	Document Type	CC:Evidence	Version	V1.15
kt	Author	KT Corp.	Publication Date	2017.04.13

PersonalUTM 1.0 for wizStick 1.0

Security Target

Table of Contents

List of Tables

List of Figures

I. ST Introduction

This document presents the Security Target (ST) for “PersonalUTM 1.0 for wiz stick 1.0” that describes the security requirements and evaluation rationale.

1. ST Reference

Table 1. ST Reference

Classification	Description
Title	PersonalUTM 1.0 for wiz stick 1.0 Security Target
Version	v1.15
Author	Safety and Security Development TF at KT Future Convergence Business Office
Publication Date	April 13, 2017
CC and Version	Common Criteria V3.1 R4
Evaluation Assurance Level	EAL1
Key Words	Detection and blocking of access to harmful sites, Detection and Blocking of Access to Pharming Sites, IPsec VPN

2. TOE Reference

Table 2. TOE Reference

Classification	Description
TOE Title	PersonalUTM 1.0 for wiz stick 1.0
TOE Version (build version)	1.0.8
TOE Component	- wiz stick adminAgent 1.0.4 - wiz stick userAgent 1.0.4 - wiz stick Portable 1.0.8
Developer	KT Corp.
Evaluation Requestor	KT Corp.
Final Release	April 13, 2017

3. TOE Overview

3.1. TOE Type

PersonalUTM 1.0 for wiz stick 1.0 (hereinafter referred to as the "TOE") is defined as "a product consisting of firmware and software, which provides the 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 function of VPN client.[1]

3.2. TOE Usage

The main usage of the TOE is primarily to provide the safe PC security without complicated settings for users who do not have in-depth security knowledge.

When a user connects the device in a form of USB stick that contains the TOE to a personal computer, the TOE analyzes traffic transmitted between the user PC and an external network, thereby providing the following functions:

- The function of "detection and blocking of access to a harmful site" that detects if a website a user is accessing is harmful, based on its URL, and blocks access to a harmful site by using the detected IP address
- The function of "detection and blocking of access to a pharming site" that forwards DNS query packet (TCP/UDP 53 port) generated from a user PC to the Secure DNS server operated by KT Corp. and receives normal DNS information, and then detects and blocks access to a pharming site by comparing it against accurate URL and IP information of banking sites and portal sites that have been damaged by pharming in the past
- The function of "IPsec VPN client" that sets up a secure VPN with an external IPsec VPN gateway

The TOE is a part of the known product, wiz stick 1.0, which also includes other functions described below in addition to the TOE functions. In other words, the functions described below are not the functions provided for the usage of the TOE, even though they are included in the physical scope of the TOE.

[1] Please see Chapter 1.5 "Terms and Definitions" for the definition of the functions of detection and blocking of access to a harmful or pharming sites.

- Fingerprint Security Token: It provides the function of PKCS#11 standard-based security token(HSM) to encrypt a certificate within a device by using encrypted fingerprint of a user.
- Control of Certificate Use: It provides the function of approval of a higher-level approver, certificate use tracking and loss management, which is necessary to use the certificate within the wiz stick device. The "wiz stick 1.0" product is linked to an external "certificate management server," which makes it possible to offer the function to control the certificate for a user.
- Wired/Wireless Network Settings: It provides the network setting function for a user so that the "wiz stick 1.0" product can be linked to an external network. The product can be linked to a wired or wireless network.

3.3. Hardware, Firmware and Software Required by the TOE

Non-TOE required by wiz stick adminAgent and wiz stick userAgent is identified as follows:

Table 3. Specifications of Non-TOE Required by wiz stick Agent

Category	Item	Requirement
H/W	CPU	Intel Pentium4 1.6 GHz or higher
	HDD	100 GB or higher
	Memory	1 GB or higher
	NIC	100/1000 Mbps
S/W	OS	Windows 7 Professional (SP1, 32 bit)
	Others	.NET Framework 4.5

Non-TOE required by wiz stick Portable is dedicate hardware (hereinafter referred to as "wiz stick Device"), and models and specifications of wiz stick Device are identified as below:

Table 4. Models and Specifications of wiz stick Device(Non-TOE)

Category	Requirement	
Model Name	WS01-001W	
	WS01-001B	

Category	Requirement	
	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	

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

Table 5. List of External Entities

External Entity	Use
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

3.4. TOE Security Services

The TOE provides the security services as described below:

Detection and Blocking of Access to Harmful Sites

The TOE detects a user PC's access to a harmful site based on packet URL information, and records the access history as audit logs. The TOE, based on detected IP addresses of harmful sites, blocks access to harmful sites. The rule used for detection and blocking of access to harmful sites is updated on a regular basis by the Update Server operated by the developer, KT Corp, so that it maintains the up-to-date security status.

Detection and Blocking of Access to Pharming Sites

The TOE detects and blocks a user PC's access to a pharming site by using the following methods:

- When DNS query packet (TCP/UDP 53 port) is generated from a user PC, the TOE forwards the packet to the Secure DNS Server operated by KT Corp. and receives normal DNS information.
- The TOE maintains accurate URL and IP information of major banking websites and portal websites that have been damaged by pharming in the past, and detects access to a pharming site by conducting a comparison when a user accesses such websites. Then, it records the access history as audit logs.
- When a user access a pharming site, the TOE redirects access towards a normal website based on IP address of the detected pharming site, thereby blocking a user's access to the pharming site. The rule used for detection and blocking of access to harmful sites is updated on a regular basis by the Update Server operated by the developer, KT Corp, so that it maintains the up-to-date security status.

IPsec VPN Client

The TOE provides the function of VPN client that creates a secure VPN with an external IPsec VPN gateway to which IPsec protocol standard applies mutatis mutandis.

Security Audit

The TOE provides the function to generate and store audit records for security-related events and to enable an administrator and PC users to retrieve them. The TOE generates audit data with reference to time values in sync with an external NTP server. If a threshold on the audit trail is exceeded, it deletes the 300 oldest audit data in response to any possible loss of audit data.

Cryptographic Support

The TOE provides functions for cryptographic key generation, cryptographic key distribution, cryptographic key destruction, cryptographic operation, network layer cryptographic communication and random number generation for the purpose of encryption of data transmitted with an external update server, encryption of data transmitted among TOE components, encryption of data transmitted with an external VPN gateway based on IPsec VPN and storage of TSF data encryption within the TOE.

Authentication of VPN Access User

The TOE provides the function of authentication of VPN access users and maintains attributes of "VPN access authorisation" until VPN is terminated. VPN access password, which is necessary for authentication of a VPN access user, requires a complicated combination rule that allows for a high level of secrets.

Security Management

The TOE provides PC users with the function to manage security functions and TSF data and also provides an administrator with the function to manage security attributes of VPN connection SFP and some TSF data.

TSF Protection

The TOE encrypts all TSF data transmitted to an external Update Server and thus protects them from disclosure during transmission. At the same time, it provides the function of the integrity verification and scrapping of data whose integrity was compromised. All the data transmitted among TOE components are encrypted, thereby safely protected from disclosure or modification.

