets.

Based on Stateful Inspection technology, a security technology invented and patented by Check Point Software Technologies, FireWall-1 provides security at the highest level currently available. Stateful Inspection incorporates communication, application state and context information, which is stored and updated dynamically.

Check Point Software Technologies Ltd
3A Jabotinsky St., Diamond Tower,
Ramat-Gan 52520, Israel
Point of contact: Nigel Mould
Telephone: +44 (0) 1223 713611
Facsimile: +44 (0) 1223 713621
Email: nigelm@checkpoint.com
URL: http://www.checkpoint.com

Check Point VPN-1/Firewall-1

v4.1 SP2

ITSEC E3
Certificate Number: P149 January 2001
CLEF: CMG Admiral

This evaluation addresses 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 is the most comprehensive security suite available today. Providing an integrated solution that scales to meet the demands of organizations large and small, securing your enterprise network – LAN, Internet, intranet and extranets.

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.

Check Point Software Technologies Ltd
3A Jabotinsky St., Diamond Tower,
Ramat-Gan 52520, Israel
Point of contact: Nigel Mould
Telephone: +44 (0) 1223 713611
Facsimile: +44 (0) 1223 713621
Email: nigelm@checkpoint.com
URL: http://www.checkpoint.com

Cisco Secure PIX Firewall Software

Version 5.2(3)

Hardware Models 515, 520 & 525

COMMON CRITERIA EAL4
Certificate Number: P152 January 2001
CLEF: Syntegra

The Cisco Secure PIX Firewall is a dedicated firewall appliance from Cisco Systems. The family of firewalls delivers strong security without impacting network performance. The product line scales to meet a range of customer requirements, and has only two license levels - one restricted licence and an unlimited licence.

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. The PIX 525 is able to support over 340Mbps of throughput and over 250,000 concurrent sessions.

Cisco Systems
3, The Square, Stockley Park,
UXBRIDGE, Middlesex UB11 1BN
Point of contact: Paul King
Telephone: +44 (0) 20 8756 8349
Facsimile: +44 (0) 20 8576 8099
Email: securitysolutions@cisco.com
URL: http://www.cisco.com/uk/securitysolutions

CyberGuard Firewall for Windows NT

Certificate Maintenance Scheme

The latest CMS Approved version of CyberGuard Firewall for Windows NT is 4.2 PSU1. All intermediate releases and updates are also CMS approved.
ITSEC E3
Certificate Number: P118 January 1999
CLEF: Logica

CyberGuard Firewall for Windows NT is closely linked to Microsoft Windows NT® to maximise performance, accuracy and security of the network. The evaluated firewall is a multi-homed configuration providing both IP packet filtering and application-level proxies. A Graphical User Interface (GUI) for configuration and reporting and up to 16 multiple network interfaces are available. To ease installation and management, the firewall interacts with and exploits existing NT domain controllers to obtain user and authentication information. The Windows NT environment is secured with SecureGuard™for NT, providing protection against security threats such as uncontrolled access to system resources. Available for systems with a minimum of 133MHz Intel Pentium Processor, 32MB Memory running Windows NT rev 4.0 with Service Pack 3 or 4.

CyberGuard Europe Ltd
Asmec Centre, Eagle House, The Ring,
Bracknell, Berkshire RG12 1HB
Point of contact: Andrew Clarke
Telephone: + 44 (0)1344 382550
Facsimile: + 44 (0)1344 382551
Email: aclarke@cyberguard.com
URL: http://www.cyberguard.co.uk

CyberGuard Firewall for UnixWare 4.1

(also available as CyberGuard Firewall Appliances) Certificate Maintenance Scheme

The latest CMS Approved version of CyberGuard Firewall for UnixWare 4.1 is 4.2 PSU1. All intermediate releases and updates are also CMS approved.
ITSEC E3
Certificate Number: P117 January 1999
CLEF: Logica

CyberGuard® Firewall for UnixWare® is provided with a MLS UNIX operating system. It safeguards information held on internal networks, by controlling the access of external users and protecting the integrity, availability, authentication data and anonymity of the internal network. Configuration and Reporting is performed with a local Graphical User Interface (GUI). Additional network interfaces (up to 32) provide DMZ or further internal/ external network connections. The firewall runs on either single or multi-processor Intel servers with UnixWare 2.1.3. CyberGuard Firewall for UnixWare is available from Release 4.2 onwards as a pre-staged appliance known as FireSTAR, KnightStar and STARLord Premium Appliance Firewalls.
These variants are therefore CMS Approved.

CyberGuard Europe Ltd
Asmec Centre, Eagle House, The Ring,
Bracknell, Berkshire RG12 1HB
Point of contact: Andrew Clarke
Telephone: + 44 (0)1344 382550
Facsimile: + 44 (0)1344 382551
Email: aclarke@cyberguard.com
URL: http://www.cyberguard.co.uk

CyberGuard Firewall v2

Certificate Maintenance Scheme CyberGuard Firewall 2.2.1e has CMS approved versions up to CyberGuard Firewall 2.2.3r9.

ITSEC E3
Certificate Number: 97/78 March 1997
CLEF: Logica

CyberGuard Firewall Version 2 is an appliance firewall that controls and monitors user access to local- and wide-area networks by leveraging the advantages of a multi-level secure architecture. CyberGuard Firewall runs on B1 secure operating system and networking products. CyberGuard is designed to reduce the area of risk to a single system; it operates as a packet-filtering gateway, a proxy gateway and a Bastion Host in a multi-system environment. For example, when located between an internal network, an Intranet and/or the internet, it provides valuable protection of a company's computing resources and data. CyberGuard Firewall has been evaluated on both the NH4000 and NH5000 platforms, in either tower or rack-mounted packaging.

CyberGuard Europe Ltd
Asmec Centre, Eagle House, The Ring,
Bracknell, Berkshire RG12 1HB
Point of contact: Andrew Clarke
Telephone: + 44 (0)1344 382550
Facsimile: + 44 (0)1344 382551
Email: aclarke@cyberguard.com
URL: http://www.cyberguard.co.uk

CyberGuard Firewall for UnixWare/Premium Appliance Firewall 4.3

COMMON CRITERIA EAL4
Certificate Number: P150 December 2000
CLEF: Logica

CyberGuard Firewall is a packet filter, (stateful inspection) and application level proxy firewall provided with a MLS (secure) Unix operating system. It safeguards internal networks by controlling external access and protects the integrity, availability, authentication data and anonymity of the internal network. Configuration/reporting is performed via local GUI. Additional interfaces (up to 32) provide DMZ or further internal/external connections. Evaluated security features include: Connection level Access Control for IP packets; Accounting, auditing and statistics; Alerts for security events; Network Address Translation and Split Domain Name Server (DNS). The firewall runs on single or multi-processor Intel IA-32 processors and as a packaged solution – the CyberGuard Premium Appliance family: FireSTAR, KnightSTAR and STARLord.

CyberGuard Europe Ltd
Asmec Centre, Eagle House, The Ring,
Bracknell, Berkshire RG12 1HB
Point of contact: Andrew Clarke
Telephone: + 44 (0)1344 382550
Facsimile: + 44 (0)1344 382551
Email: aclarke@cyberguard.com
URL: http://www.cyberguard.co.uk

Gauntlet Internet Firewall for Windows NT

v3.01

ITSEC E3
Certificate Number: P127 June 1999
CLEF: EDS

The Gauntlet Internet Firewall for Windows NT is a native development for Windows NT 4.0.
The Gauntlet Internet Firewall for Windows NT combines an application gateway with user transparency and ease of management. Security functions evaluated include:

- Prevention of internal IP addess spoofing;
- System integrity checking;
- Comprehensive auditing and accounting functions;
- Alarms raised to the Administrator on defined events;
- Packet level filtering;
- SMTP, telnet, rlogin, HTTP, ftp, SQL*net, pop3 and PLUG proxies;
- Strong user Authentication with the ability to insert user definable mechanisms;
- Configurable option to prevent JAVA applets, JAVA scripts and ActiveX;
- URL filtration mechanisms;
- Content Vectoring Protocol support.

