UK ITSEC SCHEME CERTIFICATION REPORT No 98/95

INFORMIX-OnLine

Version 7.23

Issue 1.0

March 1998

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

CERTIFICATION STATEMENT

Informix Software Corporation Limited's INFORMIX-OnLine Version 7.23 is a multi-threaded relational database management system designed to provide on-line transaction processing in standalone and distributed configurations with the capability to process queries in parallel.

INFORMIX-OnLine Version 7.23 has been evaluated under the terms of the UK ITSEC Scheme and has met the requirements of ITSEC Assurance Level E2. INFORMIX-OnLine relies on the underlying operating system to provide identification and authentication, audit, discretionary access control and networking. When used in conjunction with an operating system of ITSEC F-C2 functionality or greater, INFORMIX-OnLine can be used to provide security for systems which require F-C2 security functionality for databases.

Originator	**CESG** Certifier
Approval	**CESG** Head of the Certification Body
Authorisation	**CESG** Senior Executive UK ITSEC Scheme
Date authorised	_____

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

AAO	Audit Administration Officer
AFE	Administrative Front End
ASF	Association Services Facility
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
DAC	Discretionary Access Control
DBA	Database Administrator
DBSA	Database System Administrator
DBSSO	Database System Security Officer
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
OLA	OnLine Administrator
OSA	Operating System Administrator
RDBMS	Relational Database Management System
SEF	Security Enforcing Function
SoM	Strength of Mechanisms
SQL	Structured Query Language
TCSEC	Trusted Computer Systems Evaluation Criteria
TOE	Target of Evaluation
UFE	User Front End
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

1. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 3.0, 2 December 1996.

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

3. INFORMIX-OnLine V7.23 Claims Document,
Informix Software Limited
Version 1.03, 8 October 1997.

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

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

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

7. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 1.0, June 1994.

8. LFA/T106 Evaluation Technical Report,
Admiral CLEF,
7017B/T16/1, Issue 2.0, January 1998.

9. Certification Report No 95/46,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 1995.

10. Certification Report No 96/59,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 1996.

11. Informix Guide to SQL Reference,
Informix Software, Inc.,
Version 7.2, December 1994.

12. Informix Guide to SQL Syntax,
Informix Software, Inc.,
Version 7.2, December 1994.

13. Informix Guide to SQL Tutorial,
Informix Software, Inc.,
Version 7.2, December 1994.

14. DB-Access User Manual,
Informix Software, Inc.,
Part No. 000-7636, Version 7.2, December 1994.

15. INFORMIX-OnLine Dynamic Server Trusted Facility Manual,
Informix Software, Inc.,
Version 7.2, December 1995.

16. INFORMIX-OnLine Dynamic Server Administrator's Guide, Volume 1,
Informix Software, Inc.,
Version 7.2, December 1994.

17. INFORMIX-OnLine Dynamic Server Administrator's Guide, Volume 2,
Informix Software, Inc.,
Version 7.2, December 1994.

18. UNIX Products Installation Guide,
Informix Software, Inc.,
Version 7.23, December 1994.

19. Documentation Notes
Informix Software, Inc.,
ONLINEDOC_7.2, 4 February 1998.

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of INFORMIX-OnLine Version 7.23 to the Sponsor, Informix Software Limited, 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:

INFORMIX-OnLine Version 7.23.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Informix Software, Inc.

3. INFORMIX-OnLine Version 7.23 is a multi-threaded Relational Database Management System (RDBMS). The TOE provides on-line transaction processing with the capability to process queries in parallel in standalone and distributed configurations.

4. The TOE can be operated in standalone and client/server configurations. The standalone and client/server configurations allow one or more users to access a database stored on a single platform. In standalone configuration the application software is stored and run on the same platform as the database server, while in a client/server configuration the application software and the database server are stored on different platforms connected via a network.

5. The TOE relies on the underlying operating system to provide identification and authentication, Discretionary Access Control (DAC), audit and networking.

6. The TOE was evaluated on the DEC Digital UNIX 4.0c operating system running on a DEC Alpha processor-based hardware platform as required by the Security Target [Reference c]. The Evaluators performed all their functional and penetration testing of the TOE on the DEC Digital UNIX 4.0c operating system running on a DEC AlphaServer 4200. Since the TOE relies on the operating system to provide identification and authentication, DAC, accountability and audit and networking functionality, it is assumed for the purposes of this evaluation that the operating system has provided the correct information to the INFORMIX-OnLine RDBMS and that the security enforcing and security relevant functionality provided by the operating system functions correctly. However, as the Security Target contained functionality claims for Identification and Authentication, DAC and Accountability and Audit, some assurance that the operating system provided the correct information to the TOE was gained through the Evaluators' functional testing.

