KECS-CR-15-40

AITHER v1.0

Certification Report

Certification No.: KECS-NISS-0612-2015

2015. 6. 10

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2015.06.10	-	Certification report for AITHER v1.0 - First documentation

This document is the certification report for AITHER v1.0 of Korea Information Security System Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

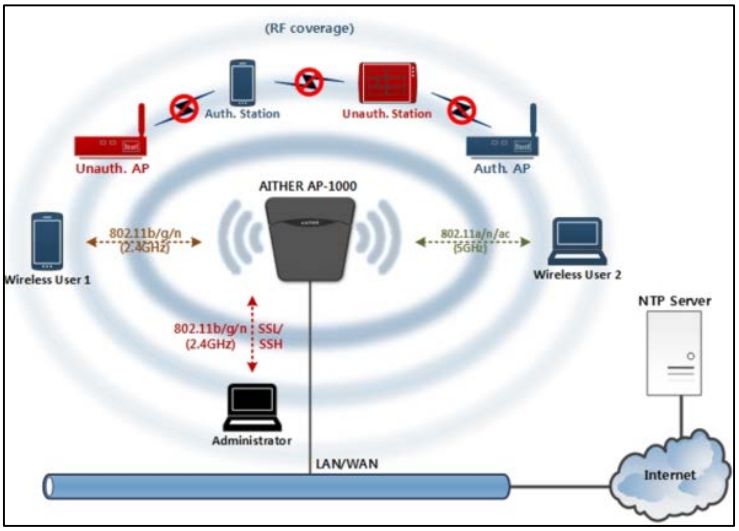
This report describes the certification result drawn by the certification body on the results of the EAL2 evaluation of AITEHR v1.0 with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

AITHER v1.0 (hereinafter TOE) is a Wireless Access Point (AP) that connects wireless devices to the wired network by configuring WLAN, and provides security functions such as Rogue AP/Station detection and unauthorized network connection prevention. The TOE consists of dedicated H/W (AITHER AP-1000), Firmware (AITHER v1.0.003), and User Manual (User Operation Manual and Preparation Process Manual).

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on June 8th, 2015. This report grounds on the evaluation technical report (ETR) [5]. TTA had submitted and the Security Target (ST) [6][7].

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL2. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

Certification Validity: The certificate is not an endorsement of the IT product by the

government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is composite product consisting of the following components and related guidance documents.

Type	Identifier	Release	Delivery Form
HW	AITHER AP-1000	-	Firmware in dedicated hardware equipment has been distributed is installed
Firmware	AITHER	v1.0.003	
DOC	AITHER v1.0 Operational User Guidance	v1.2	Softcopy (CD)
	AITHER v1.0 Preparative Procedures Guidance	v1.2	

[Table 1] TOE identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 8, 2013) [3] Korea Evaluation and Certification Scheme for IT Security (November 1, 2012) [4]
TOE	AITHER v1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012 [1]
EAL	EAL2
Developer	Korea Information Security System Co., Ltd.

Sponsor	Korea Information Security System Co., Ltd.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	June 8th, 2015
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The TOE complies with security policies defined in the ST [6][7] by security objectives and security requirements. The TOE provides the security functions as follows.

- Security Audit
  - TOE provides audit log creation and query execution functions to the subject that require audit.
- Cryptographic Support
  - TOE provides cryptographic functions to protect user data between TOE and wireless user and TSF data between TOE and administrator PC.
- User Data Protection
  - TOE provides threat detection and prevention functions by configuring secure WLAN and by monitoring wireless network traffic.
- Identification and Authentication
  - TOE provides authorization and authentication functions to control administrator who accesses the management UI and wireless devices connected to WLAN.
- Security Management
  - TOE provides functions for system configuration, security policy planning and security function management, wireless intrusion detection and prevention sensor (WIDPS), etc.
- Protection of the TSF
  - TOE provides self-test function for TOE itself.
- TOE Access
  - TOE provides functions that constrains duplicated sessions from establishing for an administrator account and destroys the authenticated

session after the defined idle time.

- Trusted Path/Channels
  - TOE provides secure paths and channels for data transmission between TOE and wireless users as well as TOE and an administrator PC.

For more details refer to the ST.