Network Associates – UK
227 Bath Road, Slough, Berkshire SL1 5PP
Point of contact: Evan Garricks
Telephone: +44 (0) 1753 217 500
Facsimile: +44 (0) 1753 217 520
Email: evan_garricks@nai.com
URL: http://www.nai.com

MailGuard Bastion 1.0

ITSEC E3
Certificate Number: P144 May 2000
CLEF: Admiral

MailGuard Bastion is a high assurance messaging firewall that allows the exchange of X.400 and SMTP/MIME messages between networks of differing security levels or conflicting security policies.

MailGuard Bastion is evaluated and assured to ITSEC E3, making it ideally suited to meet the most stringent security policies. The product builds upon the Trusted Solaris operating system, which itself is ITSEC E3/F-B1 and E3/F-C2 approved. MailGuard Bastion can be supplied as a software package or as a turnkey system (comprising hardware and software) configured and working to requirements.

NET-TEL Computer Systems Ltd
4 Place Farm, Wheathampstead
Herts AL4 8SB, United Kingdom
Point of contact: Nick Ward
Telephone: +44 1582 830500
Facsimile: +44 1582 830501
Email: Nick.Ward@net-tel.co.uk
URL: http://mailguard.co.uk

Safegate v2.0.2

COMMON CRITERIA EAL3
Certificate Number: P139 January 2000
CLEF: Logica

Safegate (Version 2.0.2) firewall has the following functions:

- IP packet filtering;
- application gateway (non-transparent and transparent);
- security management (containing the audit functions);

IP packet filtering 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.

Fujitsu Ltd
1405, Ohmaru, Inagi-shi,
Tokyo 206-8503, Japan
Point of contact: Takehiko Yahagi
Telephone: +81 44 370 7637
Facsimile: +81 44 370 7737
Email: t-yahagi@jp.fujitsu.com
URL: http://www.fujitsu.co.jp/en/

SWIPSY Firewall Toolkit

ITSEC E3
Certificate Number: P147 August 2000
CLEF: EDS

The SWIPSY (Switch IP SecurelY) firewall toolkit provides an extensible framework for constructing assured Bastion 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, although formal evaluation of the software may be necessary if certain TSol privileges are needed.

Central Enquiry Desk
Defence Evaluation and Research Agency,
Ively Road, Farnborough, Hampshire GU14 0LX,
United Kingdom
Point of contact: Sharon Lewis
Telephone: +44 1684 896535
Facsimile: +44 1684 896660
Email: S.Lewis@eris.dera.gov.uk
URL: http://www.dera.gov.uk/html/it/secure-e-business/network_boundary_service.htm

Symantec Enterprise Firewall v6.5

IN EVALUATION COMMON CRITERIA EAL4
Projected Certification Date: July 2001
CLEF: Syntegra

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 of companies connecting to the Internet. Some of the features unique to the Symantec Enterprise Firewall include:

(1) initial & continuous system hardening,
(2) DDoS attack protection,
(3) support for authenticating sessions,
(4) consolidated, non-order-dependent rule setting, and
(5) generic and port-range service proxies supporting legacy, proprietary or emerging protocols.

SYMANTEC Corporation
266 Second Avenue, Waltham,
Massachusetts 02451
Point of contact: Regina Hammond
Telephone: +1 781-530-2305
Facsimile: +1 781-487-6755
Email: rhammond@symantec.com
URL: http://www.symantec.com

VCS Firewall v3.0

COMMON CRITERIA EAL1
Certificate Number: P123 March 1999
CLEF: IBM Global Services

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. The VCS Firewall is proxy-based. Proxies for HTTP, Telnet, 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 Knowledge Group
Knowledge House, Concorde Road,
Patchway, Bristol BS34 5TB, United Kingdom

Point of contact: Alan Jones
Telephone: +44 (0) 117 900 7500
Facsimile: +44 (0) 117 900 7501
Email:
URL: http://www.ktgroup.co.uk

Baltimore ED2048R3

Government Use Only

ITSEC E3 and CAPS approved
Certificate Number: 96/60 April 1996
CLEF: IBM Global Services

The ED2048R3 provides cryptographic protection for up to 2.048 Mbps point-to-point links. The ED2048R3 has 2 interface options:

- X21
- G.703/G.732/G704

The X.21 interface is suited to protecting flexible bandwidth services as line speeds can be increased without reconfiguration. The G704 interfaces support an nx64 Kbps fractional service.

The ED2048R3 offers a two-tier key hierarchy. Four data encryption keys (DEKs) can be entered into the master encryptor from a swipe card and downloaded over the link to slave units. Alternatively, the ED2048R3 can be managed from the Baltimore Network Security Workstation, to provide automated key and equipment management.

Baltimore Technologies Ltd
39/41 Parkgate Street, Dublin 8, Ireland
Point of contact:
Telephone: +61 2 9409 0300
Facsimile: +61 2 9409 0301
Email: info@baltimore.com
URL: http://www.baltimore.com/

Baltimore ED600RTS

ITSEC E3 and CAPS approved
Certificate Number: 95/55 September 1995
CLEF: Syntegra

The ED600RTS is a RAMBUTAN Encryptor for synchronous data transmitted on a point-to-point link, at speeds of up to 128 Kbps using an X.21 interface. The ED2048R3 offers a two-tier key hierarchy. Four data encryption keys (DEKs) can be entered into the master encryptor from a swipe card and downloaded over the link to slave units. Alternatively, the ED2048R3 can be managed from the Baltimore Network Security Workstation, to provide automated key and equipment management

Baltimore Technologies Ltd
39/41 Parkgate Street, Dublin 8, Ireland
Point of contact:
Telephone: +61 2 9409 0300
Facsimile: +61 2 9409 0301
Email: info@baltimore.com
URL: http://www.baltimore.com/

Baltimore ED8000RL

Government Use Only

ITSEC E3 and CAPS approved
Certificate Number: 97/92 December 1997
CLEF: IBM Global Services

The ED8000RL is an Ethernet encryptor using the RAMBUTAN algorithm. It provides cryptographic protection for user data transmitted between LANs using Internet Protocol across WANs. The encryptor is interposed between a local Ethernet LAN subnet and the router giving access to the WAN.

- Central management
- Supports Ethernet V2.0 and IEEE 802.3 frame format incorporating SNAP
- Holds up to 16 data keys to enable creation of separate cryptographic zones
- Supports up to 512 destination IP subnet or device addresses
- Data rate exceeds 2Mbits per second
- SNMP TRAPs can be sent to a separate NMC

Baltimore Technologies Ltd
39/41 Parkgate Street, Dublin 8, Ireland
Point of contact:
Telephone: +61 2 9409 0300
Facsimile: +61 2 9409 0301
Email: info@baltimore.com
URL: http://www.baltimore.com/

Cisco 3640 Router

IN EVALUATION ITSEC E2
PROJECTED CERTIFICATION DATE: MAY 2001
CLEF: CMG Admiral

The Cisco 3640 is a multifunction platform that combines dial access, routing, LAN-to-LAN services and multiservice integration of voice and data in the same device. As a modular solution, the Cisco 3640 has the flexibility to meet both current and future connectivity requirements. The Cisco 3640 is fully supported by Cisco IOSTM software, which includes LAN-to-LAN routing, data and access security and WAN optimization. Applications supported are asynchronous and synchronous serial interfaces.

SUPPLIER:
Cisco Systems Limited
3 The Square, Stockley Park, Uxbridge, Middlesex
UB11 1BN, United Kingdom
Point of contact: Jon Arnold (For Cisco)
Telephone: +44 (0) 208 756 8651
URL: http://j0arnold@cisco.com

SYSTEM DESIGNER:
INCA
Post Point C2, North Star House,
North Star Avenue, Swindon, Wiltshire SN2 1BS
Point of contact: David Grant
Telephone: +44 (0) 1793 863173
Facsimile: +44 (0) 1793 863010
Email: david.w.grant@marconi.com

DataCryptor 2000 (Synchronous Line Encryptor)

ITSEC E3
Certificate Number: P126 August 1999
CLEF: CMG Admiral

The Datacryptor 2000 Link product range are encryption devices specifically designed to provide secure communications over circuits at speeds of up to 2Mbps 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 2000 series employ the Zaxus Key Management Scheme to securely generate 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.