7. INFORMIX-OnLine Version 7.23, 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

Identification and Authentication, DAC, Accountability and Audit, Object Reuse, Accuracy, Constraints, Reliability of Service and Distributed Operation.

8. Any operating system on which the TOE is to be used must include in its evaluated configuration all of the networking functionality required by the TOE, ie remote login functionality and the functionality provided by the network files `~/.rhosts` and `/etc/hosts.equiv`.

9. In its evaluated configuration, the TOE must be configured with administrator role separation. The evaluated configuration of the TOE includes the separation of the administration of the TOE into 5 role types: Database Administrator (DBA), Operating System Administrator (OSA), OnLine Administrator (OLA), Database System Security Officer (DBSSO) and Audit Analysis Officer (AAO). Further details are provided in Annex A.

10. Previously certified versions of the TOE include the INFORMIX-OnLine/Secure and INFORMIX STAR/Secure products, Version 5.0, Release UD7 (see Certification Report No 95/46 [i]). These 2 products were combined in INFORMIX-OnLine Version 7.10 UD1X5 (see Certification Report No 96/59 [j]) to give the required standalone or distributed functionality for a given installation.

Evaluation

11. The evaluation was carried out in accordance with the rules of the UK IT Security Evaluation and Certification Scheme which is 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.

12. 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] and UKSP 05 [f, g].

13. The Certification Body monitored the evaluation which was carried out by the Admiral Commercial Evaluation Facility (CLEF). The evaluation was completed in January 1998 when the CLEF submitted an Evaluation Technical Report (ETR) [h] to the Certification Body which, in turn, produced this Certification Report.

14. The Target Assurance Level for the product, as required by the Security Target [c], was E2. As claimed in the Security Target, there are no critical mechanisms in INFORMIX-OnLine. It is therefore not appropriate to make a claim for the minimum Strength of Mechanisms (SoM).

General Points

15. 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 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 INFORMIX-OnLine meets their requirements.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

17. The evaluation of INFORMIX-OnLine Version 7.23 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 the ETR [h] 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

18. 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 takes place. The results were as follows:

1. The final version of the Security Target [c] stated the Security Enforcing Functions (SEFs) provided by the TOE, and contained a product rationale identifying its method of use and intended environment; it also stated how the product's functionality was adequate to counter the assumed threats.

2. The Architectural Design properly stated 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.

3. The final version of the Detailed Design identified all security mechanisms, stated 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.

4. The correctness of the Implementation was satisfactory, ie all security enforcing functions offered in the Security Target were identifiable in the test documentation and the associated tests were repeatable.

5. Repeating the Sponsor's functional tests on a Digital UNIX 4.0c operating system running on an AlphaServer 4200 machine using a local-loopback link produced no differences in the test results. The test configuration is detailed in Annex B.

6. The configuration control and security aspects of the Developer’s working environment were satisfactory.

19. The above findings enabled the Evaluators to conclude that the TOE fully met the requirements for ITSEC E2 in respect of its Security Target, Architectural and Detailed Designs, Implementation and Development Environment.

Correctness - Operation

20. The Evaluators checked and confirmed that:

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

2. the delivery and configuration documentation stated the delivery arrangements from the development environment to the customer and the required system generation aspects;

3. the startup and operation documentation adequately stated the procedures for secure start-up and operation and, where relevant, for the deactivation or modification of SEFs; and

4. the information supplied stated how these procedures maintain the security of the TOE.

21. The Evaluators concluded that the operational documentation and the operational environment satisfied the requirements for ITSEC E2.

Effectiveness - Construction

22. This aspect of the evaluation dealt with:

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

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

3. the ability of the TOE’s security mechanisms to withstand direct attack; and

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

23. The Evaluators were satisfied that:

1. 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;

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

3. the procedural measures in the Sponsor's Security Target [c] and the Developer’s operational documentation [k-s] were sufficient to prevent all known construction vulnerabilities from being exploited; and

4. penetration testing did not reveal any exploitable vulnerabilities in the TOE that were not satisfactorily corrected or neutralised.

24. The Evaluators found that the Sponsor's SoM Analysis gave a good justification that the TOE contains no critical mechanisms. All critical mechanisms are provided by the underlying operating system. As such the mechanisms of the TOE are not subject to a SoM analysis. It is therefore inappropriate to award a minimum SoM rating. However, it is also true that any minimum SoM rating arising from the combination of the TOE and an underlying operating system would be limited by the minimum SoM claimed for the operating system.

25. As a result of the above findings, the TOE is adjudged fully to have met the requirements for ITSEC E2 in respect of Suitability, Binding, SoM and Construction Vulnerability.

