C075 Certification Report

Huawei Access Terminal Platform ATP V200R001C03

File name: ISCB-5-RPT-C075-CR-v2
Version: v2
Date of document: 6 December 2016
Document classification : PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726830-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C075 Certification Report

Huawei Access Terminal Platform ATP V200R001C03

25 November 2016

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C075 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C075-CR-v2
ISSUE:	v2
DATE:	6 December 2016

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 6 December 2016 and the Security Target (Ref **Error! Reference source not found.**). The c ertification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	25 November 2016	All	Initial draft of certification report
v1	1 December 2016	All	Final version of certification report
V2	6 December 2016	All	2nd Revision of Final version

Executive Summary

The TOE ATP (Access Terminal Platform) is a software platform for Huawei Access Terminals, which is a type of network and network-related devices and systems, that supports rich WAN interfaces and user access interfaces to provide WAN access, data access and voice services for home, personal and small office.

At the core of each Access Terminal is the ATP (Access Terminal Platform) deployed on SOC (System on chip) chip, the software for managing and running the gateway's access networking functionality. ATP provides extensive security features. These features include authentication control for user login; log auditing of user operation; communication and data security. SOC also supports rich type of interfaces such as Xdsl/Ethernet/3G/4G/WiFi/USB for WAN side and user side to provide internet, data, and voice access service.

The major security features of the Huawei Access Terminal products are audit, Identification & Authentication (I&A), security management, access to the product, and information flow control (i.e., network packets sent through the TOE are subject to router information flow control rules setup by the administrator or pre-defined in default configuration). The System also provides protection against Denial of Service (DoS) attacks.

The scope of the evaluation is defined by the Security Target (Ref Error! Reference source not found.) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security function requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 4th November 2016.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Huawei Access Terminal Platform meet their requirements. It is recommended that a potential user of the TOE refer to the Security Target (**Ref Error! Reference source not found.**) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 ATP is a software platform for Huawei Access Terminals, which is a type of network and network-related devices and systems, that supports rich WAN interfaces and user access interfaces to provide WAN access, data access and voice services for home, personal and small office.

2 Huawei Access Terminals consists of home gateway, wireless router and mobile broadband products. Residing in these devices is the ATP software, which is the TOE.

3 ATP is an application platform based on Linux OS, so the chip platform and product hardware are non-TOE. Additionally, the operational environment is defined by the following to be outside the TOE boundary:

- A browser or APP for local administration;
- ACS for remote administration;
- HOTA servers for online upgrade;
- A Simple Network Time Protocol server for external time synchronization.

4 The security functionalities covered under the scope of the evaluation are:

- **Security Audit**: Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The TOE also generates audit records for all user activities on the management plane and stores the audit records in FLASH memory by FIFO mode in the TOE. Limit the number of stores to the FIFO (usually 100 items), save to the Flash in the way of the loop, and then cover the earliest of the low priority records.
- **Identification and Authentication**: The TOE can be managed by the Web GUI. It authenticates the local user based on the username and password. The TOE also provides authentication failure handling and the ability for the administrator to define password complexity requirements.

  Authentication is enforced for WiFi station access if the TOE acts as a WiFi AP (such as home gateway/wireless router). WiFi access authentication is not covered in the scope of the evaluation as it relies on the authentication of the WiFi standard.
- **User Data Protection**: The TOE provides firewall and packet filtering for information flow control policy on the network packets sent through the TOE. The TOE provides ACL as information flow control policy for the network packets sent to the TOE (The destination IP address is the TOE).
- **Security Management:** The TOE offers management functionality for its security functions. Security management functionality can be executed by the administrator through the Web GUI or ACS. However, ACS remote management needs to be customized by the ISP, and it is not a common function of the TOE.
- **TOE Access:** There are mechanisms in place that controls administrators' sessions. Web administrator's sessions are dropped after a pre-defined time (can be modified by ACS) period of inactivity. Dropping the connection of Web sessions (after the specified time

period) reduces the risk of an unauthorized user accessing the machines where the session was established, thus gaining unauthorized access to the session. Administrators' can initiate the termination of Web sessions by clicking the "Logout" button. The TOE will deny session establishment based on maximum number (for example: 10) of concurrent Web management sessions that have been established.

