Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 40/2007

19 January 2007

Version 1.0

Amendment Record

Version	Date	Description
1.0	19/1/2007	Public release.

Executive Summary

1 The BAE Systems Mobile Trusted Filter Version 1.0 is a special purpose device that is designed to provide RED/BLACK separation in systems where control data, which cannot be protected by encryption or other means, must cross a RED/BLACK boundary. The device allows the control equipment (on the RED side) to transmit only a specified set of control commands to the BLACK side equipment. If the Mobile Trusted Filter receives an invalid command, an alarm status flag is raised and the command is discarded. The device allows the BLACK side equipment to pass data (typically a command response) from the BLACK to the RED side. Mobile Trusted Filter Version 1.0 is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of BAE Systems Mobile Trusted Filter Version 1.0 to the Information Technology Security Evaluation Criteria (ITSEC) evaluation level E5. The report concludes that the TOE has met the target evaluation level of E5 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by LogicaCMG and was completed in October 2006.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) provides additional recommendations in this report concerning the following topics:

a) Tamper seal and cable integrity.

b) Installation considerations.

c) Operational considerations.

d) Residual risk of covert channels.

e) Data diode considerations.

4 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target (Ref [1]), and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

5 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

6 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Mobile Trusted Filter Version 1.0, against the requirements of the Information Technology Security Evaluation Criteria (ITSEC) evaluation level E5, and

b) provide a source of detailed security information about the TOE.

7 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

8 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Section 2.5.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Mobile Trusted Filter Version 1.0
Software Version	Front End Firmware V 1.02 Back End Firmware V 1.02
Security Target	HFMP Mobile Trusted Filter Security Target, BAE Systems, Issue 1.9, June 2006
Evaluation Level	ITSEC E5
Evaluation Technical Report	Mobiles Trusted Filter Evaluation Technical Report Issue 1.0, LogicaCMG, 12 October 2006
ITSEC Version	ITSEC Version 1.2, June 1991
Methodology Used	Information Technology Security Evaluation Manual (ITSEM) Version 1.0, 10 September 1993
	ITSEC Joint Interpretations Library (JIL) Version 2.0, November 1998
	Manual of Computer Security Evaluation Part I – Evaluation Procedures (EM4), Issue 1.0, April 1995
	Manual of Computer Security Evaluation Part II – Evaluation Techniques and Tools (EM5), Issue 1.0, April 1995
Sponsor	BAE Systems Australia Ltd
Developer	BAE Systems Australia Ltd
Evaluation Facility	LogicaCMG

Chapter 2 - Target of Evaluation

2.1 Overview

9 This chapter contains information about the Target of Evaluation (TOE), including:

a) A description of the TOE functionality.

b) TOE architecture.

c) Scope of the evaluation.

d) Secure usage.

2.2 Description of the TOE

10 The TOE is the Mobile Trusted Filter Version 1.0 developed by BAE Systems. Its primary role is to provide RED/BLACK separation in systems where control data which cannot be protected by encryption or other means must cross a RED/BLACK boundary.

11 The Mobile Trusted Filter allows equipment on the RED side to send a specified set of commands to equipment on the BLACK side. If the Mobile Trusted Filter receives an invalid command an alarm status flag is raised and the command is discarded. The Mobile Trusted Filter will allow equipment on the BLACK side to send information to equipment on the RED side without restrictions.

2.3 TOE Architecture

12 The TOE is implemented using a mixture of hardware and firmware. Apart from various signal conditioning functional components concerning the input/output standard used (RS-232), the components of interest include the Analyser and Data Diode components. The Analyser component examines data from the RED side and passes valid data through to the BLACK side. The Data Diode component passes all data from the BLACK side through to the RED side.

2.4 Clarification of Scope

13 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.4.1 Evaluated Functionality

14 The TOE provides the following evaluated Security Enforcing Functions (SEFs):

a) Filtering SEF: The TOE shall ensure that only data strings which are validated against a pre-defined set of allowable strings can be transmitted from a RED to BLACK area.

b) Data Diode SEF: The TOE shall ensure any BLACK to RED data path it controls is strictly one way.

c) Secure Failure SEF: The design of the TOE shall ensure that any conceivable failure of any single discrete hardware component shall not compromise the security objective of the TOE.

2.4.2 Non-evaluated Functionality

15 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Communications Technology Security Manual (ACSI 33) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

16 The functions and services that have not been included as part of the evaluation are provided below:

a) The optional remote monitoring panel.

2.5 Usage

2.5.1 Evaluated Configuration

17 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration. Australian Government users should refer to ACSI 33 (Ref [2]) to ensure that configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

18 The evaluated TOE is comprised of hardware and firmware running in a self-contained metal box that can be configured for mounting in a Versa Module Eurocard (VME) chassis or for a simple panel mount. In the evaluated configuration the unit is supplied with an appropriate power connection, a RED side serial data (RS-232) connection and a BLACK side serial data (RS-232) connection. The remote monitoring panel was not part of the evaluated configuration.