Zaxus Technical Sales
Sussex Innovation Centre, Science Park Square,
University of Sussex, Brighton BN1 9SB,
United Kingdom
Point of contact: Chris Woods, Product Manager
(Network Security)
Telephone: +44 (0)1273 384600
Facsimile: +44 (0)1273 384601
Email: chris.woods@zaxus.com
URL: http://zaxus.com

Meridian Option 1 (22.46) SPC Switch

IN EVALUATION ITSEC E2
Projected Certification Date: 2Q 2001
CLEF: CMG Admiral

The Meridian Option 61C (22.46) is a state-of-the-art Software Stored Program Control Digital Switch. Utilised as a platform for integrated voice and data, Meridian Option 61C (22.46) 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 is being evaluated specifically for the MOD's Defence Fixed Telecommunications Service.

SUPPLIER:
Nortel Networks
Maidenhead Office Park, Westacott Way,
Maidenhead, Berkshire SL1 3OH,
United Kingdom
Point of contact: Nortel
Telephone: +44 (0) 1628 432566
Facsimile: +44 (0) 1628 432657
URL: http://nortelnetwork.com

SYSTEM DESIGNER:
INCA
Post Point C2, North Star House,
North Star Avenue, Swindon, Wiltshire SN2 1BS
Point of contact: David Grant
Telephone: +44 (0) 1793 863173
Facsimile: +44 (0) 1793 863010
Email: david.w.grant@marconi.com

Network Security Workstation Automated Security Management

ITSEC E3 and CAPS approved
Certificate Number: 97/75
CLEF: Syntegra

Baltimore's RAMBUTAN Network Security Workstation (NSW) offers users automated security management for the ED2048R3 and ED600RTS link encryptors or the ED8000RL LAN IP encryptor. The NSW comprises a PC and a cryptographic processor, the CG600R. Key distribution is authenticated and encrypted between the NSW and target encryptors.
A physical key has to be loaded into encryptors six monthly. All other keys are supplied to the NSW by CESG. Status, alarm and audit information can be collected automatically or under operator control. The NSW is protected by password protection mechanisms. Plain text key material is not accessible by an NSW operator.

Baltimore Technologies Ltd
39/41 Parkgate Street, Dublin 8, Ireland
Point of contact:
Telephone: +61 2 9409 0300
Facsimile: +61 2 9409 0301
Email: info@baltimore.com
URL: http://www.baltimore.com

Nortel Switch Nortel DPN - 100/20 vG36.03

ITSEC E1
Certificate Number: P142 March 2000
CLEF: Logica

The Nortel DPN -100/20 switch running software Version G36.03 was developed by Nortel and is a switch within DFTS 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. The switch is a component of the DFTS PSS, which has also been evaluated. The Nortel DPN - 100/20 switch was evaluated against ITSEC E1 assurance requirements.

SUPPLIER:
Nortel Networks
Maidenhead Office Park, Westacott Way,
Maidenhead, Berkshire SL1 3OH,
United Kingdom
Point of contact: Nortel
Telephone: +44 (0) 1628 432566
Facsimile: +44 (0) 1628 432657
URL: http://nortelnetwork.com

SYSTEM DESIGNER:
INCA
Post Point C2, North Star House,
North Star Avenue, Swindon, Wiltshire SN2 1BS
Point of contact: David Grant
Telephone: +44 (0) 1793 863173
Facsimile: +44 (0) 1793 863010
Email: david.w.grant@marconi.com

Nortel Passport Switch 6480

ITSEC E1
Certificate Number: P143 March 2000
CLEF: Logica

The Nortel Passport Switch 6480 running software Version 5.0.16 was developed by Nortel Networks and is a switch within DFTS designed to form part of a packet switched data communications service. Its purpose is to support high capacity services on the network. It provides access protocol support for Frame Relay, Asynchronous Transfer Mode and LAN interconnect. The switch is a component of the DFTS PSS, which has been evaluated. The Nortel Passport Switch 6480 was evaluated against ITSEC E1 assurance requirements.

SUPPLIER:
Nortel Networks
Maidenhead Office Park, Westacott Way,
Maidenhead, Berkshire SL1 3OH,
United Kingdom
Point of contact: Nortel
Telephone: +44 (0) 1628 432566
Facsimile: +44 (0) 1628 432657
URL: http://nortelnetwork.com

SYSTEM DESIGNER:
INCA
Post Point C2, North Star House,
North Star Avenue, Swindon, Wiltshire SN2 1BS
Point of contact: David Grant
Telephone: +44 (0) 1793 863173
Facsimile: +44 (0) 1793 863010
Email: david.w.grant@marconi.com

OMEGA v7.12 Increment 19
Government Use Only

ITSEC E3
Certificate Number: P134 January 2000
CLEF: CMG Admiral

OMEGA is a multi-level secure message-handling product 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, archiving and traceability
- Acceptance and generation of almost all message formats including ACP127 and X.400 (1984 and 1988);
- Gateways to a number of recognised defence systems, ranging from RS232 and ITA5 to X.25;
- Facilities for communications with ships via a range of LF, HF and satellite bearers;
- Access for PC's and a CMW platform connected via LAN and WAN.

ICL
Jays Close, Basingstoke, Hampshire RG22 4BY
Point of contact: John Reynolds
Telephone: +44 (0) 1256 428235
Facsimile: +44 (0) 1256 428389
Email: john.reynolds@icl.com
URL: http://www.icl.com

Realitis (6.1) DX SPC Switch

IN EVALUATION ITSEC E2
CLEF: CMG Admiral

The Realitis (6.1) DX Communication Switch is a state-of-the-art Software Stored Program Control Digital Switch. Utilised as a platform for integrated voice and data, Realitis (6.1) DX Communications Switch supports industries standard interfaces and open communication 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 is being evaluated specifically for the MOD's Defence Fixed Telecommunications Service.

SUPPLIER:
SIEMENS
Brickhill Street, Willen Lake, Milton Keynes,
Buckinghamshire MK15 0DS, United Kingdom
SYSTEM DESIGNER:
INCA
Post Point C2, North Star House,
North Star Avenue, Swindon, Wiltshire SN2 1BS
Point of contact: David Grant (For INCA)
Telephone: +44 (0) 1793 863173
Facsimile: +44 (0) 1793 863010
Email: david.w.grant@marconi.com
URL:

SafeDial v1.27

ITSEC E3 and CAPS approved*
Certificate Number: 98/90 January 1998
CLEF: CMG Admiral

SafeDial is a V.34 compatible modem specifically designed to provide secure communications for personal computers. SafeDial is a credit card size (type 2 PCMCIA) communication and cryptographic processor combination particularly suited to laptop use. It prevents unauthorised information access and provides privacy for data transmissions using public telephone networks. The unit is tamper resistant, easily transportable and once commissioned only requires a password for normal operation. This product inserts into a standard PCMCIA socket, and is provided with a linking cable suitable for attachment to a standard UK telephone socket. The device employs the Zaxus Key Management Scheme to securely distribute data encryption keys.

*SafeDial v1.37 approved for baseline and enhanced grade

Zaxus Technical Sales
Sussex Innovation Centre, Science Park Square,
University of Sussex, Brighton BN1 9SB,
United Kingdom
Point of contact: Chris Woods, Business Manager
(Network Security)
Telephone: +44 (0)1273 384600
Facsimile: +44 (0)1273 384601
Email: chris.woods@zaxus.com
URL: http://zaxus.com

Trusted Oracle7, Release 7.0.13.6

ITSEC E3
Certificate Number: 94/33 September 1994
CLEF: Logica

Trusted Oracle7 is a Multi-Level Secure Relational Database Management System Server. Trusted Oracle7, Release 7.0.13.6, in conjunction with an operating system of functionality ITSEC F-B1 or greater, can be used to provide database security for systems which require F-B1 security functionality for databases. In addition to the security functions listed for Oracle7, Release 7.0.13.6, Trusted Oracle7 also supports Mandatory Access Control and Labelling for the multi-level secure environment.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire, RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Informix OnLine Dynamic Server v7.23

ITSEC E2
Certificate Number: 98/95 February 1999
CLEF: CMG Admiral

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 OnLine Dynamic Server 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.