- **TSF Protection:** The TOE supports importing/exporting of configuration files and online upgrade. Digital signature algorithm RSA2048 (SHA256) is used to protect the data integrity for the configuration and image file. In addition, encryption is used to prevent the configuration file and image file from information disclosure.
- **Trusted path/channels:** The TOE supports the use of a trusted path (HTTPs) for user authentication in local management and, is mandatory for remote management via the Web UI. However, access from WAN side is disabled by default.

  TR069 remote management supports the use of a trusted channel (HTTPs). Using HTTP or HTTPS depends on the ISP who deploys the ACS. However, the TOE supports setting the ACS server URL to use HTTPS only, requiring the management traffic to be transferred through a secure channel.

  WiFi channel implements WPA2 authentication and AES encryption. Usually, the product with WiFi AP feature uses WPA2+AES as the default configuration. A security risk notification will be prompted if unsecure authentication mode is used.

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C075
TOE Name	Huawei Access Terminal Platform ATP (Huawei ATP V200R001C03)
TOE Version	V200R001C03
Security Target Title	Huawei Access Terminal Platform ATP V200R001C03 Security Target
Security Target Version	Version 1.71
Security Target Date	3 November 2016
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant

	Package conformant to EAL 2
Sponsor	Huawei Technologies Co., Ltd.
Developer	Huawei Technologies Co., Ltd. Huawei Industrial Base, Bantian Longgang, Shenzhen P.R.C.
Evaluation Facility	BAE Systems Applied Intelligence MySEF

1.3 Security Policy

6 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries as described in Section 1.4 of the Security Target (Ref **Error! Reference source not found.**).

8 This document gives a brief description:

- WEB provides local management from Web GUI
- CWMP provides remote management by ACS according to TR-069 protocol.
- Route makes the device to forward packets from LAN to WAN
- SNTP Client is used to synchronize the network time from SNTP Server.
- UPG model is used for online upgrading.
- LOG model is used for audit and records system log.

9 The typical LTE router series B525 will be used to run the ATP software during this evaluation. B525 is customer premises equipment (CPE). On the network side, it provides a high-speed LTE CAT6 for wide area network (WAN) access. B525 provides internet access with highest bandwidth and speed for customers.

10 For users, the B525 supports both the 2.4 GHz and 5 GHz Wi-Fi functions, it provides dual concurrent 802.11b/g/n (2.4 GHz) and 802.11a/n/ac (5 GHz) interfaces, one USB interface, one phone interface and four Ethernet interfaces for home users to connect various terminals, such as a PC, an IP set-top box. By integrating the Foreign Exchange Station (FXS) module, the B525 can be set to voice over Internet protocol (VoIP) or circuit switch (CS) voice mode.

