KECS-CR-17-24

PersonalUTM 1.0 for wiz stick 1.0

Certification Report

Certification No.: KECS-CISS-0788-2017

2017. 5.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2017.5.2	-	Certification report for PersonalUTM 1.0 for wiz stick 1.0 - First documentation

This document is the certification report for PersonalUTM 1.0 for wiz stick 1.0 of KT Corp.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the certification body on the results of the EAL1 evaluation of PersonalUTM 1.0 for wiz stick 1.0 developed by KT Corp with reference to the Common Criteria for Information Technology Security Evaluation (hereinafter “CC”) [1]. It describes the evaluation result and its soundness as well as conformity.

The Target of Evaluation (TOE) is PersonalUTM 1.0 for wiz stick 1.0 (hereinafter “TOE”) and it is composed of firmware and software, which provide the security function of detecting access to harmful sites or pharming sites, and blocking access to those sites based on the detection result, as well as the security function of VPN client.

The TOE consists of wiz stick Portable in a stick type portable device (wiz stick Device), wiz stick adminAgent installed and operated in an administrator PC and wiz stick userAgent installed and operated in a user PC.

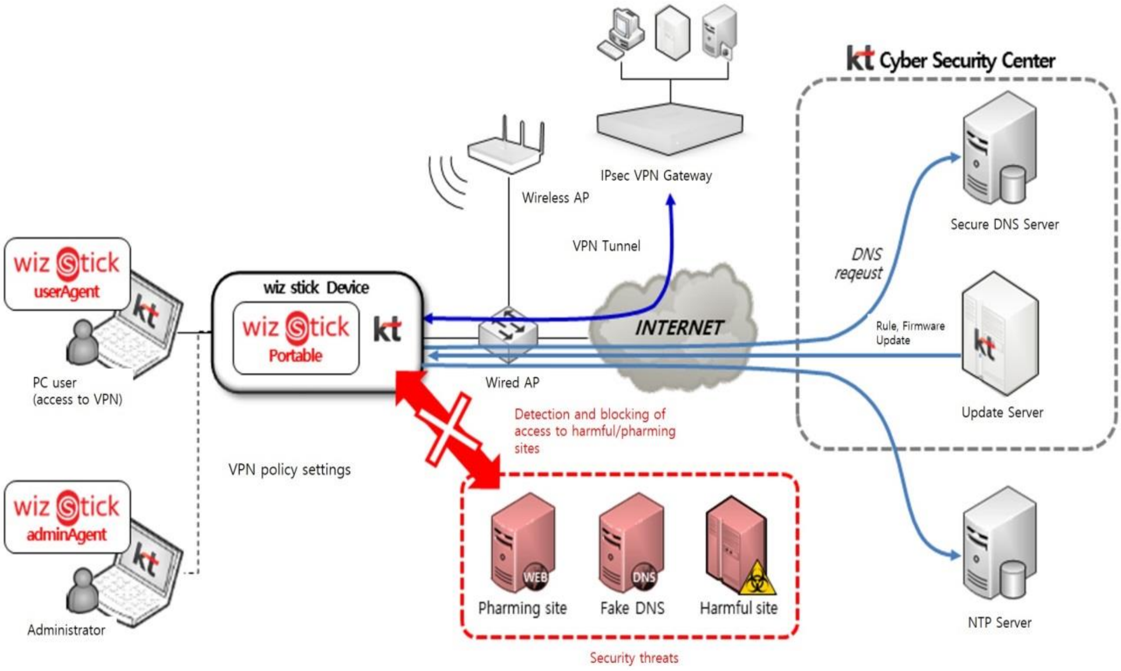
The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on April 19th, 2017. This report grounds on the evaluation technical report (ETR)[3] TTA had submitted and the Security Target (ST) [4].

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 EAL1. 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 for the TOE. When wiz stick Device is recognized in a form of RNDIS (Remote Network Driver Interface Specification) through a user PC’s USB port, wiz stick adminAgent or wiz stick userAgent makes wiz stick Device as the single point of connection between a user PC and the internet. wiz stick Portable offers the function to detect harmful or pharming sites by analyzing traffic transmitted between a user PC and an external network and to block access based on the detection result, as well as the function of IPsec VPN client.