The abovementioned security properties of the TOE are intended to provide a basic security environment for safe internet use by simply connecting a portable device (wiz stick Device) to a PC without the necessity for in-depth security knowledge or special measures by an individual. Therefore, the TOE does not require individual users to have complicated security policy management for detection and blocking of access to harmful or pharming sites, but rather, enables them to download security policies from the Update Server operated by the developer, KT Corp. Eventually, the TOE is a form of a security product that does not provide functions that other types of security products have, such as administrator identification and authentication or detection and blocking policy settings.

3.5. TOE Operational Environment

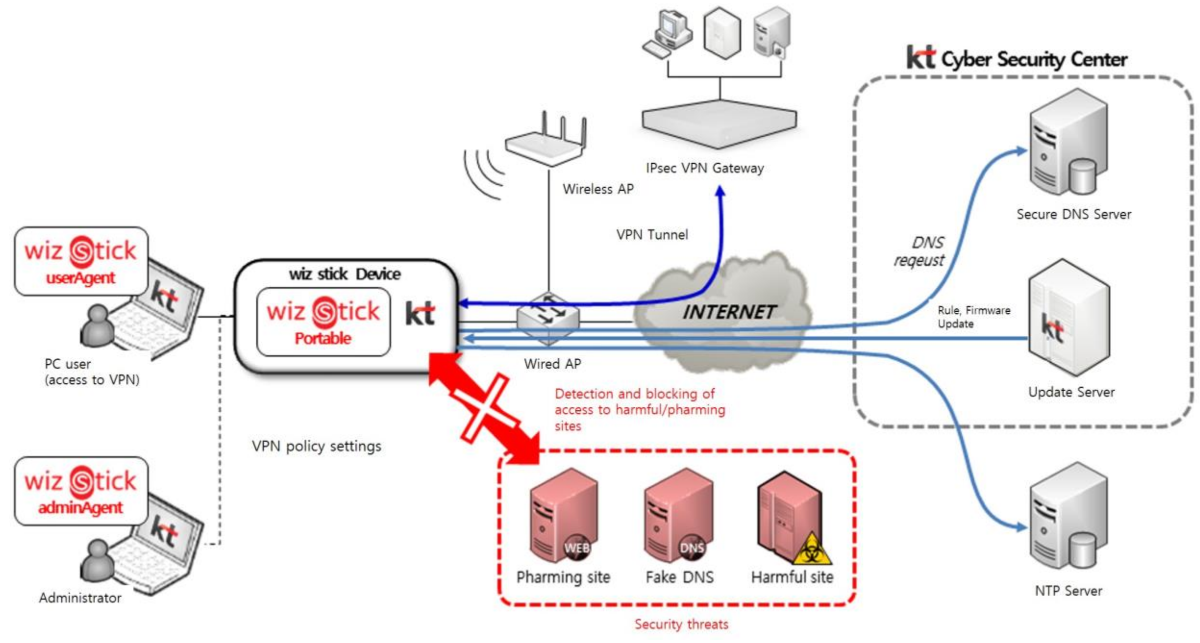
The TOE consists of wiz stick Portable in a stick type portable device (wiz stick Device), wiz stick adminAgent installed and operated in an administrator PC and wiz stick userAgent installed and operated in a user PC.

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 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.

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

Figure 1. TOE Operational Environment



Although an external "certificate management server" is necessary in order to provide 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 of the TOE.

4. TOE Description

4.1. Physical Scope

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.

Figure 2. Diagram of the Physical Scope

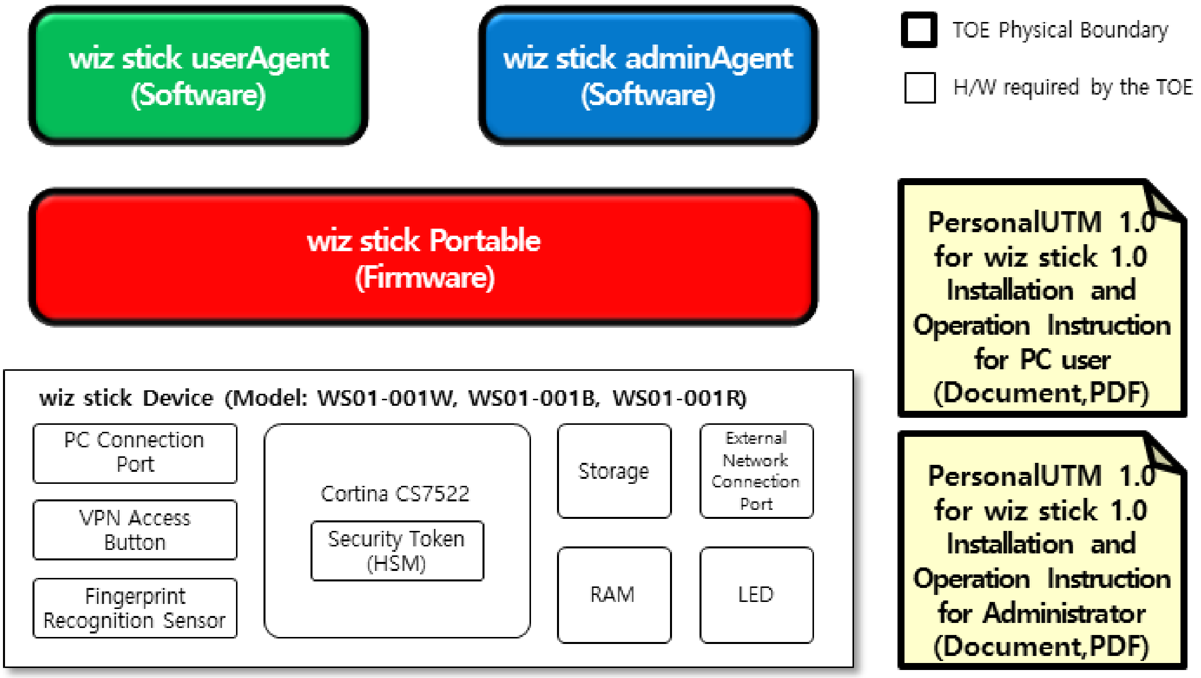

wiz stick userAgent (Software)
wiz stick adminAgent (Software)
TOE Physical Boundary
H/W required by the TOE
wiz stick Portable (Firmware)
PersonalUTM 1.0 for wiz stick 1.0 Installation and Operation Instruction for PC user (Document,PDF)
wiz stick Device (Model: WS01-001W, WS01-001B, WS01-001R)
PC Connection 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)

Table 6. Physical Scope of the TOE

TOE Component	Distribution Type	Distribution Method
wiz stick adminAgent 1.0.4 (AdminWizStick_1.0.4.exe)	S/W	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)	S/W	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)	F/W	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)

※ In case of the description on common functionality of both wiz stick userAgent and wiz stick adminAgent, or in case of the description that does not need to separate users, wiz stick userAgent and wiz stick adminAgent are collectively referred to as “wiz stick Agent.”

