UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

CERTIFIED PRODUCT LIST

UKSP 06

April 2000


UKITsec

About This Publication

CONTENTS

INTRODUCTION

The Certified Product List is published twice yearly by the Certification Body of the UK IT Security Evaluation and Certification Scheme (the UK Scheme). It provides information about products evaluated and certified under the UK, Canadian, French, German and US Schemes. This issue supersedes all previous issues.

Under the UK Scheme, products are evaluated either against ITSEC or Common Criteria to the appropriate level of assurance, based on the claims made by the vendor for his product. For ITSEC evaluations the assurance levels range from E1 to E6 and for Common Criteria evaluations the levels range from EAL1 to EAL7. We recommend that prospective purchasers review the functionality contained within the claims to ensure the certified products' applicability in the purchasers' environment. This information can be found in the product's Security Target which is available from the vendor.

Further information on the UK Scheme can be obtained from the address below. Or you can visit the UK Scheme website which features a regularly updated version of this product list as well as downloadable versions of all publicly-available Scheme documents.

Certification Body Secretariat
UK IT Security Evaluation & Certification Scheme
PO Box 152 Cheltenham
Gloucestershire GL52 5UF
Tel: +44 (0)1242 238739
Fax: +44 (0)1242 235233
http://www.itsec.gov.uk
email:info@itsec.gov.uk

EVALUATION

Computer security evaluation is the detailed examination of IT security features culminating in comprehensive and informed functional and penetration testing, to ensure that those features work to meet an agreed security target. Evaluation is only carried out on the logical security features of a product. Purchasers should make appropriate arrangements for the prevention or detection of unauthorised tampering with hardware. The certification process should normally take 6-12 months from submission to certification.

CERTIFICATION REPORTS

Evaluation results are published in Certification Reports which contain additional information on how a product should be used. In a certified product not all security features may be evaluated; its configuration may be restricted or its use confined to specific platforms. Use of a product with a different operating system, hardware platform or with extended networking facilities may expose vulnerabilities not present during the evaluation of the certified configuration. Certification Reports are available from product vendors, or in some cases, the UK Scheme web site (http://www.itsec.gov.uk).

CLEFS

Evaluations are carried out by independent third parties known as Commercial Evaluation Facilities or CLEFs, appointed by the Certification Body of the Scheme. These meet rigorous security and quality standards. There are five CLEFs, which can be contracted to carry out both evaluation and pre-evaluation work. Their contact details can be found inside the back cover.

CMS

Evaluation results apply to a specific version of a given product. Any change to that product may invalidate those results. The Certificate Maintenance Scheme has been devised in order to address the problem posed by the developmental evolution of certified products. CMS aims, within certain limits, to provide a means of maintaining the same level of security assurance without the need for formal re-evaluation, by a CLEF. This is achieved by the developer appointing a Security Analyst to assess the security impact of all changes affecting the certified product. Potential security problems can be identified and rectified at an early stage with a consequential streamlining of the assurance process. Further details of the CMS and the meaning of the phrase “CMS approved” are set out in UKSP 16.

FUNCTIONALITY CLASSES

Functionality classes are becoming widely used to label security functionality. The Certification Body will only certify that the requirements of a particular functionality class have been met where the required security functionality is provided wholly by the product. Where functionality needs to be provided by the underlying hardware or software for the full requirements of the functionality class to be met, reference will be made to the fact in the Certification Report.

The ITSEC lists a number of functionality classes, e.g. F-C2, F-B1, F-B2, based on the

FUNCTIONALITY CLASSES (cont)

US TCSEC, e.g. C2, B1, B2, respectively. These were based on the 1985 version of TCSEC. Some of these ITSEC classes were recently revised to take account of the numerous interpretations that the US authorities have made over the intervening years. The Certification Reports make it clear where the revised versions have been used.

ASSURANCE LEVELS

Most of the products listed in this document have been evaluated using the IT Security Evaluation Criteria (ITSEC) leading to an E level of assurance. Evaluations are carried out with increasing rigour from E1 to a maximum level of E6. Evaluations are now being undertaken against the Common Criteria which has seven assurance levels, EAL1 to EAL7. The approximate correspondence with the ITSEC and the old UK criteria is shown in the table. The new EAL1 level is no more than a health check or security audit of the product which requires a minimum of documentary evidence.

Common Criteria	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	–	E1	E2	E3	E4	E5	E6
Old UK Criteria	–	UKL1	UKL2	UKL3	UKL4	UKL5	UKL6

STRENGTH OF MECHANISM

The term Strength of Mechanism is used in respect of security features which are required to be of sufficient strength to guard against exploitation. Strength of Mechanism complements the evaluation level in quantifying the confidence which a purchaser may have in a product and is accordingly linked to the evaluation level. The UK will comment on Strength of Mechanism security features as appropriate in Certification Reports. It will not usually comment on the difficulty of exploiting vulnerabilities, as its policy is that identified vulnerabilities are removed.

VULNERABILITIES

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities may be discovered after a certificate has been awarded. The Certificate and Certification Report reflect the Certification Body's view at the time of the product or system's certification. The entries in this document reflect the Certification Body's view at the time of publication. Users (both prospective and existing) should check regularly for themselves whether any security vulnerabilites have been discovered since certification and, if appropriate, should check with the vendor to see if any patches exist for the product and whether such patches have been evaluated and certified. Users are reminded of the security dangers inherent in downloading 'hot-fixes' where these are available, and that the UK Scheme provides no assurance whatsoever for patches obtained in this manner.

More up to date information on security vulnerabilites within individual products and systems can be found on the ITSEC web site www.itsec.gov.uk.

SYSTEM EVALUATIONS

The evaluation and certification of systems is a less well-known but nevertheless important area of UK ITSEC activities. Evaluations are carried out typically as part of a system accreditation exercise.

The UK Scheme has experience of a wide range of systems evaluations that embody both certified and uncertified products, and guidance is contained in UKSP 04 - The Developer's Guide. Systems composed of certified products may not always be secure and may themselves require evaluation. System builders should obtain Security Targets and Certification Reports from product vendors. Where systems include products certified in another country, some top-up evaluation work may be required in relation to them, as indicated below under "Evaluation in Other Countries".

Until now evaluation work has mainly been in support of UK Government systems for clients such as the Ministry of Defence, the Home Office and HM Customs and Excise. The increasing harmonisation across Departments since the Review of Protective Security has increased the relevance of systems evaluation to a wider range of Government customers.

System evaluation is equally relevant to commercial institutions as a means of minimising risk and is a confidence hallmark for trading partners. It is essential wherever data integrity and availability are key issues. Demonstrable compliance with the provisions of the Data Protection Act is an important benefit of such an evaluation.

The variety of system evaluations, either completed or still in progress, ranges from small department systems through to large networked inter-departmental systems with many thousands of users. The UK Scheme has completed over 80 such evaluations to date.

COMMON CRITERIA

The Common Criteria represents the outcome of international efforts to align and develop the existing European and North American criteria. Significant effort was expended in ensuring that the current investment in ITSEC evaluations was protected. The Common Criteria includes some welcome extra flexibility not found in the ITSEC.

Evaluations against Common Criteria version 1 started in the latter part of 1997. Version 2 was formally published in 1998 and is now ratified as ISO standard 15408. An initial version of the Common Evaluation Methodology 1.0 has been issued (Aug 99). It is expected that given sufficient effort during the evaluation, certificates to both the ITSEC and Common Criteria can be issued.

EVALUATION IN OTHER COUNTRIES

In November 1997, the Senior Officials Group for Information Security (SOG-IS) of the European Commission approved the Recognition Agreement of Information Technology Security Evaluation Certificates based on ITSEC. The agreement came into force in March 1998, and now covers France, Finland, Germany, Greece, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland and the United Kingdom. These nations agree to recognise ITSEC certificates from the Qualifying Certification Bodies, which initially are SCSSI of France, BSI of Germany and CESG of the UK.

The agreement was extended to cover Common Criteria up to EAL7 in April 1999 and at the time of printing the following countries have signed up to the changes; Finland, Italy, Norway, Netherlands, Sweden, Switzerland and United Kingdom.

In October 1998 the representatives of the security agencies of the USA, Canada, France, Germany and the United Kingdom signed an arrangement to formally recognise certificates of evaluation up to EAL4 (for both Protection Profiles and products) from each other, based on version 2.0 of the Common Criteria. Australia and New Zealand have also signed up to this agreement.

An agreement has also been negotiated between CESG of the UK and DSD of Australia for the recognition of each other's ITSEC certificates.

In each memorandum or agreement there is a clause which states that where National Security is at stake, certificates issued by other countries will not necessarily be recognised. HMG Departments wishing to use foreign certified products where National Security is an issue are advised to consult CESG.

This edition of UKSP 06 contains summaries of foreign certified products recognised under the above agreements. It is important to note that recognition of foreign certificates by CESG is not a guarantee or a warranty by CESG in relation to the certified product or the certificate or certification report and CESG does not accept any liability in respect of the same. Full details of products certified in other countries and the effect of certification in other countries may be obtained from the respective national authorities at the addresses given on page 59.

We are pleased to announce that the Certification Body of the UK IT Security Evaluation and Certification Scheme was accredited to the European Standard for Certification Bodies (EN 45011:1988) by the United Kingdom Accreditation Service on 16 March 2000.

Products at a Glance

	Product Title	Assurance Level	Supplier Name	Date Certified	CESG Controlled	Page
SMARTCARDS	MONDEX Purse Release 2.0 on MULTOS v3 and Hitachi H8/3112 ICC	E6	Mondex International	Aug 1999		47
	Multos v3 on Hitachi H8/3112 ICC	E6	Mondex International	Aug 1999		46
COMMUNICATIONS	CASM CryptServe 1.02	E3	CESG	Mar 1998	✓	50
	CERBERUS Guard Processor	E4	EDS Ltd	Apr 1998		48
	Datacryptor 2000	E3	Racal Security & Payments	Jul 1999		18
	ED600 RAMBUTAN Data Encryption Unit	UKL2	Baltimore Technologies (UK) Ltd	Feb 1992	✓	54
	ED600RTS RAMBUTAN Link Encryptor	E3	Baltimore Technologies (UK) Ltd	Sep 1995	✓	54
	ED2048R RAMBUTAN Data Encryption Unit	E3	Baltimore Technologies (UK) Ltd	Jul 1994	✓	52
	ED2048R3 RAMBUTAN Data Encryption Unit	E3	Baltimore Technologies (UK) Ltd	Apr 1996	✓	53
	ED2048RU RAMBUTAN Data Encryption Unit	E3	Baltimore Technologies (UK) Ltd	Mar 1995	✓	53
	ED8000RL RAMBUTAN LAN Interconnect IP Encryptor	E3	Baltimore Technologies (UK) Ltd	Dec 1997	✓	55
	Network Security Workstation	E3	Baltimore Technologies (UK) Ltd	Jan 1997	✓	55

	Product Title	Assurance Level	Supplier Name	Date Certified	CESG Controlled	Page
COMMS	OMEGA Version 7.12 Increment 19	E3	ICL Defence	Jan 2000	✓	50
	Racal RAMBUTAN SAFE 2M	E3	Racal Security & Payments	May 1995	✓	51
	Racal RAMBUTAN SAFE X.25	E3	Racal Security & Payments	Feb 1994	✓	51
	Racal RAMBUTAN SAFE 64K	E3	Racal Security & Payments	Jul 1994	✓	52
	SafeDial Version 1.27	E3	Racal Security & Payments	Jan 1998		19
DATABASES	CA-Open INGRES and Open INGRES/ Enhanced Security Release 1.1	E3	Computer Associates	Feb 1999		21
	INFORMIX OnLine Dynamic Server V7.23	E2	Informix Software Ltd	Mar 1998		20
	INFORMIX OnLine/Secure B1 and C2 Version 5.0	E3	Informix Software Ltd	Apr 1995		19
	Oracle7 and Trusted Oracle7 Release 7.0.13.6	E3	Oracle Corporation	Sep 1994		22
	Oracle7 Release 7.2.2.4.13	EAL4	Oracle Corporation	Sep 1998		24
	Oracle7 Release 7.2.2.4.13	E3	Oracle Corporation	Feb 1998		23
	Oracle7 Release 7.3.4 on NT 4.0	E3	Oracle Corporation			23
	Oracle8 Release 8.0	EAL4	Oracle Corporation			20

Products at a Glance

	Product Title	Assurance Level	Supplier Name	Date Certified	CESG Controlled	Page
DATABASES	Oracle8i Release 8.1	EAL4	Oracle Corporation			21
	Trusted Oracle7 Release 7.1.5.9.3	E3	Oracle Corporation	Mar 1998		22
	Trusted Oracle7 Release 7.2.3.0.4	E3	Oracle Corporation	Jul 1999		24
NETWORKING	Banyan VINES Version 7.0	E2	Banyan Systems Inc	Apr 1997		29
	Borderware Firewall Server Version 6.1	EAL4	Borderware Technologies Inc	Jan 2000		32
	BrainTree AUDITOR Plus	E1	BrainTree Technology Ltd	Oct 1996		26
	Check Point FireWall-1 Version 4.0	E3	Check Point Software Technologies Ltd	Mar 1999		29
	CyberGuard Firewall 2.2.1e	E3/CMS	CyberGuard Europe Ltd	Mar 1997		30
	CyberGuard Firewall for Unixware 4.1	E3	Cyberguard Europe Ltd	Jan 1999		31
	CyberGuard Firewall for Windows NT 4.1	E3	Cyberguard Europe Ltd	Jan 1999		31
	Data Track Technology Tracker 2650	E2	Data Track Technology plc	Mar 2000		28
	DXE Router	E3	StorageTeK Network Systems Group	Feb 1999		34
	Entrust 4.0	EAL3+	Entrust Technologies Ltd	Mar 1999		26

	Product Title	Assurance Level	Supplier Name	Date Certified	CESG Controlled	Page
NETWORKING	Entrust 5.0	EAL3	Entrust Technologies Ltd	Mar 2000		25
	Gauntlet Firewall V3.01 for Windows NT, Build 113	E3	Network Associates Ltd	Jun 1999		30
	Guardian PRO	EAL4	Net Guard Ltd			32
	MailGuard Bastion 1.0	E3	Net-Tel Computer Systems Ltd			27
	MLPF 3.3.0	E3	Hitachi Data Systems	Mar 1999		25
	Safegate Version 2.0.2	EAL3	Fujitsu Ltd	Mar 2000		27
	Trusted EDI	E3	EDS Ltd	Jul 1997		48
OPERATING SYSTEMS	VCS FIREWALL 3.0	EAL1	The Knowledge Group	Mar 1999		33
	Argus B1/CMW and C2/TMW Release 1.2	E3	Argus Systems Group Inc.	Dec 1996		37
	Argus C2/TMW and B1/CMW Release 1.3	E3	Argus Systems Group Inc	Sep 1999		37
	BEST-X/B1 (Bull Enhanced Security Technology) 1.1.1.9	E3	Bull Information Systems Ltd	Apr 1997		36
	BEST-X/C2 (Bull Enhanced Security Technology) 1.1.1.9	E3	Bull Information Systems Ltd	Jun 1997		36
	ED8000EG Enhanced Grade LAN Interconnect IP Encryptor	E3	Baltimore Technologies (UK) Ltd			56
	HP-UX Version 10.20	E3	Hewlett Packard Ltd	Jan 1997		43