Rules or TOE firmware used for detection and blocking of access to harmful or pharming sites are updated on a regular basis by the Update Server managed and operated by the developer KT Corp.

Although an external "certificate management server" is necessary in order to support the function of "secure certificate management" categorized as Non-TSF, such "certificate management server" was not identified in the TOE operational environment because it is not an external entity that corresponds to the usage and security objectives of the TOE.



[Figure 1] TOE Operational Environment

TOE users are classified into "administrator" who performs VPN settings and "PC user" who is an actual user of a user PC.

- Administrator
  Administrator uses "wiz stick adminAgent" that only includes the wiz stick Agent functions such as basic product information check, audit record viewing and VPN settings.

- PC user
  PC user uses “wiz stick userAgent” that supports the implementation of the security function of wiz stick Portable through product information check, audit record viewing, environment settings, etc. A PC user can receive wiz stick Device whose VPN policy is set by an administrator and perform VPN connection with an external VPN gateway developed based on IPsec standard protocol.

External entities required as IT environment for the operation of the TOE are as follows.

- Secure DNS Server
  DNS server managed by the developer, KT Cyber Security Center, for the purpose of blocking an attempt to access a pharming site through DNS packet corruption.

- Update Server
  Server that updates policies and firmware of wiz stick Portable.

- IPsec VPN Gateway
  External VPN gateway that creates IPsec-based VPN with wiz stick Portable according to wiz stick Portable’s VPN connection settings.

- NTP Server
  External NTP server through which the TOE receives reliable time stamp

[Table 1] identifies hardware and software for non-TOE required by wiz stick adminAgent and wiz stick userAgent.

Category		Minimum Specifications
Hardware	CPU	Intel Pentium4 1.6 GHz or higher
	HDD	100 GB or higher
	Memory	1 GB or higher
	NIC	100/1000 Mbps
Software	OS	Windows 7 Professional (SP1, 32 bit)
	Others	.NET Framework 4.5

[Table 1] Non-TOE requirements for wiz stick adminAgent and wiz stick userAgent.

Non-TOE required by wiz stick Portable is dedicate hardware (hereinafter “wiz stick Device”), and models and specifications of wiz stick Device are identified as below.

Category	Requirements	
Model Name	WS01-001W	
	WS01-001B	
	WS01-001R	
CPU	ARM Cortex-A9 (400 MHz) * 2 (in Cortina CS7522 multi-service processor)	
RAM	256 MB (DDR2)	
Storage	128 MB (NAND Flash memory)	
External Network Port	Wireless	IEEE 802.11 a/g/n (2.4 GHz, 5 GHz)
	Wired	USB Mini-B (10/100 Base-T, RJ-45 gender connection required)
PC Connection Port	USB Micro-B	

[Table 2] Models and Specifications of wiz stick Device(Non-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 reference is identified as follows.

TOE	PersonalUTM 1.0 for wiz stick 1.0
Version(Build)	1.0.8
TOE Components	wiz stick adminAgent 1.0.4 (AdminWizStick_1.0.4.exe) wiz stick userAgent 1.0.4 (UserWizStick_1.0.4.exe) wiz stick Portable 1.0.8 (kernel-rootfs-upgrade-1.0.8.img)
Guidance Documents	PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for Administrator v1.7 (CC-wiz_stick_1.0-ADM.pdf) PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for PC User v1.7 (CC-wiz_stick_1.0-USR.pdf)

[Table 3] TOE identification

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (June 27, 2016) Korea Evaluation and Certification Regulation for IT Security (November 1, 2012)
TOE	PersonalUTM 1.0 for wiz stick 1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL1
Protection Profile	ST does not claim conformance to PP
Developer	KT Corp.
Sponsor	KT Corp.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	April 19, 2017
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [4] by security objectives and security requirements. The TOE provides security features to detect access to harmful sites or pharming sites and block access to those sites based on the detection result, as well as the function of VPN client. For more details refer to the ST [4].