3rd parties included in the TOE are identified as below:

Table 7. 3rd-party Included in the TOE

3rd-party Product	Use
Snort 2.8.4.1	Software that performs detection of access to harmful or pharming sites
iptables 1.4.10	Software that performs blocking of access to harmful or pharming sites
libreSWAN 3.18	Open source library that provides IPsec-based VPN connection with an external VPN gateway
NSS crypto library 3.16.3	Cryptographic library used for VPN connection with an external VPN gateway

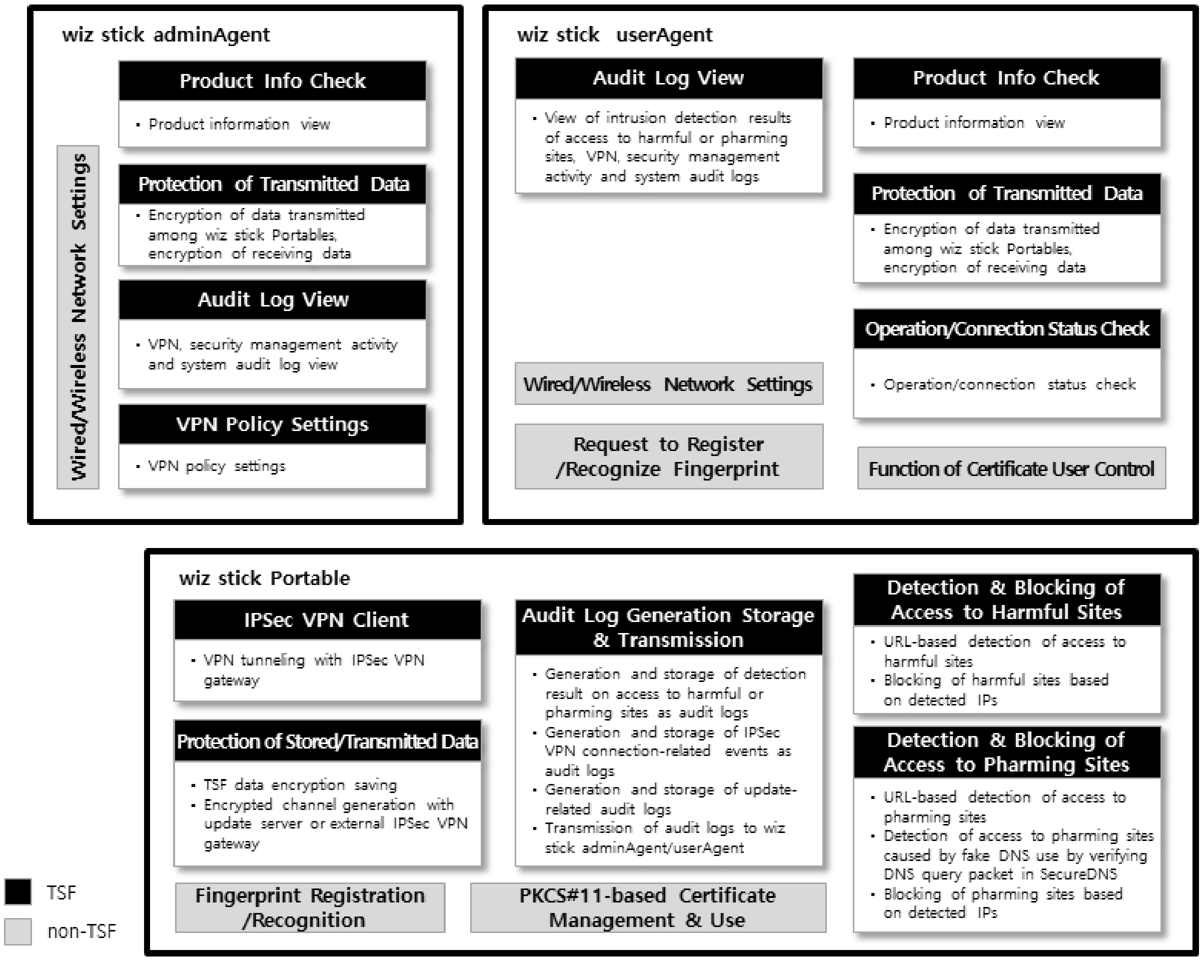
3rd-party Product	Use
Pycrypto 2.6.1	Cryptographic library used for storage of communication encryption among TOE components, communication encryption for the Update Server and TSF data encryption
SQLite 3.6.20	DBMS software used for safe storage of audit records

Since wiz stick Portable is in a form of firmware, it contains OpenWRT Backfire 10.03.1(Linux kernel 3.4.86) which is an operating system.

4.2. Logical Scope

The logical scope of the TOE is classified as below:

Figure 3. Diagram of the Logical 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

❍ wiz stick adminAgent

wiz stick adminAgent shall be distributed to an authorised administrator only in a safe manner according to the policy, and it provides an administrator with the function to view product information and make VPN settings.

Product Info Check
wiz stick adminAgent provides product information such as the TOE and TOE component version only for an administrator.

Protection of Transmitted Data

wiz stick adminAgent safely protects all TSF data sent to and received from wiz stick Portable by using a cryptographic (AES (256 bit, CBC mode) algorithm. To this end, cryptographic key is generated by using variable information created whenever wiz stick Device is connected, as well as hash value of wiz stick Device's unique information. Here, SHA-256 algorithm that complies with FIPS 180-4(Secure Hash Standard) is used. In addition, it carries out cryptographic operation and cryptographic key destruction in a safe manner according to the method specified in FIPS PUB 197(Advanced Encryption Standard).

Audit Log View

wiz stick adminAgent provides an administrator with a function to read and view the following system-related audit records from the wiz stick Portable: audit records on VPN connection phase; security management including product information view; and start-up and shut-down of the audit function.

VPN Policy Settings

wiz stick adminAgent provides an administrator with the function for VPN client settings, which allows for building of VPN with IPsec VPN gateway. An administrator is capable of make settings for the partner's VPN server IP address in the form of IPsec VPN, pre-shared key, password for VPN access authentication, and so forth. VPN client information set by an administrator is applied to wiz stick Portable.

non-TSF

- **Wired/Wireless Network Settings:** It is a function that suspends PC's wired and wireless network adaptor to make it unavailable except for the connection between wiz stick Device and the PC, and enables an administrator to perform wired/wireless network settings for wiz stick Device IP address, subnet mask, etc. Although the function is not TOE security function implemented to satisfy SFR of the TOE, it is classified as non-TSF because it cannot be physically separated from TOE components but includes source codes compiled/built together.

❍ wiz stick userAgent

wiz stick userAgent provides PC users with the function of environment settings and view to ensure that wiz stick Portable within wiz stick Device connected to user PC provides accurate security functions and that secure internet access is provided.

Audit Log View

wiz stick userAgent provides PC users with a function to read and view the following system-related audit records from wiz stick Portable: results of the detection of access to harmful or pharming sites; security management activities such as audit records on VPN connection phase and product information view; and start-up and shut-down of the audit function.

Product Info Check

wiz stick userAgent provides product information such as the TOE and TOE component version for PC users.

Protection of Transmitted Data

wiz stick userAgent safely protects all TSF data sent to and received from wiz stick Portable by using a cryptographic (AES (256 bit, CBC mode) algorithm. To this end, cryptographic key is generated by using variable information created whenever wiz stick Device is connected, as well as hash value of wiz stick Device's unique information. Here, SHA-256 algorithm that complies with FIPS 180-4(Secure Hash Standard) is used. In addition, it carries out cryptographic operation and cryptographic key destruction in a safe manner according to the method specified in FIPS PUB 197(Advanced Encryption Standard).