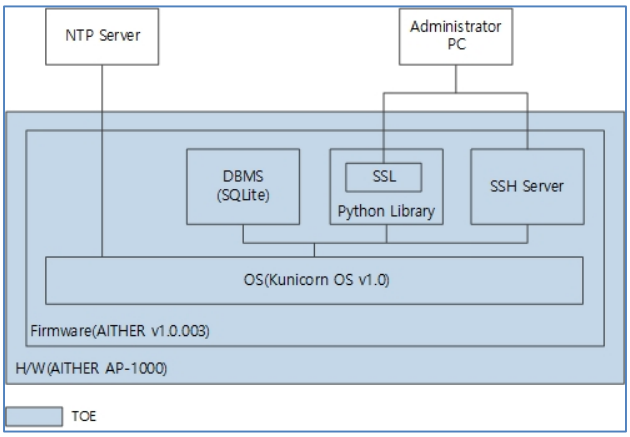
4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [6][7], chapter 3.4):

- An external NTP Server is to be reliable and stable.
- A WLAN Key for the wireless terminal should be managed securely.
- An authorized administrator of the TOE is not malicious, and well trained about the TOE management functions and carries out his/her duties accurately in accordance with the administrator guidelines

5. Architectural Information

[Figure 2] shows the physical scope of the TOE. The TOE is a wireless AP that connects wireless devices to the wired network by configuring WLAN.



[Figure 2] TOE physical scope

The TOE consists of the following components.

- OS(Kunicorn OS v1.0)

  - This component is a Linux based customized operating system. It connects a wired network and wireless network via router functions and supports AP and wireless traffic data collection functions and performs authentication and authorization, security management, security audit.

- DBMS(SQLite)

  - This component is storage for audit logs and use SQLite v3.8.9

- Python Library

  - This component is a library for the web server based administration UI support and use Python 2.7.9.

- SSL

  - This component supports HTTPS based secure server and use the default of Python Library.

- SSH Server

  - This component provides administrative console to the administrator and use Dropbear server v2015.67.

The following summarizes TOE hardware, which takes a role to start up through firmware:

- H/W(AITHER AP-1000)

TOE hardware and detailed specifications for each component are summarized in [Table 3]

Classification	Hardware Specification
CPU	Intel N2600 1.6 Ghz dual core x 1ea
Chipset	Intel NM10 x 1ea
RAM	2GByte x 1ea
ROM	NAND Flash MiSD 8Gbyte x 1ea

Classification	Hardware Specification
Ethernet Port	10/100/1000 Base-T(VIA VT6122) x 1ea
Wireless Interface	AR9382 (802.11a/b/g/n) x 3ea QCA9880 (802.11ac) x 1ea
PoE	802.3AF Type Watt/Port : 15.4W
Power Input	DC 12V Min : 1A, Max : 4A

[Table 3] TOE Hardware Detailed Specifications

For the detailed description is refer to the ST [6][7].

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
AITHER v1.0 Operational User Guidance	v1.2	April 17, 2015
AITHER v1.0 Preparative Procedures Guidance	v1.2	April 17, 2015

[Table 4] Documentation

7. TOE Testing

Tests for the TOE are:

- ST-based SFR tests
  - Testing the correct implementation of the security functional requirements described in ST
- TSFI-based tests
  - Testing the functionality of TSFI which consists TOE
- Integration tests
  - Testing the integrity of security functions provided by the TOE

The developer tested all the TSF and analyzed testing results according to the

assurance component ATE_COV.1. This means that the developer tested all the TSFI defined for SFR-enforcing of the TOE, and demonstrated that the TSFI behaves as described in the functional specification. The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1

The evaluator performed all tests provided by developer and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures, according to the guidance.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is AITHER v1.0. The TOE is product consisting of the following components:

- Hardware Device : AITHER AP-1000
- Embedded software(Firmware) : AITHER v1.0.003

The product name and the firmware version of TOE are in the product box, the warrant document. Administrator can identify those in the initial screen after logging into the management system. Also, HW model information of TOE is written on the warrant document.

Administrator can identify those in the initial screen after log in the management system.

And the guidance documents listed in chapter 6 of this report, [Table 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [11] which references Work Package Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL2.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The ST does not contain extended security requirements. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer uses a CM system that uniquely identifies all configuration items. Therefore the verdict PASS is assigned to ALC_CMC.2.

The configuration list includes the TOE, the parts that comprise the TOE, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.2.