4. Assumptions and Clarification of Scope

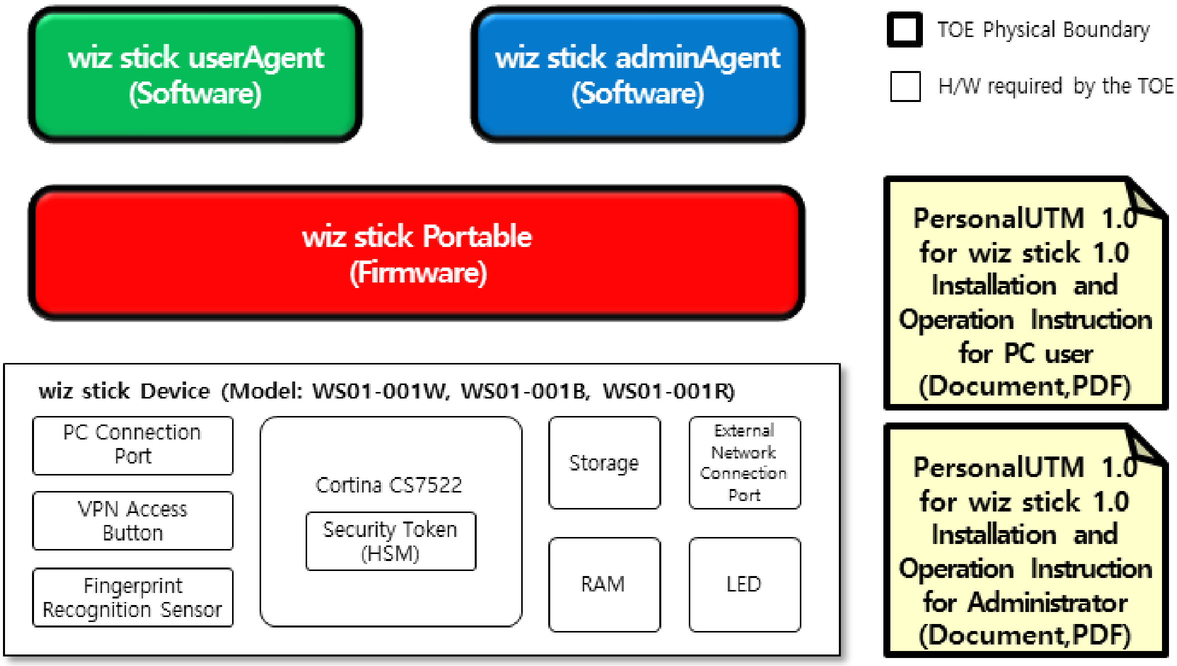
There are no Assumptions in the Security Problem Definition in the ST. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target. Wiz Stick device is out of TOE scope. For example, the Fingerprint sensor and Security Token are included in Wiz Stick device but those are not assessed as part of this evaluation. In addition to this, the logical scope of Wired/Wireless Network Settings, Request to Register/Recognize Fingerprint, Function of Certificate Use Control, Fingerprint Registration/Recognition and PKCS#1-based Certificate Management & Use are classified as non-TSF because those cannot be physically separated from TOE components but includes source codes compiled/built together (see Figure 2 and Figure3). This evaluation covers only the specific software version and guidance documents described in [Table 3].

5. Architectural Information

The TOE consists of wiz stick Portable in a portable device (wiz stick Device), wiz stick adminAgent installed and operated in an administrator PC and wiz stick userAgent installed and operated in a user PC. The developer KT Corp. directly delivers wiz stick adminAgent and wiz stick userAgent to a designated administrator or PC users in an organization.

The TOE is a part of the already known product, wiz stick 1.0, and wiz stick Device is not included in the physical scope of the TOE. The Fingerprint Recognition Sensor and Security Token is out of TOE scope (see Figure 2).

