UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

CERTIFICATION REPORT No. P168

ICL OMEGA

Version 7.12 Increment 42

Issue 1.0

June 2002

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

Trademarks:

CERTIFICATION STATEMENT

ICL OMEGA is a computer based message handling product, intended for use in military systems.

ICL OMEGA Version 7.12 Increment 42 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the requirements of ITSEC Assurance Level E3 and Functionality Class F-B1 as defined in SIN No. 052 when running on the platforms specified in Annex B.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body
Date authorised	24 June 2002

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CMW	Compartmented Mode Workstation
DAC	Discretionary Access Control
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
LAN	Local Area Network
MAC	Mandatory Access Control
MLS	Multi Level Secure
MP-TE	Multi Platform Terminal Executive
SEF	Security Enforcing Function
SIN	Scheme Information Notice
SoM	Strength of Mechanisms
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

c. OMEGA Security Target,
ICL Defence,
IDS(1)01 Issue 6.2, 16 August 2001.

d. Harmonised Information Technology Security Evaluation Criteria (ITSEC),
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

e. Information Technology Security Evaluation Manual (ITSEM),
Commission of the European Communities,
Version 1.0, 10 September 1993.

f. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.

g. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.

h. Evaluation Technical Report,
CMG,
111632/T7.4/1, Issue 1.0, March 2002.

i. LFA/T158 ETR Supplement,
CMG,
111632/T7.4/2, 17 June 2002.

j. Trusted Computer Systems Evaluation Criteria,
Department of Defense, United States of America,
DOD 5200.28-STD, December 1985.

k. Operating OMEGA from a CMW,
ICL Defence,
IDS(4)04.02, Issue 6.0, 10 February 1998.

l. Operating OMEGA from a System High Workstation,
ICL Defence,
IDS(4)04.4, Issue 1.0, 2 February 2002.

m. Installing the OMEGA Client on a CMW,
ICL Defence,
IDS(4)04.01, Issue 9.0, 17 December 1997.

n. System Construction of Windows NT Workstation for connections to the TANDEM MHS,
ICL Defence,
DPN M932/1, Issue 1.0, 14 August 2001.

o. System Construction Mechanisms - Windows NT Workstation for OMEGA Client,
ICL Defence,
IDS(3)12/03/1, Issue 2.0, 23 January 2002.

p. OMEGA Command Reference Manual,
ICL Defence,
IDS(4)05, Issue 3.0, 5 February 2002.

q. OMEGA - Computer Operators Guide,
Fujitsu,
IDS(4)03, Issue 2.0, 1 May 2002.

r. OMEGA - Staff Users Guide,
ICL Defence,
IDS(4)04, Issue 1.0, 31 December 1994.

s. Secure Log Interrogation Functions,
ICL Defence,
UID 57, Issue 1.0, 15 October 1998.

t. System Security Base Data Maintenance,
ICL Defence,
UID 59, Issue 2.0, 30 October 1998.

u. ITSEC Certification Report 95/54 - DESC OMEGA Version 7.05, Increment 24,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, September 1995.

v. ITSEC Certification Report 96/66 - DESC OMEGA Version 7.05, Increment 38,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, 27 June 1996.

w. ITSEC Certification Report 96/68 - DESC OMEGA Version 7.05, Increment 43,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, 30 August 1996.

x. ITSEC Certification Report 97/80 - DESC OMEGA Version 7.05, Increment 50,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 1997.

y. ITSEC Certification Report 97/87 - DESC OMEGA Version 7.10, Increment 11,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, September 1997.

z. ITSEC Certification Report 98/98 - ICL OMEGA Version 7.11 Increment 11,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 1998.

aa. ITSEC Certification Report P102 - ICL OMEGA Version 7.12 Increment 09,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, September 1998.

bb. ITSEC Certification Report P134 - ICL OMEGA Version 7.12 Increment 19,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, January 2000.

cc. Guardian 90 Version C20 with Safeguard Version C22L,
Das Bundesamt für Sicherheit in der Informationstechnik,
BSI-ITSEC-0017-1993, October 1993.

dd. Scheme Information Notice No. 052, F-B1 Functionality Class,
UK IT Security Evaluation and Certification Scheme,
Issue 3.0, 1 May 1997.

ee. FIRESTONE Approval for OMEGA,
CESG,
L/2997LB/8006/179/5, 2 December 1993.