Informix Software Ltd
6 New Square, Bedfont Lakes, Feltham,
Middlesex TW14 8HA. United Kingdom
Point of contact: Andy Legge
Systems Engineer -
High Performance Solutions
Telephone: Direct +44 (0) 20 8818 1017
Mobile+44 (0) 7801 684 017
Switchboard +44 (0) 20 8818 1000
Facsimile: +44 (0) 20 8818 1118
Email: andy.legge@informix.com
URL: http://www.informix.com/
UK www: http://www.informix.co.uk/

CA Open INGRES/Enhanced Security 1.2/01

ITSEC E3
Certificate Number: P146 July 2000
CLEF IBM Global Services

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
Computer Associates House,
183/187 Bath Road, Slough, Berks SL1 4AA
Point of contact: Adrian Oldfield
European Director
Strategic Alliances
Telephone: +44(0)1753 242819
Facsimile: +44 (0)1753 825464
Email: adrian.oldfield@ca.com
URL: http://www.ca.com

Oracle7, Release 7.0.13.6

ITSEC E3
Certificate Number: 94/33 September 1994
CLEF: Logica

Oracle7 is a Relational Database Management System Server. Oracle7, Release 7.0.13.6, in conjunction with an operating system of functionality ITSEC F-C2 or greater, can be used to provide database security for systems which require F-C2 security functionality for databases. Under these conditions, the main security functions are Discretionary Access Control, Identification and Authentication, Object Reuse, Secure Data Exchange, and Audit and Accountability.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Trusted Oracle7, Release 7.1.5.9.3

ITSEC E3
Certificate Number: 98/96 March 1998
CLEF: EDS

Trusted Oracle7 is a Multi-Level Secure Relational Database Management System. Trusted Oracle7, Release 7.1.5.9.3, when used in conjunction with an operating system of ITSEC F-B1 or greater, provides database security for systems that require F-B1 functionality. In addition to the security functions listed for Trusted Oracle7, Release 7.0.13.6, Trusted Oracle7, Release 7.1.5.9.3, also supports multi-level secure stand-alone and client/server distributed database environments.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle7, Release 7.2.2.4.13

COMMON CRITERIA EAL4
Certificate Number: P103 September 1998
CLEF: Logica

Oracle7 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 UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle7, Release 7.2.2.4.13

ITSEC E3
Certificate Number: Certified 98/94 February 1998
CLEF: Logica

Oracle7 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. The main security functions include granular privileges for enforcement of least privilege, user-configurable roles for privilege management, flexible auditing, views, stored procedures and triggers for enhanced access control and alert processing, row-level locking, robust replication and recovery mechanisms, secure distributed database communication and the ability to use external authentication mechanisms.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Trusted Oracle7, Release 7.2.3.0.4

ITSEC E3
Certificate Number: P124 July 1999
CLEF: Logica

Trusted Oracle7 is a Multi-Level Secure Relational Database Management System. Trusted Oracle7, Release 7.2.3.0.4, when used in conjunction with an operating system of ITSEC F-B1 or greater, provides database security for systems that require F-B1 functionality. In addition to the security functions listed for Trusted Oracle7, Release 7.1.5.9.3, Trusted Oracle7, Release 7.2.3.0.4, also supports trusted stored procedures, flexible label management, label policy enforcement and multiple security architectures

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle7, Release 7.3.4.0.0

ITSEC E3
Certificate Number: P109 December 1998
CLEF: Logica

Oracle7 is a Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environments. Oracle7, Release 7.3.4.0.0, when used in conjunction with an operating system of ITSEC F-C2 or greater, provides database security for systems that require F-C2 functionality.
The main security functions are identical to those given in the Oracle7, Release 7.2.2.4.13, ITSEC E3 evaluation entry.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle8, Release 8.0.5.0.0

COMMON CRITERIA EAL4
Certificate Number: P106 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 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 databases, single sign-on, password management, data dictionary protection, global roles and X.509 certificate based authentication.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle8i, Release 8.1.7

IN EVALUATION COMMON CRITERIA EAL4
CLEF: Logica

Oracle8i is an Object/Relational Database Management System, providing advanced security and functionality for multi-user, distributed database environments. Oracle8i, Release 8.1.7, is in evaluation against the Database Management System protection profile. In addition to the security functions listed for Oracle8, 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 UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

AUDITOR Plus
v1.4-03 Revision S

ITSEC E1
Certificate Number: 96/70 October 1996
CLEF: CMG Admiral

AUDITOR Plus is an integrated set of software tools for security auditing and management of Compaq's OpenVMS operating system. OpenVMS 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 Technologies
Ashby House, 3 Derbyshire Road South,
Sale, Manchester M33 3JN, United Kingdom

Point of contact: John Ream
Telephone: +44 (0) 870 121 0990
Facsimile: +44 (0) 870 121 0995
Email: sales@ibsltech.com
URL: http://www.ibsltech.com

Hitachi Multiple Logical Processor Facility

v3.3.0

ITSEC E3
Certificate Number: P116 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
750 Central Expressway, MS 32/36,
PO Box 54996, Santa Clara, CA 95056-0996,
USA

Point of contact: Nelson King
Telephone: +1 408 970 1023
Facsimile: +1 408 988 8601
Email:
URL:

Trusted EDI on Trusted Solaris 1.2

Government Use Only

ITSEC E3
Certificate Number: 97/85 July 1997
CLEF: EDS Ltd

Trusted EDI passes AECMA S2000M format EDI messages (EDIMs) between trading partners using X.435/X.400 messages over Public Switch Stream (X.25) connections. The security features that Trusted EDI provides are as follows:

- Integrity checking of received X.435 messages
- Non-repudiation of origin of X.435 messages
- Origin Authentication of X.435 messages
- Validation of format of EDIMs against AECMA S2000M.

The X.435 security features are implemented through the use of encryption techniques which, in the evaluated configuration, use the Secure Hashing Standard (SHS) algorithm and the RSA algorithm.

This product was developed specifically for the MoD's Logistic Support System.

EDS Systems Assurance Group
1-3 Bartley Wood Business Park, Hook,
Hampshire, United Kingdom

Point of contact: Geoff Lambert
Telephone: +44 (0) 1256 742000
Facsimile: +44 (0) 1256 742700
Email: geoff.lambert@edl.uk.eds.com
URL: http://www.eds.com

PROTECTION PROFILES

A Protection Profile is a set of requirements designed for a set of circumstances. It consists of:

- A list of threats
- A list of functional requirements
- A list of assurance activities
- A justification that these address the threat

Protection Profiles 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. Certification against a PP will specify the extent to which requirements of the Profile have been met.

A PP is particularly useful in assisting the formulation of procurement specification.

PP's certified by the UK Scheme are shown here. Additional PPs can be found at the CC website:

www.commoncriteria.org

Biometric Device Protection Profile (Draft)

IN EVALUATION COMMON CRITERIA EAL4

This is a draft Protection Profile intended for the Common Criteria evaluation and certification of biometric devices at evaluation assurance levels EAL1-EAL4. This draft has been produced by CESG with the collaboration and support of the German and US CC authorities. It will be used on a trial basis until validated and approved for normal use.

Common Criteria Biometric product evaluation will include independent performance testing using CESG developed ‘Best Practices for Biometric Testing’ standards.

CESG
PO Box 152, Cheltenham,
Gloucestershire GL52 5UF, United Kingdom
Point of contact: Phillip Statham
Telephone: +44 (0) 1242 221491
Facsimile: +44 (0) 1242 235233
Email: info@itsec.gov.uk
URL: www.itsec.gov.uk

Controlled Access Protection Profile
v1.d

COMMON CRITERIA EAL3
Certificate Number: PP006 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 Defense’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
POC: Howard Holm
Telephone: +1 410 854 4458
Facsimile:
URL: http://www.radium.ncsc.mil/tpep

Labeled Security Protection Profile
v1.b

COMMON CRITERIA EAL3
Certificate Number: PP007 October 1999
CLEF: Logica

Labeled Security Protection Profile is designed for use as a Protection Profile under Common Criteria. It is suitable for systems requiring a security policy based on a combination of user-controlled access to objects and 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 Defense's Trusted Computer System Evaluation Criteria (TCSEC).

Products evaluated against the LSPP 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 Labelled Security Protection Profile, which has been withdrawn.

National Security Agency
POC: Howard Holm
Telephone: +1 410 854 4458
Facsimile:
URL: http://www.radium.ncsc.mil/tpep

Privilege Directed Content Protection Profile

COMMON CRITERIA EAL4
Certificate Number: PP009 January 2001
CLEF: IBM Global Services

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 authorisations granted to that visitor, and to protect such a website from subversion.