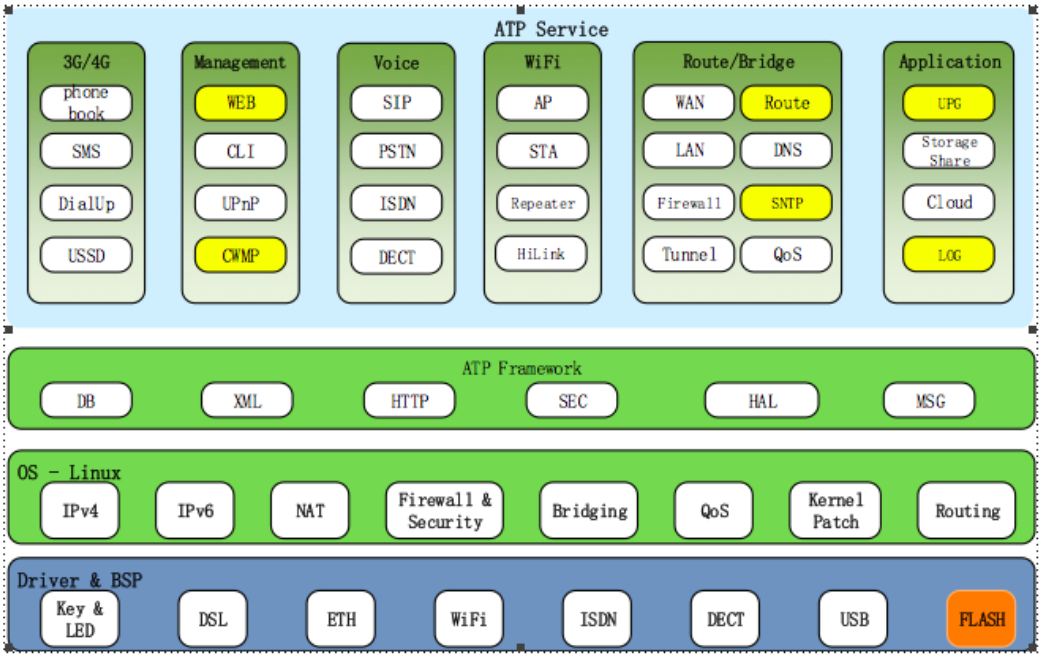

Figure 1: ATP System Architecture

1.4.1 Logical Boundaries

11 The scope of the evaluation was limited to those claims made in the Security Target (Ref **Error! Reference source not found.**) and includes only the following evaluated security f unctionality:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

12 **Security audit:** Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. The TOE also generates audit records for all user activities on the management plane and stores the audit records in FLASH memory by FIFO mode in the TOE. Limit the number of stores to the FIFO (usually 100 items), save to the Flash in the way of the loop, and then cover the earliest of the low priority records.

13 **User data protection:** The TOE provides firewall and packet filtering as information flow control policy for the network packets sent through the TOE. The TOE provides ACL as information flow control policy for the network packets sent to the TOE (The destination IP address is the TOE).

14 **Identification and authentication:** The TOE can be managed via the Web GUI. It authenticates the local user based on the username and password. The TOE also provides authentication failure handling and the ability for the administrator to define password complexity requirements.

Authentication is enforced for WiFi station access when the TOE acts as a WiFi AP (such as home gateway/wireless router). WiFi access authentication is not evaluated since the authentication is according to the WiFi standard completely.

For home gateway and CPE, the ISP could customize the remote management via the TR-069. TR-069 authentication method is according to the standard, such as HTTP basic, HTTP Digest and Certification authentication, which depends on the ACS (Automatic Configuration Server). However, the document will not focus on this since it depends on the ISP's network environment absolutely.

15 **Security management:** The TOE offers management functionality for its security functions. Security management functionality can be executed by the administrator through Web UI or ACS. However, ACS remote management need to be customized by the ISP, and it is not a common function of the TOE.

16 **Protection of the TSF:** The TOE supports importing/exporting configuration files and online upgrade. Digital sign algorithm RSA2048 (SHA256) is used to protect the data integrity for the configuration file and image file. Besides, encryption is used to prevent the configuration file and image file from information disclosure.

17 **TOE access:** There are mechanisms in place that controls administrators' sessions. Web administrator's sessions are dropped after a pre-defined time (can be modified by ACS) period of inactivity. Dropping the connection of Web sessions (after the specified time period) reduces the risk of an unauthorized user accessing the machines where the session was established, thus gaining unauthorized access to the session. Administrators' can initiate the termination of Web sessions by clicking the "Logout" button. The TOE will deny session establishment based on maximum number (for example: 10) of concurrent Web management sessions that have been established.

18 **Trusted path/channels:** The TOE supports the use of a trusted path (HTTPs) for user authentication in **local** management and, is mandatory for remote management via the Web UI. However, access from WAN side is disabled by default.

TR069 remote management supports the use of a trusted channel (HTTPs). Using HTTP or HTTPS depends on the ISP who deploys the ACS. However, the TOE supports setting the ACS server URL to use HTTPS only, requiring the management traffic to be transferred through a secure channel.

WiFi channel implements WPA2 authentication and AES encryption. Usually, the product with WiFi AP feature uses WPA2+AES as the default configuration. A security risk notification will be prompted if unsecure authentication mode is used.

1.4.2 Physical Boundaries

19 The following figure shows the TOE boundary, and the IT environment used for these functions in the scope of evaluation.