Operation/Connection Status Check

wiz stick userAgent provides PC users with the function to check and view service-wise connection phases such as physical connection with wiz stick Device and safe internet access.

It provides the function of approval of a higher-level approver, certificate use

non-TSF

- **Function of Certificate Use Control:** It is a function to control a higher-level approver, certificate use tracking and loss management that are necessary to use the certificate inside the wiz stick Device in linkage with an external "Certificate Control Server." Although the function is not TOE security function implemented to satisfy SFR of the TOE, it is classified as non-TSF because it cannot be physically separated from TOE components but includes source codes compiled/built together.
- **Request to Register/Recognize Fingerprint:** It is a function that registers user fingerprint for the purpose of certificate use control and PKCS#11-based certificate management and use, and outputs a screen that guides a user to enter user fingerprint when using a certificate. Although the function is not TOE security function implemented to satisfy SFR of the TOE, it is classified as non-TSF because it cannot be physically separated from TOE components but includes source codes compiled/built together.
- **Wired/Wireless Network Settings:** It is a function that suspends the wired and wireless network adaptor to make it unavailable except for the connection with wiz stick Device once it is

connected with a user PC, and enables a user to perform wired/wireless network settings for wiz stick Device IP address, subnet mask, etc. Although the function is not TOE security function implemented to satisfy SFR of the TOE, it is classified as non-TSF because it cannot be physically separated from TOE components but includes source codes compiled/built together.

❍ wiz stick Portable

wiz stick Portable offers the function of "detection and blocking of access to harmful sites" and the function of "detection and blocking of access to pharming sites" by analyzing traffic transmitted between a user PC connected with wiz stick Device and an external network. In addition, it also provides users with the function of "IPsec VPN client" to create a secure VPN with an external IPsec VPN gateway.

IPsec VPN Client

When a PC user physically clicks on the "VPN Access Button" in wiz stick Device, wiz stick Portable goes through password-based VPN access user authentication and creates a secure VPN with an external IPsec VPN gateway by using pre-defined VPN settings.

wiz stick Portable uses FIPS PUB 197 standard-based AES algorithm as encryption algorithm for Phase 1/2 according to IKE standard, and uses FIPS 180-4 (Secure Hash Standard)-based SHA as integrity-protection (authentication) algorithm in order to provide the VPN client function.

Audit Log Generation Storage & Transmission

wiz stick Portable generates results of harmful or pharming access detection, VPN connection phase and security-related events sent from wiz stick adminAgent or wiz stick userAgent as audit records and store them. In case the number of stored audit data exceeds 999, wiz stick Portable deletes the 300 oldest audit data to secure the capacity for audit trail without any data loss.

Detection and Blocking of Access to Harmful Sites

wiz stick Portable detects a user PC's access to a harmful site based on packet's URL information by using Snort. wiz stick Portable blocks access to a harmful site by setting IP address, protocol and port information of the detected harmful site as ACL referenced by iptables. The rule used for detection and blocking of access to harmful sites is updated on a regular basis by the Update Server operated by the developer, KT Corp, so that it maintains the up-to-date security status.

Detection and Blocking of Access to Pharming Sites

wiz stick Portable forwards DNS query packet (TCP/UDP 53 port) generated from a user PC to the Secure DNS server operated by KT Corp. to receive normal DNS information, and then use Snort to carry out comparison to check if URL and IP of the site that the user tries to access match accurate URL and IP information of banking sites and portal sites that have been damaged by pharming in the past. wiz stick Portable sets IP address, protocol and port information of the detected pharming site as the policy referenced by iptables, thereby redirecting access to a pharming site towards a normal site to block the user's access to the pharming site. The rule used for detection and blocking of access to pharming sites is updated on a regular basis by the Update Server operated by the developer, KT Corp, so that it maintains the up-to-date security status.

Protection of Stored/Transmitted Data

wiz stick Portable safely protects all TSF data sent to and received from wiz stick Agent or wiz stick userAgent through encryption.

wiz stick Portable performs encryption by using IETF RFC 3447-based RSA and FIPS PUB 197-based AES algorithm in order to protect data transmitted to and from an external update server.

wiz stick Portable encrypts important TSF data such as VPN policy or pattern information by using FIPS PUB 197-based AES algorithm and then store them securely.

wiz stick Portable performs encryption to safely protect all TSF data sent to and received from wiz stick adminAgent or wiz stick userAgent by using AES (256 bit, CBC mode) algorithm. To this end, cryptographic key is generated by using variable information created whenever wiz stick Device is connected, as well as hash value of wiz stick Device's unique information. Here, SHA-256 algorithm that complies with FIPS 180-4(Secure Hash Standard) is used. In addition, it carries out cryptographic operation and cryptographic key destruction in a safe manner according to the method specified in FIPS PUB 197(Advanced Encryption Standard).

non-TSF

- **PKCS#11-based Certificate Management & Use:** It provides the function of PKCS#11 standard—based security token(HSM) to encrypt and store the certificate in the security token(HSM) storage of wiz stick Device. Although the function is not TOE security function implemented to satisfy SFR of the TOE, it is classified as non-TSF because it cannot be physically separated from TOE components but includes source codes compiled/built together.
- **Fingerprint Registration/Recognition:** It provides the function to store core information (statistical value) of a user's fingerprint from the fingerprint sensor (IDX1120) as the user's unique identification information. Then, if the user enters the fingerprint to use a certificate, the function compares it against the user's previously-stored fingerprint to check if they match. Although the function is not TOE security function implemented to satisfy SFR of the TOE, it is classified as non-TSF because it cannot be physically separated from TOE components but includes source codes compiled/built together.

5. Terms and Definitions

ACL (Access Control List)

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 (Command & Control) 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 (Domain Name System)

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 (Remote Network Driver Interface Specification)

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 (Virtual Private Network)

VPN is a private network across a public network that enables users to communicate securely, not being exposed to others outside the network. VPN sends and receives messages by using the standard protocol on a public network such as the internet.

IPsec (Internet Protocol Security)

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 to harmful sites, 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.

6. Conventions

This ST uses English, as well as Korean, for some abbreviations and to deliver clearer meanings. The orthography, formats and conventions herein comply with the Common Criteria. Furthermore, this ST defines additional conventions in order to prevent any confusion with operations already performed in the protection profile with which this ST complies.

The Common Criteria allows for selection, assignment, refinement and iteration operations to be performed on Security Functional Requirements.

Each operation is used in this ST as described below:

Iteration
Iteration is used when the same component is repeated for multiple operations. The result of the iteration operation is indicated by the iteration number within parentheses, that is, (iteration number), following the component identifier.

Selection
Selection is used to select one or more options provided by the Common Criteria for the Information Technology Security Evaluation when describing requirements. The result of the selection operation is indicated in underlined italicized characters.

Refinement
Refinement is used to further restrict requirements by adding details to the requirements. The result of the refinement operation is indicated in bold characters.

Assignment
Assignment is used to allocate a specific value to an unspecified parameter (e.g. length of password). The result of the assignment is indicated by square brackets, that is, [Assignment_Value].

.