19 The BAE Systems Mobile Trusted Filter V1.0 hardware part number is: 680A00041-001-01.

20 The TOE embedded firmware is not user accessible, but the versions and checksums are listed below:

a) Front End HFFN module Version 1.02 – checksum 0x73A6.

b) Back End module Version 1.02 – checksum 0x9916.

2.5.2 Documentation

21 The documentation kit for the TOE is BAE Systems part number 680A00042-001-05 (Ref [3]). It consists of the documents:

a) Mobiles Trusted Filter User & Maintenance Manual, Issue 2.0, September 2005.

b) Mobiles Trusted Filter Special Handling Procedures, Issue 2.0, April 2005.

22 The User & Maintenance Manual provides important information on the usual operation of the TOE and how the user can detect faulty units.

2.5.3 Delivery procedures

23 Each unit will bear a stamped metal identification plaque with a unique serial number.

24 The consumer should verify that the unit serial number matches the serial number recorded in the delivery manifest. The User & Maintenance Manual indicates that the user should verify that the tamper evident wafer seals protecting the unit are intact upon receipt. The manual also indicates that the user should record the unit serial number and wafer seal serial numbers and send these numbers to BAE Systems.

2.5.4 Determining the Evaluated Configuration

25 Each Mobile Trusted Filter unit will be sealed using numbered wafer seals applied to screws on the case. The serial numbers on the wafer seals are associated with unit serial numbers in a register held by BAE Systems. These serial numbers can be verified if required by contacting BAE Systems.

2.5.5 Intended Operational Environment

26 It is assumed that the Mobile Trusted Filter will operate in an environment where there is no threat of unauthorised physical access to the device or its connections.

Chapter 3 - Evaluation

3.1 Overview

27 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

28 The criteria against which the Target of Evaluation (TOE) has been evaluated are expressed in the Information Technology Security Evaluation Criteria (ITSEC) (Ref [4]). The methodology used by the Australasian Information Security Evaluation Facility (AISEF) is described in the Information Technology Security Evaluation Manual (ITSEM) (Ref [5]), Joint Interpretations Library (JIL) (Ref [6]), and Evaluation Memoranda (EM) 4 and 5 (Refs [7], [8]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [9], [10]).

29 A similar TOE (Trusted Filter V1.0) was evaluated by the AISEP with original certification in July 2001. Via a series of incremental changes the original Trusted Filter V1.0 product was updated to Version 1.2A.2 under the AISEP's AISEP Certificate Extension (ACE) scheme. The Mobile Trusted Filter V1.0 is a further variation that is smaller in size. Due to the total cumulative impact of these variations the Australasian Certification Authority (ACA) required the Mobile Trusted Filter V1.0 product to undergo re-evaluation with the July 2001 evaluation as the basis.

30 The evaluators reviewed the ITSEC E5 Evaluator Actions required in the light of the changes to the evaluation inputs. This plan formed the basis of the re-evaluation. The re-evaluation included a development environment assessment and testing effort.

3.3 Testing Effort

31 Testing included functional testing of the three Security Enforcing Functions (SEFs) – Filtering SEF, Data Diode SEF and Secure Failure SEF. The evaluators also conducted penetration tests that attempted to bypass the TOE SEFs. The penetration tests failed to cause the TOE to behave in an insecure manner.

Chapter 4 - Certification

4.1 Overview

32 This chapter contains information about the result of the certification, an overview of the assurance provided by the evaluation level chosen, and recommendations made by the certifiers.

4.2 Certification Result

33 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [11]), the Australasian Certification Authority (ACA) certifies the evaluation of Mobile Trusted Filter Version 1.0 performed by the Australasian Information Security Evaluation Facility (AISEF), LogicaCMG.

34 LogicaCMG has found that the Mobile Trusted Filter Version 1.0 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Information Technology Security Evaluation Criteria (ITSEC) evaluation level E5.

35 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Evaluation Level Information

36 Table 2 below provides a description of the requirements for the ITSEC E5 evaluation level. These levels of evaluation criteria are defined within the context of the ITSEC correctness criteria and are described below.

Table 2: ITSEC Evaluation Levels

Evaluation Level	Description
E1	At this level there shall be a security target and an informal description of the architectural design of the evaluated Target of Evaluation (TOE). Functionality testing shall indicate that the TOE satisfies its security target.
E2	In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.

Evaluation Level	Description
E3	In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.
E4	In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.
E5	In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.

