



**UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME**



122-B

CERTIFICATION REPORT No. P220

**TRACKER 2700
(Data Collection Unit)**

running software 10235

Issue 1

October 2005

© Crown Copyright 2005

Reproduction is authorised provided the report
is copied in its entirety

UK IT Security Evaluation and Certification Scheme,
Certification Body, CESG, Hubble Road,
Cheltenham, GL51 0EX
United Kingdom

[Trademarks:]

All product or company names are used for identification purposes only and may be trademarks of their respective owners.

CERTIFICATION STATEMENT

The Tracker 2700, referred to in DFTS as the Data Collection Unit (DCU), is a commercial multi user, multi tasking communications management device. It can also be used as a sophisticated alarm monitor, or an intelligent multi port access device. In the context of DFTS, it is used for managing the connectivity between the controlled switches and DVMS.

The Tracker 2700 DCU running software 10235 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the requirements of ITSEC Assurance Level E2 when running on the platform as specified in Annex B.

Originator	CESG Certifier
Approval and Authorisation	CESG Technical Manager of the Certification Body
Date authorised	25 October 2005

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT.....iii

TABLE OF CONTENTS.....v

ABBREVIATIONS.....vii

REFERENCES.....ix

I. INTRODUCTION.....1

 Intended Audience 1

 Identification of Target of Evaluation 1

 Evaluation 2

 General Points..... 2

II. EVALUATION FINDINGS5

 Introduction..... 5

 Correctness - Construction 5

 Correctness - Operation 6

 Effectiveness - Construction 6

 Effectiveness - Operation 7

 Specific Functionality..... 7

III. CONCLUSIONS.....9

 Certification Result..... 9

 Recommendations 9

ANNEX A: SUMMARY OF THE SECURITY TARGET 11

ANNEX B: EVALUATED CONFIGURATION..... 13

(This page is intentionally left blank)

ABBREVIATIONS

CLEF	Commercial Evaluation Facility
CSS	Circuit Switched Service
DCU	Data Collection Unit
DFTS	Defence Fixed Telecommunications Service
DVMS	DFTS Voice Management System (called the Exchange Management System in [c])
EPROM	Erasable Programmable Read Only Memory
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
I/O	Input/Output
ROM	Read Only Memory
SEF	Security Enforcing Function
SoM	Strength of Mechanisms
SSP	System Security Policy
SSS	Secure Switched Service
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 5.0, July 2002.
- b. CLEF Requirements,
UK IT Security Evaluation and Certification Scheme,
UKSP 02 Part I, Issue 4.0, April 2003.
- c. Security Target for the DTT Tracker 2700 Data Collection Unit,
BT Global Services,
DCN 20041011005, Issue 6.3b, 18 March 2005.
- 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, Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02 Part II, Issue 1.1, October 2003.
- g. Manual of Computer Security Evaluation, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05 Part III, Issue 3.1, October 2003.
- h. ITSEC Joint Interpretation Library (ITSEC JIL),
Joint Interpretation Working Group,
Version 2.0, November 1998.
- i. LFL/T188 Tracker 2700 Evaluation Technical Report,
LogicaCMG,
310.EC.200188/T7.4/1, Issue 1.0, 13 June 2005.
- j. DFTS DATA COLLECTION UNIT Certification Report No. P181,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, May 2003.
- k. Tracker 2700 Configuration Instruction,
BT Global Services,
DCN 20040802002, Issue Draft, 1 July 2004.

- l. DFTS SyOPs Annex J DVMS,
BT Global Services,
DCN 1998081811, Issue 3.0, 18 October 2004.

- m. DFTS SSP,
BT Ignite Solutions,
DCN 1997081403, Issue 5.3, 13 January 05.

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of Tracker 2700, also referred to as the DCU, running Software 10235 to the Sponsor, BT Global Services, formally BT Ignite Services, who also integrated the DCU into the Defence Fixed Telecommunications Service (DFTS) Voice Services. The evaluation was conducted in the context of the DFTS.

Identification of Target of Evaluation

2. The version of the product evaluated was:

Tracker 2700 (Data Collection Unit) running Software 10235.
3. This product is also described in this report as the Target of Evaluation (TOE). The Developer was Data Track Technology.
4. An earlier version of the DCU, the Tracker 2650, was evaluated and certified [j]. The design of the Tracker 2700 DCU has been completely changed from that of the Tracker 2650.
5. The DCU provides connectivity between the switches and DVMS in the DFTS and provides the following functionality:
 - a. it prevents access to the DVMS from the switch subscriber ports
 - b. it allows management of the switches from the DVMS
 - c. it collects alarms from the switches and passes them to DVMS.
6. The DCU is an Intel processor computer running a tailored version of Linux. It is fitted with the following interfaces:
 - a. a modem port for communication with DVMS; this interface has a SafeDial encryption unit installed internally, so that all traffic through the interface requires a compatible SafeDial device on the communicating equipment.
 - b. an Ethernet port for management of the DCU or management of controlled switches. (this interface is used for initial configuration only, and is not used in DFTS operational use).
 - c. a serial control port for management of the DCU. (this interface is used for initial configuration only, and is not used in DFTS operational use).
 - d. four RS232 data ports which are used to gather data from the controlled switches, allow management of the switches, or both.

- e. a Digital I/O port which provides sixteen digital inputs which are used to receive notification of errors from the switches, and seven digital outputs.
7. The following software components are included within the DCU software:
 - a. Linux kernel.
 - b. Linux processes.
 - c. Python Interpreter and Python Applications.
 - d. File Store.
 8. Note that, although the SafeDial is physically contained within the Tracker 2700 DCU, it is not within the TOE, and therefore out of scope of this evaluation.