Products at a Glance

	Product Title	Assurance Level	Supplier Name	Date Certified	CESG Controlled	Page
OPERATING SYSTEMS	IBM PR/SM ES/9000	E4	IBM United Kingdom Ltd	Sep 1995		43
	Maxion/OS Version 1.2	E3	Concurrent Computer Corporation Ltd	Dec 1996		35
	Microsoft Windows NT Workstation 3.51	E3	Microsoft Ltd	Oct 1996		42
	Microsoft Windows NT Workstation 4.0	E3	Microsoft Ltd	Mar 1999		42
	Open VMS & SEVMS for VAX and ALPHA, Version 6.2-1H3	E3	Compaq Computer Ltd			44
	Remote Management Centre	E1	IBM			33
	Sequent DYNIX/ptx Unix 4.1 SLS and 4.1a SLS	E3/CMS	Sequent Computer Systems Ltd	Feb 1997		38
	Sequent DYNIX/ptx Unix Version 4.4.2	E3	Sequent Computer Systems Ltd	Nov 1998		38
	SCO CMW+ Release 3.0	E3	SCO	Sep 1999		35
	SCO Unixware2.1	E2	SCO	Feb 1999		34
	Sun Solaris 2.4SE	E2	Sun Microsystems Federal	Nov 1995		39
	Sun Solaris 2.5.1SE	E2	Sun Microsystems Federal	Mar 1998		40
	Sun Solaris 2.6 SE	E3/CMS	Sun Microsystems, Inc.	Jan 1999		40
	Sun Trusted Solaris 1.2 ITSEC(E)	E3	Sun Microsystems Federal	Nov 1995		39

	Product Title	Assurance Level	Supplier Name	Date Certified	CESG Controlled	Page
OPERATING SYSTEMS	Sun Trusted Solaris 2.5.1	E3/CMS	Sun Microsystems Federal	Sep 1998		41
	VME O/S with HSO Version SV294	E3	International Computers Ltd	Sep 1994		41
	VME O/S with GSO Version SV294	E3	International Computers Ltd	Sep 1994	✓	56
PC ACCESS CONTROL	Disknet NT Version 1.70	E2	Reflex Magnetics Ltd	Jul 1999		45
	GUARDIAN ANGEL Version 5.01D1	E2	Portcullis Computer Security Ltd	Jan 1998	✓	58
	HARDWALL 45KILGETTY 1.2h	E3 E3	Calluna Technologies Ltd Software Box Ltd	Feb 1999	✓	46
	KILGETTY PLUS 1.2h	E3	Software Box Ltd	Feb 1999	✓	57
	KILGETTY PLUS NT 4.V1.0	E3	Software Box Ltd	Feb 1999	✓	57
	SeNTry 2020	EAL1	MIS - Corporate Defence Solutions	Jul 1998		44
	STOPLOCK V Various Versions	E3	Netlexis Ltd	Sep 1996		45

Canadian Certified Products

Product Title	Assurance Level	Supplier Name	Date Certified
Black Hole (SecurIT) Firewall Version 3.01E2	EAL3	Milkyway Networks Corporation	Aug 1997

French Certified Products

Product Title	Assurance Level	Supplier Name	Date Certified	Certificate reference
FOX Software filter 1.0	E4	THOMSON-CSF	Jan1998	97/03
MC68HC05SC0401 SCOT300 ref. ZC438408	E3	Motorola	Jun 1998	98/02
MICRO-SAMFLEX 1.0 ST 16601 H	E3	SOLAIC	Dec 1997	97/05
MICRO-SAMFLEX 1.0 ST16601 G	E3	SOLAIC	Mar 1997	97/02
PC SECU-C V2.00	E3	ActivCard	May 1996	96/01
ST 16CF54B CPS2 V3.3	E3	ST Microelectronics Schlumberger	Oct 1998	98/03
ST16SF44 A/RHQ SCOT400 Version 1	E3	STMicroelectronics	Apr 1998	98/01
ST 16SF48A PC2.3 Version 2	E3	Bull CP8 ST Microelectronics	Nov 1998	98/04
ST16SF48 A/RHBB PC2.3 Version 2	E3	CP8 Transac	Jan1997	97/01
ST16601 G/SKG B4/B0' V2	E3	STMicroelectronics	May 1996	96/02
ST16601 H/SKG B4/B0' V2	E3	STMicroelectronics	Dec 1997	97/04
UNISAM 1.0 ST 16SF48C/RMH	E3	Gemplus	Oct 1998	98/05

German Certified Products

	Product Title	Assurance Level	Supplier Name	Date Certified	Certificate reference
MIDSIZE	AIX Version 4.2	E3	IBM Deutschland	Apr 1997	0126
	AIX Version 4.3	E3	IBM Deutschland	May 1998	0138
	Midsize Systems B1/EST-X Version 2.0.1 with AIX, Version 4.3.1	EAL4	Bull S.A. and IBM Informationssysteme Deutschland GmbH	Mar 1999	0143
	GUARDIAN 90 Version C20 with SAFEGUARD VC22L	E3	Tandem Computers GmbH	Oct 1993	0017
	Reliant UNIX 5.43/AUDIT 2.0	E3	Siemens Nixdorf	Apr 1997	0127
	SINIX V5.42/AUDIT V1.0	E2	Siemens Nixdorf	Oct 1995	0083
PC SECURITY	Firmloc 2.11	E2	PSB GmbH	Oct 1994	0052
	Integrity Protection SFile 4.0	E1	Deutsche Telekom AG	Jul 1997	0117
	PC-Safe B I V Version 9.1 PC-Safe privat v9.1	E1 E1	PHS Peter Hoffmann Service GmbH	Apr 1994 Sep 1995	0015 0101
	Safeguard Easy OS/2 Safeguard Easy for DOS v2.0 Safeguard Professional 4.1A English Version of above	E2 E2 E2 E2	Utimaco Safeware AG	Sep 1997 Jun 1995 Mar 1994 Oct 1994	0058 0012 0013 0072
	Security Shells SIKOM-TIBIS V002.05	E3	Deutsche Telekom AG	Jul 1996	0069
	WISO-Crypt 1.2	E1	Computer Elektronik Infosysy GmbH	Dec 1994	0057
COMMS	**Data Communication** DORKRYPT 4.0	E1	Deutsche Telecom AG	Mar 1998	0118

German Certified Products

	Product Title	Assurance Level	Supplier Name	Date Certified	Certificate reference
COMMS	KryptoGuard X.25 V 1.0	E2	KryptoKom GmbH	Mar 1995	0023
	X*PRESSO Security Pack 1.1	E3	BROKAT	Jun 1997	0116
	X*PRESSO Security Package 1.3	E3	BROKAT	Oct 1998	0128
CHIPCARD READERS	B1-Chipcard-reader, B1 KLC, V4.0 (FirmWare)	E2	Siemens Nixdorf	Feb 1998	0119
	Cardreader G80-1501 HAD Index/10	E2/basic	Cherry GmbH	Mar 1999	0149
	Cardreader PC-Chip -KVK Version 6.50	E2	Preh-Werke GmbH	Dec 1994	0070
	CARD STAR/medic V2.4	E3	Celectronic GmbH	Apr 1995	0094
	CARD STAR/medic V2.5	E2	Celectronic GmbH	Jun 1996	0113
	CARD STAR/medic Version 2.6 item no: 4210 and 4211	E2/basic	Celetronic GmbH	Feb 1999	0147
	CARD STAR/medic 4211	E2	Celectronic GmbH	Apr 1995	0087
	CARD STAR/memo	E2	Celectronic GmbH	Mar 1996	0092
	CARD STAR/memo V4.0	E2	Celectronic GmbH	Feb 1997	0120
	CARD STAR/visit V2.4	E3	Celectronic GmbH	Apr 1995	0093
	CARD STAR/visit V2.5	E2	Celectronic GmbH	Jun 1996	0114
	G80-1501 HAD, Index /04 bis Index/08	E2	Cherry Mikroschalter GmbH	Jan 1994	0026

CHIPCARD READERS

Product Title	Assurance Level	Supplier Name	Date Certified	Certificate reference
G80 -1501HAD Index /09	E2	Cherry Mikroschalter	Jan 1994	0074
GCR550 v2.22	E2	Gemplus Card International GmbH	Dec 1993	0090
HML 500 Version 2.6	E2	ORGA Kartensysteme	Dec 1993	0080
HML 825 Version 3.2	E2	ORGA Kartensysteme	Mar 1996	0078
HML 825 Version 3.3	E2	ORGA Kartensysteme	Aug 1997	0121
IBM 5937-B05 S/N 51066	E2	IBM Deutschland Entwicklung GmbH	Jan 1994	0067
KV-CKT	E2	Siemens AG	Nov 1994	0055
KVT1 V2.03A	E2	Krone AG	Oct 1994	0073
*Medi*Card▲handy	E2	etp	Sep 1996	0112
MEDItype Version with PC-Interface E004/006	E2	Optima Burotechnik GmbH	Oct 1994	0062
MEDItype Version without PC-Interface	E2	Optima Burotechnik GmbH	Apr 1994	0046
Mobile Datenerfassung Versichertenkarte Version 1.1	E2	Wesser GmbH	Oct 1997	0089
PE 115	E2	TRT Phillips Communications Systems	Oct 1994	0044
PSR2 Firmware Rev 2.27	E2	SCM Microsystems GmbH	Mar 1998	0134
SNI B1 PC-Card Rev 2.27	E2	Siemens Nixdorf	Mar 1998	0133
Walther Cardtype Version E004/006	E2	Silver Büromaschinen Vertrieb	Jan 1995	0076

German Certified Products

	Product Title	Assurance Level	Supplier Name	Date Certified	Certificate reference
SMARTCARDS	Setcad 202	E4	Setec Oy	Feb 1996	0097
	Setcad 202 Software V1.43	E4	Setec Oy	Feb 1998	0124
	Setcos 3.1 Version 3.1.1.1 Setcos 3.1 Version 3.1.1	E4 E4	Setec Oy Setec Oy	May 1997 Feb 1996	0125 0098
	Operating Systems and Cardreaders SICRYPT® Payphone Security Module Typ: Deutsche Telekom AG "SM-K"	E3	Siemens AG	Dec 1998	0096
MISCELLANEOUS	**Electronic Immobilizer** EWS II, Version 01	E2	BMW AG	Apr 1996	0086
	MAWIS Mülltonnen-identifikationssystem 1.0	E2	MOBA Dresden GmbH	Jun 1996	0060
	Philips Smart Card controller P8WE5032VOB	EAL3	Philips Semiconductors Hamburg Unternehmensbereich der Philips GmbH	Nov 1999	0153
	PR/SM for IBM S/390 CMOS Computer Systems Family 9672-G5/ (Mainframe Systems)	E4	IBM Corporation	Mar 1999	0142
	Identification System Tixi-Mail Box Pro with E-Mail Firewall Firmware Version 300.2.34	E1	Tixi.Com	Aug 1998	0137

US Certified Products

Product Title	Assurance Level	Supplier Name	Date Certified
CISCO PIX Firewall 520 V4.3(1)	EAL2	Cisco Systems Inc	Dec 1998
ITT Dragonfly Guard Model G1.2 V3.0	EAL2	ITT Industries	Oct 1998
Lucent Managed Firewall V3.0 Build 150	EAL2	Lucent Technologies	Jan 1999

Australasian Certified Products

Product Title	Assurance Level	Supplier Name	Date Certified	Certificate reference
Vision Abell Data Diode Device F1 D003 V.1.2	E6	Vision Abell Pty Ltd	Nov 1999	1999/10

Commercially Available Products

This section contains some products which can also offer Government approved algorithms suitable for the protection of sensitive data.

Certification Mark

The official Certification Mark (above)
shows that a product has been awarded a Certificate by the UK ITSEC scheme.
Certificates issued by the Certification Body may be withdrawn if security vulnerabilities are discovered after the date of issue.

Datacryptor 2000 (Synchronous Line Encryptor)

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 varietyy 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 Racal 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.

Product Type: Communications
Assurance Level: E3
Supplier: Racal Security & Payments
Evaluation Facility: Admiral
Certification Status: Certificate P126 July 1999
Point of Contact: Chris Woods
Telephone: 01273 384600
Fax: 01273 384601
e-mail: chris.woods@racalitsec.com

COMMERCIALLY AVAILABLE

Racal SafeDial Version 1.27

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 eavesdropping for data transmissions using public telephone networks.

The unit is tamper resistant, easily transportable and once commissioned only requires a password for normal operation. The tamper resistance, in combination with the use of a new and random strong key generated each time SafeDial is used, obviates the need for the laborious and time consuming task of generating, updating and distributing encryption keys.

This product inserts into a standard PCMCIA socket, available on most laptops and is provided with a linking cable suitable for attachment to a standard UK telephone socket.

The device employs the Racal Data Group Key Management Scheme to securely distribute data encryption keys.

Product Type: Communications
Assurance Level: E3
Supplier: Racal Security & Payments
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 98/90 January 1998
Point of Contact: Chris Woods
Telephone: 01273 384600
Fax: 01273 384601
e-mail: chris.woods@racalitsec.com

INFORMIX OnLine/Secure B1 and OnLine/Secure C2 Version 5.0 Release UD7

When used in conjunction with an F-B1 operating system (OS), OnLine/Secure-B1 provides database security for systems requiring F-B1 functionality. When used in conjunction with an F-C2 OS, OnLine/Secure-C2 provides database security for systems requiring F-C2 functionality. Both OnLine/Secure-B1 and OnLine/Secure-C2 can operate stand-alone or, with STAR/Secure, in a distributed client-server database mode. With the OS, the main security functions provided by the product are Identification and Authentication, Object Re-use, Discretionary Access Control, Data Integrity, Accountability and Audit. Archiving, Rollforward, Fast Recovery and Disk Mirroring facilities are also supported. OnLine Secure-B1 supports Mandatory Access Control with mechanisms to eliminate high bandwidth covert channels between processes operating at different sensitivity levels.

The products are designed to be portable across trusted UNIX platforms. This simplifies the evaluation of systems requiring alternative UNIX platforms. Subject to the OS providing a defined set of security primitives, the product architecture is platform independent. Tailoring the products to specific platforms involves changes to a small and well defined set of source modules requiring a minimal amount of re-evaluation.

The B1 product was evaluated on Sun Trusted Solaris CMW and the C2 Product was evaluated on Sun Solaris.

Product Type: Database
Assurance Level: E3
Supplier: Informix Software Ltd
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 95/46 April 1995
Point of Contact: David Hann
Telephone: 0181 818 1000
Fax: 0181 818 1111

Commercially Available Products

INFORMIX-OnLine Dynamic Server Version 7.23

Product Type: Database
Assurance Level: E2
Supplier: Informix Software Ltd
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 98/95 March 1998
Point of Contact: Andy Legge
Telephone: 0181 818 1000
Fax: 0181 818 1064
e-mail: alegge@informix.com

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's core technology is based on INFORMIX's Dynamic Scalable Architecture (DSA) which provides a parallel database architecture for distributed enterprise - from the desktop to departments to the data centre. DSA is designed explicitly to help the management of increasingly larger and more complex databases while improving overall system performance and scalability.