(This page is intentionally left blank)

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of ICL OMEGA Version 7.12 Increment 42 to the Sponsor, ICL Defence, and is intended to assist potential users when judging the suitability of the product for their particular requirements.

2. Previous Increments of ICL (originally DESC) OMEGA have been certified to Assurance Level E3:

- Version 7.05 Increment 24 in September 1995 (Reference [u])
- Version 7.05 Increment 38 in June 1996 [v]
- Version 7.05 Increment 43 in August 1996 [w]
- Version 7.05 Increment 50 in April 1997 [x]
- Version 7.10 Increment 11 in September 1997 [y]
- Version 7.11 Increment 11 in April 1998 [z]
- Version 7.12 Increment 09 in September 1998 [aa]
- Version 7.12 Increment 19 in January 2000 [bb]

Identification of Target of Evaluation

3. The version of the product evaluated was:

ICL OMEGA Version 7.12 Increment 42.

This product is also described in this report as the Target of Evaluation (TOE) and referred to as 'OMEGA'. The Developer was ICL Defence.

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

- Mandatory Access Control (MAC), Discretionary Access Control (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, a System High workstation and a CMW platform connected via local and wide area networks

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

6. OMEGA is a software product which has been implemented to run on a Compaq TANDEM "NonStop" server, running on the GUARDIAN 90 Operating System. The Operating System was outside the scope of this product evaluation; version C30, which has not been evaluated, was resident during testing. However, an earlier version, C20, does have a German IT Security Evaluation Criteria (ITSEC) certificate (number 0017-1993) [cc]. Additionally, during each OMEGA re-evaluation the Evaluators have been able to confirm that there have been no changes in dependency on the operating system - ie it is relied on to function correctly but does not implement any security enforcing functionality other than error recovery procedures. Only OMEGA Administrators have access to the operating system - users of the system access OMEGA via OMEGA clients on the platforms identified in Annex B of this report.

7. The enhancements introduced to ICL OMEGA Version 7.12 Increment 42 that were not present in the previously certified version are as follows:

a. porting of the Multi Platform Terminal Executive (MP-TE) to Windows NT4 SP6a;

b. printing to LAN printers;

c. enhancements to Secure Logging;

d. introduction of 'Releasable To' caveats; and

e. minor bug fixes.

8. A number of items of existing functionality were excluded from the re-evaluation:

a. link to TRAWLERMAN;

b. link to NICS Tare; and

c. MP-TE on HP-UX 10.10 workstation.

9. As these items were also excluded from the previous re-evaluation (Increment 19), the results from the evaluation of OMEGA Version 7.12 Increment 09 remain valid for them.

Evaluation

10. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UKSP 01 and UKSP 02 [a, b]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry on behalf of Her Majesty's Government.

11. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c], which users are advised to read. (A copy of the Security Target may be obtained from the Sponsor. The criteria against which the TOE was judged are described in the ITSEC [d]. This describes how the degree of assurance is expressed in terms of

the levels E0 to E6 where E0 represents no assurance. The methodology used is described in the IT Security Evaluation Manual (ITSEM) [e] and UKSP 05 [f, g].

12. The Certification Body monitored the evaluation which was carried out by the CMG Commercial Evaluation Facility (CLEF). The evaluation was completed in March 2002 when the CLEF submitted an Evaluation Technical Report (ETR) [h] and Supplement [i] to the Certification Body which, in turn, produced this Certification Report.

13. The Target Assurance Level for the product, as required by the Security Target [c], was E3 together with ITSEC [d] Functionality Class F-B1 as defined in Scheme Information Notice (SIN) No. 052 [dd].

