# UK ITSEC SCHEME CERTIFICATION REPORT No. P124

**Trusted Oracle7**

**Release 7.2.3.0.4**

Issue 1.0

July 1999



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

**RECOGNITION AGREEMENT OF**
**INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Agreement Group and as such:

- indicates that it is the issuer's claim that this certificate is a conformant certificate as defined in this Agreement; and

- therefore gives grounds for confidence, though it cannot in itself guarantee, that the certificate is a conformant certificate and that it will in practice be recognised by the other Members of the Agreement Group.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

# CERTIFICATION STATEMENT

Oracle Corporation's Trusted Oracle7 Release 7.2.3.0.4 is a multilevel secure relational database management system which can be used to provide security for systems which require F-B1 security functionality for databases.

Trusted Oracle7 Release 7.2.3.0.4 has been evaluated under the terms of the UK ITSEC Scheme and has met the requirements of ITSEC Assurance Level E3. The product also complies with the Functionality Class F-B1 when used in conjunction with an operating system of ITSEC F-B1 functionality or greater. Trusted Oracle7 Release 7.2.3.0.4 was evaluated on the HP-UX CMW Version 10.16 operating system which has since been renamed as the HP-UX Trusted Operating System (TOS) Version 10.16.

| | |
|---|---|
| **Originator** | **CESG**<br>Certifier |
| **Approval** | **CESG**<br>Head of the<br>Certification<br>Body |
| **Authorisation** | **CESG**<br>Senior Executive<br>UK ITSEC<br>Scheme |
| **Date authorised** | 27 July 1999 |

(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 |
| DBMS | Database Management System |
| ETR | Evaluation Technical Report |
| ITSEC | Information Technology Security Evaluation Criteria |
| ITSEM | Information Technology Security Evaluation Manual |
| MAC | Mandatory Access Control |
| MLS | Multilevel Secure |
| RDBMS | Relational Database Management System |
| ROWID | Row Identifiers (within Database tables) |
| SEF | Security Enforcing Function |
| SIN | Scheme Information Notice |
| SoM | Strength of Mechanisms |
| SQL | Structured Query language |
| TOE | Target of Evaluation |
| TOS | Trusted Operating System |
| 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 3.0, 2 December 1996.

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

c. Security Target for Trusted Oracle7 Database Server, Release 7.2,
Issue 1.8, January 1999.

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

e. Information Technology Security Evaluation Manual,
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. ITSEC Joint Interpretation Library (ITSEC JIL),
Joint Interpretation Working Group,
Version 2.0, November 1998.

i. LFL/T087 Evaluation Technical Report 1,
Logica CLEF, Logica UK Ltd,
CLEF.23399.16.1, Issue 1.0, 12 September 1997.

j. LFL/T087 Evaluation Technical Report 2,
Logica CLEF, Logica UK Ltd,
CLEF.23399.16.2, Issue 1.0, 7 August 1998.

k. LFL/T087 Evaluation Technical Report 3,
Logica CLEF, Logica UK Ltd,
CLEF.23399.16.4, Issue 1.0, 26 February 1999.

l. Scheme Information Notice No. 052, F-B1 Functionality Class,

UK IT Security Evaluation and Certification Scheme,
Issue 3.0, 1 May 1997.

m. Certification Report No. P114, Hewlett-Packard HP-UX Version 10.16 TOS,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, January 1999.

n. SQL*Net Administrator's Guide, Version 2,
Oracle Corporation,
A11325-1, July 1993.

o. Oracle7 Server Administrator's Guide, Release 7.2,
Oracle Corporation,
A20322-2, April 1995.

p. Oracle7 Server SQL Reference, Release 7.2,
Oracle Corporation,
A20325-2, April 1995.

q. Oracle7 Server Reference, Release 7.2,
Oracle Corporation,
A20327, April 1995.

r. Oracle7 Server Concepts, Release 7.2,
Oracle Corporation,
A20321-2, March 1995.

s. Oracle7 Server Utilities, Release 7.2,
Oracle Corporation,
A19485-2, March 1995.

t. Oracle7 Server Messages, Release 7.2,
Oracle Corporation,
A19483-2, April 1995.

u. Oracle Tools for UNIX Administrator's Reference Guide, Release 7.2,
Oracle Corporation,
A33679-1, May 1995.

v. Trusted Oracle7 for HP-UX CMW System Release Bulletin, Release 7.2.3,
Oracle Corporation,
A49289-6, February 1999.

w. Trusted Oracle7 for HP-UX CMW Installation Guide, Release 7.2.3,
Oracle Corporation,
A48381-1.