4.4 Recommendations

37 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the Australian Government Information and Communications Technology Security Manual (ACSI 33) (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

38 In order to ensure the secure operation of the TOE, the ACA recommends that it should only be used in accordance with the intended method of use and intended operational environment, as described in sections 2.3 and 2.4 of the Security Target (Ref [1]) and that the guidance documents (Ref [3]) are followed by users and administrators. Further, it is recommended that an appropriate security authority accredit the TOE installation, to ensure that the following conditions exist, or have been implemented.

Tamper Seal and Cable Integrity

39 A regular inspection procedure should be incorporated into the site or system security plan. The integrity of all relevant tamper seals should be regularly inspected for any sign of damage as explained in the TOE Documentation (Ref [3]). The administrator should immediately report any discovery of damage or tampering to their appropriate security authority and the command data transfer path should be disabled.

40 When inspecting the tamper seals on the Mobile Trusted Filter, administrators should also check the cabling connections from the Mobile Trusted Filter to the RED equipment and the BLACK equipment, to ensure that the Mobile Trusted Filter is correctly connected and not bypassed.

Installation Considerations

41 The installation of the Mobile Trusted Filter is only to be carried out by qualified personnel approved by BAE Systems Australia Ltd. Under no circumstances should any other personnel attempt to install, configure or undertake maintenance on the device.

Operational Considerations for the Mobile Trusted Filter

42 The unit's Operate Status Light Emitting Diode (LED) must be visible to the end user in order to monitor correct operation of the unit.

43 Note that the Mobile Trusted Filter will still filter further commands, even if the unit's Alarm Status is activated by the detection of an invalid command.

Guidance for Purchasers - Residual Risk of Covert Channels

44 Given that the Mobile Trusted Filter protects the confidentiality of information in the RED area from the BLACK area, covert channels are a consideration for prospective purchasers. The evaluation determined that potential exploitable covert channels do exist. If the Mobile Trusted Filter is only used within its intended operational environment, then these covert channels are unlikely to be exploitable within that operational environment, due to the appropriate security clearance and training of staff.

45 The Mobile Trusted Filter has been evaluated and certified with a particular command set. The severity of the covert channels noted in the previous recommendation are largely dependent on the command set. In particular, the types of parameters and/or arguments supplied to each of the commands will determine the capacity of potential covert channels. Therefore, it is strongly recommended that the Mobile Trusted Filter command set be approved by an appropriate accreditation authority in order to assess the possible impact of residual covert channels in their operating environment.

Data Diode Considerations

46 The unit does not check data moving from BLACK to RED for any attacks on the high side equipment. If the BLACK side equipment is compromised it could be used to attack the RED side equipment. If the RED side equipment was also compromised it could be used to setup the covert channels from RED to BLACK discussed above.

47 Equipment connected to both sides of the Mobile Trusted Filter must be free of vulnerabilities that allow unauthorised remote control to ensure the correct operation of the trusted filter.

References and Abbreviations

A.1 References

[1] HFMP Mobile Trusted Filter Security Target, Issue 1.9, June 2006, BAE Systems Australia Ltd.

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2006, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] TOE Documentation Kit, BAE Systems Part Number 680A00042-001-05, comprising of:

a) Mobiles Trusted Filter User & Maintenance Manual, Issue 2.0, September 2005.

b) Mobiles Trusted Filter Special Handling Procedures, Issue 2.0, April 2005.

[4] Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991, Commission of the European Communities.

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

[6] Information Technology Security Evaluation Criteria, Joint Interpretations Library (JIL), Version 2.0, November 1998, Joint Interpretation Working Group.

[7] Manual of Computer Security Evaluation Part I – Evaluation Procedures (EM 4), Issue 1.0, April 1995, Defence Signals Directorate (EVALUATION-IN-CONFIDENCE).

[8] Manual of Computer Security Evaluation Part II – Evaluation Techniques and Tools (EM 5), Issue 1.0, April 1995, Defence Signals Directorate (EVALUATION-IN-CONFIDENCE).

[9] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.0, 21 February 2006, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3, Version 3.0, 21 February 2006, Defence Signals Directorate (EVALUATION-IN-CONFIDENCE).

[11] Mobiles Trusted Filter Evaluation Technical Report, Issue 1.0, 12 October 2006, LogicaCMG.

A.2 Abbreviations / Glossary

ACSI 33	Australian Government Information and Communications Technology Security Manual
ACE	AISEP Certificate Extension
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
BLACK	Unclassified Data in an Insecure Domain
DSD	Defence Signals Directorate
E5	Evaluation Level 5
GCSB	Government Communications Security Bureau
HFMP	High Frequency Modernisation Project
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
JIL	Joint Interpretations Library
LED	Light Emitting Diode
RED	Classified Data in a Secure Domain
RS-232	Recommended Standard 232 for Serial Communication
SEF	Security Enforcing Function
ST	Security Target
TOE	Target of Evaluation
VME	Versa Module Eurocard