The delivery documentation describes all procedures used to maintain security of the

TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.
Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the configuration management used throughout TOE development and the delivery activity.
The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.
The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. Therefore the verdict PASS is assigned to ADV_TDS.1.
The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, for the SFR-enforcing TSFIs the developer has described the SFR-enforcing actions and direct error messages. Therefore the verdict PASS is assigned to ADV_FSP.2.
The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.
Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or

bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.1.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.2.
Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE, don’t allow attackers possessing basic attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	PASS
	ALC_CMC.2	ALC_CMC.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.1	ADV_TDS.1.1E	PASS	PASS	PASS
		ADV_TDS.1.2E	PASS	PASS	
	ADV_FSP.2	ADV_FSP.2.1E	PASS	PASS	
		ADV_FSP.2.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_COV.1	ATE_COV.1.1E	PASS	PASS	PASS
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE administrator must operate after changing the default SSID and password of the product.
- The TOE administrator must maintain a safe condition, such as changing the password of the administrator and the user periodically.
- The TOE administrator is recommended to avoid WEP cracking and WLAN sniffing using WPA2 method between the product and the device when configuring WLAN.
- The TOE administrator must decide the installation place, and quantities considering protection range, because RF coverage of WLAN is different depending on the environment.
- The TOE administrator must check the free space in the audit data storage and perform backups periodically to prepare for the loss of audit trail.

11. Security Target

AITHER v1.0 Security Target V1.5 [6] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [7] according to the CCRA supporting document ST sanitizing for publication [8].

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
WIDPS	Wireless Intrusion Detection & Prevention Sensor
AP	Access Point
SSID	Service Set Identifier
WPA	Wi-Fi Protected Access
PBKDF2	Password-Based Key Derivation Function 2
PSK	Pre-Shared Key
RF	Radio Frequency

WIDPS	A sensor (or function) that detects and blocks intrusion threats by continually monitoring wireless network traffic
IEEE 802.11	Computer wireless network technology for local area called Wireless LAN or Wi-Fi. It is developed by the 11th working group of IEEE LAN/MAN standard committee (IEEE 802)
AP	Wired-Wireless connection bridge device that performs transfer frames from one wireless device to another device
Station	A device equipped with IEEE base WNIC (Wireless Network Interface card), which performs operations of physical layer and MAC layer operations based on IEEE 802.11 standard
Authorized AP	An AP registered in the whitelist of TOE by the

	administrator
Authorized Station	A station registered in the whitelist of TOE by the administrator
Unauthorized AP	An AP not registered in the whitelist of TOE
Unauthorized Station	A station not registered in the whitelist of TOE
SSID	A connection identifier between wireless device and AP that are used by the service provider to differentiate various basic service sets in the wireless LAN
Rogue AP	An AP, installed without permission by the administrator, can cause a security threat that induces malicious internal network intrusion by the insider or by the outsider
Honeypot AP	An AP that disclosure use information such as user IDs and passwords by stealing the SSID of the attack target AP and by pretending that you are connected to a normal AP
WPA	Wireless LAN encryption technology that uses TKIP (Temporal Key Integrity Protocol), which uses RC4 stream encryption that improves the WEP vulnerabilities specified in the IEEE 802.11i standard
WPA2	Wireless LAN encryption technology that uses CCMP (CCM Mode Protocol), which uses AES encryption method specified in IEEE 802.11i standard
Ad-hoc Network	A network that communicates each other between devices without fixed wired network
PBKDF2	An one-way hash function algorithm approved by NIST (National Institute of Standards and Technology, American Institute of Standards and Technology) and used to generate an encrypted digest of the user password
PSK	AP and wireless user share specific string as password and use it for authentication
RF Coverage	Distance capable of wireless communication between TOE and other AP or wireless device. TOE can search for all wireless network traffic within the RF coverage

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] Korea Evaluation and Certification Guidelines for IT Security (August 8, 2013)

[4] Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)

[5] TTA-CCE-14-018 AITHER v1.0 Evaluation Technical Report V1.7, June 8th, 2015

[6] AITHER v1.0 Security Target v1.5, May 21th, 2015 (Confidential Version)

[7] AITHER v1.0 Security Target Lite v1.5, May 21th, 2015 (Sanitized Version)

[8] ST sanitizing for publication, CCDB-2006-04-004, April 2006