# I. INTRODUCTION

## Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of Trusted Oracle7 Release 7.2.3.0.4 to the Sponsor, Oracle Corporation, and is intended to assist potential users when judging the suitability of the product for their particular requirements.

## Identification of Target of Evaluation

2. The version of the product evaluated was:

Trusted Oracle7 Release 7.2.3.0.4

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Oracle Corporation.

3. Trusted Oracle7 Release 7.2.3.0.4 is a Multilevel Secure (MLS) Relational Database Management System (RDBMS) which operates under, or can be used to enforce, a Mandatory Access Control (MAC) policy. The product provides the foundation of data management facilities for applications which are incorporated within standalone and distributed systems, especially where such systems are operating in MLS or compartmented modes.

4. Trusted Oracle7 Release 7.2.3.0.4 when used in conjunction with an underlying operating system of functionality ITSEC F-B1 or greater, provides security for systems which require F-B1 security functionality for databases. Under these conditions, the main security functions are Identification and Authentication, Access Control, Audit and Accountability and Object Reuse.

5. Trusted Oracle7 Release 7.2.3.0.4 relies on the operating system to provide identification and authentication of the user as well as assigning a session label. Architecturally, in DBMS MAC mode, the unit of RDBMS storage is a row and the MAC policy is based on the row's label.

6. Trusted Oracle7 Release 7.2.3.0.4 was evaluated on the Hewlett-Packard operating system HP-UX CMW Version 10.16 which has been certified to ITSEC Assurance Level E3 and Functionality Class F-B1 [m].

## Evaluation

7. 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.

8. 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. The criteria against which the TOE was judged are described in the IT Security Evaluation Criteria (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], UKSP 05 [f, g] and the ITSEC Joint Interpretation Library [h].

9. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in February 1999 when the CLEF submitted the final Evaluation Technical Report (ETR) [k] to the Certification Body which, in turn, produced this Certification Report.

10. The Target Assurance Level for the product, as required by the Security Target [c], was E3. The TOE has no critical security mechanisms which are open to direct attack. As the underlying operating system provides the basic user authentication mechanism, no claim is made for a minimum Strength of Mechanisms (SoM) rating.

11. The minimum SoM associated with the search for vulnerabilities performed by the Evaluators was High.

**General Points**

12. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities remain undiscovered. 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 software configuration (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 Trusted Oracle7 Release 7.2.3.0.4 meets their requirements.

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

# II. EVALUATION FINDINGS

## Introduction

14. The evaluation of Trusted Oracle7 Release 7.2.3.0.4 followed the generic Evaluation Work Programme described in the ITSEM [e] with work packages structured around the evaluator actions described in the ITSEC [d]. The results of this work were reported in ETRs [i-k] under the ITSEC headings. This Certification Report summarises the assurance results in relation to the security functionality claimed in the Security Target [c].

## Correctness - Construction

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

a. The 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 appropriate for that method of use and was adequate to counter the assumed threats.

b. The Security Target also demonstrated compliance of the security objectives, threats, and SEFs with the requirements of the ITSEC F-B1 functionality class as described in SIN No. 052 [l].

c. The 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.

d. The final version of the 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. Due to some minor deficiencies in the Detailed Design documentation, additional assurance was obtained through examination of source code and header files, supplemented by further information provided by the Sponsor.

e. 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.

f. Repeating a sample of the Developer’s functional tests on HP-UX CMW Version 10.16 as specified in Annex B, produced no differences in the test results.

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

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

**Correctness - Operation**

17. 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 generation 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.

18. The Evaluators concluded that the Operational Documentation and the Operational Environment satisfied the requirements for ITSEC E3.

**Effectiveness - Construction**

19. 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.

20. 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 [n-w] were sufficient to prevent all known construction vulnerabilities from being exploited; and

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

21. The Sponsor's SoM analysis consisted of a statement that there are no critical mechanisms. The TOE was configured to provide the Identification mechanism with Authentication being performed independently by the underlying operating system. All mechanisms within the TOE were confirmed to be non-critical and the Evaluators were satisfied with the claim that a SoM rating was not appropriate.

22. Penetration testing did not identify any exploitable vulnerabilities associated with the use of the TOE beyond 2000 AD. The Evaluator's analysis showed that Trusted Oracle7 stores dates ranging from 1 January, 4712 BC to 31 December, 4712 AD within its own internal format. When inserting or retrieving date information to or from a Trusted Oracle7 database, the user can specify a format mask which is used to interpret the date. The default format mask is "DD-MON-YY" which assumes the date lies within the 20th century. The Oracle7 Server Concepts manual [r] states that a different date format mask should be used for dates outside the 20th century. A date format mask of "DD-MON-YYYY", for example, allows dates in the 20th and 21st centuries.