Authoriszor Ltd
Windsor House, Cornwall Rd,
Harrogate HG1 2PN, United Kingdom
Point of contact: Richard Atkinson
Telephone: +44 (0) 1423 730300
Facsimile: +44 (0) 1423 730315
Email: richard.atkinson@authoriszor.com
URL: http://www.authoriszor.com

Role-Based Access Control Protection Profile

v1.0

COMMON CRITERIA EAL2
Certificate Number: PP001 September 1998
CLEF: Logica

Role-based access control allows the system administrator to define roles based on job functions within an organization. As the user's job responsibilities change,user membership in roles can be granted and revoked easily. As the organization inevitably changes, roles can be modified easily through role hierarchies. As the job changes, privileges are changed for the individual roles not for individual users.

The RBAC 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
Point of contact: Ramaswamy Chandramouli
Telephone: +1 301 975 5013
Facsimile: +1 301 948 0279
Email: mouli@nist.gov
URL: http://csrc.nist.gov/cc

Oracle Database Management System Protection Profile

COMMON CRITERIA EAL3
Certificate Number: PP008 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" basis), integrity and availability of information stored in the database. The Oracle Database Management System protection profile which is an ISO-15408 certified protection profile, was evaluated against the Common Criteria at EAL3.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle Commercial Database Management System Protection Profile

COMMON CRITERIA EAL3
Certificate Number: PP002 September 1999
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" basis), integrity and availability of information stored in the database. The Oracle Commercial Database Management System protection profile was evaluated against the Common Criteria at EAL3.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

Oracle Government Database Management System Protection Profile

COMMON CRITERIA EAL3
Certificate Number: PP003 October 1998
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" basis), integrity and availability of information stored in the database. The Oracle Government Database Management System protection profile was evaluated against the Common Criteria at EAL3.

Oracle Corporation UK Limited
560 Oracle Parkway, Thames Valley Park,
Reading, Berkshire RG6 1RA
Point of contact: Shaun Lee
Security Evaluations Manager
Telephone: 0118-924-3860
Facsimile: 0118-924-7400
Email: seceval_us@oracle.com
URL: http://otn.oracle.com/deploy/security/seceval/listing.htm

CAPS

The CAPS scheme has been established to provide design consultancy for developers and vendors of products utilising cryptographic security measures. The scheme also provides cryptographic verification of these products to government standards and formally approves their use by HMG and other public sector organisations.

What do we mean by Cryptographic products?

Cryptographic products use encryption to provide security. HMG policy determines the standards required for the use of approved encryption which is employed to protect sensitive government data.

HMG Cryptographic Standards

Cryptographic products are graded in terms of three different Cryptographic Protection Levels:

Baseline:

These products can use CESG designed or more normally public domain cryptographic algorithms. Within the UK, Baseline products are suitable for the protection of data up to the RESTRICTED protective marking. This is also the 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 for 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 require CESG designed cryptographic algorithms. Enhanced grade products can protect data up to and including the CONFIDENTIAL protective marking. In some circumstances Enhanced grade approved products can be used to protect data up to the SECRET protective marking.

High Grade:

This level of cryptographic protection is for data protectively marked SECRET and above. Currently this is beyond the scope of CAPS approval processes.

The CAPS scheme has been very successful in ensuring that a wide range of approved cryptographic products is available for use by HMG and public sector customers as can be seen by the list of products featured in this section of the directory.

The latest 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.

The listing is categorised as follows to aid identification of products appropriate to your requirement:

- Data Encryption
- Communications Security
- Access Control
- Miscellaneous

Contact details for advice on products and for sales enquiries are given in the product listing. In addition, for MOD customers, many of the CAPS approved products featured in this directory are available through the MOD DCSA catalogue, the current agent of supply being The Software Box, who can be contacted as follows:

The Software Box
East Moor House
Green Park Business Centre
Sutton on the Forest
YORK
YO6 1ET

Tel: 01347 812100
Fax: 01347 811220

The sale of any 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 requirement.

CESG Assisted Products Scheme
PO Box 144
Cheltenham
Gloucestershire
GL52 5UE
Tel: +44 (0)1242 221491 Ext.4130
Fax: +44 (0)1242 236742
www.cesg.gov.uk
email: pda@cesg.gsi.gov.uk

PGP for HMG

Assurance Level: CAPS approved baseline

PGP for HMG provides complete e-mail, file and network security in a single, tightly integrated pack encryption. PGP for HMG consists of file and e-mail-based encryption, the ability to import keys and to send keys to an LDAP server.

PGP protects messages against unauthorized reading - digital signatures guarantee authenticity and data integrity. PGP e-mail plug-ins support the majority of e-mail applications.

Quick, seamless integration of PGP's tools encourages data security. The intuitive interface assures corporate policies are carried out daily. E-mails and files can be secured and authenticated.

On removing or replacing sensitive information, users are a click away from secure file deletion.

Network Associates International Ltd.
227 Bath Road, Slough, Berkshire SL1 5PP
Telephone: 01753 217588
Facsimile: 01753 217520
E-mail: mark_tucker@nai.com
URL: www.nai.com/international

REFLEX DATA VAULT (HMG)

for NT v1.0, 1.0B, HMG-3DES v1.0

Assurance Level: CAPS approved baseline

Reflex Data Vault (HMG versions) allow users to store up to 4 Gigabytes of data securely in a dedicated "logical" drive on their hard disk. Data is automatically encrypted. The encrypted drive is secured by FIREGUARD and RED PIKE. A triple DES version is also available. This system is fully compatible with Windows NT's NTFS filing system and security features. If a user forgets his password, Data Vault can "inject" a new key, which will totally disregard old key/passwords. The main encryption key can also be changed. Running on Windows NT version 4.0, Reflex Data Vault requires less than 1Mb of hard disk space.

Reflex Magnetics Ltd
31-33 Priory Park Road, London NW6 7HP
Telephone: 020 7372 6666
Facsimile: 020 7372 2507
E-mail: sales@reflex-magnetics.com
URL: www.reflex-magnetics.com

SECRETS for HMG

Assurance Level: CAPS approved baseline

“Drag and drop” file encryptor for encryption of files prior to transmission over an untrusted network.

Entegrity Solutions Limited
Avis House, Park Road, Bracknell
Berkshire, RG12 2BW
Telephone: 01344 782950
Facsimile:
E-mail:
URL:

SERCO DATASENTRY NT

Assurance Level: CAPS evaluation in progress

A highly secure data protection scheme for PCs running Windows-NT4 offering total disk protection and wave encryption. Access to any DataSentry protected PC is by the use of a personalised touch token (iButton) together with the entry of a PIN number and user name.

Serco Ltd
Pavilion 2, Olympus Park Business Centre,
Quedgeley, Gloucester GL2 4NF
Telephone: 01452 726300
Facsimile: 01452 726393
E-mail: aewilliams@serco.com
URL:

TOPSOFT CYBERLOCK DATA

Assurance Level: CAPS approved baseline

Topsoft's file encryption product TS CyberLock Data provides transparent token-based file encryption. The product utilises a kernel-mode file system filter driver for NTFS and FAT file systems running on Windows NT and Windows 2000. On-the-fly file encryption is provided to support flexible security policies allowing encryption of:

- selected files
- specific directories
- file patterns (wild cards) or
- mapped network drives.

When sensitive data is shared over a network, TS Data ensures data is transmitted in encrypted form and decrypted locally on the client machine. Key material is stored securely on a physical token, typically an ISO 7186-4 smartcard. TS Data is integrated with TS Access, a CAPS-approved password authentication product, allowing a single token to be used for access control and file encryption.

Product design has prioritised usability and ease of installation. Encryption is performed using triple DES, though product modularity allows algorithm options to be considered by application.

Topsoft Ltd
Woodgate House, Games Road,
Cockfosters, Herts EN4 9HN
Telephone: 020 8275 0808
Facsimile: 020 8275 0044
E-mail: sales@topsoft-security.com
URL: www.topsoft-security.com

DATACRYPTOR 2000 SERIES

Assurance Level: CAPS approved

The Datacryptor 2000 series from Zaxus Ltd (formerly Racal) are built on a high performance cryptographic platform which uses hi density FPGA (programmable Gate Array) technology to deliver high performance encryption solutions for UK Government and Defence type networks. The Datacryptor 2000 UKG series use both publicly available and CESG encryption algorithms and key management schemes to deliver the appropriate security solutions. The equipment is supplied with designated software, network interface cables, and a CD containing supporting applications, utilities and manuals.