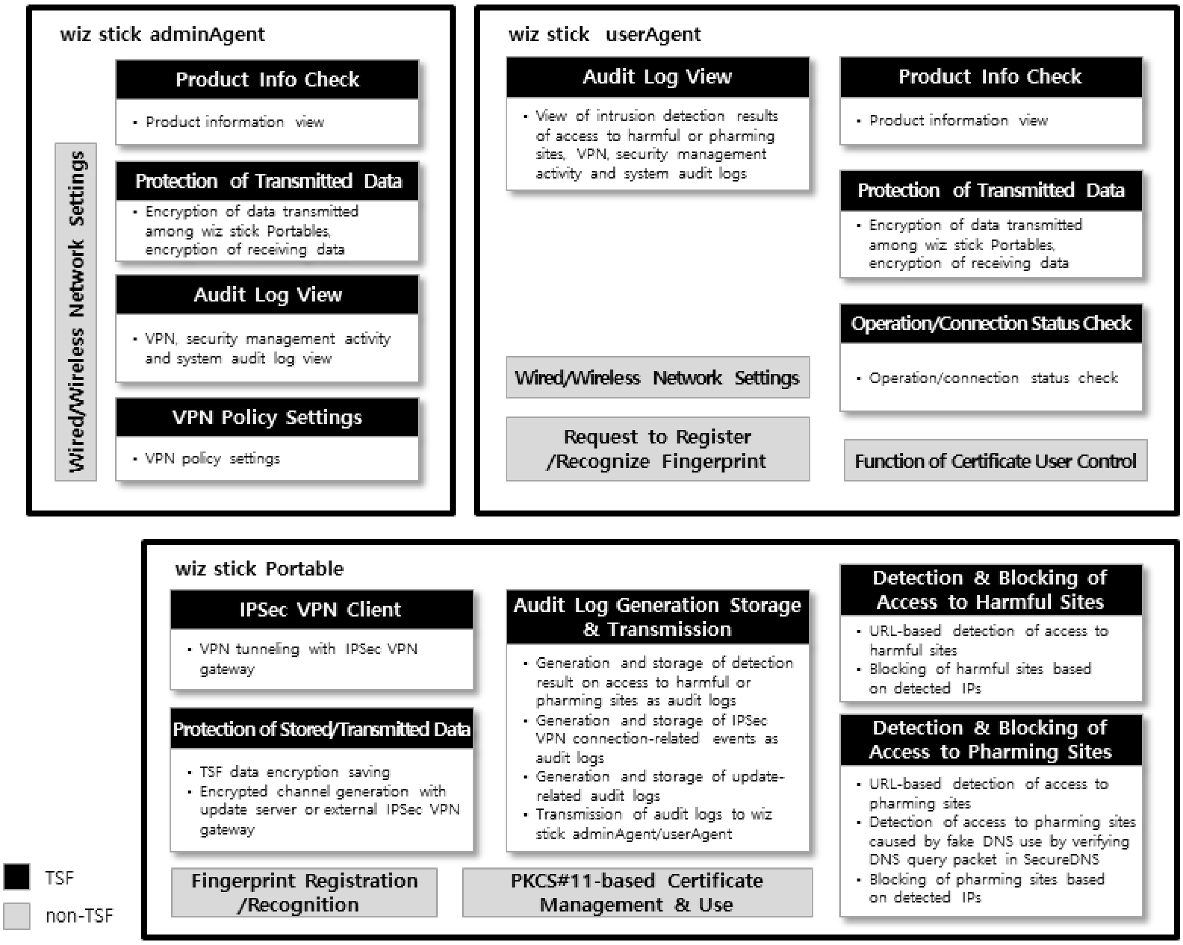
[Figure 2] and [Figure 3] show the scope of the TOE.


wiz stick userAgent (Software)
wiz stick adminAgent (Software)
TOE Physical Boundary
H/W required by the TOE
wiz stick Portable (Firmware)
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for PC user (Document,PDF)
wiz stick Device (Model: WS01-001W, WS01-001B, WS01-001R)
PC Connection Port
VPN Access Button
Fingerprint Recognition Sensor
Cortina CS7522
Security Token (HSM)
Storage
External Network Connection Port
RAM
LED
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for Administrator (Document,PDF)