II. Conformance Claims

1. Conformance Claims for Common Criteria, Protection Profile and Security Requirement Package

Table 8. Conformance Claims for Common Criteria, Protection Profile and Security Requirement Package

Category	Conformance
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4 (CCMB-2012-09-001, Sep, 2012), Korean Ver. • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4 (CCMB-2012-09-002, Sep, 2012), Korean Ver. • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4 (CCMB-2012-09-003, Sep, 2012), Korean Ver.
Common Criteria Part 2	Extended : FCS_IPSEC.1, FCS_RBG.1
Common Criteria Part 3	Conformant
Protection Profile	N/A
Assurance Package	Conformance with EAL1

2. Conformance Rationale

This ST does not have a protection profile to comply with.

III. Security Objectives

1. Security Objectives for the Operational Environment

The following is the Security Objective to be addressed based on technical/procedural means supported by the operational environment so that the TOE can provide the security functionality.

Table 9. Security Objectives for the Operational Environment

Label	Security Objectives for the Operational Environment
OE.Single Point of Connection	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.
OE.Trusted NTP Server	The TOE shall be provided with timestamps from an external trusted NTP server in order to accurately record security-related events.
OE.Application of Security Policy through External Server	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.
OE.adminAgent Management	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.
OE.Trusted Admin	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.
OE.VPN Security Policy Initial Value Settings	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.
OE.Physical Security	The TOE is directly delivered to a designated person in an organization (administrator or PC user) by the developer KT Corp. 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. Hence, the safety against

Label	Security Objectives for the Operational Environment
	unauthorised deletion and modification of TSF data shall be ensured.
OE.Operating System Reinforcement	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.
OE.Secure VPN Gateway Settings	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).

IV. Extended Components Definition

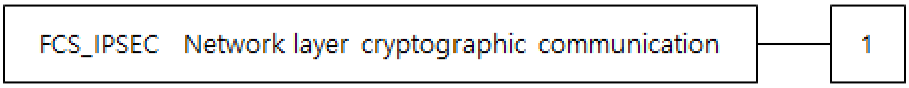
1. FCS, Cryptographic Support

1.1. Network layer cryptographic communication

Family Behaviour

Network layer cryptographic communication(FCS_IPsec, Internet Protocol Security) family shall be defined to require IPsec VPN related functions.
This family defines requirement for TSF to provide the capability for IPsec VPN.

Component leveling



FCS_IPSEC.1 Network layer cryptographic communication requires that the TSF provides the IPsec VPN.

Management: FCS_IPSEC.1
The following actions could be considered for the management functions in FMT:
a) IPsec VPN operation mode(transmission mode, tunnel mode) management
b) Cryptographic algorithm management for IPsec VPN cryptographic communication

Audit: FCS_IPSEC.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimum: IPsec VPN policy's all modifications (modification of cryptographic algorithm modification of operation mode, etc.)
b) Minimum: Success/failure of IPsec VPN mechanism (success/failure of key exchange, authentication, and cryptographic communication, etc.)

1.1.1. FCS_IPSEC.1 Network layer cryptographic communication

FCS_IPSEC.1 Network layer cryptographic communication

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.2 Cryptographic key distribution
FCS_COP.1 Cryptographic operation

FCS_IPSEC.1.1 The TSF shall implement the specified IPsec protocol that meets the following the [assignment: list of standards].

FCS_IPSEC.1.2 The TSF shall support [selection: tunnel mode, transport mode].

FCS_IPSEC.1.3. The TSF shall support IPsec ESP, [selection: *AH, None*].

FCS_IPSEC.1.4 The TSF shall support [selection: *IKEv1, IKEv2*] key exchange protocol.

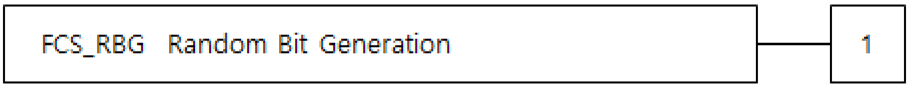
FCS_IPSEC.1.5 The TSF shall support mutual authentication using [selection: *X.509v3 certificates, Pre-shared Keys*, [assignment: *other mutual authentication method*]].

1.2. Random bit generation

Family Behaviour

This family defines requirements for the TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Component leveling



FCS_RBG.1 Random bit generation requires TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Management: FCS_RBG.1
There are no management activities foreseen.

Audit: FCS_RBG.1
There are no auditable events foreseen.

1.2.1. FCS_RBG.1 Random bit generation

FCS_RBG.1 Random bit generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG.1.1 The TSF shall generate random bits necessary for encryption key generation and cryptographic operation by using the specified random bit generator that satisfies the following [assignment: list of standards].

V. Security Requirements

This chapter describes the functions and assurance requirements that need to be satisfied by the TOE.

1. Security Functional Requirements (SFRs)

Security functional components used in the ST are described as below:

Table 10. Security Functional Components

Security Functional Class	Security Functional Components	
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_STG.3	Action in case of possible audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_IPSEC.1	Network layer cryptographic communication
	FCS_RBG.1	Random bit generation
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFC.2(1)	Complete information flow control (1)
	FDP_IFC.2(2)	Complete information flow control (2)
	FDP_IFF.1(1)	Simple security attributes (1)
	FDP_IFF.1(2)	Simple security attributes (2)
	FDP_IFF.1(3)	Simple security attributes (3)
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
Security Management	FMT_SMF.1	Specification of management functions
TSF Protection	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps

1.1. Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit function;

b) All auditable events for the *not specified* level of audit; and

c) [Specifically defined auditable events listed in Table 11]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identify (if applicable) and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [additional audit-related information specified in Table 11]

Table 11. Auditable Events and Additional Audit-related Information

Security Functional Component	Auditable Events	Additional Audit-related Information
FAU_SAR.1	Reading of information from the audit records	
FAU_STG.3	Actions to be taken if a threshold on the audit trail is exceeded	
FCS_IPSEC.1	IPsec VPN policy's all modifications (modification of cryptographic algorithm, modification and operation mode, etc.)	
	Success/failure of IPsec VPN mechanism (success/failure of key exchange, authentication, and cryptographic communication, etc.)	
FDP_IFF.1(1)	Detection of access to harmful sites	Detailed detection information (detection direction, detected IP address)
FDP_IFF.1(2)	Detection of access to pharming sites	Detailed detection information (URL, detected IP address, redirected IP address)

Security Functional Component	Auditable Events	Additional Audit-related Information
FDP_IFF.1(3)	All decisions on requests for VPN information flow	
FIA_SOS.1	Rejection by the TSF of any tested secrets	
FIA_UAU.1	Unsuccessful use of the authentication mechanism	
FMT_SMF.1	Use of the management functions	Modified TSF data value

FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [authorised users specified in Table 12] with the capability to read [list of audit information specified in Table 12] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Table 12. List of Audit Information That Individual Authorised Users are allowed to View

Authorised User	Audit Information List	Auditable Event
Administrator	VPN	- IPSec VPN policy's all modifications (modification of cryptographic algorithm modification and operation mode, etc.) - Success/failure of IPSec VPN mechanism (success/failure of key exchange, authentication, and cryptographic communication, etc.) - Rejection by the TSF of any tested secret - All decisions on requests for VPN information flow (success/failure of IPsec VPN mechanism (key exchange, authentication, cryptographic communication)) - Unsuccessful use of authentication mechanism
	Security Management Activity	- Reading of information from the audit records - Use of management functions
	System	- Start-up and shut-down of the audit function - Actions taken due to exceeding of a threshold.
PC User	VPN	- All decisions on requests for VPN information flow

Authorised User	Audit Information List	Auditable Event
		(success/failure of IPsec VPN mechanism (key exchange, authentication, cryptographic communication)) - Unsuccessful use of authentication mechanism
	Security Management Activity	- Reading of information from the audit records - Use of management functions
	System	- Start-up and shut-down of the audit function - Actions taken due to exceeding of a threshold.
	Detection of access to harmful sites	- Detection of access to harmful sites (FDP_IFF.1(1))
	Detection of access to pharming sites	- Detection of access to pharming sites (FDP_IFF.1(2))

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [delete the 300 oldest audit records] if the audit trail exceeds [999 audit records].