23. Within the scope of the evaluation, the Evaluators' analysis showed that the only potential area for Year 2000 vulnerabilities lies within the security auditing feature. Therefore, penetration testing was performed on the audit functionality and this demonstrated that:

a. the implementation of dates for auditing in Trusted Oracle7 is correct;

b. the date information, including the century, is stored correctly when an audit record is created; and

c. the date information can be viewed by a user/application provided an appropriate date format mask is used.

24. In conclusion, the analysis and penetration testing for Year 2000 did not identify any exploitable vulnerabilities within the TOE.

25. The independent vulnerability analysis and penetration testing investigated the potential for a covert channel using Row Identifiers (ROWIDs) as a signalling channel. The tests showed that a low bandwidth of 74 bits per second was possible on the configuration used. The SQL commands used in creating ROWIDs are all auditable, and the bit rate is less than 100 bits per second. This falls within the criteria set by the ITSEC Joint Interpretation Library [h] and it is therefore the Evaluator's conclusion that the ROWID covert channel is not exploitable. However, the impact on using a different hardware and operating system platform needs to be monitored in future evaluations.

26. The independent vulnerability analysis showed that a potential vulnerability exists whereby some Trusted Oracle error messages will reveal the operating system MAC labels to users who are not cleared to view the labels. Penetration testing confirmed that in all but one case labels are disclosed to lower classified users. The Sponsor has addressed this vulnerability by recommending the use of aliases for label names and this has been incorporated into an updated Security Target [c].

27. As a result of the above findings, the TOE is adjudged fully to have met the requirements for ITSEC E3 in respect of Suitability, Binding, SoM and Construction Vulnerability.

**Effectiveness - Operation**

28. 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.

29. 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. the independent vulnerability analysis and penetration testing did not reveal any exploitable vulnerabilities in the operation of the TOE.

30. The TOE thus meets the requirements for ITSEC E3 in respect of Ease of Use and Operational Vulnerability.

**Specific Functionality**

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

- Identification and Authentication
- Database Resources Access Control
- Mandatory Access Control
- Discretionary Access Control
- Administration of Privileges
- Audit and Accountability

## Unresolved Issues

32. There are no unresolved issues.

(This page is intentionally left blank)

# III. CONCLUSIONS

## Certification Result

33. After due consideration of the ETRs [i-k], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Trusted Oracle7 Release 7.2.3.0.4 running on HP-UX CMW Version 10.16 meets the requirements of ITSEC Assurance Level E3.

34. Trusted Oracle7 Release 7.2.3.0.4 also meets the requirements of Functionality Class F-B1 when used in conjunction with an underlying operating system of functionality ITSEC F-B1 or greater.

35. The Evaluators' analysis and penetration testing associated with Year 2000 did not identify any exploitable vulnerabilities within the TOE.

## 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 Developer's operational documentation [n-w].

37. The potential vulnerability of ROWIDs being used as a covert signalling channel should be re-assessed in future evaluations. This is to ensure that the currently identified bandwidth of 74 bits per second remains within the limit of 100 bits per second as advised by the ITSEC Joint Interpretation Library [h].

38. It should be noted that, under certain circumstances, the names of operating system labels can be disclosed to uncleared users. This is exploitable only when Trusted Oracle7, configured in DBMS MAC mode, is placed on an operating system which includes as part of its security policy, the aim of protecting the confidentiality of labels. In such circumstances, it is recommended that alternative (non-confidential) aliases be chosen for the label names.

39. It should be noted that user identification names on Trusted Oracle7 are not case sensitive. Therefore, when being used on operating systems that are case sensitive, user names should not be distinguished by case alone. This will help to preserve the concept of maintaining a single domain of unique user identification between Trusted Oracle7 and the underlying operating system. The A.E.IDOM environmental assertion in the Security Target [c] provides further guidance.

40. During this evaluation, it was necessary for the Sponsor to provide additional information to enable the Evaluators to complete their examination of the Detailed Design. It is recommended that this additional information be incorporated into the Detailed Design documentation if a further ITSEC evaluation is undertaken on Trusted Oracle7.

41. If the product is to be used to hold dates outside of the 20th century (eg in the 21st century), then a suitable date format mask should be configured to hold 4-digit years using the

NLS_DATE_FORMAT parameter file in the init.ora file. The Oracle7 Server Concepts manual [r] provides further details.

