122-B

CERTIFICATION REPORT No. CRP246

Aruba 6000 and Aruba 800 Series Mobility Controller
Running ArubaOS Version 2.4.8.14-FIPS

Issue 1.0

June 2008

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them 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

The products detailed below have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and have met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.

Sponsor	Aruba Networks
Developer	Aruba Networks
Product and Version	Aruba 6000 and Aruba 800 Series Mobility Controller running ArubaOS Version 2.4.8.14-FIPS
Platform	Aruba 6000 and Aruba 800 Series hardware
Description	The Mobility Controllers are wireless LAN (WLAN) switches
CC Part 2	Extended
CC Part 3	Conformant
EAL	EAL2 augmented with ACM_SCP.1, ALC_FLR.2 and AVA_MSU.1
SoF	SoF-Basic
PP Conformance	US Government WLAN Access System PP for Basic Robustness Environments
CLEF	Logica
Date Certified	27 June 2008

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1, UKSP02P2]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance[1] with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

Trademarks:

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

[1] All judgements contained in this Certification Report are covered by the Recognition Arrangement.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of the Aruba 6000 and Aruba 800 Series Mobility Controller running ArubaOS Version 2.4.8.14-FIPS to the Sponsor, Aruba Networks, as summarised in the Certification Statement, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following products completed evaluation to CC EAL2 augmented with ACM_SCP.1, ALC_FLR.2 and AVA_MSU.1 on 30 April 2008:

- **Aruba 6000 and Aruba 800 Series Mobility Controller running ArubaOS Version 2.4.8.14-FIPS**

4. The Developer was Aruba Networks. The Aruba 6000 and 800 Series Mobility Controllers are wireless LAN (WLAN) switches. A WLAN switch is a gateway device which controls operation of multiple access points, processes network data flows between wireless and wired networks, and implements various wired and wireless network and security protocols. All Aruba Mobility Controllers are hardware devices that run the ArubaOS software suite. Aruba 6000 and Aruba 800 series Mobility Controllers have a steel case that physically encloses the complete set of hardware and software components.

5. The evaluated configuration of these products is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

6. An overview of the TOE and its security architecture can be found in Chapter IV 'Product Architecture'. Configuration requirements are specified in Section 2.2 of [ST] and in [ECG].

Protection Profile Conformance

7. The Security Target [ST] is certified as achieving conformance to the following protection profile (PP):

- US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments [PP]

8. The Security Target [ST] includes objectives and SFRs that are additional to those of the protection profile.

Security Claims

9. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) and Security Functions that elaborate the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

10. The TOE security policies are detailed in [ST]. The Organisational Security Policies (OSPs) that must be met are specified in [ST] Section 3.3.

11. The environmental assumptions related to the operating environment are detailed in Chapter III under 'Environmental Requirements'.

Strength of Function Claims

12. The minimum Strength of Function (SoF) was claimed to be SoF-Basic. This is claimed for I&A and TOE Access Security Sub-function IA-1 and Trusted Path/Channels Security Sub-functions TP-1 and TP-2. The Evaluators have determined that these claims were met.

13. The cryptographic mechanisms contained in the TOE used for the User Data and TSF Protection Security Function and the Trusted Path/Channels Security Function are FIPS 140-2 approved and as such it is the policy of CESG, as the National Authority for cryptographic mechanisms, not to comment on its appropriateness or strength. Therefore the Evaluators merely confirmed its correct implementation.

Evaluation Conduct

14. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in April 2008, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

15. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

16. Prospective consumers of Aruba 6000 and Aruba 800 Series Mobility Controller running ArubaOS Version 2.4.8.14-FIPS should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

17. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' below

includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

18. In addition, the Evaluators recommend that particular note should be taken of the assumptions that the installation and initial configuration must be performed by an Aruba Engineer and that any modifications following the initial configuration will be minor, albeit that a trained administrator must be provided. These assumptions are further expanded in Chapter II 'TOE Security Guidance' below.

Disclaimers

19. This Certification Report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration'.

20. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered by a Scheme-approved Assurance Continuity process.

II. TOE SECURITY GUIDANCE

Introduction

21. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

22. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

Installation and Guidance Documentation

23. The installation and initial configuration of the TOE must be performed by an Aruba Engineer. This is due to the detailed expertise required for the configuration for both the mobility controller and the IT environment, i.e. authentication server, syslog server, NTP server and wireless stations. It is assumed that any modifications to the configuration after initial installation are minor. However, even with this caveat, the Administrator needs to be trained and also needs to be familiar with the required configurations for the TOE in order to maintain the product in its evaluated configuration. The wireless users have no direct interface to the TOE and there is no TOE documentation directed to them.