1.2. Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key size [cryptographic key size in Table 13] that meet the following: [None]

Application Note: This Security Functional Requirement is required for cryptographic key generation under the following situation.

Table 13. List of Cryptographic Key Generation

Use Condition (Circumstance)		Cryptographic Algorithm	Encryption Key Size
Decryption of transmitted data that wiz stick Portable receives from an external update server		AES	128 bits
Encryption/Decryption of data transmitted between wiz stick Agent and wiz stick Portable		AES	256 bits
Encryption/Decryption of data stored in wiz stick Portable		AES	128 bits
VPN communication of wiz stick Portable with an external IPsec VPN gateway	Phase1	AES	128 bits 192 bits 256 bits
	Phase2	AES	128 bits 192 bits 256 bits

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [IKE] that meets the following: [IETF RFC 2409].

Application Note: This Security Functional Requirement is required for cryptographic key distribution for the purpose of VPN communication between wiz stick Portable and an external IPsec VPN gateway.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization of all cryptographic keys] that meets the following: [None].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Cryptographic operation according to the use condition specified in Table 14] in accordance with a specified cryptographic algorithm [Cryptographic operation algorithm specified in Table 14] and cryptographic key size [cryptographic key size specified in Table 14] that meet the following: [list of standards in Table 14].

Application Note: This Security Functional Requirement is required for cryptographic key operation under the following conditions.

Table 14. List of Cryptographic Operation Standards

Use Condition (Circumstance)	List of Standards	Cryptographic Operation Algorithm	Cryptographic Key Size
Encryption of data transmitted by wiz stick Portable to an external update server (Encryption only)	IETF RFC 3447 – Public-Key Cryptography Standards(PKCS) #1 : RSA Cryptography Specifications	RSAES-OAEP	2048 bits
Assurance of integrity of data transmitted by wiz stick Portable to an external update server	FIPS 180-4 Secure Hash Standard(SHS)	SHA2	256 bits
Decryption of data received by wiz stick Portal from an external update server	FIPS PUB 197, Advanced Encryption Standard(AES)	AES (CBC mode)	128 bits
Verification of integrity of data wiz stick Portable received from an external update server	FIPS 180-4 Secure Hash Standard(SHS)	SHA2	256 bits
Encryption/decryption of data exchanged between wiz stick	FIPS PUB 197, Advanced Encryption Standard(AES)	AES (CBC mode)	256 bits

Use Condition (Circumstance)		List of Standards	Cryptographic Operation Algorithm	Cryptographic Key Size
Agent and wiz stick Portable				
Encryption/decryption of data stored in wiz stick Portable		FIPS PUB 197, Advanced Encryption Standard(AES)	AES (CBC mode)	128 bits
VPN communication between wiz stick Portable and an external IPsec VPN gateway	Phase1	FIPS PUB 197, Advanced Encryption Standard(AES)	AES (CBC mode)	128 bits 192 bits 256 bits
		FIPS 180-4 Secure Hash Standard(SHS)	SHA2	256 bits 384 bits 512 bits
		IETF RFC 3526 – More Modular Exponential(MODP) Diffie-Hellman groups for Internet Key Exchange	DH group 14	2048/256 bits
	Phase2	FIPS PUB 197, Advanced Encryption Standard(AES)	AES (CBC mode)	128 bits 192 bits 256 bits
		IETF RFC 4868 - Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	HMAC	256 bits 384 bits 512 bits
		FIPS 180-3 Secure Hash Standard(SHS)	SHA2	256 bits 384 bits 512 bits
		IETF RFC 3526 – More Modular Exponential(MODP) Diffie-Hellman groups for Internet Key Exchange	DH group 14	2048/256 bits

FCS_IPSEC.1 Network layer cryptographic communication

Hierarchical to:	No other components
Dependencies:	FCS_CKM.1 Cryptographic key generation FCS_CKM.2 Cryptographic key distribution FCS_COP.1 Cryptographic operation

FCS_IPSEC.1.1 The TSF shall implement the specified IPsec protocol that meets the following the

[IETF RFC 4301].

FCS_IPSEC.1.2 The TSF shall support *tunnel mode*.

FCS_IPSEC.1.3 The TSF shall support IPsec ESP, *None.*

FCS_IPSEC.1.4 The TSF shall support *IKEv1, IKEv2* key exchange protocol.

FCS_IPSEC.1.5 The TSF shall support mutual authentication using *Pre-shared Keys*.

FCS_RBG.1 Random bit generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG.1.1 The TSF shall generate random bits necessary for encryption key generation and cryptographic operation by using the specified random bit generator that satisfies the following [NIST SP 800-90].

1.3. User Data Protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [VPN SFP] on [the following list]:

a) Subject:
  - External IT entities that send and receive information through the TOE

b) Information: data transmitted through the TOE

c) Operation:
  - Sending and receving of information through the TOE

FDP_IFC.2(1) Complete information flow control (1)

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [SFP for detection and blocking of access to harmful sites] on [the following list] and all operations that cause that information to flow to and from subjects covered by the SFP.

a) Subject: IT entities that send and receive information through the TOE

b) Information: Traffic that passes through the TOE

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by **SFP for detection and blocking of access to harmful sites.**

FDP_IFC.2(2) Complete information flow control (2)

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [SFP for detection and blocking of access to pharming sites] on [the following list] and all operations that cause that information to flow to and from subjects covered by the SFP.

a) Subject: IT entities that send and receive information through the TOE

b) Information: Traffic that passes through the TOE

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by **SFP for detection and blocking of access to pharming sites.**

FDP_IFF.1(1) Simple security attributes (1)

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static Attribute Initialisation

FDP_IFF.1.1 The TSF shall enforce the [SFP for detection and blocking of access to harmful sites] based on the following types of subject and information security attributes: [list of subjects and information controlled under the indicated SFP for detection and blocking of access to harmful sites, and for each, the security attributes].

a) Subject (external IT entity) security attributes:
   - N/A

b) Information (traffic) security attributes:
   - Source IP address
   - Destination IP address
   - Service (protocol, port)
   - Packet data (header, payload)

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [an information flow requested by the subject shall be permitted if the comparison between the information security attributes that go through the TOE (header, payload) against the list of harmful sites (URL, IP) owned by the TOE concludes that the information security attributes do not match.]