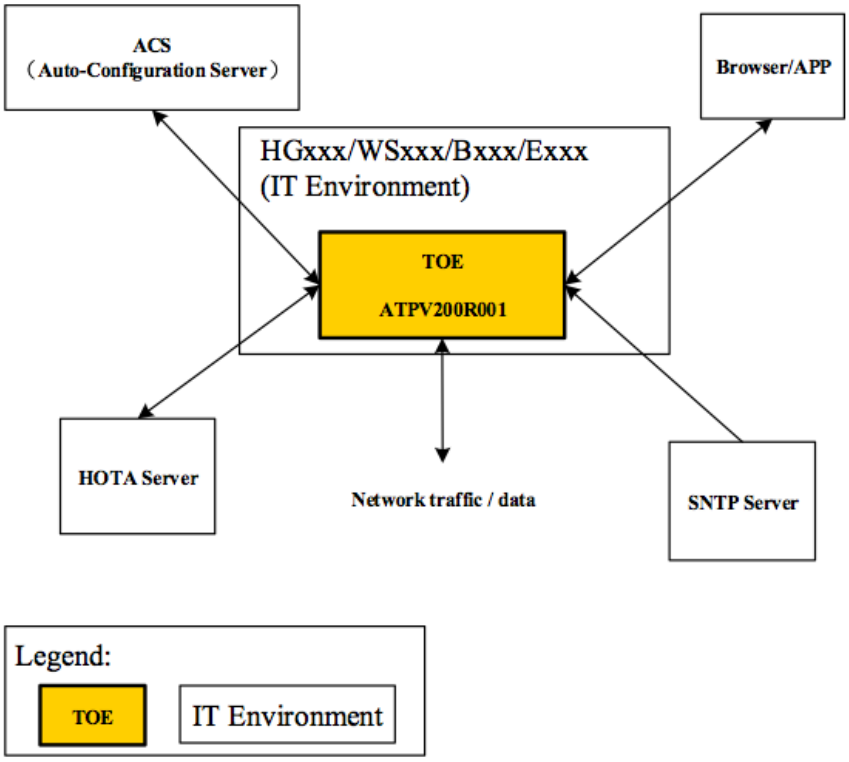

Figure 2: TOE Boundary

20 The ATP software runs on various hardware products (HGxxx/WSxxx/Bxxx/Exxx) but the hardware platforms are excluded. ACS for limited remote administration (used by ISP), browser/APP access for local administration (Browser used by the end user and ISP and APP used only by the end user), HOTA servers for online upgrade, and a Simple Network Time Protocol (SNTP) server for external time synchronization. All TSFIs are evaluated.

1.5 Clarification of Scope

21 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel and secure communication in accordance with the user guidance that is supplied with the product.

22 Section 1.4 of this document described the scope of the evaluation, which is limited to those claims made in the Security Target (Ref **Error! Reference source not found.**).

23 ATP is an application platform based on Linux OS, so the chip platform and product hardware are non-TOE. Additionally, the operational environment is defined by the following to be outside the TOE boundary:

- A browser or APP for local administration;
- ACS for remote administration;
- HOTA servers for online upgrade;
- A Simple Network Time Protocol server for external time synchronization.

24 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirement for using functions and services outside of the evaluated configuration.

1.6 Assumptions

25 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE as defined in the Security Target (Ref **Error! R eference source not found.**).

1.6.1 Usage assumptions

26 Assumptions for the TOE usage as listed in the Security Target:

a) It is assumed that authorized end users who own the device are trustworthy and the ISP authorized remote administrators are trustworthy.

b) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

c) The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

1.6.2 Environment assumptions

27 In order to provide a baseline for the IT product during the evaluation effort, certain assumptions about the environment the product is to be used in have to be made. This section documents any environmental assumptions made about the IT product during the evaluation. Assumptions for the TOE environment listed in Security Target are:

a) It is assumed that the TOE is protected against unauthorized physical access. For home gateway and CPE, the direct connection by ETH port is secure.

b) It is assumed that the TR069 remote management network access to the TOE is separated from the Internet service networks.

c) The operational environment (SNTP Server in the Internet) must provide the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

1.7 Evaluated Configuration

28 The evaluated configuration of the TOE consisted of the following configuration and environment set-up to sufficiently test the security functions claimed in the ST (Ref. **Error! R eference source not found.**).