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 - all within a single, client/server-ready package. It supports Informix's entire line of SQL-based application development tools and a large number of third party tools.

The product is designed to be portable across E2/F-C2 UNIX platforms. Tailoring the product 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.

Oracle8 Release 8.0

Product Type: Database
Assurance Level: EAL4
Supplier: Oracle Corporation
Evaluation Facility: Logica
Certification Status: In Evaluation Since 1998
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

Oracle8 is an Object/Relational Database Management System (O/RDBMS), providing advanced security and functionality for multi-user, distributed database environments. Oracle8 is available on many operating system platforms and supports hundreds of client/server application, development and systems management tools, as well as on-line transaction processing, decision support, and data warehousing architectures.

The advanced security functionality in Oracle8 includes 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 including mutual authentication of databases, and the ability to exploit single sign-on and external authentication mechanisms. New security features in Oracle8 include password management, data dictionary protection, global roles and X.509 certificate based authentication.

During this evaluation, Oracle8, Release 8.0 will be tested on Microsoft Windows NT 4.0 using Compaq hardware, against the Government Database Management System (G.DBMS) protection profile.

COMMERCIALLY AVAILABLE

Oracle8i Release 8.1

Oracle8i is an Object/Relational Database Management System (O/RDBMS), providing advanced security and functionality for multi-user, distributed database environments. Oracle8i is available on many operating system platforms and supports hundreds of client/server and web-enabling application, development and systems management tools, as well as on-line transaction processing, decision support, and data warehousing architectures.

The advanced security functionality in Oracle8i includes granular privileges for enforcement of least privilege, user-configurable local and global roles for privilege management, a wide variety of authentication mechanisms including X.509 certificate-based authentication, extensive password management facilities for database authenticated users, data dictionary protection, flexible auditing, views, stored procedures and triggers for enhanced access control and alert processing, row-level locking, robust replication and recovery mechanisms and secure distributed database communication including mutual authentication of databases. New security features in Oracle8i include 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.

During this evaluation Oracle8i Release 8.1 will be tested on Microsoft Windows NT and on Sun Solaris, against the Government Database Management System (G.DBMS) protection profile.

Product Type: Database
Assurance Level: EAL4
Supplier: Oracle Corporation
Evaluation Facility: Logica
Certification Status: In Evaluation UK Scheme
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

CA-Open INGRES and Open INGRES/ Enhanced Security Release 1.1

Open INGRES/Enhanced Security 1.1 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 seure system by providing a set of database security functions that cover the areas of identification, DAC, MAC, Accountability, Audit and Object Reuse. These security functions are described in detail in the Security target. When used with an F-C2 operating system, Open INGRES 1.1 provides F-C2 functionality, in applications where there is no requirement for MAC. The product provides support for a variety of decision support and application tools, including OpenINGRES/Replicator, Open ROAD products (such as Vision and Windows4GL) as well as various third generation languages, although these are not under evaluation.

Product Type: Database
Assurance Level: E3
Supplier: Computer Associates
Evaluation Facility: IBM Global Services
Certification Status: Certified P120 February 1999 UK Scheme
Point of Contact: Adian Oldfield
Telephone: 01753 679819
Fax: 01753 825464

Commercially Available Products

Oracle7 and Trusted Oracle7 Release 7.0.13.6

Product Type: Database
Assurance Level: E3
Supplier: Oracle Corporation
Evaluation Facility: Logica
Certification Status: Certificate 94/33
September 1994
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

Oracle7 is a Relational Database Management System Server and Trusted Oracle7 is a multi-level secure version of it.

Oracle7, in conjunction with an underlying operating system of functionality ITSEC F-C2 or greater, can be used to provide the 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.

Trusted Oracle7, in conjunction with an underlying operating system of functionality ITSEC F-B1 or greater, can be used to provide the database security for systems which require F-B1 security funtionality for databases. In addition to the security features listed for Oracle7, the Trusted version also supports Mandatory Access Control and Labelling for the multi-level secure environment.

Trusted Oracle7 Release 7.1.5.9.3

Product Type: Database
Assurance Level: E3
Supplier: Oracle Corporation
Evaluation Facility: EDS
Certification Status: Certificate 98/96
March 1998
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

Trusted Oracle is a multi-level Relational Database Management System. Version 7.1.5.9.3 of this product was evaluated on a version of the Sun Trusted Solaris CMW 1.2 Operating System.

Trusted Oracle7, Release 7.1.5.9.3 in conjunction with an underlying operating system of ITSEC functionality F-B1 or greater, can be used to provide the database security for systems which require F-B1 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 along with Mandatory Access Control for multi-level secure stand-alone and distributed environments.

With Trusted Oracle7, Release 7.1.5.9.3 Oracle is able to offer a secure client/server distributed database environment.

Oracle7 Release 7.2.2.4.13

Oracle7 is a relational database management system (RDBMS), providing advanced security and functionality for multi-user, distributed database environments. Oracle7 supports client/server application, development and systems management as well as on-line transaction processing, decision support and data warehousing architectures.

The advanced security functionality in Oracle7 includes granular privileges for enforcement of least privilege, user-configurable roles for privilege management, flexible auditing, 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. Oracle7, Release 7.2.2.4.13, when used in conjunction with an underlying operating system of ITSEC F-C2 or greater, provides database security for systems that require F-C2 functionality. During this evaluation, Oracle7, Release 7.2.2.4.13, was evaluated on Compaq NT 3.51 build 1057.

Product Type: Database
Assurance Level: E3
Supplier Oracle Corporation
Evaluation Facility: Logica
Certification Status: Certificate 98/94
February 1998
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

Oracle7 Release 7.3.4 on NT 4.0

Oracle7 is a relational database management system (RDBMS), providing advanced security and functionality for multi-user, distributed database environments. Oracle7 supports hundreds of client/server application, development and systems management tools, as well as on-line transaction processing, decision support, and data warehousing architectures.

The advanced security functionality in Oracle7 includes granular privileges for enforcement of least privilege, user-configurable roles for privilege management, flexible auditing, 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.

Oracle7, Release 7.3, when used in conjunction with an underlying operating system of ITSEC F-C2 or greater, provides database security for systems that require F-C2 functionality. During this evaluation, Oracle7, Release 7.3.4 was evaluated on Microsoft Windows NT 4.0 using Compaq hardware.

Product Type: Database
Assurance Level: E3
Supplier: Oracle Corporation
Evaluation Facility: Logica
Certification Status: Certificate P109
December 1998
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

Commercially Available Products

Oracle7 Release 7.2.2.4.13

Product Type: Database
Assurance Level: EAL4
Supplier: Oracle Corporation
Evaluation Facility: Logica
Certification Status: Certificate P103 September 1998
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9245007
email: djharris@uk.oracle.com

Oracle7 is a relational database management system (RDBMS), providing advanced security and functionality for multi-user, distributed database environments. Oracle7 supports hundreds of client/server application, development and systems management tools, as well as on-line transaction processing, decision support, and data warehousing architectures.

The advanced security functionality in Oracle7 includes granular privileges for enforcement of least privilege, user-configurable roles for privilege management, flexible auditing, 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.

Oracle7, Release 7.2.2.4.13 when used in conjunction with an underlying 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 Common Criteria - Commercial Database Protection Profile, on Microsoft Windows NT 3.51,on Intel platforms.

Trusted Oracle7 Release 7.2.3.0.4

Product Type: Database
Assurance Level: E3
Supplier: Oracle Corporation
Evaluation Facility: Logica
Certification Status: Certificate P124 July 1999
Point of Contact: Duncan Harris
Telephone: 0118 9246201
Fax: 0118 9247400
email: djharris@uk.oracle.com

Trusted Oracle7 is a multilevel secure Relational Database Management System, providing all the features of Oracle7, with the added functionality of mandatory access control and labelling.

With Trusted Oracle7, Release 7.2, Oracle is able to offer all the advanced security functionality of Oracle7, Release 7.2 including granular privileges for enforcement of least privilege, user-configurable roles for privilege management, flexible auditing, 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.

In addition, Trusted Oracle7 provides a full set of multilevel security functionality including flexible label management and policy enforcement, multiple security architectures, and information flow and dissemination control. Trusted Oracle7, in conjunction with an underlying operating system of ITSEC functionality F-B1 or greater, can be used to provide the database security for systems which require F-B1 security functionality for databases.

Trusted Oracle7, Release 7.2, was evaluated on HP-UX CMW 10.16.

COMMERCIALLY AVAILABLE

Multiple Logical Processor Facility Version 3.3.0

The Hitachi Data Systems Multiple Logical Processor Facility (MLPF), version 3.3.0 logically partitions a single hardware platform with respect to several operating systems. This provides the ability to define and allocate 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 the operating systems in other logical partitions. Information in logical partition is not directly or indirectly accessible to other logical partitions unless sharing is deliberately set by users. This means that a user on the operating system of a logical partition is not aware of other operating systems on other logical partitions. Logical partitions also increase system efficiency, through time and resource sharing.

Product Type: Miscellaneous
Assurance Level: E3
Supplier: Hitachi Data Systems
Evaluation Facility: Logica
Certification Status: Certificate P116 March 1999
Point of Contact: Nelson King
Telephone: +1 408 970 7583
Fax: +1 408 988 8601
e-mail:nelson.king@hds.com

Entrust 5.0

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

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

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

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

Entrust/RA is an administrative interface to an Entrust public-key infrastructure. Primary uses for Entrust/RA include: adding and deleting users, revoking certificates and initiating key recovery operations.

Security officers, Administrators, and other Entrust/RA Roles connecting to Entrust/Authority authenticate themselves using digital signatures. Once complete, all messages between Entrust/RA and Entrust/Authority are then secured for confidentiality, integrity and authentication. Cryptographic operations for Entrust/RA and Entrust/Authority are performed on the FIPS 140-1 (Level2)-validated Entrust Security kenel 5.0 cryptographic module or optional hardware cryptographic module, although these are not included in the Common Criteria evaluation.

Product Type: Miscellaneous
Assurance Level: EAL3 Augmented
Supplier: Entrust Technologies Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate P141 March 2000
Point of Contact: Darryl Stal
Telephone: +1 613 247 3483
Fax: +1 613 247 3450

Commercially Available Products

Entrust/Admin 4.0
Entrust/Authority 4.0

Product Type: Miscellaneous
Assurance Level: EAL3 Augmented
Supplier: Entrust Technologies Limited
Evaluation Facility: Syntegra
Certification Status: Certificate P122 March 1999
Point of Contact: Marc Laroche
Telephone: +1 613 247 3446
Fax: +1 613 247 3450
e-mail: marc.laroche@entrust.com
URL: www.entrust.com

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

- creating certificates for all public keys
- creating encryption key pairs for users
- managing a secure database of Entrust information
- enforcing an organisation's security policy

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

- ability to interoperate with other Entrust CAs or with other vendors' CA products
- use of flexible certificates (to include any extensions in the X.509v3 standard)
- ability to change the distribution of setup information to users
- use of flexible password rules
- ability to specify either RSA or DSA as the CA signing algorithm

Entrust/Admin is an administrative interface to an Entrust public-key infrastructure. Primary uses include:- adding and deleting users, revoking certificates and performing key recovery operations.

Security Officers and Administrators connecting to Entrust/Authority authenticate themselves using digital signatures. Once complete, all messages between Entrust/Admin and Entrust/Authority are then secured for confidentiality, integrity, and authentication. Cryptographic operations for Entrust/Admin and Entrust/Authority are performed on the FIPS 140-1 validated Entrust Security Kernel 4.0 cryptographic module or optional hardware cryptographic module. Entrust/Admin and Entrust/Authority are currently certified on Microsoft Windows NT 4.0 Service Pack 3. Further evaluation work is planned to extend certification to cover a range of operating system platforms.

BrainTree AUDITOR Plus
Version 1.4-03
revision S

Product Type: Miscellaneous
Assurance Level: E1
Supplier: BrainTree Technology Ltd
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 96/70 October 1996
Point of Contact: Kevin Else
Telephone: 0161 945 1511
Fax: 0161 945 2150
e-mail:info@braintree.co.uk
URL: www.braintree.co.uk

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.

COMMERCIALLY AVAILABLE

MailGuard Bastion 1.0

The MailGuard Bastion is a messaging firewall that allows the exchange of messages between networks of differing security levels or differing security policies. MailGuard Bastion operates as a stand-alone system providing a bi-directional messaging firewall for both X.400 and SMTP/MIME e-mail traffic.

MailGuard Bastion is based upon the Trusted Solaris operating system (itself assured to ITSEC E3/F-B1 and E3/F-C2) and is provided as a turnkey system utilising Sun SPARC hardware.

Messages that need to pass between the networks connected by MailGuard Bastion may only flow through the trusted processes of the application and labelled operating system. No other forms of communication are permitted between the networks, thus providing assurance of network selection.

MailGuard Bastion maintains separate channels for message flow between networks allowing different policies to be applied in each direction, to the extent that all message traffic can be blocked in one direction. An audit trail of all message traffic is maintained.

MailGuard Bastion offers a protected environment (or DMZ) into which modules can be introduced to perform specific inspection and filtering, filtering based on sensitivity labels or digital signature verification. The architecture MGB ensures that these modules cannot be modified or by passed without authorisation. Please note that any functionality provided by these modules is outside of the scope of this evaluation.

Product Type: Networking
Assurance Level: E3
Supplier: NET-TEL Computer Systems
Evaluation Facility: Admiral
Certification Status: In Evaluation
UK Scheme
Point of Contact: Nick Ward
Telephone: +44 1582 830500
Fax: +44 1582 830501
e-mail:nick.ward@net-tel.co.uk

Safegate Version 2.0.2

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

Product Type: Firewall
Assurance Level: EAL3
Supplier: Fujitsu Ltd
Evaluation Facility: EDS
Certification Status: Certificate March 2000
Point of Contact: Takehiko Yahagi
Telephone: +81 44 370 7695
Fax: +81 44 370 7737

Commercially Available Products

CISCO Secure PIX Firewall

Product Type: Networking
Assurance Level: EAL4
Supplier: CISCO
Evaluation Facility: Syntegra
Certification Status: In Evaluation UK Scheme
Point of Contact: Paul King
Telephone: 44 (0) 181 756 8349
Fax: 44 (0) 181 756 8099

The Cisco Secure PIX Firewall is the dedicated firewall appliance in Cisco's firewall family. The Cisco Secure PIX Firewall delivers strong security without impacting network performance. the product line scales to meet a range of customer requirements, and has three licence levels. The Cisco Secure PIX Firewall is the leading product in its segment of the firewall market. The Cisco Secure PIX Firewall provides full firewall protection that completely conceals the architecture of an internal network from the outside world.