[Figure 2] Physical Scope

TOE Component	Distribution Form	Distribution Method
wiz stick adminAgent 1.0.4 (AdminWizStick_1.0.4.exe)	Software	Software in CD safely distributed only to a designated administrator in an organization by the developer KT Corp.
wiz stick userAgent 1.0.4 (UserWizStick_1.0.4.exe)	Software	Software in CD safely distributed only to a designated administrator or PC users in an organization by the developer KT Corp.
wiz stick Portable 1.0.8 (kernel-rootfs-upgrade-1.0.8.img)	Firmware	Firmware initially contained in wiz stick Device and directly distributed to a customer by the developer's person in charge, and during the operation, distributed through communication with an external update server
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for Administrator v1.7 (CC-wiz_stick_1.0-ADM.pdf)	PDF	Document in CD directly distributed to a customer by the developer's person in charge (PDF)
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for PC User v1.7 (CC-wiz_stick_1.0-USR.pdf)	PDF	Document in CD directly distributed to a customer by the developer's person in charge (re-distributed by an administrator to PC users off-line) (PDF)

[Table 5] TOE physical scope


wiz stick adminAgent
Wired/Wireless Network Settings
Product Info Check
• Product information view
Protection of Transmitted Data
• Encryption of data transmitted among wiz stick Portables, encryption of receiving data
Audit Log View
• VPN, security management activity and system audit log view
VPN Policy Settings
• VPN policy settings
wiz stick userAgent
Audit Log View
• View of intrusion detection results of access to harmful or pharming sites, VPN, security management activity and system audit logs
Product Info Check
• Product information view
Protection of Transmitted Data
• Encryption of data transmitted among wiz stick Portables, encryption of receiving data
Operation/Connection Status Check
• Operation/connection status check
Wired/Wireless Network Settings
Request to Register /Recognize Fingerprint
Function of Certificate User Control
wiz stick Portable
IPSec VPN Client
• VPN tunneling with IPSec VPN gateway
Protection of Stored/Transmitted Data
• TSF data encryption saving
• Encrypted channel generation with update server or external IPSec VPN gateway
Audit Log Generation Storage & Transmission
• Generation and storage of detection result on access to harmful or pharming sites as audit logs
• Generation and storage of IPSec VPN connection-related events as audit logs
• Generation and storage of update-related audit logs
• Transmission of audit logs to wiz stick adminAgent/userAgent
Detection & Blocking of Access to Harmful Sites
• URL-based detection of access to harmful sites
• Blocking of harmful sites based on detected IPs
Detection & Blocking of Access to Pharming Sites
• URL-based detection of access to pharming sites
• Detection of access to pharming sites caused by fake DNS use by verifying DNS query packet in SecureDNS
• Blocking of pharming sites based on detected IPs
Fingerprint Registration /Recognition
PKCS#11-based Certificate Management & Use
■ TSF
□ non-TSF

[Figure 3] Logical Scope

6. Documentation

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

Identifier	Version	Date
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for Administrator v1.7.PDF	v1.7	April 13th, 2017
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for PC User v1.7.PDF	v1.7	April 13th, 2017

[Table 6] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. The developer's tests were performed on each distinct operational environment of the TOE (see chapter 1 of this report for details about operational environment of 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 in the functional specification, and demonstrated that the TSF behaves as described in the functional specification.

Therefore the developer tested all SFRs defined in the ST [4].

The evaluator performed all the developer's tests, and conducted independent testing listed in ETR [3], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [4]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of source code, privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, flaws in networking protocol implementation, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [3].

8. Evaluated Configuration

The TOE is software and firmware consisting of the following components::

- wiz stick adminAgent 1.0.4,
- wiz stick userAgent 1.0.4, and
- wiz stick Portable 1.0.8.

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 6 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] which references Single Evaluation 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 EAL1.