The Datacryptor 2000 series is used to protect the confidentiality of traffic as described in the Manual of Protective Security. In particular:

- the Baseline Grade version of the product (using Triple DES) may be used to protect the confidentiality of traffic protectively marked up to and including RESTRICTED in the UK and overseas, and
- the Enhanced Grade version of the product (using EMBATTLE) may be used to protect the confidentiality of traffic protectively marked up to and including Short Term Sensitivity SECRET (i.e. traffic with intelligence life of less than one year) in the UK and overseas. A further version (using BATON) may be used to protect Long Term SECRET.

The Datacryptor 2000 series is suitable for reverse tunnelling and is available with a number of communications configurations.

Thales E-Security Ltd
Meadow View House, Crendon Industrial Estate,
Long Crendon, Bucks HP18 9EQ
Telephone: 01844 201800
Facsimile: 01844 208850
E-mail:
URL: www.zaxus.com

DIAL THRU CRYPTO (DTC)

Assurance Level: CAPS approved baseline

A low cost solution for a transparent encryption device designed to work over ISDN. It provides encryption for the two B channels enabling two simultaneous 64Kb/s (standard rate) encrypted data streams for voice, data, fax and video.
The modular and flexible design enables DTC to be adapted for future support of other protocols such as (A)DSL or to use other encryption algorithms such as AES.

Marconi Secure Systems Ltd
2 Wavertree Boulevard,
Wavertree Industrial Park, Liverpool L7 9PE
Telephone: 0151 282 5294
Facsimile: 0151 254 1194
E-mail: sales@marconi_securesystems.com
URL: www.marconi_securesystems.com

MULTITONE Z-PAGE

Assurance Level: CAPS approved baseline

A PC-based paging system using CESG-approved algorithms specially designed for Government, Military and NHS use.

Z-Page is used with a special version of Multitone's Fourline Alphanumeric pager. The PC software is simply installed and the system enabled by connecting to the network via a serial post.

The user of the Z-Page has 64-bit Encryption/decryption keys known only to that pager and the PC Software.

Compatible with Wide Area, Z-Page can receive both secure and conventional messaging.

Full security features include:
Automatic Key Changes, Password (PNI) Entry, Full Password Entry, Automatic Erase Secure Data after incorrect password entries.

Multitone Electronics plc
Multitone House, Beggarwood Lane,
Kempshott Hill, Basingstoke,
Hants, RG23 7LL
Telephone: 01256 320292
Facsimile: 01256 462643
URL: www.multitone.com

SECURITY ENHANCEMENTS

FOR MICROSOFT EXCHANGE – EXCHANGE(SE)

Assurance Level: CAPS evaluation in progress

Versions: v1.0 to v3.1 working with Microsoft Exchange v5.5-SP2 to Exchange 2000 and Outlook 98 or Outlook 2000, for NT4 or Windows 2000

Microsoft Exchange E-MAIL Security Enhancement comprises a client extension built on Microsoft's standard Outlook product and a server based Policy Manager. Security features are provided to allow controlled release of emails and for sensitive data to be transmitted across insecure networks including the Internet.
The following features are available:

- Centralised Policy Enforcement based on Destination and Message Label
- Confidentiality – CESG-approved Data Encryption
- Proof of Content Origin – CESG-approved Electronic Signatures
- Classification Labelling
- Release Authority – Boundary Compliance Checking
- Additional security features

Compaq Computer Ltd
Secure Solutions Team, 2 Kelvin Close,
Birchwood Science Park North, Risley,
Warrington, Cheshire, WA3 7PB
Telephone: 01925-841881
Facsimile: 01925-841800
E-mail: security.enhancements@compaq.com
URL: www.compaq.com/services/nt/nt_security.html

X-KRYPTOR

Assurance Level: To be evaluated under CAPS

X-Kryptor is a dedicated network encryption device that provides domain based security and network traffic encryption. The device has two active 10/100Mb LAN interfaces and will segment network domains, a trusted domain will pass clear data, the un-trusted domain will pass only encrypted data. Communications across the un-trusted network can be to either another trusted X-Kryptor, or to a Network Client device with the X-Kryptor Secure Device Driver installed. Encryption techniques available include AES with 128bit key. CESG approved algorithms can be implemented upon request.

Barron McCann Limited
BeMac House, Fifth Avenue,
Letchworth, Herts SG6 2HF
Telephone: 01462 482333
Facsimile: 01462 482112
Email: petera@bemac.com
URL: www.x-kryptor.com

CASQUE-HMG

Assurance Level: CAPS approved

CASQUE-HMG enables the access control of sensitive information on remote servers; it provides strong authentication, key management and key distribution on open platforms.

The system comprises optical tokens that can use any light-emitting screen (e.g. any workstation monitor, backlit TFT laptop screens etc), a Standalone Administration System and server software for any platform.

CASQUE-HMG server side can interface directly to application programs by using http, or provide user authentication at firewalls eg Checkpoint.

CASQUE-HMG does not interfere with proxy servers or firewalls and has as its principal aim to provide authentication that is easy to integrate, use and administer.

Distributed Management Systems Ltd
Stockclough Lane, Blackburn BB2 5JR
Point of Contact: Basil Philips
Telephone: 01254 208419
Facsimile: 01254 208418
Mobile: 07887 524907
E-Mail basil@casque.co.uk
URL: www.dms-soft.com

EDS FIREGUARD ON SOLARIS 2.6

Assurance Level: CAPS approved

The EDS FIREGUARD software module replaces the commercial password encryption algorithm with the CESG-approved FIREGUARD password generation and encryption algorithm and ensures users can only operate with these passwords. The product is delivered as an easy-to-install patch tape.

EDS
1-3 Bartley Wood Business Park
Bartley Way, Hook, Hampshire RG27 9XA
Telephone: 01256 742584
Facsimile: 01256 742060
E-mail: mike.fugeman@edl.uk.eds.com
URL: www.eds.com

HEWLETT PACKARD HP-UX 10.20 ENHANCED AUTHENTICATION

Assurance Level: CAPS approved

The HP-UX Enhanced Authentication package is a CESG-approved implementation of the FIREGUARD algorithms for HP-UX 10.20 that includes:

- FIREGUARD Application Programming Interface (API) – to allow applications to perform user authentication with the FIREGUARD algorithm
- FIREGUARD Header files and libraries Installation mechanism for the installation of project specific 'seed' values

Modified HP-UX commands to support user authentication with the FIREGUARD algorithm through the following commands and utilities:

- passwd
- su
- login
- initcon ftpd ftpd
- ftpd
- rexecd
- CDE login

Hewlett-Packard Ltd
Nine Mile Ride, Wokingham,
Berkshire RG40 3LL
Telephone: 01344 365029
Facsimile: 01344 763747
E-mail: christopher_simpson@hp.com
URL: http://www.hp.com/uk

PORTCULLIS GUARDIAN ANGEL NT

Assurance Level: CAPS approved baseline

The security mechanisms of this pre-boot loader are designed to protect the Windows NT boot-manager by:

- Displaying screen-warning facilities to meet the requirements of current UK legislation.
- Asset Tagging to aid recovery of stolen hardware.
- Authentication using passwords encrypted by an endorsed implementation of the CESG FIREGUARD algorithm.
- Control of access to floppy disk and hard disks.
- Remote configuration and administration.

Portcullis Computer Security Ltd
The Grange Barn, Pikes End
Pinner, Middlesex, HA5 2EX
Telephone: 020 8868 0098
Facsimile: 020 8868 0017
E-mail: consult@portcullis-security.com
URL: www.portcullis-security

PORTCULLIS GUARDIAN ANGEL (SECURE PARTITION)

Assurance Level: CAPS approved (FIREGUARD implementation only)

In addition to the screen-warning, asset-tagging, and boot protection provided by GANT, this derivative provides an additional feature designed to store data of differing protective markings securely.

Using a CAPS-approved implementation of the FIREGUARD authentication algorithm, GASP ensures that selection of a specific hard disk partition is controlled in order that the user may choose to:

- Connect to the network and the non-sensitive data store, or
- Connect to a sensitive data storage area with the network disconnected.