The Cisco Secure PIX Firewall is a dedicated appliance running its own real-time operating system on the PIX515, PIX520, and PIX525 hardware platform with a dedicated link to an audit workstation/server and an optional AAA authentication server. As there is no underlying operating system such as NT or UNIX the PIX Firewwall can support over 250,000 concurrent sessions and data rates in excess of 160Mbps. It is a stateful packet filtering firewall which controls the flow of IP traffic between two networks by matching information contained in the headers of connection-oriented or connectionless IP packets against a set of rules specified by the firewall's administrator. This header information includes source of destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection. Services permitted through the firewall may include Finger, DNS, HTTP, FTP, Telnet, Echo, POP3 and NNTP.

Tracker 2650 Data Collection Unit

Product Type: Networking
Assurance Level: E2
Supplier: Data Track Technology plc
Evaluation Facility: Logica
Certification Status: Certificate P133 UK Scheme
Point of Contact: Mike Terry
Telephone: 01425 270333
Fax: 01425 271978
e-mail: mterry@dtrack.demon.co.uk
www.dtrack.demon.co.uk

The Data Track Technology Tracker 2650 is a solid state data buffer device, designed to log data into internal solid state memory. It receives information on data ports, or digital inputs; reliably store this data in internal buffers until requested to pass the information out; and generates alarms and trigger a dial out based on the information received.

The Tracker 2650 supports either one or two serial control interfaces. Two slots can be fitted with PC compatible ISA bus cards that can be configured as COM 1 or COM 2 and used for the remote operation and management of the unit. Typically one modem and one serial card are fitted, however, it is not necessary to utilise both slots and equallly two modems or two serial ports are supported.

The unit has four RS232 data ports, (Port 1 to Port 4) for the collection of data and for two-way communication with the data source. Each data port can be configured to have its own data storage area allocated from up to 32 Megabytes of RAM. Additionally, the digital port can handle 16 digital (relay) inputs all of which can be configured to trigger alarms, and a further 7 digital outputs. Connections to the digital ports are made through a female 25 pin D-type connector.

When configured as part of a communications network management system, the device prevents subscribers on a switch from gaining access to the remote management system and thus provides an assured separation between such subscribers and management traffic. It can also protect the switch from unauthorised access when used to replace diagnostic modems connected to the PSTN.

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

Banyan VINES Version 7.0

VINES is a network operating system, that integrates diverse sites, servers, users and network applications into one manageable system. A distributed directory with automatic synchronisation, StreetTalk, and the VINES Security Service, provide a global naming structure and access control for all users, services and objects on the network. The network services that can run under VINES, using all the global directory and security functions include network file, print and message handling services, plus application specific services. APIs are available in the VINES Application Toolkit to allow network systems controllers or third party applications suppliers to build in their own services using the directory and security facilities.

The VINES product is supplied as a plug-in network server on a dedicated UNIX platform with the NOS installed. The product supplies configurable security functionality meeting the ITSEC example Functionality Class F-C2. The security components include Discretionary Access Control, Identification and Authentication and Audit and Accountability.

Product Type: Networking
Assurance Level: E2
Supplier: Banyan Systems Incorporated
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 97/79 April 1997
Point of Contact: Robert Dees
Telephone: 01293 612284
Fax: 01293 612288
e-mail: rdees@banyan.com

Check Point FireWall-1 Version 4.0

Check Point FireWall-1 is a network security solution for Internet, intranet and extranets. FireWall-1 is a comprehensive software application suite that integrates access control, authentication, encryption, network address translation, content security, auditing and connection control. The suite is unified by Check Point's OPSEC policy management framework, which provides integration and enterprise management for FireWall-1 and many third-party network security applications. FireWall-1 supports hundreds of services, applications and protocols.

Firewall-1 uses Stateful Inspection technology, invented by Check Point, and now the standard in network security technology. It provides full application-layer awareness to deliver the highest level of security and because it does not require a separate proxy for every service to be secured, customers experience higher performance, scalability and the ability to support new and custom applications more quickly than with older architectures.

The core functionality of Firewall-1 (ie Stateful Inspection, the Command Line Interface, address translation and auditing) was evaluated on the following platforms: Microsoft NT Version 4.0 with Service Pack 3; Solaris Version 2.6; AIX Version 4.2.1 and HP-UX Version 10.10. The evaluation excluded the facilities for Graphical User Interface, authentication, encryption and the security server. The GUI, Remote Management, LDAP client interface, and VPN facility used to establish a secure communications channel between two Firewall-1 firewalls are among the subjects of a new evaluation which started in August 1999.

Product Type: Networking
Assurance Level: E3
Supplier: Check Point Software Technologies Ltd
Evaluation Facility: Admiral Management Services
Certification Status: Certificate P107 March 1999
Point of Contact: Nigel Mould
Telephone: +44(0) 1233 713611
Fax: +44(0) 1233 236847

Commercially Available Products

CyberGuard Firewall Version 2.2.1e

Product Type: Networking
Assurance Level: E3
Supplier: CyberGuard Europe Ltd
Evaluation Facility: Logica
Certification Status: Certificate 97/78 March 1997
Point of Contact: Andrew Clarke
Telephone: +44 (0) 1344 382550
Fax: +44 (0) 1344 382551
URL www.cyberguard.com
e-mail:aclarke@cyberguard.co.uk

CyberGuard Firewall is a network security product which 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 a secure operating system and networking products, originally evaluated to NCSC B1 and now subject to the NCSC Ratings Maintenance Programme (RAMP). 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.

Evaluated features include: Network Application Proxies (Telnet, FTP, SMTP, HTTP, NNTP); Network Packet Filtering; Support for TCP/IP, UDP, ICMP and other protocols; Network Address Translation (NAT); Split Domain Name System (DNS); Address/Machine name masking; Alarms on suspicious activities; Multiple Network Interfaces; Easy-to-use Graphical User Interface (GUI) administration facility.

The GUI provides the means to specify and load filtering rules; display current configuration and status; display firewall statistics; perform auditing and set alarms which notify an administrator of specific network events.

CyberGuard Firewall was evaluated on NH 4000 and NH 5000 platforms. CyberGuard Firewall 2.2.1e has full membership of CMS; the latest CMS approved version is CyberGuard Firewall 2.2.3r9.

Gauntlet Firewall V3.01 for Windows NT, Build 113

Product Type: Networking
Assurance Level: E3
Supplier: Network Associates Ltd
Evaluation Facility: EDS
Certification status: Certificate P127 June 1999
Point of contact: Government Sales
Telephone: +44(0) 1753 827500

Gauntlet® Firewall v3.01 for Windows NT combines a very secure method of firewall protection - an application gateway - with important features including user transparency, integrated management, strong encryption interfaces and content security for the popular NT Server 4.0 platform (with service pack 4 or later together with the nprpcfxi.exe.hotfix). Application proxies protect both in-bound and out-bound services, supporting high throughput and the latest web-based technologies without sacrificing security. The Gauntlet Firewall v3.01 for Windows NT is a hardware and software-based application gateway firewall that supports only those services specifically configured by the Firewall administrator, and only those that can be implemented securely. Features such as Win32 GUI, support for popular authentication services and a network management capability enable organisations worldwide to reap the benefits of using the internet, intranets and extranets securely for their global business needs.

The product may be configured as a dual-homed bastion host or as a multi-homed bastion host between 2 or 3 networks. Evaluated security functions include: Prevention of internal IP address spoofing; Comprehensive auditing and accounting functions; Packet level filtering; SMTP, telnet, HTTP, ftp, SQL*net, POP3, NNTP, LDAP and PLUG proxies; Interfaces to Strong User Authentication mechanisms; Configurable option to prevent JAVA applets, JAVA scripts, ActiveX, multi-part forms, non html2 and frames; Network Address Translation; Local administration using Win32 GUI. The evaluated configuration includes a range of single or dual Pentium II processor based PCs and network interface cards (as defined in the Windows NT 4.0 Hardware Compatability List).

CyberGuard Firewall for UnixWare 4.1

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 16) provide DMZ or further internal/external network connections.

The firewall runs on either single or multi-processor Intel Pentium Pro or Pentium II servers with UnixWare 2.1.3.

Evaluated security features include:

- Connection level Access Control for IP packets e.g. permit/deny source & destination addresses or ports, divert IP packets to a proxy process (FTP, HTTP, SMTP, NNTP, TELNET)
- Accounting, auditing and statistics of firewall traffic and security related events
- Alerts (e.g. log-file, e-mail, SNMP traps) for security events
- Network address translation facility for networks and hosts
- Split Domain Name Server (DNS)

The evaluated configuration has passed Y2K testing of security functionality within the scope of the evaluation.

The firewall relies on unevaluated functionality provided by the Unix operating system to perform identification and authorisation of the FTP and TELNET proxies. The auditing perfomed by the firewall is an extension of the UnixWare® auditing subsystem. CyberGuard Firewall for UnixWare 4.1 has full membership of CMS, the latest version being 4.2.

Product Type: Networking
Assurance Level: E3
Supplier: CyberGuard Europe Ltd
Evaluation Facility: Logica
Certification status: Certified P117 January 1999 UK Scheme
Point of contact: Andrew Clarke
Telephone: +44 (0) 1344 382550
Fax: +44 (0) 1344 382551
email: aclarke@cyberguard.co.uk
www:cyberguard.com

CyberGuard Firewall for Windows NT 4.1

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. Free evaluation copies are available upon request.

Evaluated security features include:

- Connection level Access Control for IP packets e.g. permit/deny source and destination addresses or ports, divert IP packets to a proxy process (FTP, HTTP, SMTP, NNTP, TELNET)
- Accounting, auditing and statistics of firewall traffic and security related events
- Alerts (e.g. log-file, e-mail, SNMP traps) for security events
- Network address translation facility for networks and hosts

The evaluated configuration has passed Y2K testing of Security Functionality within the scope of the evaluation.

CyberGuard Firewall for Windows NT 4.1 has full membership of CMS, the latest version being 4.2

Product Type: Networking
Assurance Level: E3
Supplier: CyberGuard Europe Ltd
Evaluation Facility: Logica
Certification status: Certified P118 January 1999 UK Scheme
Point of contact: Andrew Clarke
Telephone: +44 (0) 1344 382550
Fax: +44 (0) 1344 382551
email: aclarke@cyberguard.co.uk
www.cyberguard.com

Commercially Available Products

BorderWare Version 6.1.1 Firewall Server

Product Type: Networking
Assurance Level: EAL4
Supplier: BorderWare Technologies Inc
Evaluation Facility: Syntegra
Certification status: Certified P136 January 2000 UK Scheme
Point of contact: Peter Cox
Telephone: +44 181 893 6066
Fax: +44 181 574 8384

The BorderWare Firewall Server (BFS) is an application proxy Firewall designed to combine robust security with the complete set of ancillary services necessary to implement an Internet connection or to provide secure Intranet connections. BFS is built on the S-CORE operating system.S-CORE is a hardened operating system that has been specifically designed by BorderWare Technologies Inc and is derived from BSD 4.4 Unix. S-CORE has had all non essential functions removed and is further optimised for security and throughput. The purpose-designed operating system provides a separate domain of execution for each critical subsystem and implements kernel-level packet filtering to compliment the application proxies and application servers. The proxies manage connections for all commonly used TCP/IP applications. The servers provide facilities such as DNS and mail relay. BFS provides dual Domain Name Servers, which together with Network Address Translation, ensure complete separation between internal and external networks. The mail relay service protects e-mail servers by allowing mail despatch and delivery without ever permitting a connection between a protected mail server and the untrusted network.

The BFS operating system does not permit any user logins, all configuration and administration is carried out on a console GUI or from a secure remote management application. All connections to the administration system are authenticated. BFS provides an audit trail for all connections and generates alarms for unsuccessful connection attempts.

BFS runs on a standard intel hardware and needs two or three network cards. The optional 3rd interface provides a Secure Server Network or SSN for connecting application servers.

The EAL4 certification awarded to the BorderWare Firewall Server includes the S-CORE operating system, all application servers, all system defined outbound application proxies and the remote management capability when used from the protected network.

Guardian PRO Version 5.0

Product Type: Networking
Assurance Level: EAL4
Supplier: NetGuard Ltd
Evaluation Facility: Syntegra
Certification Status: In Evaluation UK Scheme
Point of Contact: Tim Alberry
Telephone: +44 (0) 1628 533 433
Fax:
Email: tim@netguard.co.uk
www.netguard.co.uk

NetGuard Ltd, is a leading provider of enterprise-class network security and privacy solutions, provides GuardianPRO, a native Windows/NT/2000-based firewall solution that secures corporate headquarters for small and medium-sized businesses.

GuardianPRO delivers the utmost in security and connectivity in one simple, easily supported package that includes bandwidth management, IPSec VPN, Network Address Translation and Authentication. GuardianPRO is endowed with features ranging from the market's only real-time performance monitoring and reporting facility (RPM) to Media Access Control-Layer Stateful Inspection, while maintaining ease of installation and dedication to high quality customer support.

The fundamental functionality of GuardianPRO is to be evaluated on Intel Pentium II 350MHz computers with Windows/NT Workstation or Windows/NT Server 4.0 and service pack 3 with Y2K patches applied. The evaluation excludes the facilities for authentication, VPN, NAT, RPM and Bandwidth Management. The evaluated configuration will test GuardianPRO's capability to restrict any traffic between 2 networks. The features in evaluation include: access control; local administrator authentication; real-time monitoring of suspicious events; alert generation or suspension of session; auditing and connection control.

NetGuard intends to annually maintain CC EAL4 certification.

VCS FIREWALL Version 3.0

The VCS FIREWALL manages data communications between trusted and untrusted networks. It supports four independent networks and can manage simultaneously traffic between all pairs of networks. For example a common implementation is a general office network, a secure internal network, and an Internet connection, with the fourth network available for expansion.

The VCS FIREWALL is proxy-based and includes proxies for HTTP, Telnet, FTP and Mail Exchange. There is a Generic proxy for all other proxiable protocols. Packet filtering of TCP, UDP and ICMP is also supplied.

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

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

Product Type: Networking
Assurance Level: EAL1
Supplier: The Knowledge Group
Evaluation Facility: IBM Global Services
Certification Status: Certificate P123 March 1999
Point of Contact: Alan Jones
Telephone: 0117 900 7500
Fax: 0117 900 7501
Email: sales@ktgroup.co.uk

Remote Management Centre

IBM Remote Management Centre provides a focal point for the service offerings of Remote Network Management, Remote Systems Management and Remote Environmental Monitoring

The security of the unit allows multiple customers to be securely 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 the 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 to ensure the security. The individual customers monitoring stations integrate into this secure environment allowing the display of individual alarms on a centralised videowall.

Product Type: Networking
Assurance Level: E1
Supplier: IBM
Evaluation Facility: Admiral Management Services
Certification Status: In Evaluation Since September 1999
Point of Contact: David Dawson
Telephone: 01932 814979
Fax: 01932 814982

Commercially Available Products

DXE Router

Product Type: Networking
Assurance Level: E3
Supplier: StorageTek Network Systems Group
Evaluation Facility: Logica
Certification Status: Certificate P113 February 1999
Point of Contact: Sean Walsh
Telephone: 01483 737433
Fax: 01483 737463

The StorageTek Network Systems Group DXE router provides access mediation between datagrams and networks. The mediation is based upon mandatory (label-based) access controls and discretionary (identity-based) access filters.