Effectiveness - Operation

26. This work involved:

1. checking the ease of use of the TOE in a secure manner and assessing whether known vulnerabilities in its operation could, in practice, compromise its security; and

2. 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.

27. The evaluation confirmed that:

1. 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;

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

3. no vulnerabilities were revealed during comprehensive penetration testing.

28. The TOE thus meets the requirements for ITSEC E2 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

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

- Identification and Authentication
- DAC

- Accountability and Audit
- Object Reuse
- Accuracy
- Constraints
- Reliability of Service
- Distributed Operation

30. Although Identification and Authentication, DAC and Audit and Accountability have SEFs associated with them in the Security Target [c], and as such were tested as part of the Evaluators' functional testing of the TOE, the SEFs are implemented in the underlying operating system.

III. CONCLUSIONS

Certification Result

31. After due consideration of the ETR [h], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that INFORMIX-OnLine Version 7.23 meets the requirements of ITSEC Assurance Level E2.

Recommendations

32. 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 products are configured and used in accordance with the operational documentation [k-s].

33. 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.

34. Users of the product should be aware that the underlying operating system provides the identification and authentication, audit, DAC and networking functionality of the TOE. In particular, users should be aware of the security limitations of operating system passwords and the need to keep them secret.

35. Product administrators are recommended to read the operational documentation [k-s] thoroughly, in particular the Trusted Facility Manual [o], before attempting to configure the product for auditing.

36. Product administrators are recommended to use the default setting of ADTERR (see Trusted Facility Manual [o] page B-2), viz ADTERR=0, in order to write the failure of an audit write to the operating system message log.

37. The “informix” user account has the ability to bypass role separation and access control mechanisms by editing the system master database. Product administrators are therefore recommended to create dedicated OLA accounts and then to lock the “informix” account from the “root” account.

38. Product administrators are recommended to audit the actions of all privileged users of the TOE, in particular the OLA and AAO administrators, because their actions could breach the security of the TOE.

39. Users of the product are recommended to enter dates as complete 4 digit numbers. If 2 digit numbers are entered, depending on the setting of the DBCENTURY environment variable, the numbers may be interpreted as 20th century dates. The TOE documentation [k] provides full details of the settings of DBCENTURY.

40. Product administrators should note that audit masks and user permissions are associated with a username. If the username is deleted and re-created, the username will keep the permissions associated with the username before deletion. Procedures to remove user permissions from the TOE environment using the SQL REVOKE statement are detailed in the TOE documentation [l, m].

41. Product administrators should note that external security measures for the TOE are documented in the Security Target [c] and not in the administrative documentation.

ANNEX A: SUMMARY OF THE SECURITY TARGET

Introduction

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

Product Rationale

Intended Method of Use

43. The TOE is a general purpose, distributed RDBMS which may be used in a wide variety of applications in an open systems environment.

44. The TOE is designed to run on a TCSEC C2 (ITSEC F-C2) operating system, either standalone or with secure networking support. The design does not require any specific implementation of such an operating system but the operating system must provide identification and authentication, audit, DAC and networking.

45. In conjunction with an underlying operating system of ITSEC F-C2 functionality certified to ITSEC E2, the TOE is suitable for use in systems requiring E2/F-C2 assurance and functionality.

46. The product supports 4 distinct types of user role:

a. regular users, who have no special privileges;

b. Database System Administrator (DBSA), who is responsible for the general maintenance of the product;

c. DBSSO, who is responsible for maintaining audit masks; and

d. AAO, who is responsible for configuring auditing and maintaining and analysing the audit trail.

47. It is assumed that there is an OSA who is responsible for maintaining the underlying operating system and, in particular, for creating and maintaining user accounts.

48. A DBSA may be of 2 types: a DBA, who is responsible for controlling access to databases, or an OLA, who is responsible for maintaining, administering and operating the database server.

49. There may be multiple DBSA, DBSSO and AAO accounts. The AAO account is not intrinsically different from a regular user account; exclusive access to audit data is achieved by means of the operating system DAC mechanism.

Environmental Assumptions

50. It is assumed that the TOE and the underlying operating system are installed, operated and maintained in accordance with the TOE's Administrator's Guide [p, q].

51. It is assumed that the operating system is configured to provide the reserved operating system group "informix" for use in controlling access to the device or devices containing the TOE's data stores and for use in managing and assisting system operations. It is also assumed that no regular user is a member of the "informix" group.

52. It is assumed that the TOE's Global Language Support feature is configured to use the default US English locale.

53. It is assumed that the product is configured to use the operating system managed audit trail.

54. It is assumed that the High Performance Loader will be used in "Deluxe Mode".

Assumed Threats

55. The primary threat to the TOE is the unauthorised disclosure or modification of sensitive material that it may handle.