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 Objectives for the operational environment are clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.1.

Extended Components have been clearly and unambiguously defined, and whether they are necessary, i.e. they may not be clearly expressed using existing CC Part 2 or CC Part 3 components. Therefore the verdict PASS is assigned to ASE_ECD.1.

The SFRs and SARs are clear, unambiguous and well-defined and whether they are internally consistent. Therefore the verdict PASS is assigned to ASE_REQ.1.

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 has clearly identified the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.

The developer performs configuration management on the TOE and the evaluation evidence. Therefore the verdict PASS is assigned to ALC_CMS.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include life-cycle model used by developer, the configuration management, the security measures 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 developer has provided a high-level description of at least the SFR-enforcing TSFIs, in terms of descriptions of their parameters. Therefore the verdict PASS is assigned to ADV_FSP.1.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore the verdict PASS is assigned to ATE_IND.1.

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.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), 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_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
ATE	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	PASS
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 7] 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 shall be installed and connected in a user PC to be protected from an external intrusion, as the single point of connection for internet access for a user. Therefore, all wired/wireless network adaptors shall be made unavailable except for the TOE by an administrator and a PC user.
- The TOE shall be provided with timestamps from an external trusted NTP server in order to accurately record security-related events. Therefore, the TOE shall be configured to be connected to a NTP Server by an administrator and a PC user.
- The TOE shall download a secure internet access policy from the update server managed by Cyber Security Center of the developer KT Corp. and apply it to the execution of the security function. Therefore, the TOE shall be configured to be connected to the update server by an administrator and a PC user.
- The TOE provides the function that enables VPN policy settings of wiz stick Portable used by PC users through wiz stick adminAgent. Therefore, an administrator of an organization shall be careful in managing adminAgent so that it is not distributed without permission or a PC user does not use it at his/her discretion.
- An authorised administrator of the TOE shall not be ill-intended and shall be properly trained for TOE admin functions and fulfill obligations accurately according to the administrator guidelines.
- Since the TOE is released from the manufacturer without specified initial values for VPN security policy, an authorised administrator of the TOE shall set up initial values of VPN security policy during the initial TOE operation according to the administrator guideline.
- An authorised administrator of the TOE shall change confidential values such as VPN access password, per-shared key periodically for maintaining secure state.
- The person in charge in the organization to whom the TOE was handed over shall keep and maintain the TOE in a physically safe location. Especially, wiz stick Device that is distributed together with wiz stick Portable shall be managed safely so that it is used only by actual users.
- The reliability and the safety of an operating system of PC on which TOE components are installed shall be assured by deleting all unnecessary services or

means and by reinforcing vulnerabilities of the operating system.

- For the TOE to provide normal security functions, VPN gateway connected with the TOE shall comply with IPsec VPN standard and apply safe set values (e.g. a length and combination rule shall apply so that pre-shared key is not easily guessed).

11. Security Target

PersonalUTM 1.0 for wiz stick 1.0 Security Target v1.15 [4] is included in this report for reference.

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
ACL	Access Control List
C&C	Command & Control
DNS	Domain Name System
RNDIS	Remote Network Driver Interface Specification
VPN	Virtual Private Network
IPsec	Internet Protocol Security
ACL	Access Control List is a method used to define a network (subnet, IP address) or to control traffic based on the defined network. ACL uses two type of commands – Permit and Deny. It is used for the purpose of filtering and traffic definition and is capable for filtering up to Layer 4.
C&C Server	C&C Server plays a role as “brain” of cyber-attacks that remotely manages zombie PCs and gives commands. A hacker distributes malicious codes in advance to infect PCs to turn them into zombies. Then, he can remotely control zombie PCs as he wants through the C&C server.
DNS	DNS refers to the Domain Name System for computer and network service consisting of a domain hierarchical structure. DNS naming is used in TCP/IP network such as the internet to find computers and services by using