The discretionary access control is performed on the basis of any information contained in the protocol header (source/destination address, port number etc) or in the datagram payload.

Any attempted mandatory or discretionary access violations are audited, with the audit data being forwarded to the administrative console, or optionally to an external audit host. Administrative actions include the setting up or altering of configuration data performing diagnostics etc.

The network interfaces supported by the DXE Router includes Synchronous link (9.6kbps up to 52Mbps), HSSI, FDDI, Ethernet, Token Ring, IBM, Channel and HIPPI.

SCO UnixWare 2.1.0 on Fujitsu-ICL C530i and G550i Teamservers with consoles

Product Type: Operating System
Assurance Level: E2
Supplier: SCO
Evaluation Facility: EDS
Certification Status: Certificate P119 February 1999
Point of Contact: Jon Coyle
Telephone: 01923 813656
Fax: 01923 813804
email: jonco@sco.com
URL: http://www.sco.com

SCO UnixWare2.1 is a UNIX operating system with functionality designed to exceed ITSEC F-C2. SCO UnixWare2.1 provides the following functions:

- Discretionary Access Control
- Audit
- Identification and Authentication
- Access Control Lists

SCO UnixWare2.1 was evaluated on Fujitsu-ICL's industry standard Intel architecture platforms (the I-series teamservers).

COMMERCIALLY AVAILABLE

SCO CMW+ is a complete line of trusted workstation, server and development environment based on SCO Open Desktop/Open Server 3.0 with CMW+ security enhancements and MaxSix secure networking software. SCO CMW+ is a multi-level, multi-user, multi-tasking operating system that runs on 386/486/Pentium platforms. It is designed to meet and exceed the functionality requirements of the pre-defined ITSEC F-B1 functionality class.

SCO CMW+ provides the following functions:

- Mandatory Access Control
- Discretionary Access Control
- Least Privilege
- Audit
- Data Interchange (import/export)
- Trusted Administrative Roles
- Identification and Authentication
    - Trusted Recovery
    - Access Control Lists
    - Trusted Window System (trusted path)

SCO CMW+ Release 3.0.1 running on Elonex PC590/1, Elonex PC575/1 and Unisys SMP 5400 workstations

Product Type: Operating System
Assurance Level: E3
Supplier: SCO
Evaluation Facility: EDS
Certification Status: Certificate P131 September 1999
Point of Contact: Jon Coyle
Telephone: 01923 813656
Fax: 01923 813804
email:jonco@sco.com
URL: http://www.sco.co

MAXION/OS is Concurrent's standard real-time commercial operating system that runs on the MAXION range of symmetric multiprocessor computers.
MAXION/OS is based on Novell/USG System V release 4.2MP UNIX with the addition of a resilient file system. It supports both single and multiprocessor stand alone MAXION configurations. Security features, derived from Concurrent's F-B2 version of the MAXION/OS operating system have been added to make standard MAXION/OS F-C2 compliant as have extensions to provide deterministic real-time capabilities in line with the POSIX 1003.1b and 1003.1c real-time and threads extensions.

MAXION/OS Version 1.2

Product Type: Operating System
Assurance Level: E3
Supplier: Concurrent Computer Corporation Ltd
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 96/67 December 1996
Point of Contact: Mike Baker/Philip Martin
Telephone: 01753 513413
Fax: 01753 513218

Commercially Available Products

BEST-X/B1 (Bull Enhanced Security Technology) Version 1.1.1.9

BEST-X/B1(Bull Enhanced Security Technology) is a secure system evaluated to ITSEC E3, F-B1 (using a stand alone system with dumb terminals).

BEST-X/B1 is derived from and compliant with the AIX operating system and provides support for the latest hardware platforms including BULL DPX/20 and ESCALA multi-processor machines.

BEST-X/B1 provides support for Mandatory Access Control Policy, Multi-Level Directories, Labelled Printing, Labelled Import/Export Tools, Password Encryption and Generation module interfaces and Extended Audit, over and above the standard AIX Identification and Authentication, DAC, Accounting and Auditing features. BEST-X/B1 is harmonised with unlabelled AIX communications.

Product Type: Operating System
Assurance Level: E3
Supplier: Bull S.A.
Evaluation Facility: EDS
Certification Status: Certificate 97/81
April 1997
Point of Contact: Son Ho-Dung/
Jean-Paul Du Bourreau
Telephone: 33 4 76 29 76 86
Fax: 33 4 76 29 78 62
email: son.ho.dung@bull.met

BEST-X/C2 (Bull Enhanced Security Technology) Version 1.1.1.9

BEST-X/C2 (Bull Enhanced Security Technology) is a secure system evaluated to ITSEC E3, F-C2 (using a stand alone system with dumb terminals).

BEST-X is derived from and compliant with the AIX operating system and provides support for the latest hardware platforms, including Bull DPX/20 and ESCALA multi processor machines.

BEST-X provides support for Password Encryption and Generation module interfaces and Extended Audit, over and above the standard AIX Identification and Authentication, DAC, Accounting and Auditing features.

Product Type: Operating System
Assurance Level: E3
Supplier: Bull S.A.
Evaluation Facility: EDS
Certification Status: Certificate 97/83
June 1997
Point of Contact: Son Ho-Dung/
Jean-Paul Du Bourreau
Telephone: 33 4 76 29 76 86
Fax: 33 4 76 29 78 62
email: son.ho.dung@bull.met

Argus Systems Group Release 1.3 of the C2/TMW and B1/CMW for Solaris 2.4 on a range of SPARC and Intel platforms

Product type: Operating System
Assurance Level: E3
Supplier: Argus Systems Group, Inc
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 98/89 September 1999
Point of Contact: Paul McNabb
Telephone: 001 217 355 6308
Fax: 001 217 355 1433

The Argus Trusted Mode Workstation C2/TMW and Compartmented Mode Workstation B1/CMW Release 1.3 offer additional security features to Release 1.2 and build upon commercial Solaris 2.4 in compliance with US DoD criteria classes C2 and B1.

The C2/TMW and B1/CMW include a common set of security features including discretionary information labels, a trusted path, labelled printing, least privilege, TSIX(RE) 1.1 compliant networking, and support for site defined password generation and encryption algorithms. C2/TMW and B1/CMW also support WABI on all platforms, allowing execution of Microsoft Windows applications such as Microsoft Office under the control of the trusted computing base.

The C2/TMW and B1/CMW product suites are available on certain vendor implementations of the SPARC and Intel architectures supported by the Sun Solaris 2.4 operating system, including symmetric multi processor implementations.

Argus C2/TMW and B1/CMW release 1.3 have entered ITSEC evaluation for certification to ITSEC F-C2 and ITSEC F-B1 respectively, with E3 assurance. These operating systems were evaluated in the multi-user mode on specific Pentium and Sparc stations, platforms, networked configuration including Argus Trusted Desktop Environment, Argus Secure Networking and Argus Trusted Windows including WABI Version 2.2.

The evaluated configuration excludes NIS, NFS, TNFS, Decaf, VSLAN6 Interface, XQM and Superuser Emulation Mode. The firmware boot protection mechanisms of the underlying platforms have not been evaluated.

Argus Systems Group Release 1.2 of the B1/CMW and C2/TMW for Solaris 2.4 on Specified SPARCstation, IntelX86 and Pentium Platforms

Product Type: Operating System
Assurance Level: E3
Supplier: Argus Systems Group, Inc
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 96/73 December 1996
Point of Contact: Paul McNabb
Telephone: 001 217 355 6308
Fax: 001 217 355 1433
email: info@argus-systems.com
www.argus-systems.com

Argus enhanced security products for Solaris 2.4 build upon the commercial Sun Soft Solaris 2.4 operating system kernel and utilities, OpenWindows, and ONC+ networking. Commercial Solaris 2.4 operating systems upgraded with Argus enhanced security products deliver enhanced security features and assurances with 100% compatability with the standard Solaris 2.4 API and application software.

The Argus B1 Compartmented Mode Workstation (B1/CMW) enables Solaris 2.4 users to process information at multiple sensitivity levels on a single workstation and is designed to meet the US DOD criteria for B1 security as well as additional US DIA CMW security requirements. The Argus C2 Trusted Mode Workstation (C2/TMW) offers enhanced C2 security and the same trusted X windows used with the B1/CMW. This combination extends commercial Solaris 2.4 C2 security to the OpenWindows environment providing Solaris 2.4 users with a single-level windowed workstation with C2 security including optional discretionary information labels on windows, files and processes and a trusted path for security relevant operations. Argus C2/TMW and B1/CMW provide full enhanced security support for WABI, and enhanced security support for Microsoft Windows applications when installed with Argus Trusted Windows.

The C2/TMW and B1/CMW products were evaluated to ITSEC F-C2 and ITSEC F-B1 respectively, in the multi-user mode, with the following components excluded: NIS, NFS, telnet, RPC, xdm, rlogin, ftp, mail, TNFS, Superuser emulation mode.

The firmware boot protection mechanisms of the underlying platforms have not been evaluated.

Commercially Available Products

Sequent DYNIX/ptx Unix Version 4.1 SLS and 4.1a SLS on Symmetry 5000 Systems (Models SE30 and SE70)

Product Type: Operating System
Assurance Level: E3
Supplier: Sequent Computer Systems Ltd
Evaluation Facility: Logica
Certification Status: Certificate 97/74
February 1997
Point of Contact: Valerie Ashton
Telephone: 01932 851111
Fax: 01932 850011
email: valeriea@sequent.com

DYNIX/ptx is a secure Operating System certified to E3 F-C2. DYNIX/ptx is Sequent's enhanced version of Unix for the Symmetry series of symmetric multiprocessing systems. DYNIX/ptx is a robust and reliable implementation of Unix for secure commercial SMP systems 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. DYNIX/ptx includes specific support for mission critical 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 CESG FIRESTONE, THUNDERBOLT and THUNDERFLASH password encryption and generation packages. Sequent DYNIX/ptx Unix Versions 4.1 SLS and 4.1a SLS on Symmetry 5000 Systems (Models SE30 and SE70) has full membership of CMS.

Sequent DYNIX/ptx Version 4.4.2 running on Symmetry 5000 Systems and NUMA-Q 2000

Product Type: Operating System
Assurance Level: E3
Supplier: Sequent Computer Systems Ltd
Evaluation Facility: Logica
Certification Status: Certificate P108 v2
January 2000
Point of Contact: Valerie Ashton
Telephone: 01932 851111
Fax: 01932 850011
email: valeriea@sequent.com

DYNIX/ptx Version 4.4.2 (with CESG algorithms) running on Symmetry 5000 Systems (Model SE40) and NUMA-Q (Non Uniform Memory Access) 2000 (with EMC² Symmetrix 3430/3700 disk arrays) is a secure Operating System evaluated to E3 F-C2. DYNIX/ptx is Sequent's enhanced version of Unix for NUMA-Q 2000 and Symmetry Systems.

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.

DYNIX/ptx includes specific support for mission critical operations with concurrent user populations in the 1000s and disk volumes in excess of 5 Terabytes. The hardware may be extended by adding more quads/processors with proven linear performance scalability.

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

COMMERCIALLY AVAILABLE

Trusted Solaris 1.2 ITSEC(E) is based on Sun's Solaris 1.1 commercial UNIX operating system. It is designed to meet the requirements of Compartmented Mode Workstations, DoD Class B1 and ITSEC Functionality Class F-B1. It runs on both desktop workstations, diskless workstations and servers. It allows sharing of resources between clients and servers in a trusted, distributed networking environment.

To protect the processing of security-sensitive information, Trusted Solaris 1.2 ITSEC(E) includes the following major components, all of which were evaluated:

- MAC, DAC and information labels
- Least Privilege
- Secure OpenWindows with support for MOTIF and X11
- Secure Networking utilising the MAXSIX and TCP/IP Protocol within a Sun configuration
- Centralised Trusted Facility Management
- Trusted Newsprint
- Diskless Client Support
- Auditing
  - a PostMaster tool which handles multi-level mail.
  - a Password tool for changing a password.

Sun Trusted Solaris Version 1.2 ITSEC(E) running on specified models of SPARCstations 5, 10 and 20

Product Type: Operating System
Assurance Level: E3
Supplier: Sun Microsystems Federal
Evaluation Facility: Logica
Certification Status: Certificate 95/58
November 1995
Point of Contact: Joe Alexander
Telephone: +1 703 204 4202
Fax: +1 703 753 2192
Web: www.sun.com

Solaris 2.4SE is the ITSEC E2/F-C2 certified version of Sun's commercial Solaris 2.4 operating system. The certified configuration includes both workstations and servers sharing information in a distributed networking environment. It is supported on both SPARC and Intel platforms and includes the following features in addition to the ITSEC Functionality Class F-C2:

- Open Windows window System
- Networking using the TCP/IP protocol
- NIS+ Distributed Naming Service
- NFS

Two additional modules may be applied for to meet CESG requirements for password encryption and generation, using the CESG FIRESTONE (MODF) and THUNDERBOLT (MODT) algorithms, (these modules are the subject of a separate report, 95/57).

It is available on all SPARC and industry standard Intel platforms, and complies with ITSEC Functionality Class F-C2.

Sun Solaris Version 2.4SE for a range of SPARC and Intel platforms

Product Type: Operating System
Assurance Level: E2
Supplier: Sun Microsystems Federal
Evaluation Facility: EDS
Certification Status: Certificate 95/56
November 1995
Point of Contact: Joe Alexander
Telephone: +1 703 204 4202
Fax: +1 703 753 2192
Web: www.sun.com

Commercially Available Products

Sun Solaris 2.5.1SE

Product Type: Operating System
Assurance Level: E2
Supplier: Sun Microsystems Federal
Evaluation Facility: Logica
Certification Status: Certificate 98/97
March 1998
Point of Contact: Joe Alexander
Telephone: +1 703 204 4202
Fax: +1 703 753 2192
Web: www.sun.com

Solaris 2.5.1SE is the latest version of Sun's commercial Solaris operating system to have undergone ITSEC evaluation to E2/F-C2. The product was evaluated on the Sun UltraSPARC-1 Workstation and servers sharing information in a distributed networking environment. The evaluation included 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

Two patches which have been certified must be included in order for the product to maintain its certified status. Refer to the Sun Security Bulletins #168, #169 and associated patches 104220-03, 104490-05.

Sun Solaris 2.6SE

Product Type: Operating System
Assurance Level : E3
Supplier: Sun Microsystems, Inc.
Evaluation Facility: Logica
Certification Status: Certificate P101
January 1999
Point of Contact: Don Hunter
Telephone: +1 650 786 7379
Fax: +1 650 786 5731
Web: www.sun.com

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.

COMMERCIALLY AVAILABLE

Sun Trusted Solaris Version 2.5.1

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 numerous defence and commercial customer requirements for secure computing, including:

- ITSEC E3/F-B1 multi-level functionality with trusted networking and trusted windowing; and
- ITSEC E3/F-C2 functionality, including the use of access control lists and trusted advisory labelling.