24. It should also be noted that the mobility controller forms the central part of a wireless system, but the other parts, i.e. the IT environment, also require configuration and their product manuals will also need to be examined.

25. The Aruba Engineer performing the installation and configuration will need to refer to:

- Evaluated Configuration Guide [ECG];
- Aruba 800, 5000 and 6000 Non-Proprietary Security Policy [FIPS].

26. The Administrator will need to refer to the following for configuration requirements of the evaluated configuration and for hardware installation:

- Evaluated Configuration Guide [ECG];
- Aruba 800, 5000 and 6000 Non-Proprietary Security Policy [FIPS];
- Aruba 800 Installation Guide [IGD800];
- Aruba 6000 Installation Guide [IGD6000].

27. The Administrator will need to refer to the following for descriptions of the management interfaces, required to perform configuration of the TOE:

- ArubaOS 2.4.8-FIPS User Guide [UG];
- ArubaOS 2.4.8-FIPS CLI Reference Guide [CLI].

III. EVALUATED CONFIGURATION

TOE Identification

28. The TOE is the Aruba 6000 and Aruba 800 Series Mobility Controller running ArubaOS Version 2.4.8.14-FIPS.

29. The Aruba 6000 Series Mobility Controller is a modular product and consists of the following modules:

- Chassis HW-CHASF (3300028 Rev. 01);
- Fan Tray HW-FTF (3300031 Rev. 01);
- Supervisor Cards SC-256-C2 (3300027 Rev. 01), SC-48-C1 (3300025- 01) and SC-128-C1 (3300025-01);
- Line Cards LC-2G24F (3300026 Rev. 01), LC-2G (3300029-01) and LC-2G24FP (3300024 Rev. 01);
- Power Supplies HW-PSU-200 and HW-PSU-400.

30. The Supervisor Card runs the ArubaOS software. The evaluated configuration includes one Supervisor Card. The Line Card provides interfaces to the access points and the wired network. Up to three Line Cards may be fitted. Two power supplies may be fitted, one acting as a backup. The HW-PSU-400 power supply is required if Power over Ethernet is to be supplied to the access points.

31. The difference between the Supervisor Cards lies purely in the licensing of how many access points they may control. The cards are identical in their hardware. The ArubaOS executes on exactly the same processors.

32. The difference between the Line Cards lies purely in the interfaces provided. The Line Cards do not run the ArubaOS software and do not enforce the TSP. They are merely relied upon to act as interfaces.

33. The Aruba 800 Series Mobility Controller is not modular. Two chassis are available:

- HW-800-CHAS-SPOE-SX, providing a fibre optic connector;
- HW-800-CHAS-SPOE-TX, providing a copper connector.

TOE Documentation

34. The relevant guidance documentation for the evaluated configuration is identified above under ‘Installation and Guidance Documentation’.