14. The only cryptographic mechanism used in OMEGA is the CESG password algorithm FIRESTONE. This has been independently assessed by CESG and has been approved [ee] for use in OMEGA. For this reason a claim for minimum Strength of Mechanisms (SoM) is not applicable.

15. The minimum SoM for the search for vulnerabilities conducted by the Evaluators was High.

General Points

16. Prospective users of the TOE are reminded that the security functionality evaluated is that claimed in the Security Target [c]. This functionality may not necessarily meet all the threats that a user has identified in a particular operating environment. The assumed threats, intended method of use and environment are as stated in the Security Target. The TOE should only be used in its evaluated configurations (as indicated in Annex B) and in accordance with the recommendations and caveats contained in this report. It is the responsibility of purchasers to ensure that OMEGA Version 7.12 Increment 42 meets their requirements.

17. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Users (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued 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 Certification Body provides no assurance whatsoever for patches obtained in this manner.

18. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

19. The evaluation of ICL OMEGA Version 7.12 Increment 42 followed the generic Evaluation Work Programme described in the ITSEM [e] with work packages structured around the evaluator actions described in the ITSEC [d] and as appropriate to this particular re-evaluation. The results of this work were reported in the ETR and Supplement [h, i] under the ITSEC headings. This Certification Report summarises the assurance results in relation to the security functionality claimed in the Security Target [c].

20. This evaluation covered the changes identified in paragraph 7 above. The Evaluators examined the Developer's deliverables for changes since the previous re-evaluation and certification [bb] and, where those deliverables had not changed, they re-used the previous results.

Correctness - Construction

21. This aspect of the evaluation examined both the development process (ie the Security Target, the Architectural and Detailed Designs and the Implementation) and the environment in which it took place. The results were as follows:

a. The revised Security Target [c] described the Security Enforcing Functions (SEFs) provided by the TOE, and contained a product rationale identifying its method of use and intended environment; it also described how the product's functionality was adequate to counter the assumed threats. The Evaluators determined that there were only minor changes to the Security Target from the previous version and that there were no changes to the SEFs and that, therefore, the results of the previous evaluation of the Suitability Analysis were still valid.

b. The updated Architectural Design properly described the general structure of the TOE, together with any external interfaces and supporting hardware or firmware; it also clearly detailed how the SEFs of the TOE are provided and how the TOE is separated into security enforcing and other components.

c. The updated Detailed Design identified all security mechanisms, described all SEFs and other security relevant functions, mapped SEFs to mechanisms and components, documented interfaces adequately and enabled the relationships between levels of specification to be identified.

d. The correctness of the implementation was satisfactory, ie all security enforcing and security relevant functions offered in the Detailed Design were identifiable in the source code and test documentation and the associated tests were repeatable.

e. By witnessing and re-running a sample of the Developer's functional tests, the Evaluators were satisfied that their findings could be applied to all the platforms detailed in Annex B of this report.

f. The configuration control, programming standards and security aspects of the Developer's working environment were satisfactory.

22. The above findings enabled the Evaluators to conclude that the TOE met the requirements for ITSEC E3 in respect of its Security Target, Architectural and Detailed Designs, Implementation and Development Environment.

Correctness - Operation

23. The Evaluators checked and confirmed that:

a. the operational documentation adequately described the SEFs relevant to end users and administrators and how to operate the TOE in a secure manner;

b. the delivery and configuration documentation described the delivery arrangements from the development environment to the customer and the required system installation aspects;

c. the startup and operational documentation adequately described the procedures for secure startup and operation and, where relevant, for the deactivation or modification of SEFs; and

d. the information supplied described how these procedures maintain the security of the TOE.

24. The Evaluators concluded that the operational documentation [k - t] and the operational environment met the requirements for ITSEC E3.