	a name that users find familiar. If a user enters DNS name in an application program, DNS service checks the name by using other information (IP address, etc.) linked to the name.
iptables	iptables is software that determines the packet flow with reference to tables that contain rules and chains. The TOE enforces an information flow control policy by using iptables, including permitting, blocking or delivering packets to a designated location.
Pharming	Pharming is a type of an attack intended to redirect access to normal website address such as a banking company to a phishing site, even if a user accesses the site by using the internet “Favorites” or searching on a portal website, so that an attacker can obtain banking transaction or other information surreptitiously.
RNDIS	RNDIS is a specification for network device on dynamic plug-and-play I/O bus such as USB, IEEE1394, InfiniBand and Bluetooth wireless technology. wiz stick Device follows RNDIS for PC connection.
Snort	Snort is a system that detects access to harmful sites. It has the ability to perform real-time traffic analysis and packet logging on IP networks.
VPN	VPN is a private network across a public network that enables users to communicate securely, not being exposed to others outside the network. VPN delivers and receives messages by using the standard protocol on a public network such as the internet.
IPsec	IPsec is a network protocol that authenticates and encrypts each IP packet of a communication session for safe internet protocol (IP) communication. The security is processed by authenticating and encrypting individual IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys for use during the session. In the TOE, IPsec is used to protect the data

	flow between the security gateway and the host wiz stick. IPsec uses the cryptographic security service in order to protect communication between the internet protocol networks.
PC User	As an end-user of the TOE, a PC User is a human user who uses a user PC in which wiz stick userAgent is installed and operated. The user PC is connected to wiz stick Device.
Administrator	Administrator is a person who manages wiz stick product in an organization and sets VPN policies by using wiz stick adminAgent for wiz stick Device that will be distributed to PC users. Since an administrator deals with VPN policy of an organization, only one or a small number of persons should be authorised as administrator.
wiz stick Device	wiz stick Device is a name that identifies the case and H/W of wiz stick 1.0 product. wiz stick Portable, which is a TOE component, is distributed to an end user together with wiz stick Device. Technically speaking, however, wiz stick Device does not include wiz stick Portable.
Harmful Site	Harmful Site means a source of malicious codes that can spread malicious codes (malware, virus, etc.) to user PCs, or C&C server that can issue commands to zombie user PCs for DDoS attack or other types of attacks. The list of harmful sites used in the TOE is defined by the developer KT Corp.
Detection and Blocking of Access to Harmful Sites	The function of detection and the function of blocking of access to harmful sites provided by the TOE are clearly distinguished. “Detection of access to harmful sites” is to analyze packets in the traffic passing through the TOE and to judge if there is any access to URL defined as harmful sites. “Blocking of access to harmful sites” means a function to block incoming packets from IPs defined as harmful sites by applying blocking policies that were created and added on the basis of the detection result. In other words, the TOE does not block access to harmful sites immediately upon its detection

	of access, but rather blocking is carried out after ACL for blocking of harmful site access is registered in the blocking policy based on the detection result.
Detection and Blocking of Access to Pharming Sites	The function of detection and the function of blocking of access to pharming sites provided by the TOE are clearly distinguished. “Detection of access to pharming sites” is to analyze packets in the traffic passing through the TOE and to judge if there is any access to URL defined as pharming sites. “Blocking of access to pharming sites” means a function to redirect to normal sites instead of pharming sites by applying blocking policies created and added on the basis of the detection result. In other words, the TOE does not block access to pharming sites immediately upon its detection of access to pharming sites, but rather blocking (redirecting to normal sites) is carried out after the policy for blocking of pharming site access is registered in the blocking policy on the basis of the detection result. However, the first web page of a pharming site will be displayed as it is, so that the user realizes that he/she is accessing the pharming site, and then, it will be redirected to a normal site from the next web page request.
Normal Site	Normal Site is an actual site of URL disguised by a pharming site.

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

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

[3] TTA-CCE-16-031 PersonalUTM 1.0 for wiz stick 1.0 Evaluation Technical Report V1.3, April 27th, 2017

[4] PersonalUTM 1.0 for wiz stick 1.0 Security Target v1.15, April 13th, 2017