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [None].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [a situation where source/destination IP address and port information among security attributes of information that goes through the TOE match the list of access blocking owned by the TOE].

FDP_IFF.1(2) Simple security attributes (2)

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [SFP for detection and blocking of access to pharming sites] based on the following types of subject and information security attributes: [list of subjects and information controlled under the indicated SFP for detection and blocking of access to pharming sites, and for each, the security attributes].

a) Subject (external IT entity) security attributes:
   - N/A

b) Information (traffic) security attributes:
   - Source IP address
   - Destination IP address
   - Service (protocol, port)
   - Packet data (header, payload)

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) An information flow is permitted if, among security attributes of information that goes through the TOE (header, payload), information such as host name and IP address matches normal site URL and IP matching information owned by the TOE.

b) If, among security attributes of information that goes through the TOE (header, payload), information such as host name and IP address does not match normal site URL and IP matching information owned by the TOE, an information flow is permitted after modifying host name among security attributes (header, payload) to a normal site URL.

c) An information flow is permitted if, among security attributes of information that goes through the TOE (header, payload), information such as host name does not match normal site URL owned by the TOE.]

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [a rule that if a destination port of information (packet) imported to a user PC is DNS query packet with TCP/UDP 53, the packet is forwarded to the Secure DNS operated by the developer KT Corp].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [None].

FDP_IFF.1(3) Simple security attributes (3)

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [VPN SFP] based on the following types of subject and information security attributes: [the following subject and information security attributes]:

a) Subject (external IT entity) security attributes:
   - IP address of an external IT entity (external IPsec VPN gateway) that send and receive information through the TOE
b) Information security attributes:
   - Source and destination IP address from/to which information data packet is transmitted
   - Header information to process IPsec protocol (ESP header)

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) Communication with communication partner: For traffic that arrives from the communication partner and traffic that leaves to the communication partner, in accordance with the security policy, the TOE shall:
   - Create a security channel for communication with the partner or use an existing security channel.
   - Not call a security mechanism for communication with the partner nor form a security channel.
b) Communication with non-communication partner: For traffic that arrives from non-partner and traffic that leaves to non-partner, the TOE shall not call a security mechanism nor form a security channel.]

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [None].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

[packet without header information to process IPsec protocol].

1.4. Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **VPN access user**: [VPN access authorisation]

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that the **VPN access password** meets [Table 15].

Table 15. Quality Metric for Acceptable Password

Category	Quality Metric	
Allowable Characters	English Capital/Small Letter	A-Z, a-z
	Number	0-9
	Special Character	!@#$%^&*()_-+=
Combination Rule	Min/Max Length	9-16 digits
	Password shall be a combination of all the allowable characters (English capital/small letters, numbers and special characters).	

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [all TSF-mediated actions other than VPN SFP] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

1.5. Security Management

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [List of security management functions in Table 16].

Table 16. List of Security Management Functions

TOE Component	Category	Management Function
wiz stick adminAgent	Security function management	Stop/start VPN
	Security attribute management	Inquire, modify, delete VPN SFP security attribute
	TSF data management	Check wiz stick product information
wiz stick userAgent	Security function management	Stop/start VPN
	TSF data management	Check wiz stick product information, check safe internet access service operation status, check wiz stick connection

1.6. Protection of the TSF

FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to **the update server** from unauthorised disclosure during transmission.

FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and **the update server** within the following metric: [None].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and **the update server** and perform [destruction of data for which the integrity was compromised] if modifications are detected.

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

2. TOE Security Assurance Requirements

The assurance requirements of this ST are composed of the assurance components of the CC, Part 3 of, the assurance level being EAL1. The table below shows a summary of assurance components:

Table 17. Assurance class/component

Assurance class	Assurance components	
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

2.1. Security Target Evaluation

ASE_INT.1 ST introduction

Dependencies : No dependencies

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies : ASE_INT.1 ST introduction
ASE_ECD1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies : No dependencies

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements

ASE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies : No dependencies

Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies : ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements

ASE_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies : ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

2.2. Development

ADV_FSP.1 Basic functional specification

Dependencies : No dependencies

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

2.3. Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies : ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies : No dependencies.

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

2.4. Life-cycle Support

ALC_CMC.1 Labeling of the TOE

Dependencies : ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies : No dependencies

Developer action elements

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2.5. Tests

ATE_IND.1 Independent testing - conformance

Dependencies : ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements

ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

2.6. Vulnerability Assessment

AVA_VAN.1 Vulnerability survey

Dependencies : ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

3. Dependency Rationale

3.1. Dependency Rationale of Security Functional Requirements

Dependency rationale of security functional components described in this ST is as follows:

Table 18. Functional Component Dependency

No.	Functional Component	Dependency	Ref. No.
1	FAU_GEN.1	FPT_STM.1	23
2	FAU_SAR.1	FAU_GEN.1	1
3	FAU_STG.3	FAU_STG.1	*
4	FCS_CKM.1	FCS_COP.1	7
		FCS_CKM.4	6
5	FCS_CKM.2	FCS_CKM.1	4
		FCS_CKM.4	6
6	FCS_CKM.4	FCS_CKM.1	4
7	FCS_COP.1	FCS_CKM.1	4
		FCS_CKM.4	6
8	FCS_IPSEC.1	FCS_CKM.1	4
		FCS_CKM.2	5
		FCS_COP.1	7
9	FCS_RBG.1	No dependencies	-
10	FDP_IFC.1	FDP_IFF.1(3)	15
11	FDP_IFC.2(1)	FDP_IFF.1(1)	13
12	FDP_IFC.2(2)	FDP_IFF.1(2)	14
13	FDP_IFF.1(1)	FDP_IFC.1	11**
		FMT_MSA.3	***
14	FDP_IFF.1(2)	FDP_IFC.1	12***
		FMT_MSA.3	*****
15	FDP_IFF.1(3)	FDP_IFC.1	10
		FMT_MSA.3	******
16	FIA_ATD.1	No dependencies	-
17	FIA_SOS.1	No dependencies	-
18	FIA_UAU.1	FIA_UID.1	*******
19	FMT_SMF.1	No dependencies	-
20	FPT_ITC.1	No dependencies	-
21	FPT_ITI.1	No dependencies	-

No.	Functional Component	Dependency	Ref. No.
22	FPT_ITT.1	No dependencies	-
23	FPT_STM.1	No dependencies	-

* FAU_STG.3 is dependent on FAU_STG.1. However, Wiz Stick Device where Wiz Stick Portable is installed shall be kept and managed safely in accordance with the security objective "OE.Physical Security" for the TOE operational environment, which ensures unauthorised deletion and modification of TSF data including audit data are assured, and satisfies the dependency of FAU_STG.3.

** FDP_IFF.1(1) is dependent on FDP_IFC.1. However, "SFP for detection and blocking of access to harmful sites" was defined by FDP_IFC.2(1) that is hierarchical to FDP_IFC.1, and thus the dependency of FDP_IFF.1(1) is satisfied.