29 In its operational environment, the TOE requires the following components to fulfil its claimed security functionality:

- A browser for local administration
- An ACS server for remote administration
- HOTA servers for online upgrade

- An SNTP server for time synchronisation

30 The TOE test environment was subsequently set-up as the following:

Huawei B525 CPE Router	CPE LTE router provided by Huawei, and is used to run the Huawei ATP software version V200R001C03
TR069 Server	Hosting the HandyACS Server used for remote administration and the SNTP server used for time synchronisation
Test Machine	Evaluators test machine used to conduct the functional and penetration testing activities

31 The evaluators had conducted the functional testing and vulnerability assessment with the above-mentioned test environment and configuration. The details are described in Section 3.3 of the Evaluation Technical Report (Ref. [7]).

1.8 Delivery Procedures

32 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

33 In overall, delivery process consists of the following phases:

- Packing,
- Finished goods warehouse – storage
- Shipment: distribution

34 All delivery process details are described in Section 1 of the Delivery documentation (Ref. [c]).

1.9 Documentation

35 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

36 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) Huawei Access Terminal Platform ATP V200R001C03 Security Target version 1.71, 3 November 2016

b) 31507711-B520s-93a Quick Start-(V100R001_01,en,SI,L)

c) CC Huawei Access Terminal Platform ATP Software V200R001C03 - ALC_DEL_V1.2 Version 1.2, 13 July 2016

d) Huawei Access Terminal Platform ATP V200R001C03 Operational User Guidance, version 1.3, 03 November 2016

e) Huawei Access Terminal Platform ATP V200R001C03 Preparative Procedures, version 1.2, 03 November 2016

2 Evaluation

37 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]).The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [4]).

2.1 Evaluation Analysis Activities

38 The evaluation activities involved a structured evaluation of the TOE, including the following components:

The evaluators testing consisted of independent testing efforts, which comprises both functional and penetration test cases to address testing requirements for the ATE_IND.2 and AVA_VAN.2 evaluation components. The testing approach for both testing was commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2).

For functional testing the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to those attacks that are commensurate to an attacker with equal or less than Basic attack potential.

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability

39 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

40 The evaluators confirmed that the TOE references used are consistent.

41 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

42 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

2.1.1.2 Configuration Management Scope

43 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE;
- the evaluation evidence required by the SARs in the ST.

44 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

45 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.3 TOE Delivery

46 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

47 The evaluators determined that the delivery procedures are used. All the details are provided in Section 4 of the Life Cycle documentation.

2.1.2 Development

2.1.2.1 Architecture

48 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

49 The security architecture description describes the security domains maintained by the TSF.

50 The initialisation process described in the security architecture description preserves security.

51 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

52 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,
- the completeness of the TSFI representation,
- it is a complete and accurate instantiation of the SFRs.

53 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all SFR-enforcing actions associated with every SFR-enforcing TSFI,

54 The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

55 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

56 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

57 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

58 The evaluators determined that all Security Target SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operating Guidance

59 The evaluators examined the operational user guidance (Ref. b)) and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

60 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

61 The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

62 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

63 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

64 The evaluators examined the provided delivery acceptance documentation (contained in c)) and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

65 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

66 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

67 Testing at EAL2 consists of assessing developer tests, performing independent functional tests and penetration tests. The TOE testing was conducted by the evaluators of BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

68 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

69 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

70 At EAL2, independent functional testing is the evaluation conducted by the evaluator based on information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of developer's test plan and creating test cases that developer tests.

71 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were developed and performed by the evaluators and are consistent with the expected test documentation.