Trusted Solaris 2.5.1 was evaluated on the Sun UltraSPARC-1 workstation and servers sharing information in a distributed networking environment. Sun intend that it will subsequently be evaluated on a wide range of Sun platforms, from uni-processor MicroSPARC desktop workstations, to multi-processor UltraSPARC Enterprise servers, using the Certificate Maintenance Scheme.

Trusted Solaris 2.5.1 includes the following major facilities, which are all 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 MAXSIX protocols
- Trusted NFS - Auditing - Multi-level mail
- Trusted Solaris 2.5.1 has full membership of CMS.

Product Type: Operating System
Assurance Level: E3
Supplier: Sun Microsystems Federal
Evaluation Facility: Logica
Certification Status: Certificate P104 September 1998
Point of Contact: Joe Alexander
Telephone: 703 204 4202
Fax: 703 753 2192
Web: www.sun.com

VME Operating System with High Security Option, Version SV294, running on Series 39 Processors

VME with the High Security Option (HSO) is a secure operating system for the ICL Series 39 mainframe computers. This version of the product is updated from the SV291 release, which was the subject of Computer Security Product Evaluation Certificate No 92/22.

The HSO Security Target claims compliance with the ITSEC Functionality Class F-B1. This version offers additional security features beyond the requirements of F-B1 and TCSEC B1, which are:

- implementation of a Mandatory Integrity Policy based on integrity markings
- import of data on magnetic media
- page totals of spooled output
- audited regrading of objects
- variable run-time clearance
- authentication assurance (including password expiry and terminal lockout)

Product Type: Operating System
Assurance Level: E3
Supplier: International Computers Ltd (ICL)
Evaluation Facility: Logica
Certification Status: Certificate 94/38 September 1994
Point of Contact: Bryn Bircher
Telephone: 0161 230 5525
Fax: 0161 230 5957
email: bryn.bircher@icl.com
URL: www.icl.com

Commercially Available Products

Microsoft Windows NT Workstation and Windows NT Server Version 4.0

Product Type: Operating System
Assurance Level: E3
Supplier: Microsoft Ltd
Evaluation Facility: Logica
Certification Status: Certificate P121 March 1999
Point of Contact: Peter Birch
Telephone: 0870 60 10 100
Fax: 0870 60 20 100
e-mail: peterbir@microsoft.com

Windows NT is a multi-tasking operating system for controlling and managing networks of computers and electronic resources in a distributed multi-user environment. Trusted log on for user authentication, DAC of electronic resources, accounting and audit of user activities, and controlling system policies and user profiles in arbitrary network configurations, including interconnection of trusted domains, have been evaluated.

The evaluated Windows NT 4.0 SP3 security enforcing functions specified in its Security Target provide the essential evaluating basis on which other specialised security enforcing functions of evaluatable systems such as messaging, electronic business, firewall, virtual private network, and PKI related systems could depend. Microsoft are participating in the development of Common Criteria Protection Profiles of such systems.

Additional Microsoft products such as Exchange Server, System Management Server, Outlook and Office Clients, Remote Access Services and the Clipbook Viewer are excluded from the Target of Evaluation (TOE). Domain based security functionality is included to the transport driver interface; underlying network protocols are also excluded from the evaluation.

Microsoft Windows NT Workstation and Windows NT Server Version 3.51

Product Type: Operating System
Assurance Level: E3
Supplier: Microsoft Ltd
Evaluation Facility: EDS
Certification Status: Certificate 96/71 October 1996
Point of Contact: Peter Birch
Telephone: 0870 60 10 100
Fax: 0870 60 20 100
e-mail: peterbir@microsoft.com

WINDOWS NT is a multi-user, multi-platform client-server operating system which combines highly advanced features and benefits with the user-friendliness of the Microsoft WINDOWS Graphical User Interface. WINDOWS NT is two products: WINDOWS NT Workstation providing full operating system functionality on a desktop and WINDOWS NT Server which is designed to operate as a network Server providing centralised security and network administration.

WINDOWS NT Workstation provides ITSEC pre-defined F-C2 security functionality including user account policies, Workstation locking, user roles, Access Control Lists and privileges, plus a trusted path for logon. WINDOWS NT Server provides these facilities extended to the network, including centralised security management, multiple logical domains of workstations and servers, domain-wide user account and accountability policy, domain-wide global groups, restriction on logon hours, trust relationships between domains.

The evaluation of Windows NT 3.51 excluded Exchange Server, System Management Server (SMS), MS Mail, remote access services and Clipbook viewer. Domain based security functionality was included up to the transport driver interface; underlying network protocols and architectures were excluded. Windows NT 3.51 Server and Workstation are no longer available on Microsoft Select CDs. However, purchase of a Windows NT 4.0 licence allows the owner to run Windows NT 3.51 and Microsoft will supply the 3.51 software on application to Jeremy Smith at the Microsoft address.

COMMERCIALLY AVAILABLE

HP-UX Version 10.20

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 and encryption

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

HP-UX Version 10.20 on a single workstation or server in a standalone mode has been evaluated under the UK ITSEC scheme and has met the requirements of ITSEC Assurance Level E3 and Functionality Class F-C2. Restricted SAM, X-Windows and HP-VUE were excluded from the evaluation.

Product Type: Operating System
Assurance Level: E3
Supplier: Hewlett Packard Ltd
Evaluation Facility: Admiral Management Services
Certification Status: Certificate P111 February 1999
Point of Contact: Chris Simpson
Telephone: 01344 365029
Fax: 01344 763747

IBM Processor Resource Systems Manager

IBM Processor Resource/Systems Manager (PR/SM) is a hardware facility of the ES/9000 series of processor that enables the resources of a single processor to be divided between distinct, predefined logical machines called "logical partitions". Each logical partition can be isolated from all other logical partitions, and each is capable of running, without modification, any S/370, 370-XA, ESA/370 or ESA/390 operating system.

Product Type: Operating System
Assurance Level: E4
Supplier: IBM United Kingdom Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 95/53 September 1995
Point of Contact: Peter Dare
Telephone: 01256 343274
Fax: 01256 331621

Commercially Available Products

OpenVMS and SEVMS for VAX and ALPHA, Version 6.2-1H3

Product Type: Operating Systems
Assurance Level: E3
Supplier: Compaq Computer Ltd
Evaluation Facility: Admiral
Certification status: In Evaluation
UK Scheme
Point of contact: David Surman-Roberts
Telephone: 01256 371123
Fax: 01256 371164

OpenVMS is a general-purpose multi-user operating system that runs in both production and development environments on 64-bit Alpha and 32-bit VAX computers. OpenVMS meets and exceeds the functionality of F-C2 and features an integrated security reference monitor, Auditing, Discretionary Access Controls (DAC) and Access Control Lists (ACL); the last to meet F-B3 DAC requirements. SEVMS is the security-enhanced version of the OpenVMS operating system, and adds mandatory access controls (MAC) and enhanced security auditing for a F-B1 level secure standalone or clustered OpenVMS systems.

OpenVMS Clusters provides a highly integrated OpenVMS computing environment distributed over as many as 96 systems. VMScluster systems provide a uniform computing environment that is highly scalable, highly available and secure. OpenVMS Cluster Software implements a single security environment within a cluster configuration. The security subsystem ensures that all cluster-visible objects maintain consistent security profiles, and that system security auditing controls operate across the entire cluster, including mixed-architecture Alpha and VAX Clusters.

OpenVMS and SEVMS Version 6.2-1H3 are Year 2000-ready operating systems.

SeNTry 2020

Product Type: PC Access Control
Assurance Level: EAL1
Supplier: MIS - Corporate Defence Solutions
Evaluation Facility: IBM Global Services
Certification Status: Certificate P100 July 1998
Point of Contact: Julie Kenward
Telephone: 01622 723400
Fax: 01622 728580
e-mail: julie.kenward@mis-cds.com
URL: http://www.miseurope.co.uk

SeNTry 2020 is a Windows NT software product that enables the users to store files securely. To facilitate this SeNTry 2020 generates an encrypted virtual drive on the host PC hard disk.

Access to the virtual drive is restricted to the owner by a passphrase. The virtual drive is then seen by the operating system as another disk but is actually a file on the physical disk. The virtual drive can then be formatted to either NTFS or FAT file systems. All files written to the drive are encrypted in real-time and once the drive has been dismounted (either on demand or when the user logs off) all files remain secure inside the virtual drive.

At any time the user can dismount the drive or if required, may set an inactivity threshold at which point the drive will automatically dismount and become unavailable. This protects against the user leaving the computer unattended with the disk mounted.

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, MDC/RIPM, Cast, Square, DES, MDC/SHA1, Blowfish, Triple DES, Safer.

Verification of the correctness of the various cryptographic algorithms was not performed as it is not required by the EAL1 assurance level.

COMMERCIALLY AVAILABLE

STOPLOCK V
Version 2.23a
STOPLOCK V/SC
Version 2.23
STOPLOCK V SCenSOS
Version 2.23a

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.

These Stoplock product variants are designed to counter threats as set out in the Security Target through various Security Enforcing Functions. The evaluated functions include:

Identification and authentication: Access to files not allowed unless user is logged in; users, administrators, temporary account types; password requirements and configurations; softhold timeout screen blanker.

Access Control: Enhanced boot protection to protect stored files; access restrictions to files and directories by user, group or world rights; file/directory rights defined as Read, Write, Execute, Create, Rename/Delete; 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.

Accuracy, password and encryption mechanisms are also ITSEC E3 evaluated functions.

Product Type: PC Access Control
Assurance Level: E3
Supplier: Netlexis Ltd
Evaluation Facility: Logica
Certification Status: Certificate 96/65a September 1996
Point of Contact: Steve Matthews
Telephone: 01628 470909
Fax: 01628 470901
email: sales@netlexis.com

Disknet NT
Version 1.70

Disknet is a multi-layered security system, providing management and protection against unauthorised disks, unauthorised and malicious software (e.g. viruses), unauthorised access, theft and hacking.

With many sophisticated options available it is the system of choice for disk control. Simple to use, easy to install and fast in operation with minimal overhead.

Major features include:

- access control with passwords
- restricts 'imports' of floppy diskettes enforcing scanning
- optionally controls the 'export' of floppy disks
- protection against malicious software
- protection against malicious users
- stops users changing configuration files
- prohibits the use of unauthorised software
- anti-tamper function to prevent unauthorised removal

Disknet is designed for IBM compatible PCs running Microsoft Windows NT.

Product Type: PC Access Control
Assurance Level: E2
Supplier: Reflex Magnetics Limited
Evaluation Facility: Logica
Certification Status: Certificate P125 September 1998
Point of Contact: Andy Campbell
Telephone: 020 7372 6666
Fax: 020 7372 2507
email: sales@reflex-magnetics.com

Commercially Available Products

HARDWALL Version 7.01

Product Type: PC Access Control
Assurance Level: E3
Supplier: Calluna Technology Limited
Evaluation Facility: IBM Global Services
Certification Status: In Evaluation
Since 1998
Point of Contact: Fiona Riddoch
Telephone: +44 1592 630810
Fax: +44 1592 630168
e-mail: sales@calluna.co.uk
www.calluna.com

HARDWALL version 7.01 is a hardware solution to the problem of inadvertent or malicious corruption of application and system files by authorised or unauthorised users of the protected workstation.

HARDWALL ensures computer viruses cannot permantently damage the operating system and restrains the uploaded viruses to one area of the hard disk. When appropriately used, with anti-virus software, HARDWALL limits the extent of the virus and therefore limits the cleaning up effort. Any unauthorised changes are reversed whenever the workstaion is re-booted.

HARDWALL uses partition access privileges controlled through hardware to prevent data theft. During a working session the user chooses one partition as the woking drive for data manipulation. All data on the other drives is invisible from the keyboard. To access the data on other drives the user must re-boot. By designating and using one drive as the internet access drive all data stored in other drives is invisible from the internet.

HARDWALL consists of a single electronics card that plugs into an ISA expansion slot in the PC. It connects between the hard disk drive and the motherboard and monitors disk drives activity to protect against illegal writes and unauthorised accesses to the hard disk. By using a separate microprocessor that operates independently from the main system, HARDWALL provides a level of protection that cannot be corrupted or circumvented by computer virus software or hacker attack.

HARDWALL plugs into any IBM-compatible desktop/tower PC or server with a spare ISA expansion slot. It works with hard disk drives that use the EIDE interface to the system board and runs under DOS 6.2 or higher, Windows® 95 and Windows NT® 4.0 operating systems. These systems are excluded from the Target of Evaluation, but have all been included in the scope of the HARDWALL Version 7.01 evaluated configuration environment.

Multos v3 on Hitachi H8/3112 ICC

Product Type: Smartcard
Assurance Level: E6
Developer: platform seven
Supplier: Mondex International
Evaluation Facility: Logica
Certification Status: Certificate P130
August 1999
Point of Contact: Murdo Munro
Telephone: 0171 557 5154
Fax: 0171 557 5354

MULTOS is a secure, multi-application operating system designed to be used on an Integrated Circuit Card (ICC), also known as a smartcard, to manage, segregate and execute applications written for MULTOS (such as loyalty, ticketing, credit, debit and electronic purse).

Multos is designed to provide a platform for the common development and operation of applications on ICCs. MULTOS-3 is able to:

a execute an application written for MULTOS independently of the underlying ICC hardware;

b load many applications, the applications being able to co-exist on the ICC;

c enable Application Providers to be confident of the authenticity and integrity of the loaded applications and, where applicable, of the confidentiality of data held within them; and

d ensure that the applications are not able to interfere with each other or with MULTOS.

This implementation of the MULTOS-3 specification, developed by *platform seven* and Mondex International, has been evaluated on an Hitachi H8/3112 ICC. Applications are loaded by MULTOS into the ICCs EEPROM. During the production process, each MCD 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.

MONDEX Purse Release 2.0 on MULTOS v3 and Hitachi H8/3112 ICC

Product Type: Smartcard
Assurance Level: E6
Developer: platform seven
Supplier: Mondex International
Evaluation Facility: Logica
Certification Status: Certificate P129
August 1999
Point of Contact: Alison Greensmith
Telephone: 0171 557 5012
Fax: 0171 557 5212

The MONDEX Purse is an electronic purse designed to provide individuals and businesses with an electronic alternative to the use of notes and coins for making cash payments. Mondex electronic cash is stored on Integrated Circuit Cards (ICCs), also known as smartcards. MONDEX Purse Release 2.0, developed by *platform seven* and Mondex International, has been evaluated when running on MULTOS Version 3, (which has been separately evaluated to ITSEC E6) and the Hitachi H8/3112 ICC.

Once value is available in a system of electronic purses, parties can then use purses to make and receive secure payments from one purse to another. Payments may be made to and from banks, between consumers and retailers, or directly between customers. In all cases, value may be transferred in either direction between a pair of purses, but for some classes of purse there may be constraints on the other classes of purse to which payments may be made.

The Central Bank's role of minting and issuing cash is taken on by an Originator who is responsible for manufacturing electronic value, which is then distributed via the banking system from one purse to another. The process is appropriately regulated, but only the MONDEX Purse has been evaluated.