42. The evaluated configuration requires that the underlying operating system is used to authenticate users of Trusted Oracle7. System Administrators of the TOE must disable Trusted Oracle7 authentication when creating all database accounts through use of the IDENTIFIED EXTERNALLY syntax to enforce authentication to be performed externally.

43. Potential users of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c]. Only the relevant evaluated product configuration should be installed.

# 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 Method of Use

2. The TOE is intended for use in organisations where there is a need to maintain strict separation of information in a system, but where the substantial functional, integrity and cost benefits of a single, integrated system for data sharing and management are desired. Such organisations may be concerned with processing nationally or commercially sensitive information.

3. The Security Target contains a comprehensive and detailed set of assertions specifying:

- the environmental and method of use assumptions for the minimum physical and procedural measures required to maintain security of the TOE
- the installation, configuration, operation and maintenance requirements of the TOE

Assumed Threats

4. The Security Target contains a detailed threat analysis which describes:

- threat agents - *Outsiders*, *System Users*, and *External Events*
- two generic forms of attack - *unauthorised access to objects, resources, and services* and *impersonation*
- the correlation of threats to security objectives
- individual threat statements which describe how the security objectives of the TOE might be compromised
- a suitability analysis demonstrating how each threat is countered by the security enforcing functions and environmental and method of use assumptions

Summary of Security Features

5. The Security Target demonstrates both compliance with the ITSEC functionality class F-B1 as described in SIN No. 052 [l] and the means by which Trusted Oracle7 satisfies the intended security objectives.

6. The main security features are as follows:

- Identification and Authentication
- Control of global database resources
- MAC for database objects through the use of sensitivity labels
- DAC for database objects through the use of ownership and privilege
- Administration of system and object privileges and associated roles
- Audit and Accountability through the recording and analysis of security-related events to detect anomalies and analyse security behaviour
- Object Reuse implemented by access control mechanisms preventing access to unallocated storage

**Target Assurance Level**

7. The Target Assurance Level for the product was E3 as defined in ITSEC [d].

**Target Functionality Class**

8. The Target Functionality Class for the product was F-B1 when used in conjunction with an operating system which has been certified to ITSEC F-B1 functionality or greater, as defined in SIN No. 052 [l].

# ANNEX B: EVALUATED CONFIGURATION

## Hardware

1. The TOE has no hardware components. The Evaluator's testing was performed on 2 Hewlett-Packard PA-RISC 7200, 120 MHZ Uni Processor, HP9000 Model J210XC workstations. The workstations were configured as servers, connected by a LAN, with Trusted Oracle7 Release 7.2.3.0.4 being installed on each of the machines.

## Firmware

2. The TOE has no firmware components or dependencies.

## Software

3. The following Trusted Oracle software options were installed using the Selective Product Install feature:

- Oracle7 Distributed Database Option 7.2.3.0.0
- Oracle7 Server (RDBMS) 7.2.3.0.0
- SQL*NET V2 2.2.3.0.0
- SQL*PLUS 3.2.3.0.0
- TCP/IP Protocol Adapter (V2) 2.2.3.0.0
- PL/SQL V2 2.2.3.0.0

4. Selection of the above installation options resulted in further software being installed:

- <Database Startup> Load Files 1.0.0.0.1
- Oracle Common Libraries and Utilities 7.2.3.0.0
- Toolkit 2 Base 2.0.10.21.1
- SLAX: Parser

5. Once installed, the Trusted Oracle7 Patch 4 (for HP-UX CMW) was applied to update the Trusted Oracle7 version to Release 7.2.3.0.4.

## Modes of Operation

6. Trusted Oracle7 Version 7.2.3.0.4 was configured for the evaluation in DBMS MAC mode.

7. Trusted Oracle7 Release 7.2.3.0.4 relies on the operating system to provide identification and authentication of the user, as well as assigning a session label.

## Operating System

8. The underlying operating system used for the Evaluator's testing was HP-UX CMW Version 10.16, loaded with patches: PHKL_8238, PHCO_8593, PHCO_8595, PHCO_ 8597, PHCO_8598, PHCO_8600, PHCO_10478, PHCO_12714, PHKL_12795.

9. HP-UX CMW Version 10.16 was certified to ITSEC Assurance Level E3 and Functionality Class F-B1 in January 1999 [m] and has since been renamed as HP-UX Trusted Operating System (TOS) Version 10.16.

10. Due to timing differences between the Trusted Oracle7 and HP-UX evaluations, not all of the HP-UX evaluated patches were available for use in the Trusted Oracle7 evaluation. Given that the TOE is largely operating system independent, the Evaluators confirmed that the differences between these HP-UX patched versions of 10.16 had no effect on the secure operation of the TOE.