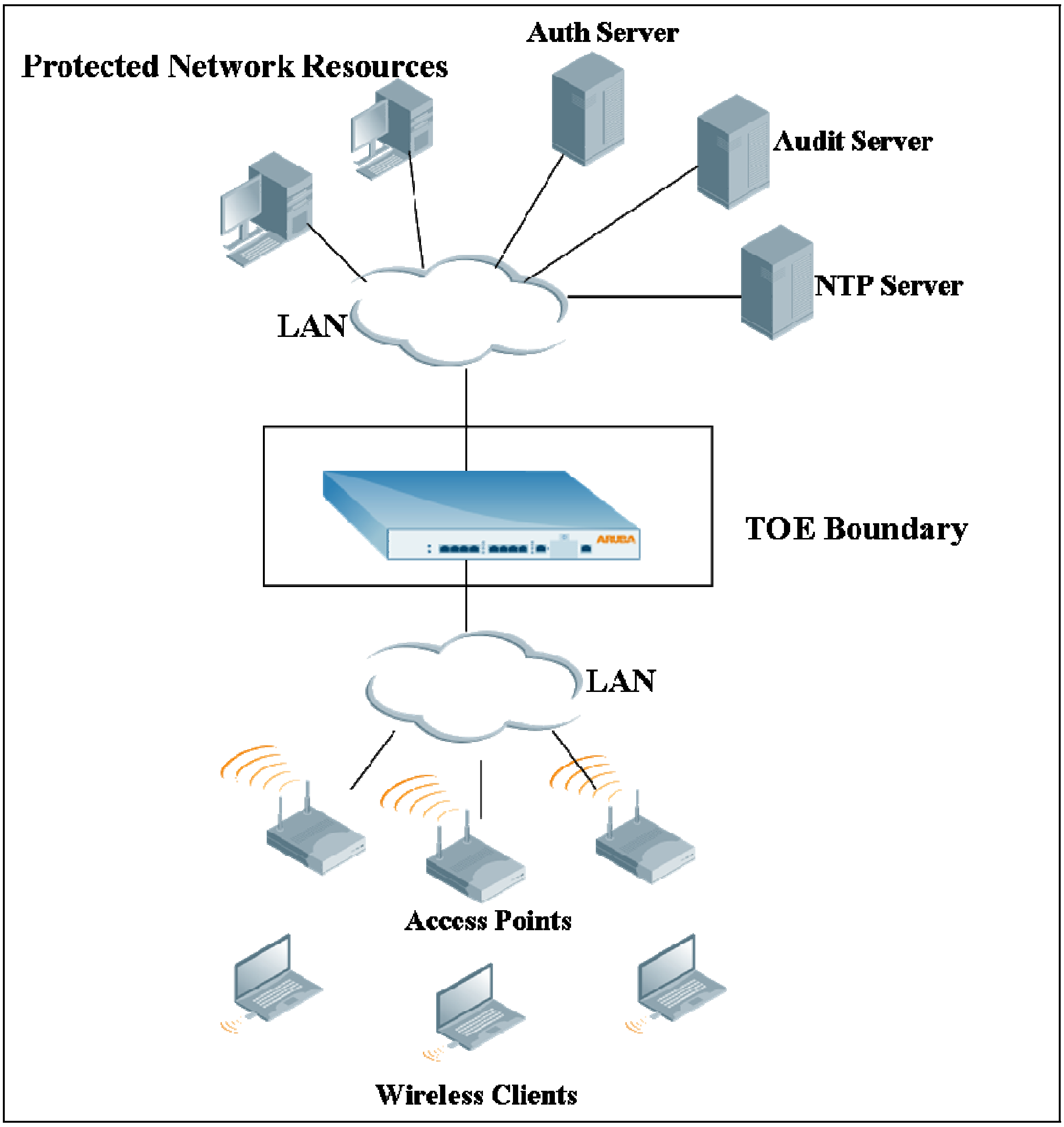
TOE Scope

35. The TOE Scope is defined in [ST] Section 2.1. The security functionality that is outside the scope of the TOE is defined in [ST] Section 2.1.2. This includes the policy enforcement firewall and protocols which are disabled in the FIPS 140-2 configuration.

TOE Configuration

36. The evaluated configuration of the TOE is defined in [ST] Section 2.2 and in [ECG]. The following diagram shows the evaluated configuration.

Figure 1: TOE Evaluated Configuration



Environmental Requirements

37. The environmental assumptions for the TOE are stated in [ST] Section 3.1.

38. The environmental IT configuration is as follows:

- Access points connected to Ethernet wired interfaces;
- Wireless clients connected via access points;
- Syslog server connected to Ethernet wired interface assigned to backend servers;
- Authentication (RADIUS) server connected to Ethernet wired interface assigned to backend servers;
- NTP server connected to Ethernet wired interface for backend servers;
- Remote administrator connected to Ethernet wired interface assigned to remote administration.

Test Configuration

39. The Aruba 6000 Series Mobility Controller configuration used for both Developer and Evaluator testing was:

- 1 x Chassis HW-CHASF (3300028 Rev. 01);
- 1 x Fan Tray HW-FTF (3300031 Rev. 01);
- 1 x Supervisor Card SC-256-C2 (3300027 Rev. 01);
- 3 x Line Cards LC-2G24FP (3300024 Rev. 01);
- 2 x Power Supplies HW-PSU-400.

40. The Aruba 800 Series Mobility Controller chassis used for both Developer and Evaluator testing was the HW-800-CHAS-SPOE-TX.

IV. PRODUCT ARCHITECTURE

Introduction

41. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III ‘Evaluated Configuration’.

Product Description and Architecture

42. The hardware architecture of the TOE is discussed in Chapter III ‘Evaluated Configuration’. The ArubaOS software consists of an embedded Linux operating system with the rest of the software running as processes on the operating system. Further details are given below. The subsystems may comprise several processes.