Evaluation

9. 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 [References a, b]. The Scheme has established a Certification Body, which is managed by the Communications-Electronics Security Group (CESG) on behalf of Her Majesty's Government.
10. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c], which prospective users are advised to read. The criteria against which the TOE was judged are described in the IT Security Evaluation Criteria (ITSEC) [j]. 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 02 [f], and UKSP 05 [g], and the ITSEC Joint Interpretation Library [h].
11. The Certification Body monitored the evaluation, which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed in June 2005 when the CLEF submitted an Evaluation Technical Report (ETR) [i] to the Certification Body, which, in turn, produced this Certification Report.
12. The Target Assurance Level for the product, as required by the Security Target [c], was E2.
13. There was no Strength of Mechanism (SoM) claim made for the TOE.

General Points

14. 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 the Tracker 2700 DCU running Software 10235 meets their requirements.

15. 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.
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 Tracker 2700 DCU running Software 10235 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 [i] 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 took place. The results were as follows:
- a. 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 appropriate for that method of use and was adequate to counter the assumed threats.
 - b. 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.
 - c. 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.
 - d. The correctness of the implementation was satisfactory, i.e. all security enforcing and security relevant functions were identifiable in the test documentation, and the associated tests were repeatable.
 - e. Repeating an agreed sample of the Developer's functional tests produced no differences in the test results.
 - f. The configuration control and security aspects of the Developer's working environment were satisfactory.
19. The Evaluators concluded that the TOE 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:
 - 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 start-up and operation documentation adequately described the procedures for secure start-up and operation and,
 - d. the information supplied described how these procedures maintain the security of the TOE.
21. The Evaluators concluded that the Operational Documentation and the Operational Environment met the requirements for ITSEC E2.

Effectiveness - Construction

22. 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.
23. 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 [e] and the Developer's operational documentation [k, l] were sufficient to prevent all known construction vulnerabilities from being exploited; and,

- d. the independent vulnerability analysis and penetration testing during March 2005 did not reveal any exploitable vulnerabilities in the TOE that were not satisfactorily corrected or neutralised.
24. The Evaluators concluded that the TOE met the requirements for ITSEC E2 in respect of Suitability, Binding, and Construction Vulnerability.

Effectiveness - Operation

25. 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.
26. 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; and
 - b. the independent vulnerability analysis and penetration testing on 16 March 2005 did not reveal any exploitable vulnerabilities in the operation of the TOE.
27. The Evaluators concluded that the TOE met the requirements for ITSEC E2 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

28. The Evaluators concluded that all the functionality claimed in the Security Target [c] had been met.

(This page is intentionally left blank)

III. CONCLUSIONS

Certification Result

29. After due consideration of the ETR [i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that the Tracker 2700 DCU running Software 10235 meets the requirements of ITSEC Assurance Level E2.

Recommendations

30. The product should only be used in accordance with the intended environment and method of use described in the Security Target [c].
31. Particular care should be taken that the product is configured and used in accordance with the operational documentation [k, l]. Particular attention should be paid to the list of alarms as used in the evaluated TOE, as changing the alarms list means changing the code contained within the Meridian and Realitis alarms rules files, *meridianal.rule* and *idxal.rule*, respectively Ref. [c] Para. 3.5 and evaluated SEF, DCU-5.
32. 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.

(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 and security features are summarised below.

Intended Method of Use

2. The DCU is used to provide separation between DFTS Voice Services switches and DVMS. The objective of the TOE is to protect the integrity of each switch and of the DVMS. This is achieved by providing a controlled interface to the management ports and functions of each switch to which the TOE is connected. The DCU was evaluated in the context of the DFTS CSS and SSS only.

Assumed Threats

3. The threats to DFTS are listed in the DFTS SSP[m], with only a limited subset of them applicable to the DFTS DCU:

- a. Switch Reconfiguration
- b. Denial of Service
- c. Alteration of Data

Summary of Security Features

4. The DCU is required to provide the following:

- a. DCU-2 The link between the DCU and the DVMS shall be closed down once the communication has ended.
- b. DCU-3 Configuration changes to the DCU can only be achieved through the DCU's management port(s).
- c. DCU-4 The only non-requested information to pass from the DCU to the DVMS shall be alarm information.
- d. ¹DCU-5 Of the alarms received by the DCU from the Meridian switch, the only ones transmitted to the DVMS shall be those with Meridian Alarm IDs listed in [c] Para 3.5.

¹ This SEF only applies to the Meridian Switch inasmuch as there is a defined subset of alarm messages that are passed, whereas all of the alarm messages generated by the Realistic Switch are passed..

Target Assurance Level

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

Claimed Minimum Strength of Mechanisms

6. There was no SoM claim for this product.

ANNEX B: EVALUATED CONFIGURATION

Hardware

1. The evaluation results apply to the following platform :
 - a. Tracker 2700 DCU in its DFTS configuration [k] with the interfaces identified in Section I, Paragraph 6 and with the SafeDial encryption unit fitted.

Firmware

2. There is no firmware, i.e. software in ROM. The TOE software is stored in EPROM and EEPROM.

Software

3. The TOE consists of the Tracker 2700 DCU running Software 10235.
 - a. The software has the following architectural components:
 - i. Linux Kernel:- this provides basic operating system facilities such as process and memory management, inter-process communication, and low level control of external interfaces.
 - ii. Linux processes :- these provide control of the interfaces, and other necessary high level operating system functions.
 - iii. Python Interpreter and Python Applications :- these provide application specific processing; for DFTS use, they collect alarms from the controlled switches (Realitis or Meridian), and generate the appropriate DCU alarms for delivery to DVMS.
 - iv. File Store:- this stores, inter alia, the executables for the Linux processes, Python Interpreter and Applications, configuration and rule files for the Python Applications, other configuration files, and data logs.

(This page is intentionally left blank)