Portcullis Computer Security Ltd
The Grange Barn, Pikes End
Pinner, Middlesex, HA5 2EX
Telephone: 020 8868 0098
Facsimile: 020 8868 0017
E-mail: consult@portcullis-security.com
URL: www.portcullis-security

SECURITY ENHANCEMENTS

FOR MICROSOFT WINDOWS NT – NT(SE)

Assurance Level: CAPS approved

Versions: v1.0 to v3.2 working with Microsoft Windows NT SP1 to SP6a

Microsoft Windows NT v4.0 Operating System Security Enhancement, designed by Compaq and Microsoft, adds the security features that are required to protect classified data at any level. The following optional features are configured centrally at the time of the system-wide installation:

- CESG Replacement Password Hashing System (Uniquely valued)
- CESG Password Generation System
- Password Obfuscation System
- Last Login and Multiple Login Information
- CD/Floppy Disk Centralised Access Control
- CD Auditing
- Single workstation with multiple desktops enabling role-based security
- Additional security features

Compaq Computer Ltd
Secure Solutions Team, 2 Kelvin Close,
Birchwood Science Park North, Risley,
Warrington, Cheshire, WA3 7PB
Telephone: 01925-841881
Facsimile: 01925-841800
E-mail: security.enhancements@compaq.com
URL: www.compaq.com/services/nt/nt_security.html

SECURITY ENHANCEMENTS

FOR MICROSOFT WINDOWS 2000 – WINDOWS 2000(SE)

Assurance Level: CAPS approved

Versions: v1.0& v2.0 working with Microsoft Windows 2000 SP1

Microsoft Windows 2000 Operating System Security Enhancement, designed by Compaq and Microsoft, adds the security features that are required to protect sensitive data at any level based on the enhancements to Windows NT provided by NT(SE). The following optional features are configured centrally at the time of the system-wide installation:

- CESG Replacement Password Hashing System (Uniquely valued)
- CESG Password Generation System
- Password Obfuscation System
- Last Login Information and Multiple Login Denial Service.
- CD and Floppy Disk Centralised Access Control
- CD usage and Floppy Disk File Transfer Auditing
- Single workstation with multiple desktops enabling role-based security
- Additional security features

Compaq Computer Ltd
Secure Solutions Team, 2 Kelvin Close,
Birchwood Science Park North, Risley,
Warrington, Cheshire, WA3 7PB
Telephone: 01925-841881
Facsimile: 01925-841800
E-mail: security.enhancements@compaq.com
URL: www.compaq.com/services/nt/nt_security.html

SECURITY ENHANCEMENTS

FOR MICROSOFT WINDOWS NT TERMINAL SERVER – WTS(SE)

Assurance Level: CAPS approved

Versions: v1.0, v1.1 and 1.0-2 working with Microsoft Windows NT Terminal Server Edition SP3 to SP6

Microsoft Windows NT Terminal Server Edition v4.0 Operating System Security Enhancement, designed by Compaq and Microsoft, adds the security features that are required to protect sensitive data at any level. The following optional features are configured centrally at the time of the system wide installation:

- CESG Replacement Password Hashing System (Uniquely valued)
- CESG Password Generation System
- Password Obfuscation System
- Last Login and Multiple Login Information
- Terminal Server CD/Floppy Disk Access Control
- Terminal Server CD Auditing
- Additional security features

Compaq Computer Ltd
Secure Solutions Team, 2 Kelvin Close,
Birchwood Science Park North, Risley,
Warrington, Cheshire, WA3 7PB
Telephone: 01925-841881
Facsimile: 01925-841800
E-mail: security.enhancements@compaq.com
URL: www.compaq.com/services/nt/nt_security.html

ABATHORN PROCESS

Assurance Level: CAPS approved

A secure data authentication solution, which allows validation of electronic (digital) or physical (printed) documents. No matter what E-Security is applied, it all vanishes immediately the document is printed out. The Abathorn solution however carries all key information to the document, transferring the trust from the electronic to the physical document.

The solution authenticates all significant data through the TTP/CA, the document issuer and incorporates a biometric template, which can identify the bearer.

If applicable the Abathorn solution can carry the digital signature to the paper.

The solution provides Data/Document Legality, Non-Repudiation, Continuity of Evidence, Integrity, Audit, Traceability, Compliance, Admissibility and Reconciliation capabilities.

Abathorn Limited
PO Box 17, Cirencester, Glos GL7 5ZF
Telephone: 01285 650781
Facsimile: 01285 740149
E-mail: info@abathorn.com
URL: www.abathorn.com

GORE D3 TAMPER RESPONDENT TECHNOLOGY

Assurance Level: CAPS approval in progress

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.

W L Gore and Associate (UK) Ltd
Dundee Technology Park
Dundee DD2 1JA
Telephone: 01382 569204
Facsimile: 01382 561007
E-mail: shunter@wlgore.com
URL: www.wlgore.com

TEMPEST

The security of information may be compromised by electromagnetic phenomena. What are electromagnetic phenomena?

Communications and IT equipments 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
- Tester training, leading to formal nationally recognised accreditation
- Specialist signals processing and analysis.

To find out about the products available, please consult the following two lists, which are arranged alphabetically by equipment category. Contact details for the manufacturers of these 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 POC for that product. For more general enquiries regarding approval of TEMPEST products, please contact the CESG TEMPEST office on:

Tel: 01242 221491 ext. 4681,
Fax: 01242 256394 or
e-mail: mike.stratford@cesg.gov.uk

A. CERTIFIED TO AMSG-720B OR BTR/01/202 STANDARD

Category	Manufacturer	Equipment
Facsimile Interface	Secure Computer Systems Ltd.	SSG 933T
Fibre Optic Converter	DRS Rugged Systems (Europe) Ltd.	QFOCV24T
Fibre Optic Converter	DRS Rugged Systems (Europe) Ltd.	QFOCX21T
Fibre Optic Dist. Unit	Lindgren-Rayproof	L2839/005T
Fibre Optic Ethernet	Volamp Ltd.	VES8042T
Fibre Optic Ethernet	Volamp Ltd.	VES8042TR
Fibre Optic Hub	Trend Communications Ltd.	643A
Fibre Optic Interface	Lindgren-Rayproof	L2243/CT/004
Fibre Optic Interface	Lindgren-Rayproof	Y21881/T
Fibre Optic Interface	Lindgren-Rayproof	Y21882/T
Fibre Optic Multiplexer	Honeywell Network Solutions Ltd.	9016T
Fibre Optic Multiplexer	Lindgren-Rayproof	Y21871
Fibre Optic Multiplexer	Lindgren-Rayproof	Y21906
Fibre Optic Transceiver	Lindgren-Rayproof	L/2840/005T
Fibre Optic Transceiver	Lindgren-Rayproof	L/2840/006T
Modem	Secure Systems Production Ltd.	COMSEC LD5010
Monitor, Colour	Secure Computer Systems Ltd.	SL 15BT001 LCD 15” MONITOR
Packet Switch Unit	International Computers Ltd.	X25T
Paper Tape Attachment	Siemens plc	T1560
Paper Tape Attachment	Trend Communications Ltd.	PC 612 PTA
Printer, Dot Matrix	Trend Communications Ltd.	614RO
Printer, Dot Matrix	Trend Communications Ltd.	610RO
Printer, Laser	Secure Computer Systems Ltd.	SC4050T
Scanner	Secure Computer Systems Ltd.	SC6250T
Scanner	Secure Computer Systems Ltd.	SS6350BT
Teleprinter	Siemens plc	T1501 RO
Teleprinter	Siemens plc	T1502 KSR
Teleprinter	Siemens plc	T1504 ESR
Teleprinter	Trend Communications Ltd.	610156
Teleprinter	Trend Communications Ltd.	615B ESR
Teleprinter	Trend Communications Ltd.	628A
Terminal	DRS Rugged Systems (Europe) Ltd.	LS20T
Terminal	Secure Systems Production Ltd.	Wyse 370 FT
Terminal, Secure Office	International Computers Ltd.	DRS M15/1TS
Terminal, Workstation	DRS Rugged Systems (Europe) Ltd.	j435T
Terminal, Workstation	DRS Rugged Systems (Europe) Ltd.	j438T
Terminal, Workstation	DRS Rugged Systems (Europe) Ltd.	j735T