56. The threats applicable to all RDBMS products from regular users are as follows:

- insider attack
- browsing
- aggregation
- denial of service
- simultaneous data access
- untrusted software

57. The threats from privileged users are as follows:

a. A DBSA can instigate actions leading to a denial of service. The "informix" user is a DBSA who can disclose unauthorised data because this user can change the DAC requirement for data access.

b. A DBSSO can disable the auditing of other users' actions.

c. The OSA is in a position to disclose or modify sensitive information. This user can also assign inappropriate privileges to users, allowing them unauthorised access to sensitive information, and to modify the operating system audit trail, effectively disabling the product's auditing facilities.

d. An AAO can read audit data which may indirectly yield information to the AAO which violates the DAC policy.

Summary of Security Features

58. In conjunction with an underlying operating system of ITSEC F-C2 functionality the TOE provides functionality for following security features:

- Identification and Authentication
- DAC
- Accountability and Audit
- Object Reuse
- Accuracy
- Constraints
- Reliability of Service
- Distributed Operation

59. The TOE relies on the underlying operating system to provide identification and authentication, DAC, audit and networking.

60. In conjunction with an underlying operating system of ITSEC F-C2 functionality, the TOE provides DAC facilities to prevent unauthorised access to sensitive information. The product enforces DAC on product objects, including databases, tables, fragments and columns, and extends to the level of the individual user.

61. The product also provides:

a. configurable auditing facilities to monitor database activity;

b. transaction management facilities to ensure data integrity when simultaneous requests are made for access to the same data; and

c. recovery, archiving and mirroring facilities to minimise disruption caused by system or hardware failures.

Target Assurance Level

62. The Target Assurance Level for the TOE, as defined in the Security Target [c], was E2 as defined in ITSEC [d].

(This page is intentionally left blank)

ANNEX B: EVALUATED CONFIGURATION

Hardware

63. The TOE has no hardware components.

64. The TOE is designed for use on symmetric multi-processor and uniprocessor architectures.

65. The TOE was evaluated on a DEC Alpha processor-based hardware platform as required by the Security Target [c].

66. All communications between the TOE database server and client were by a network connection. It is also possible for the server and client to communicate via shared memory. This was excluded from the evaluation.

67. The Evaluators' testing was performed with the TOE server and client installed on the DEC Digital UNIX 4.0c operating on an AlphaServer 4200 machine using a network local-loopback link for client/server communications.

Firmware

68. The TOE has no firmware components. There were no firmware dependencies affecting the evaluation.

Software

69. The TOE consists of INFORMIX-OnLine Version 7.23. The TOE comprises the following components:

- RDBMS kernel
- Associated Services Facility (ASF) services
- Administrative Front End (AFE)

70. The RDBMS kernel is security enforcing. The kernel parses and executes SQL requests it receives from the User Front End (UFE) client, and includes the following security enforcing software layers:

- DAC
- Object Reuse
- Identification and Authentication
- Auditing

71. The ASF services are security relevant. They provide the basis of the client/server communications of the TOE. The ASF is the transportation layer of the RDBMS kernel. It carries information from RDBMS clients to the RDBMS server and from the RDBMS server to the RDBMS clients.

72. The AFE is security enforcing. It includes the following utilities:

- onaudit
- oncheck
- oninit
- onload
- onlog
- onmode
- onparams
- onshowaudit
- onspaces
- onstat
- onload
- ontape
- onunload

73. INFORMIX-OnLine Version 7.23 was evaluated on the DEC Digital UNIX 4.0c operating system as required by the Security Target [c].

Unevaluated Security Features

74. The UFE supplied with the TOE and other UFEs (such as INFORMIX-ESQL/C V7.23 and INFORMIX-ESQL/COBOL V7.23) are outside the scope of the evaluation because they do not provide any security relevant functionality.

75. The TOE can be configured without administrator role separation, using the "root" and "informix" users to perform all administrative functions. The configuration of the TOE without administrator role separation is outside the scope of the evaluation.

76. The following components were outside the scope of the evaluation:

a. On-Monitor, viz the command utility onmonitor;

b. DB/Cockpit, viz oncockpit and onprobe;

c. On-Archive, viz onarchive, cron_autovop, onautovop, oncatlgr, ondatatr and onkeymgr;

d. the performance monitor, viz onperf, onedcu, onedpu and xtree;

e. OnBar, a backup and restore facility;

f. TOE managed auditing (a database kernel-configurable option); and

g. shared-memory client/server communications.