TOE Design Subsystems

43. The TOE ArubaOS subsystems, and their security features/functionality, are as follows:

- *TOE Management Subsystem* – controls configuration, authenticates management users;

- *Audit Subsystem* – provides functionality to log security-relevant events, using an external syslog audit server to store & review audit records and an external NTP server to obtain reliable time stamps;

- *Wireless Network Subsystem* – connects TOE to wireless clients via access points, passing authentication data to a RADIUS server;

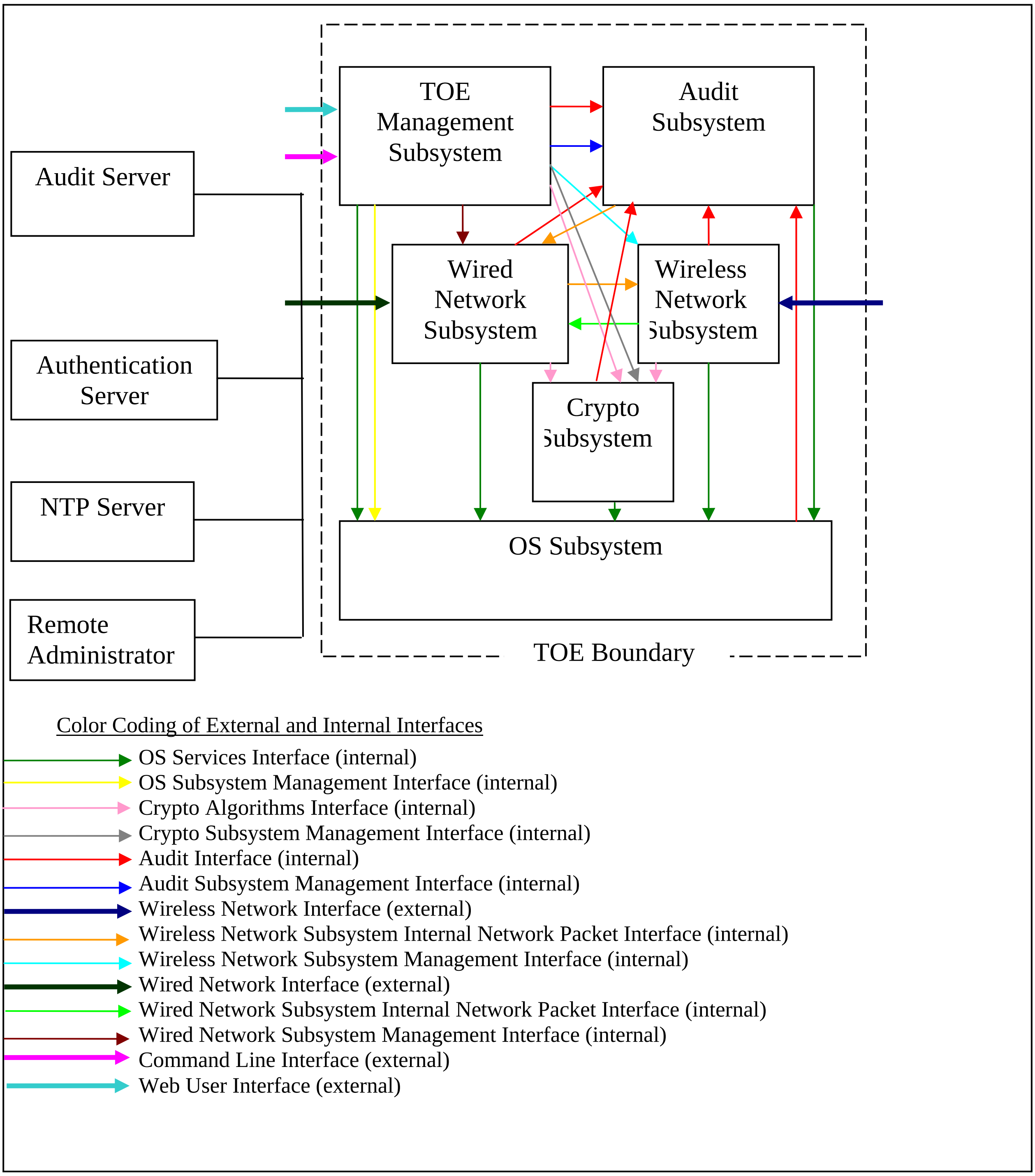
- *Wired Network Subsystem* – connects the TOE to the back-end servers (authentication, syslog, NTP) and business servers, authenticates a remote administrator at the remote administration port;

- *Crypto Subsystem* – provides hardware and software implementations of cryptographic algorithms;

- *OS Subsystem* – provides an operating system which supports and controls execution of all other subsystems in the TOE; synchronises with the NTP server.