Effectiveness - Construction

25. This aspect of the evaluation dealt with:

a. the suitability of the TOE's SEFs to counter the threats identified in the Security Target [c];

b. the ability of the SEFs and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c. the ability of the TOE's security mechanisms to withstand direct attack; and

d. the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

26. The Evaluators were satisfied that:

a. the Suitability Analysis confirmed that all the threats listed in the Security Target [c] were adequately countered by one or more of the stated SEFs and mechanisms;

b. the Binding Analysis demonstrated that it was not possible for any SEF or mechanism to conflict with or contradict the intent of any other SEF or mechanism;

c. the procedural measures in the Sponsor's Security Target [c] and the Developer's operational documentation [k - t] were sufficient to prevent all known construction vulnerabilities from being exploited;

d. the independent vulnerability analysis and penetration testing did not reveal any exploitable vulnerabilities in the TOE that were not satisfactorily corrected or neutralised; and

e. no changes had been made to the TOE which would affect the SoM Analysis that had been evaluated during the previous evaluation and certification [bb] and that, therefore, the results of the previous evaluation were still valid.

27. As OMEGA is for use with military systems, it is intended to be used with CESG approved password generation and encryption algorithms. The Evaluators confirmed the findings of earlier evaluations that the only critical mechanism, other than password generation and encryption, was 'sign-on' and this was critical only by virtue of the fact that it included the password generation and encryption mechanism, which was itself critical.

28. As a result of the above findings, the Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of Suitability, Binding, SoM and Construction Vulnerability.

Effectiveness - Operation

29. This work involved:

a. checking that the TOE can be used in a secure manner and assessing whether known vulnerabilities in its operation could, in practice, compromise its security; and

b. checking the List of Known Vulnerabilities in the operation of the TOE, as supplied by the Sponsor, and assessing the impact of these vulnerabilities and the measures proposed to counter their effects.

30. The evaluation confirmed that:

a. the TOE could not be configured or used in a manner which was insecure but which an administrator or end-user would reasonably believe to be secure;

b. the countermeasures proposed by the Sponsor in the List of Known Vulnerabilities in Operational Use were entirely satisfactory; and

c. all vulnerabilities revealed by the Sponsor or through penetration testing, had been either technically addressed or could be successfully overcome by procedural measures documented in the Security Target [c] and the operational documentation [k - t].

31. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

32. The Evaluators concluded that all the functionality claimed in the Security Target [c] had been met. This included functionality claims for:

- Identification and Authentication
- Access Control
- Accountability
- Audit
- Object Reuse
- Accuracy and Integrity
- Reliability of Service
- Data Exchange
- Administration of Security

33. This also included the claim for compliance with ITSEC Functionality Class F-B1 as defined in [dd]. Note that this version of ITSEC Functionality Class F-B1 resolves some known inconsistencies in Functionality Class F-B1 defined in Annex A of ITSEC [d] (both internal and with respect to the TCSEC [j] Class B1, and also takes into account official TCSEC interpretations relevant to B1. Compliance with the ITSEC version does not guarantee compliance with SIN No. 052; however, compliance with SIN No. 052 guarantees compliance with the ITSEC version.

III. CONCLUSIONS

Certification Result

34. After due consideration of the ETR and Supplement [h, i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that ICL OMEGA Version 7.12 Increment 42 meets the requirements of ITSEC Assurance Level E3 and Functionality Class F-B1 as defined in SIN No. 052 [dd] when running on the platforms specified in Annex B.

35. CESG has approved the use of the FIRESTONE [ee] password generation and encryption algorithm in OMEGA.

Recommendations

36. The product should only be used in accordance with the intended environment and method of use described in the Security Target [c]. Particular care should be taken that the product is configured and used in accordance with the operational documentation [k - t].

37. Potential users of the product should understand the specific scope of the Certification by reading this Report in conjunction with the Security Target [c].