B. CERTIFIED TO AMSG-788A OR BTR/01/210 STANDARD

Category	Manufacturer	Equipment
Combiner/Splitter	Secure Systems Production Ltd.	Combiner/Splitter
Computer, Personal	Joyce-Loebl Ltd.	JLTS/1/P133-FO/T
Computer, Personal	Secure Computer Systems Ltd.	SC8000T series
Computer, Personal	Secure Computer Systems Ltd.	SC6000T series
Computer, Personal	Secure Systems Production Ltd.	Alphastation 600 5/333 & DecServer 700
Computer, Personal	Trend Communications Ltd.	635B 386SX
Computer, Personal	Trend Communications Ltd.	645
Computer, Personal, Robust	DRS Rugged Systems (Europe)	HTOUA Robust 486
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	EXI
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	LXI
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	EXI Pentium
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	Application Server
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	RP6000 Buzzard 410/TEMPER002
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	GIS Client
Computer, Personal, Rugged	DRS Rugged Systems (Europe)	GRIDCASE 1587XGA
Data Link Processor System	Ultra Electronics / Data Sciences	DLPS
Facsimile	Secure Computer Systems Ltd.	SFX80T-M(R)(D)
Facsimile	Secure Computer Systems Ltd.	TS-21T
Facsimile	Trend Communications Ltd.	640
Facsimile	Trend Communications Ltd.	650
Facsimile	Trend Communications Ltd.	650A
Fibre Optic Distribution Unit	EUROPEAN DATA SYSTEMS	Battery backed fibre optic hub
Fibre Optic Distribution Unit	Lindgren-Rayproof	L2839/HX-STP
Fibre Optic Modem	Lindgren-Rayproof	FOCRS232R
Fibre Optic Modem	Secure Systems Production Ltd.	LD-7132
Fibre Optic Mux./Demux.	Lindgren-Rayproof	L3201/210/ST
Fibre Optic Transceiver	Lindgren-Rayproof	L2840/HT-ST
Ground Support System	DRS Rugged Systems (Europe)	Apache GSS
Keyboard	DRS Rugged Systems (Europe)	QK102/776/R
Monitor	DRS Rugged Systems (Europe)	EAGLE II Monitor
Monitor, Colour	DRS Rugged Systems (Europe)	HTOUB Rack 14”
Monitor, Colour	Secure Computer Systems Ltd.	SM15T-003
Monitor, Colour	Secure Computer Systems Ltd.	HM-174B High Res. Monitor
Monitor, Colour	Secure Computer Systems Ltd.	SM15T-004
Monitor, Colour	Secure Computer Systems Ltd.	SM15T-001
Monitor, Colour	Secure Computer Systems Ltd.	HM-114B
Packet Switch Unit	Secure Systems Production Ltd.	CPX10-5T X.25 UNIT

B. CERTIFIED TO AMSG-788A OR BTR/01/210 STANDARD *(Continued)*

Category	Manufacturer	Equipment
Packet Switch Unit	Secure Systems Production Ltd.	CPX10-3T
Paper Tape Punch & Reader	Secure Computer Systems Ltd.	N4000
Printer	BLAZEPOINT Ltd.	Blazepoint 400M Printer
Printer	BLAZEPOINT Ltd.	BLAZE 100L 10-PPM LED Printer
Printer	Trend Communications Ltd.	636A
Printer, Colour	Secure Computer Systems Ltd.	SC 895T
Printer, Dot Matrix	DRS Rugged Systems (Europe)	CP8240 24PIN
Printer, Dot Matrix	Secure Systems Production Ltd.	280T
Printer, Dot Matrix	Trend Communications Ltd.	636F
Printer, Dot Matrix	Trend Communications Ltd.	636C
Printer, Dot Matrix	Litton Data Systems	V2-LP(T)
Printer, Dot Matrix	Secure Systems Production Ltd.	PD-121B
Printer, Laser	BLAZEPOINT Ltd.	BLAZEPOINT OPTRA T162
Printer, Laser	Secure Systems Production Ltd.	PL-137B LED
Router	Secure Computer Systems Ltd.	SC1005T-X21 Router
Router, Packet	EUROPEAN DATA SYSTEMS	Tactical Packet Router
Terminal	DRS Rugged Systems (Europe)	LS20R
Terminal	DRS Rugged Systems (Europe)	7392 Message Terminal
Terminal	DRS Rugged Systems (Europe)	LS40R
Terminal	DRS Rugged Systems (Europe)	LSX17CR
Terminal	International Computers Ltd.	20271/001 & 20683/001 (K/B)
Terminal, CHOTS, Colour	International Computers Ltd.	20373/002
Terminal, CHOTS, Mono	International Computers Ltd.	20373T
Terminal, CHOTS, Mono	International Computers Ltd.	20683T
Terminal, Message	DRS Rugged Systems (Europe)	7392
Terminal, Secure Office	International Computers Ltd.	M15/2TS
Workstation	DRS Rugged Systems (Europe)	LWS715/50R
Workstation	DRS Rugged Systems (Europe)	LWS712/60R

COMPANY NAMES AND ADDRESSES

Manufacturer	Address	Contact
BLAZEPOINT Ltd.	Unit 2, Tower Estate, Warpsgrove Lane, Chalgrove, Oxfordshire OX44 7XZ	Telephone: 01865 891666 Contact: Mr D Selwood
DRS Rugged Systems (Europe) Ltd.	The Trading Estate, Farnham, Surrey GU9 9NN	Telephone: 01252 734488 Contact: Mr D Cockarill
EUROPEAN DATA SYSTEMS Ltd.	Cornbrash Park, Bumpers Farm Chippenham, Wiltshire SN14 6RA	Telephone: 01249 461234 Contact: Mr W Clements
GRID Defence Systems Ltd.	Highbridge House, 93-96 Oxford Rd Uxbridge, Middlesex UB8 1LU	Telephone: 01895 230650 Contact: Mr P Rushton (Piers)
Honeywell Network Solutions Ltd.	Lovelace Road, Bracknell, Berkshire RG12 8WD	Telephone: 01438 730700 Contact: Mr S Cockley (Steve) E-mail: stev.cockley@honeywell.com
International Computers Ltd.	Jays Close, Viables Industrial Estate, Basingstoke, Hampshire RG22 4BY	Telephone: 01256 428083 Contact: Mr M Conroy (Mick) E-mail: mick.conroy@icl.com
Joyce-Loebl Ltd.	Post Design and Engineering Services 390 Princeway, Team Valley, Gateshead NE11 0TU	Telephone: 0191 420 3000 Contact: Mr M Cattle
Lindgren-Rayproof	Boulton Road, Pin Green Industrial Area, Stevenage, Hertfordshire SG1 4TH	Telephone: 01438 730700 Contact: Mr C Castro
Litton Data Systems	Burlington House, 118 Burlington Road New Malden Surrey KT3 4NR	Telephone: 020 8329 2041 Contact: Mr J Yale (John)

COMPANY NAMES AND ADDRESSES *(Continued)*

Manufacturer	Address	Contact
Secure Computer Systems Ltd.	Henley House, Barnett Way, Barnwood, Gloucester Gloucestershire GL4 3RT	Telephone: 01452 371999 Contact: Mr F Foskett
Secure Systems Production Ltd.	9 Manchester Park, Tewkesbury Road Cheltenham Gloucestershire GL51 9EJ	Telephone: 01242 257800 Contact: Mr J Walker
Siemens plc	Siemens House Oldbury Bracknell Berkshire RG12 8FZ	Telephone: 01344 396000 Contact: Mr R E Miller
Trend Communications Ltd.	Knaves Beech Estate Loudwater High Wycombe Buckinghamshire HP10 9QZ	Telephone: 01628 524977 Contact: Mr P Deane
Ultra Electronics/Data Sciences Ltd.	Knaves Beech Business Centre Loudwater High Wycombe Buckinghamshire HP10 9UT	Telephone: 01628 530000 Contact: Mr S Bennison
Volamp Ltd.	Unit 3 Riverside Business Park Dogflud Way Farnham Surrey GU9 7SS	Telephone: 01252 724055 Contact: Mr W Saich

INDEX

INDEX

INDEX

CESG

The Marketing Office
10/2W25, PO Box 144, Cheltenham, Gloucestershire GL52 5UE
Tel: +44 (0)1242 237323 • Fax: +44 (0)1242 257520
email: enquiries@cesg.gov.uk

© Crown Copyright 2001