44. The following diagram shows the high level design of the TOE including the subsystems and the external and internal interfaces.

Figure 2: TOE High Level Design and Interfaces


TOE Management Subsystem
Audit Subsystem
Audit Server
Wired Network Subsystem
Wireless Network Subsystem
Authentication Server
Crypto Subsystem
NTP Server
OS Subsystem
Remote Administrator
TOE Boundary
Color Coding of External and Internal Interfaces
OS Services Interface (internal)
OS Subsystem Management Interface (internal)
Crypto Algorithms Interface (internal)
Crypto Subsystem Management Interface (internal)
Audit Interface (internal)
Audit Subsystem Management Interface (internal)
Wireless Network Interface (external)
Wireless Network Subsystem Internal Network Packet Interface (internal)
Wireless Network Subsystem Management Interface (internal)
Wired Network Interface (external)
Wired Network Subsystem Internal Network Packet Interface (internal)
Wired Network Subsystem Management Interface (internal)
Command Line Interface (external)
Web User Interface (external)

TOE Dependencies

45. The TOE is dependent on the correct configuration of the IT environment, as described in [ECG], in order to provide the security functionality.

TOE Interfaces

46. The external TSFI is described as follows:

- *Command Line Interface* – used for management;
- *Web User Interface* – used for management;
- *Wireless Network Interface* – used for wireless traffic from wireless users;
- *Wired Network Interface* – used for connection to the backend servers and remote administrators.

V. TOE TESTING

TOE Testing

47. The Developer’s tests covered all SFRs, all TOE high-level subsystems (as identified under ‘TOE Design Subsystems’) and the TSFI (as identified under ‘TOE Interfaces’ in Chapter IV). Tests were performed on the Aruba 6000 Series and the Aruba 800 Series Mobility Controllers. The test configuration was the same as the evaluated configuration, as described in Chapter III ‘Evaluated Configuration’.

48. The Evaluators devised and ran twenty-four independent functional tests, different from those performed by the Developer. No anomalies were found. The Evaluators also devised four penetration tests to address potential vulnerabilities considered during the evaluation. In addition, a specialist wireless security penetration tester performed automated penetration testing. One exploitable vulnerability was found concerning the provision of an IPSec/IKE VPN, which was corrected by mandating a more secure configuration [ECG]. A further problem found, concerning logging, was acknowledged to be a feature of the protocols used and not a vulnerability in the TOE. Tests were performed on the Aruba 6000 Series and the Aruba 800 Series Mobility Controllers.

Vulnerability Analysis

49. The Evaluators’ vulnerability analysis, which preceded penetration testing, was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

50. No platform issues were identified. The Evaluators observed, during general testing and setup, that the Aruba 6000 Series and Aruba 800 Series Mobility Controllers provided the same security functionality.

VI. REFERENCES

[A&R] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
Issue 1.4, January 2008.

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[CLI] ArubaOS 2.4.8-FIPS CLI Reference Guide,
Aruba Networks,
0510055-03, January 2008.

[ECG] Evaluated Configuration Guide,
Aruba Networks,
Version 1.3, 28 April 2008.

[ETR] LFL/T237 Evaluation Technical Report,
Logica CLEF,
310.EC202223.005.1, Issue 1.1, 29 May 2008.

[FIPS] Aruba 800, 5000 and 6000 Non-Proprietary Security Policy,
Aruba Networks,
0510000142-10, Version 15, March 2008.

[IGD800] Aruba 800 Installation Guide,
Aruba Networks,
0500021-03, May 2005.

[IGD6000] Aruba 6000 Installation Guide,
Aruba Networks,
0500024-03, May 2005.

[PP] US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments,
Information Assurance Directorate,
Version 1.0, April 2006.

[ST] Aruba 6000 and Aruba 800 Series Mobility Controller Security Target,
Aruba Networks,
Version 1.8, 28 May 2008.

[UG] ArubaOS 2.4.8-FIPS User Guide,
Aruba Networks,
0510237-05, January 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

VII. ABBREVIATIONS

This list does not include well known IT terms (such as GUI, HTML, LAN, PC) or standard Common Criteria abbreviations (such as TOE, TSF; see Common Criteria Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [A&R]).

FIPS	Federal Information Processing Standards
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial In User Service
WLAN	Wireless LAN