38. Should continued use of the product with TRAWLERMAN, NICS Tare or an HP-UX workstation be envisaged, the relevant functionality should be included in a future re-evaluation. In the case of HP-UX the Certification Body advises that the certificate for HP-UX version 10.10 has been withdrawn and that the currently certified version is 10.20. This has no impact on OMEGA itself, which does not depend on HP-UX for security, but may have an impact on the security of data stored on the workstation after export from OMEGA as Version 10.20 contains corrections to a number of minor security problems (relating to occasional audit failure and file corruption) in Version 10.10.

(This page is intentionally left blank)

ANNEX A: SUMMARY OF THE SECURITY TARGET

Introduction

1. The Security Target is given in [c]. The Product Rationale is summarised below.

Product Rationale

Intended Environment and Method of Use

2. OMEGA is designed to process and protect sensitive Multi Level Secure (MLS) military data and should therefore operate only within secure physical environments. OMEGA hardware devices not contained in electronically shielded buildings should be protected by TEMPEST countermeasures. Data passing out of the secure environment (eg over unprotected cable runs) should be appropriately encrypted.

Summary of Security Features

Identification and Authentication

3. Identification and Authentication are provided by the TOE in order to ensure that access to OMEGA is limited to authorised users who have a valid function to perform. User authentication is by username, computer-generated password, terminal location and Personal Identification Device. Repeated password guessing is prevented by locking out users after a configurable number of logon failures. OMEGA supports the use of CESG supplied algorithms for password generation and encryption.

Access Control

4. OMEGA provides both MAC and DAC on the objects contained within it, so that access to the data processed by the product is limited to those users with sufficient clearance and the appropriate need to know. This contributes both to confidentiality and integrity of data and to control of the use of resources.

Accountability and Audit

5. Accounting functionality is provided to enable relevant information to be recorded about actions performed by users, or software processes acting on their behalf. OMEGA performs auditing for a wide variety of security related events. Facilities are included for analysing the audit log. Repeated attempted security breaches are notified to trusted users and can cause the perpetrator to be logged out.

Object Reuse

6. In the case of OMEGA, which is a transaction processing product not an operating system, users do not have the ability to access storage objects directly. Therefore, OMEGA constrains access to data by using the varied facilities of Access Control.

Accuracy and Integrity

7. OMEGA provides functionality to maintain accuracy and integrity of data. Whenever data is passed between data objects and users, devices, or software processes, facilities are provided to detect or prevent loss, addition or alteration of the data. The claimed or actual source or destination of the data transfer should remain unchanged. A security label is associated with data being transferred. Facilities are also provided to enable security critical operations to be performed by 'enforced co-operation' in order to maintain the integrity of a system using the product.

Reliability of Service

8. OMEGA addresses reliability of service in order to maintain availability of specific resources and recovery from error conditions, such that any impact on the operation or availability of a system is minimised. Reliability is achieved by error recovery procedures (which include facilities provided by the underlying operating system) and by distributing messages to roles rather than individual users.

Data Exchange

9. OMEGA addresses data exchange under the headings of identification and authentication, data confidentiality, accountability and audit.

Administration of Security

10. OMEGA provides facilities to enable administrators for each system within an OMEGA network to control and monitor the security facilities at all times.

Target Assurance Level

11. The Target Assurance Level for the product, as defined in the Security Target [c], was E3 as defined in ITSEC [d].

Target Functionality Class

12. The Target Functionality Class for the product, as defined in the Security Target [c], was F-B1 as defined in SIN No. 052 [dd].

ANNEX B: EVALUATED CONFIGURATION

Hardware

1. The evaluation results apply to the following platforms:

    - Tandem CLX and VLX processors
    - DRS20 Dumb Terminal
    - Intel 486 PC Terminal
    - DEC MLS+ CMW 3000 3.1a terminal
    - Windows NT4 SP6a (with HotPatch 04-06-01) System High workstation running on a PC as specified in [o]

Firmware

2. The TOE contains no security relevant firmware.

Software

3. The TOE consists of:

    - ICL OMEGA Version 7.12 Increment 42
    - MP-TE NT Build MP0400.28
    - MP-TE DEC MLS+ Build MP0200.09

(This page is intentionally left blank)