As with notes and coins, electronic value can be in any currency. Each purse can hold several currencies at one time, each currency being held separately in a different pocket inside the purse. The value in each currency is always quite distinct from other currencies - no conversion is possible within a purse or as part of a transaction. When a payment occurs between purses, the parties involved decide on the currency to be used (and each purse will use this information to select the correct pocket). The total value of each currency in circulation does not change as a result of a successful payment. Should an attempted transfer be unsuccessful, this is recorded in an exception log of purse allowing such losses to be refunded.

MOD Specific Products

Trusted EDI on Trusted Solaris 1.2

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.

- 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 identified above are implemented through the use of encryption techniques which, in the evaluated configuration, use the Secure Hash Standard (SHS) algorithm and the RSA algorithm.

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

This product was evaluated for a specific purpose against a UK Interpretation of the criteria. The certificate, therefore, is outside the Mutual Recognition Agreement.

Product Type: Miscellaneous
Assurance Level: E3
Supplier: EDS Ltd
Evaluation Facility: EDS
Certification Status: Certificate 97/85 July 1997
Point of Contact: Chris Gibson
Telephone: 01256 742340
Fax: 01256 742700

CERBERUS Guard Processor

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

The CERBERUS Guard Processor checks that the actual security label of messages is contained within a configurable set of permitted labels for a source/destination address pair.

Furthermore, if a connection orientated protocol is used, the CERBERUS Guard Processor can be configured to permit the initiation of a link by one of the sources/destination address pair only.

If a message fails any of the checks performed by the CERBERUS Guard Processor, a potential security breach is prevented from occurring by the CERBERUS Guard Processor stopping any onward transmission of the messages and requiring operator intervention (possibly to include investigation into the cause of the failure).

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

This product was evaluated for a specific purpose against a UK Interpretation of the criteria. The certificate, therefore, is outside the Mutual Recognition Agreement.

Product Type: Communications
Assurance Level: E4
Supplier: EDS Ltd
Evaluation Facility: EDS
Certification Status: Certificate 98/99 April 1998
Point of Contact: George Thompson
Telephone: 01256 742000
Fax: 01256 742700

CESG Controlled Products

The use of products in this section is strictly controlled by CESG. Within the UK the products may only be made available to HMG departments, quasi-governmental bodies and certain UK firms. They may also be made available, on a case-by-case basis only, to certain foreign government users and international organisations, but all such releases must be cleared in advance by CESG.

It is HMG policy not to use published or publicly available cryptographic algorithms for HMG confidentiality applications (other than on an exceptional basis) due to the nature of threats against some HMG information.

All uses of cryptography to protect HMG protectively marked and other HMG sensitive data must be approved by CESG. Normally this requires the use of CESG specified algorithms.

There is a range of CESG algorithms available for incorporation into commercial products; both for software and hardware implementation. The protective marking of data which can be protected by products containing CESG algorithms depends on the requirement and on the particular algorithm which has been implemented. Advice on the suitability of products in this section to meet Government requirements must be sought from CESG.

Since 30 June 1994, new HMG INFOSEC requirements for cryptographic protection of data shall be met ONLY by devices that have had their cryptographic functionality verified and formally approved by CESG.

CESG Controlled Products

OMEGA
Version 7.12
Increment 19

Product Type: Communications
Assurance Level: E3
Supplier: ICL Defence
Evaluation Facility: Admiral Management Services
Certification Status: Certificate P134 January 2000
Point of Contact: John Reynolds
Telephone: 0118 963 5624
Fax: 0118 969 7636
email: john.reynolds@icl.com

OMEGA is a multi-level secure message handling product which provides a full range of network and secure messaging facilities:

- MAC, DAC and security labels are applied to all accessible and displayed control data and messages;
- drafting, release control, distribution, delivery, routing, servicing and correction of messages with full provision of accountability, archiving and traceability;
- acceptance and generation of most message formats, providing almost any format in and any format out, including ACP127 and X.400 (1984 and 1988);
- gateways to a number of recognised defence systems, ranging from RS232 and ITA5 to X.25 and TCP/IP thus providing access to slow and fast communications equipment;
- facilities for communications with ships via a range of LF, HF and satellite bearers;
- access for PCs and a CMW platform connected via local and wide area networks.

Omega is configurable and user friendly. It operates in a future-proofed, scalable, high availability and commercially available range of computer and communications equipment.

CASM CryptServe
Version 1.02

Product Type: Communications
Assurance Level: E3
Supplier: CESG
Evaluation Facility: Logica
Certification Status: Certificate 98/94 March 1998
Point of Contact: John Ridley
Telephone: 01242 237323
Fax: 01242 252088

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

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

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

Racal RAMBUTAN SAFE X.25

The RAMBUTAN SAFE X.25 packet encryption device secures data transmitted across X.25 networks. Offering a choice of V.24, V.35 and X.21 interface options, the unit operates at data rates of up to 64 Kbps and supports up to 4096 logical channels.

A sophisticated key distribution system minimises the overhead of managing the key material supplied by CESG. Physical key need only be loaded into the units via magnetic swipe card every six months. Thereafter, regularly updated keys are issued automatically across the network from a central key distribution unit, and no further local user intervention is required.

Configuration of SAFE X.25 system parameters, review of system audit data and system diagnostics may be carried out remotely from a security management centre reducing still further the overhead of maintaining secure network traffic. Simultaneous support for encrypted and plaintext calls maintains flexibility and permits staged installation of a secure service across a large network.

Product Type: Communications
Assurance Level: E3
Supplier: Racal Security & Payments
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 94/31 February 1994
Point of Contact: Chris Woods
Telephone: 01273 384600
Fax: 01273 384601
email: chris.woods@racalitsec.com

Racal RAMBUTAN SAFE 2M Version 2.01

The RAMBUTAN SAFE 2M encryption device secures data transmitted across synchronous high speed leased lines. The device is supplied with V.35 and X.21 interface options for use on circuits employing unstructured data. It also provides G703 interface for balanced (120R) or unbalanced (75R) circuits employing unstructured or structured G7044/732, 32 channel PCM, or N channel Kilostream data. The device operates at speeds up to 2Mbps.

The SAFE 2M supports remote management and is fully compliant with Racal Data Group's Key Management scheme. A certified key distribution system (also used by SAFE X.25 and SAFE 64K) minimises the overhead of managing the key material supplied by CESG. Physical keys need only be loaded into the units via magnetic swipe card typically every 6 months. Thereafter, regularly updated keys are issued automatically across the network from the central key distribution unit, and no further local user intervention is required. This can considerably reduce the cost of ownership of such a system.

Configuration of SAFE 2M system parameters, review of system audit data and system diagnostics may be carried out remotely from the network management centre reducing still further the overhead of maintaining secure network traffic.

Product Type: Communications
Assurance Level: E3
Supplier: Racal Security & Payments
Evaluation Facility: Syntegra
Certification Status: Certificate 95/51 May 1995
Point of Contact: Chris Woods
Telephone: 01273 384600
Fax: 01273 384601
email: chris.woods@racalitsec.com

CESG Controlled Products

Racal RAMBUTAN SAFE 64K Versions 1.00, 1.09 and 1.10

Product Type: Communications
Assurance Level: E3
Supplier: Racal Security & Payments
Evaluation Facility: Admiral Management Services
Certification Status: Certificate 94/37 July 1994
Point of Contact: Chris Woods
Telephone: 01273 384600
Fax: 01273 384601
email: chris.woods@racalitsec.com

The RAMBUTAN SAFE 64K encryption device secures data transmitted across synchronous dialup and leased lines. The unit offers a choice of V.24, V.35 and X.21 interface options, operates at data rates of up to 64 Kbps and is independent of the protocol used.

The SAFE 64K supports remote management and is fully compliant with Racal Data Group's Key management scheme. A certified key distribution system (also used by SAFE X.25) minimises the overhead of managing the key material supplied by CESG. Physical keys need only be loaded into the units via magnetic swipe card every six months. Thereafter, regularly updated keys are issued automatically across the network from the central Key Distribution Unit, and no further local user intervention is required. This can considerably reduce the cost of ownership of such a system.

Configuration of SAFE 64K system parameters, review of system audit data and system diagnostics may be carried out remotely from the network management centre reducing still further the overhead of maintaining secure network traffic.

ED2048R RAMBUTAN Data Encryption Unit

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 94/36 July 1994
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

The ED2048R provides cryptographic protection for 2.048 Mbps links with CCITT G703 interfaces using the CESG designed RAMBUTAN crypto-kernel. It has been designed and manufactured by Baltimore Technology Ltd to offer full traffic confidentiality between communicating 2 Mbps multiplexors.

Cryptovariables are provided by CESG and loaded into the ED2048R by means of an ED546 magnetic stripe key loading device. The mode of encryption employed does not result in error propagation on the G703 line.

ED2048RU RAMBUTAN Data Encryption Unit

The ED2048RU provides cryptographic protection for point-to-point at speeds of up to 2.048 Mbps. The ED2048RU has 3 interface options:

- X.21
- G.703/G.732
- V.24

The X.21 interface is particularly well-suited to the protection of flexible bandwidth services as it is clocked at the line speed, hence no re-configuration is required if the line speeds are increased to meet data traffic expansion.

Two-tier cryptovariables are provided by CESG and loaded into the ED2048 RU by means of an ED546 magnetic stripe key loading device. Encryption units work in a Master-Slave relationship and have dual power supplies. The mode of encryption employed does not result in error propagation on the line.

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 95/42 March 1995
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

ED2048R3 Data Encryption Unit

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

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

The X.21 interface is particularly well-suited to the protection of flexible bandwidth services as it is clocked at the line speed, hence no re-configuration is required if the line speeds are increased to meet data traffic expansion. The G704 interfaces support an nx64 Kbps fractional service. The mode of encryption employed does not result in error propagation.

The ED2048R3 offers a simplified two-tier key hierarchy enabling data encryption keys (DEKs) to be downloaded over the link, so reducing administrative overheads. In addition, the ED2048R3 has the functionality to be managed from a centralised facility, the Zergo Network Security Workstation, to provide fully automated key and equipment management.

Four DEKs at a time can be loaded from a single swipe card into the designated master encrypter.

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: IBM Global Services
Certification Status: Certificate 96/60 April 1996
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

CESG Controlled Products

ED600 RAMBUTAN Data Encryption Unit

Product Type: Communications
Assurance Level: UKL2
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 92/17 February 1992
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

The ED600 RAMBUTAN (ED600R) provides cryptographic protection for binary coded data using the CESG designed RAMBUTAN crypto-kernel. It was designed and manufactured by Zergo Ltd to offer end-to-end X.25 encryption, supporting up to 512 switched virtual circuits and up to 64kbps full duplex operation. Encryption and decryption is applied only to user data within an X.25 packet, not to addressing / protocol information which remains unaltered.

The ED600R operates as a transparent device interposed between a modem and computer or terminal, and can interface to three data signalling standards: X.21 or V.35 for full duplex communication at 64 kbps, and V.24 for full duplex at 19.2kbps.

Cryptovariables are provided by CESG and loaded into the ED600R by means of the ED545 key transport device. Traffic key is generated by RAMBUTAN's 8-bit cipher feedback mode of use.

ED600RTS RAMBUTAN Synchronous Link Encryptor

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 95/55 September 1995
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

The ED600RTS is a RAMBUTAN encryptor for synchronous data transmitted on a point-to-point link, at speeds of up to 128kbps using an X.21 interface. The ED600RTS also offers simplified key management through the use of a two-tier key hierarchy which enables keys to be downloaded over the link, so reducing the administrative overhead. In addition, the ED600RTS has the functionality to be managed from a centralised facility, the Baltimore Network Security Workstation, to provide fully automated key and equipment management.

The ED600RTS is self synchronising and has the facility to store a top level encrypting key (KEK) and up to 4 data encrypting keys (DEK). Data keys are loaded from magnetic stripe cards via a separate handheld Key Entry Device, the ED546. The ED600RTS can be installed on a desktop or optionally in a 19" rack.

NETWORK SECURITY WORKSTATION
Automated Security Management

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 97/75 January 1997
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

Baltimore's RAMBUTAN Network Security Workstation (NSW) offers Government encryption users the benefits of automated security management. The NSW comprises a PC and an attached cryptographic processor, the CG600R. It enables all compatible Baltimore encryptors to be centrally managed across the network. The benefits of centralised management include reduced administrative overheads, improved equipment control and greater operational flexibility.

The NSW can manage either the ED2048R3 and ED600RTS link encryptors or the ED8000RL LAN IP Encryptor. A variety of communications methods can be used to access the control port of the link encryptors; access to the ED8000RL is via in-band IP/UDP messages.

Key distribution message exchanges are authenticated and encrypted between the NSW and target encryptors in an automated fashion. A physical key only needs to be loaded into each encryptor at six monthly periods. All other key material is supplied by CESG via the NSW.

Status, alarm and audit information can be collected automatically or under operator control. All significant events are timestamped by the encryptors and stored in the NSW audit files. The NSW is protected by password protection mechanisms. At no time is plain text key material accessible by an NSW operator.

ED8000RL
RAMBUTAN LAN Interconnect IP Encryptor

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: IBM Global services
Certification Status: Certificate 97/92 December 1997
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

The ED8000RL is an ethernet, in-line, protocol sensitive encryptor that utilises the RAMBUTAN algorithm. It provides cryptographic protection for user data transmitted between LANs using Internet Protocol across WANs, while still allowing the flow of necessary control communications. The encryptor is interposed between a local Ethernet LAN subnet and the router giving access to the WAN.

- Fully automated central management available from NSW
- Supports Ethernet V2.0 and IEEE 802.3 frame format incorporating SNAP
- Functionally transparent to ICMP and ARP messages
- Holds up to 16 data keys to enable creation of separate cryptographic zones
- Supports up to 512 destination IP subnet or device addresses
- Forwarding data rate exceeds 2Mbits per second
- SNMP TRAPs can be sent to a seperate Network Management Centre
- Tamper resistant

ED8000RL Rambutan LAN has full membership of CMS, the latest version being ED8000RL 2502-G1-F and G

CESG Controlled Products

ED8000EG Enhanced Grade LAN Interconnect IP Encryptor

The ED8000EG is an Enhanced Grade, IPSEC based, IP Security gateway. It provides cryptographic protection for user data transmitted between LANs and across WANs using Internet Protocol, while still allowing the flow of control communications. The encryptor acts as a Router to the private network and as a host to the public network, via Ethernet interfaces.

- PKI Certificate based authentification between peer encryptors
- Traffic protection using IPSEC ESP (tunnelling)
- Automatic key establishment
- Supports up to 1000 secure connections
- 10Mbps and 10/100Mbps Base-t Ethernet interfaces

Product Type: Communications
Assurance Level: E3
Supplier: Baltimore Technologies (UK) Ltd
Evaluation Facility: IBM Global Services Management Services
Certification Status: In Evaluation
UK Scheme Since July 1999
Point of Contact: Charles Pierson
Telephone: 01442 342600
Fax: 01256 812901

VME Operating System with Government Security Option, Version SV294 running on Series 39 Processors

VME Version 294 with the Government Security Option (GSO), provides additional security features to those supplied by VME and the standard VME High Security Option (HSO) running on series 39 systems. It is only available to UK Government Establishments.