Test ID	Description	Security Function	Justification
F001	This test is created to ensure the minimum password requirement is enforced to newly created users as well as the auto logout mechanism when new password is created. The tests would also verify that the login credentials should be obscured and does not disclose any sensitive data during the process. The communication between the browser and TOE should be analysed to ensure it is encrypted and protected from tampering.	FIA_UAU,2 FAU_GEN.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.6 FIA_UAU.7 FIA_UID.2 FDP_IFF.1 FMT_MSA.1 FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3) FCS_CKM.1 (1) FCS_CKM.1 (2) FCS_CKM.4 (1) FCS_CKM.4 (2)	This test aims to verify that the TOE performs following security functions: • Security Audit • Identification and Authentication • User Data Protection • Security Management
F002	This test subset aims to test the scenario whereby a user should not be able to authenticate to the TOE due to wrong authentication and	FIA_AFL.1 FDP_IFC.1 FMT_MOF.1 FMT_SMF.1	This test aims to verify that the TOE performs following security functions: • Identification and

Test ID	Description	Security Function	Justification
	subsequently test the lock out period. The data profiles of the user should be protected from being accessed when the said user is not logged into the TOE. Several security functions such as firewall, SNTP and reboot is tested to ensure it can handle real life scenario of the device.	FTA_TSE.1 FPT_ITI.1	Authentication • User Data Protection • Security Management • TOE Access • Protection of the TSF
F003	This test group aims to test some of the major security functionalities of the TOE as well as the ability for the administrator to create and modify alternative values for security attributes that are used to enforce SFP. This test also features the TSF-initiated termination, whereby an inactive session would be terminated by the TOE after five (5) minutes of inactivity.	FMT_MSA.1 FMT_MSA.3 FMT_MOF.1 FTA_SSL.3	This test aims to verify that the TOE performs following security functions: • Security Management • TOE Access
F004	This test aims to test the usability of the ACL in terms of limiting connection request from a user. It further tests the update requests to the server, and checks the integrity of the said file. Multiple sessions belonging to a single user is also tested, to assess whether the default developer set limit of 10 concurrent connections is observed. Backup and Restore functionality of the TOE is tested.	FMT_MOF.1 FTA_TSE.1 FDP_IFC.1 FTA_MCS.1 FMT_SMF.1	This test aims to verify that the TOE performs following security functions: • Security Management • TOE Access • User Data Protection
F005	This test checks the security of communication between the TOE with a trusted IT product as well as between users and the TOE.	FTP_TRP.1 FTP_ITC.1 FMT_SMF.1	This test aims to verify that the TOE performs following security functions: • Trusted Path/Channels • Security Management
F006	This test aims to demonstrate the TOE's ability to capture logs based on the activities done by the users. The audit logs should also be able to associate several items to the action recorded such as the user responsive ,time and date, as well as the activities performed and whether it was successfully executed. The test also checks audit review	FAU_GEN.1 FAU_GEN .2 FPT_STM.1 FAU_SAR.1 FAU_SAR.3 FAU_STG.1 FAU_STG.3 FMT_SMF.1	This test aims to verify that the TOE performs following security functions: • Security Audit • Protection of the TSF • Security Management

Test ID	Description	Security Function	Justification
	rights as well as the maximum limit of stored logs.		

72 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

73 The evaluators performed vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, and TOE design and security architecture description.

74 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

75 The penetration tests focused on:

a) Heartbleed Vulnerability attack

b) Broken Authentication and Session Management

c) Insecure Direct Object Reference

d) SQL Injection

76 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref **Error! Reference source not found.**).

2.1.4.4 Testing Results

77 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref **Error! Reference source not found.**) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Common Criteria evaluation of the TOE was analyzed to identify possible vulnerabilities.

3 Result of the Evaluation

78 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Huawei Access Terminal Platform ATP V200R001C03 performed by BAE Systems Applied Intelligence MySEF.

79 BAE Systems Applied Intelligence MySEF found that Huawei Access Terminal Platform ATP V200R001C03 upholds the claims made in the Security Target (Ref **Error! Reference s ource not found.**) and supporting documentation, and has met the requirements of the Common Criteria (CC) Assurance Level 2 (EAL2).

80 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

81 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a basic description of the TOE architecture, to understand the security behaviours of the TOE.

82 The analysis is supported by an independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

83 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

84 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, February 2016.

[6] Huawei Access Terminal Platform ATP V200R001C03 Security Target version 1.71, 3 November 2016

[7] EAU000422-S033-ETR, Evaluation Technical Report, Version 1.3, 6 December 2016

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

Term	Definition and Source
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---