The GSO product offers extra controls restricting certain actions to authorised users, improved auditing of certain security related events and a password handling package to enable the installation to use UK Government approved password generation and encryption algorithms.

This version of GSO, Version 0030 has been evaluated under the UK ITSEC Scheme and complies with the requirements for E3 assurance and F-B1 Functionality.

Product Type: Operating System
Assurance Level: E3
Supplier: International Computers Ltd (ICL)
Evaluation Facility: Logica
Certification Status: Certificate 94/39 September 1994
Point of Contact: Bryn Bircher
Telephone: 0161 230 5525
Fax: 0161 230 5957
email: bryn.bircher@icl.com
URL: www.icl.com

KILGETTY PLUS NT4 Version 1.0

KILGETTY PLUS NT4 is a total disk encryption product, which gives CESG approved protection against unauthorised access in the event of loss for government data up to TOP SECRET stored on computer disks.

KILGETTY PLUS NT4 is for use with IBM compatible desktop / portable computers running Microsoft Windows NT4, on hard disks up to 8GB in size. Access is via a touch memory device, user identity and password. All data held on the computer's hard disk is fully encrypted, including data structure and applications.

Features: - Transparent file access on the hard disk via on-the-fly encryption and decryption - Floppy disks encrypted with a private key or with a user group key - Windows NT4 system manager (KSM) application - Multiple KSM user capability - Kilgetty Local Manager can control user's facility rights - Supports up to 2 hard disks - Supports all Windows NT4 file systems.

KILGETTY PLUS NT4 will run on any Intel based computer which can support Windows NT4 but the recommended minimum hardware specification is: 100MHz Pentium Processor, 16Mb RAM. KILGETTY PLUS NT4 was evaluated on Microsoft Windows NT4 Server and Workstation versions, with Service Pack 3 installed, on a Twinhead Slimnote-890TX laptop computer with PHOENIX BIOS version 4.04.

Product Type: PC Access Control
Assurance Level: E3
Supplier: The Software Box
Evaluation Facility: EDS
Certification Status: Certificate P112
February 1999
Point of Contact: The Security Group
Telephone: 01347 812100
email: security_group@softbox.co.uk

KILGETTY Version 1.2h KILGETTY PLUS Version 1.2h

KILGETTY and KILGETTY PLUS disk encryption products protecting government data are for use with IBM compatible desktop / portable computers running Microsoft DOS, Win 3.1 and Win 9x. Access is via a touch memory device, user identity and password. All data on the hard disk is fully encrypted, including data structures and applications.

KILGETTY - CESG approved protection for data up to CONFIDENTIAL and suitable for hard disks up to 8GB.

KILGETTY PLUS - CESG approved protection for data up to TOP SECRET and suitable for hard disks up to 4GB.

Features: Transparent file access on the hard disk via on-the-fly encryption and decryption - Floppy disks encrypted with private or user group key - DOS key manager (KKM) application - Supports all file systems supported by the operating system.

KILGETTY and KILGETTY PLUS will run on any Intel based computer which can support the relevant operating system but the recommended minimum hardware specification is: 66MHz 486 processor, 4Mb RAM.

KILGETTY and KILGETTY PLUS were evaluated on Microsoft Windows 950SR2 and Windows 98 on a Twinhead Slimnote-890TX laptop computer with PHOENIX BIOS version 4.04.

Product Type: PC Access Control
Assurance Level: E3
Supplier: The Software Box
Evaluation Facility: Admiral
Certification Status: Certificate P105
February 1999
Point of Contact: The Security Group
Telephone: 01347 812100
email: security_group@softbox.co.uk

GUARDIAN ANGEL Version 5.01D1

Product Type: PC Access Control
Assurance Level: E2
Supplier: Portcullis Computer Security Ltd
Evaluation Facility: Syntegra
Certification Status: Certificate 98/93 January 1998
Point of Contact: Mark Lane
Telephone: 0181 868 0098
Fax: 0181 868 0017
email: msl@portcullis-security.com

GUARDIAN ANGEL Version 5.01D1 is a software protection system providing PC access controls designed to prevent theft of data. It is a pre-DOS loader which provides defensive security mechanisms to control and manage a hierarchy of users.

The features of GUARDIAN ANGEL are:

- User identification and password functions which prevent illegal access to the system. Passwords are encrypted using an endorsed implementation of the CESG FIREGUARD algorithm.
- Controlled access to data and files through the use of security profiles, audit tracking and a File Access Control Matrix.
- Protection against the propagation of malicious code (e.g. viruses) by preventing the user from copying programs from floppies or changing programs on the hard disk.
- Disk certification which will prevent the use of floppy disks that are not formatted by GUARDIAN ANGEL.
- Encryption of data using an endorsed implementation of the CESG RED PIKE algorithm. This provides protection for files when exported on any media.
- Restriction of file access and ownership based on a user's identity.

GUARDIAN ANGEL Version 5.01D1 was certified in standalone mode.

Supplier Address List

Argus Systems Group, Inc
1809 Woodfield Drive
Savoy, Illinois
61874 USA
Phone: 001 217 355 6308
Fax: 001 217 355 1433
email: info@argus.cu-online.com

Baltimore Technologies (UK) Ltd
Innovation House
39 Mark Road
Hemel Hempstead
Herts HP2 7DN
Phone: 01442 342600
Fax: 01442 66438

Banyan Systems Incorporated
Banyan House
Northwood Park
Gatwick Road
Crawley
West Sussex RH10 2XN
Phone: 01293 612284
Fax: 01293 612288

BorderWare Technologies Inc
1 The Harlequin Centre
Southall Lane
Middlesex UB2 5NH
Phone: +44 181 893 6066
Fax: +44 181 574 8384
email: info@borderware.com

BrainTree Technology Ltd
Parkway House
Palatine Road
Northenden
Manchester M22 4DB
Phone: 0161 9451511
Fax: 0161 9452150

Bull S.A.
1 Rue De Provence
38432 Echirolles Cedex
France
Phone: 33 4 76 29 76 86
Fax: 33 4 76 29 78 62

Calluna Technology Ltd
One Blackwood Road
Eastfield
Glenrothes
Fife KY7 4NP
Phone: 01592 630810
Fax: 01592 630168

CESG
PO Box 144
Cheltenham
Gloucestershire GL52 5UE
Phone: 01242 237323
Fax: 01242 252088

Check Point Software Technologies Ltd
Unit 5B
Vision Park
Histon
Cambridge
CB4 9ZR
Phone: 01233 713611
Fax: 01233 236847

Cisco Systems
3 The Square
Stockley Park
Uxbridge
Middlesex
UB11 1BN
Phone: +44 (0)181 756 8349
Fax: +44 (0)181 756 8099

Compaq Computer Ltd
Defence Group
Skippets House
Skippets Lane West
Basingstoke
Hants
RG21 3AT
Phone: 01256 371123
Fax: 01256 371164

Computer Associates
Computer Associates House
183/187 Bath Road
Slough
Berks
SL1 4AA
Phone: 01753 679819
Fax: 01753 825464

Concurrent Computer Corp Ltd
227 Bath Road
Slough
Berks SL1 4AX
Phone: 01753 513413
Fax: 01753 513218

CyberGuard Europe Ltd
Asmec Centre
Eagle House
The Ring
Bracknell, Berkshire
RG12 1HB
Phone: 01344 382550
Fax: 01344 382551

Data Track Technologies plc
153 Somerford Road
Christchurch
Dorset
BH23 2TY
Phone: 01425 270333
Fax: 01425 271978

Supplier Address List

EDS Ltd
Bartley Way
Bartley Wood
Hook
Hants
RG27 9XA
Phone 01256 742000
Fax: 01256 742700

Entrust Technology Ltd
750 Heron Road
Suite E080
Ottawa
Canada K1B 1A7
Phone: +1 613 247 3446
Fax: +1 613 247 3450

Fujitsu Ltd
Development Dept 3
Application Server Software Division
Software Group
1405 Ohmaru
Inagi-shi
Tokyo 206-8503
Japan
Phone: +88 44 370 7965
Fax: +88 44 370 7737

GEC-Marconi Secure Systems
Wavertree Boulevard
Wavertree Technology Park
Liverpool
L7 9PE
Phone: 0151 228 0988
Fax: 0151 254 1194

Hewlett Packard Ltd
Cain Road
Bracknell
Berks
RG12 1HN
Phone: 01344 362730
Fax: 01344 361521

Hitachi Data Systems
750 Central Expressway
MS 32/36
PO Box 54996
Santa Clara
CA 95056-0996
USA
Phone: +1 408 970 1023
Fax: +1 408 988 8601

IBM United Kingdom Ltd
Alencon House
Alencon Link
Basingstoke
Hants
RG21 1EJ
Phone: 01256 343274
Fax: 01256 331621

ICL
Jays Close
Basingstoke
Hampshire
RG22 4BY
Phone: 01256 694684
Fax: 01256 694961

Informix Software Ltd
Informix House
6 New Square
Bedfont Lakes
Feltham
Middx
TW14 8HA
Phone: 0181 818 1000
Fax: 0181 818 1111

International Computers Ltd (ICL)
High Performance Systems
Wenlock Way
West Gorton
Manchester
M12 5DR
Phone: 0161 230 5525
Fax: 0161 230 5957

The Knowledge Group
Knowledge House
Concorde Road
Patchway
Bristol
BS34 5TB
Phone: 0117 900 7500
Fax: 0117 900 7501

Microsoft Ltd
Microsoft Campus
Thames Valley Park
Reading
Berks RG1 1WG
Phone: 0870 60 10 100
Fax: 0870 60 20 100

MIS - Corporate Defence Solutions
MIS House
Hermitage Lane
Maidstone
Kent ME16 9NT
Phone: 01622 723400
Fax: 01622 728580

Mondex International
1st Floor
47-53 Cannon Street
London EC4M 5SQ
Phone: 0171 557 5000
Fax: 0171 557 5200

NetGuard UK Ltd
Thamesbourne Lodge
Station Road
Bourne End
Bucks
SL8 5QH
Phone: 01628 533433
Fax: 01628 0000000

Supplier Address List

Netlexis
The Old Stables
Kines Lane
Cookham Dean
Berks SL6 9AT
Phone: 01628 470909
Fax: 01628 470901

Network Associates International Ltd
Minton Place
Victoria Street
Windsor
Berks SL4 1EG
Phone: 01753 827500
Fax: 01753 827520

Novell (UK) Ltd
Novell House
London Road
Bracknell
Berks RG12 2UY
Phone: 01344 724074
Fax: 01344 764200

Oracle Corporation UK Ltd IPSAG
560 Oracle Parkway
Thames Valley Park
Reading
Berks RG6 1RA
Phone: 0118 9246201
Fax: 0118 9245007

platform seven
6th Floor
1-2 Finsbury Square
London EC2A 1AA
Phone: 0207 714 8492
Fax: 0207 714 8246

Portcullis Computer Security Ltd
The Grange Barn
Pike End, Pinner
Middx HA5 2EX
Phone: 0181 868 0098
Fax: 0181 868 0017

Racal Security & Payments
Meadow View House
Long Crendon
Aylesbury
Bucks
HP18 9EQ
Phone: 01844 201800
Fax: 01844 208550

Reflex Magnetics Ltd
31-33 Priory Park Road
London NW6 7HP
Phone: 0171 372 6666
Fax: 0171 372 2507

SCO
Croxley Business Park
Hatters Lane
Watford
Herts WD1 8YW
Phone: 01923 813656
Fax: 01923 813804

Sequent Computer Systems Ltd
Sequent House
Weybridge Business Park
Addlestone Road
Weybridge
Surrey KT15 2UF
Phone: 01932 851111
Fax: 01932 850011

Siemens Nixdorf Information Systems
Siemens Nixdorf House
Oldbury, Bracknell
Berkshire RG12 8FZ
Phone: 01344 850503
Fax: 01344 850918

Software Box Ltd
Green Park Business Centre
Goose Lane
Sutton on the Forest
York YO6 1ET
Phone: 01347 812106
Fax: 01347 811220

StorageTek Network Systems Group
STK House
Woking Business Park
Albert Drive, Woking
Surrey GU21 5JY
Phone: 01483 727433
Fax: 01483 737463

Sun Microsystems Federal
2550 Garcia Avenue
MS SCJ01-104 Mountain View
CA 94043-1100
USA
Phone: +1 408 953 4825
Fax: +1 408 428 9411

Sun Microsystems, Inc.
MPK 18-211 rm 2295
901 San Antonio Road
Palo Alto
CA 94303
USA
Phone: +1 650 786 7379
Fax: +1 650 786 5731

Agency Address List

France
Service Central 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
www.scssi.gouv.fr

USA
National Security Agency
ATTN: V2 Common Criteria
Technical Adviser
Fort George G Meade,
MD 20755-6740
USA
Tel: +1 410 859 4458
Fax: +1 410 684 7512
www.nsa.gov

DTI
Information Security Policy Group
CII Directorate
Department of Trade and Industry
151 Buckingham Palace Road
London SW1W 9SS
Tel: +44(0)171 215 1962
Fax: +44(0)171 931 7194
www.dti.gov.uk

Germany
Bundesamt fur Sicherheit in der
Informationstechnik
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: +49 228 9582 141
Fax: +49 228 9582 455
web.bsi.bund.de/

Canada
Communications Security
Establishment
Criteria Coordinator
R2B IT Security Standards and
Initiatives
PO Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel: +1 613 991 7409
Fax: +1 613 991 7411
www.cse.dnd.ca

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

CLEFs

Admiral Management Services Ltd (CLEF)
Kings Court
91-93 High Street
CAMBERLEY
Surrey GU15 3RN
Tel: (01276) 686678
Fax: (01276) 691028
Ralph Worswick
worsw_r@admiral.co.uk

EDS Ltd (CLEF)
Wavendon Tower
Wavendon
MILTON KEYNES
Bucks MK17 8LX
Tel: (01908) 284234
Fax: (01908) 284393
Trevor Hutton
trevor.hutton@edl.uk.eds.com

Logica UK Ltd (CLEF)
Cobham Park, Downside Road
COBHAM
Surrey KT11 3LG
Tel: (01932) 869118
Fax: (01932) 869119
Matthew Vale or Nigel Smith
valem or smithn@logica.com

Syntegra (CLEF)
Guidion House
Harvest Crescent
Ancells Park
FLEET
Hants GU13 8UZ
Tel: (01252) 777000
Fax: (01252) 777111
Geoff Harper
geoff.harper@syntegra.bt.co.uk

IBM Global Services (CLEF)
(formerly Data Sciences)
IBM UK Ltd
Meudon House, Meudon Avenue
FARNBOROUGH
Hants GU14 7NB
Tel: 01252 558081
Fax: 01252 558001
Bob Finlay
bob_finlay@uk.ibm.com
http://www.ibm.com/security/index.html

UK Scheme Publication 06
Issue 16