*** FDP_IFF.1(1) is dependent on FMT_MSA.3. However, the TSF downloads security policy from an external update server managed and operated by the developer KT Corp. and initialises default value of SFP for detection and blocking of access to harmful sites. Thus, there is no authorised role that restricts the capability of operation on security attributes of SFP for detection and blocking of access to harmful sites. Therefore, the dependency of FDP_IFF.1(1) is satisfied based on the security objective for the operational environment, "OE.Application of Security Policy through an External Server."

**** FDP_IFF.1(2) is dependent on FDP_IFC.1. However, "SFP for detection and blocking of access to pharming sites" was defined by FDP_IFC.2(2) that is hierarchical to FDP_IFC.1, and thus the dependency of FDP_IFF.1(2) is satisfied.

***** FDP_IFF.1(2) is dependent on FMT_MSA.3. However, the TSF downloads security policy from an external update server managed and operated by the developer KT Corp. and initialises default value of SFP for detection and blocking of access to pharming sites. Thus, there is no authorised role that restricts the capability of operation on security attributes of SFP for detection and blocking of access to pharming sites. Therefore, the dependency of FDP_IFF.1(2) is satisfied based on the security objective for the operational environment, "OE.Application of Security Policy through an External Server."

****** FDP_IFF.1(3) is dependent on FMT_MSA.3. However, it initializes default value of VPN SFP in accordance with the administrator guideline such as "OE.VPN Security Policy Initial Value Setting," and thus the dependency of FDP_IFF.1(3) is satisfied.

******* FIA_UAU.1 is dependent on FIA_UID.1. Since only actual users can use Wiz Stick Device in accordance with the security objective of the operational environment “OE.Physical Security,” VPN access request is available only for authorised administrators or PC users based on an organization’s policy. The detailed procedure to meet the security objective of the operational environment is described in the TOE installation and operation guidance. Therefore, the dependency of the authentication requirements of VPN access users through password (FIA_UAU.1) is satisfied based on “AGD_PRE.1.”

3.2. Dependency Rationale of Assurance Requirements

As the dependency of EAL1-grade assurance package provided by the Common Criteria was already satisfied, this document does not provide the rationale in this regard.

4. Rationale for Mutual Complementarity and Internal Consistency

This rationale demonstrates that a series of security requirements are mutually complementary and constructed with internal consistency.

"V.3.1Dependency of Security Functional Requirements" and "V.3.2 Dependency of Security Assurance Requirements" "address back-up relationships among security requirements. This section analyzes dependencies where one security requirement is not sufficient to meet a certain security objective and thus needs to depend on another security requirement. When the dependency was not satisfied, additional rationale was provided.

VI. TOE Summary Specification

This chapter describes how the TOE meets each security functional requirement.

1. TOE Security Functions

This section presents SFRs related to the security functions of the TSF and the SFR.

The TOE performs the following security functions:

- Security audit
- Cryptographic support
- Detection and blocking of access to harmful sites
- Detection and blocking of access to pharming sites
- IPsec VPN client
- VPN access user authentication
- Security management
- TSF protection

2. Security Audit

If the following event occurs, Wiz Stick adminAgent processes it in a predefined message format and delivers it to Wiz Stick Portable.

- *Related SFR : FAU_GEN.1*

Table 19. Events That Occur in Wiz Stick adminAgent

No.	Event Description
(1)	Click '(Menu)Wiz Stick product information'
(2)	Click '(Menu)Audit record view'
(3)	Fail in VPN connection because a wrong VPN connection password was entered
(4)	Succeed when clicking the [Settings] button in '(Menu)VPN> VPN Connection Settings'
(5)	Fail when clicking the [Settings] button in '(Menu)VPN> VPN Connection Settings'
(6)	Execute Wiz Stick adminAgent
(7)	Terminate Wiz Stick adminAgent

If the following event occurs, Wiz Stick userAgent processes it in a predefined message format and delivers it to Wiz Stick Portable.

- *Related SFR : FAU_GEN.1*

Table 20. Events That Occur in Wiz Stick userAgent

No.	Event Description
(8)	Click '(Menu)Wiz Stick product information'
(9)	Click '(Menu)Audit record view'
(10)	Click '(Menu)Secure internet connection > Risk detection/blocking event check'
(11)	Click '(Menu)Secure internet connection > Status of secure internet connection service'
(12)	Fail in VPN connection because a wrong VPN connection password was entered
(13)	Click '(Menu)Check Wiz Stick connection'
(14)	Execute Wiz Stick adminAgent
(15)	Terminate Wiz Stick adminAgent

Wiz Stick Portable generates event information transmitted from adminAgent or Wiz Stick userAgent as well as internally created event information as audit data and stores them. Time stamps referenced for audit data generation refer to time value synchronized with an external NTP server when Wiz Stick Portable runs.

- *Related SFR : FAU_GEN.1, FPT_STM.1*

Table 21. List of Audit Data Generated and Stored in Wiz Stick Portable

Audit Data Type	Auditable Event	Occurring Event
VPN	Any change in IPsec VPN policy (modification of password algorithm, modification of operation mode, etc.)	(4)
	Any decision on requests for VPN information flow (Success/failure of IPsec VPN mechanism ((key exchange, authentication, cryptographic communication))	VPN connection start/termination, phase during VPN connection, success/failure of VPN connection
	Rejection by the TSF of any tested secrets	(5)
	Unsuccessful use of the authentication mechanism	(3)(12)
Security Management Activity	Reading of Audit record information	(2)(9)(10)
	Use of management functions, modified TSF data value	(1)(8)(11)(13)

Audit Data Type	Auditable Event	Occurring Event
System	Start and termination of audit function	(6)(7)(14)(15)
	Actions to be taken if a threshold on the audit trail is exceeded	If a threshold on the audit trail is exceeded, the 300 oldest audit data are deleted
Result of Detection and Blocking of Access to Harmful Sites	Detailed information on detection of access to harmful sites (detection direction, detected IP address) (FDP_IFF.1(1))	Detection of access to harmful sites
Result of Detection and Blocking of Access to Pharming Sites	Detailed information on detection of access to pharming sites (URL, detected IP address, redirected IP address) (FDP_IFF.1(2))	Detection of access to pharming sites

If an administrator clicks '(Menu) Audit record view,' Wiz Stick adminAgent reads and outputs the following audit data stored in Wiz Stick Portable.

- *Related SFR : FAU_SAR.1*

Table 22. List of Audit Data That Can Be Displayed in Wiz Stick adminAgent

Audit Data Type	Phase Definition	Description Format
VPN	VPN Connection Started	-
	VPN Negotiation	Initiate Negotiation
		Phase1 Negotiation Complete - ISAKMP SA Established
	VPN Connection Succeeded	Phase2 Negotiation Complete - IPsec SA Established
	VPN Connection Failed	Enter Wrong VPN Connection Password
		[Type_of_ErrorMsg]
	VPN Connection Terminated	Delete Connection
	VPN Policy Settings	*[VPN policy settings]*
		Entry of VPN connection password that does not comply with a combination rule

Audit Data Type	Phase Definition	Description Format
Security Management Activity	Product Information View	-
	Audit Record View	-
System	Audit Function	Audit function start
		Audit function termination
	Threshold of Audit Storage Exceeded	Audit data are overwritten as audit trail exceeded the threshold capacity.

Table 23. 'Type of ErrorMsg'

INVALID-PAYLOAD-TYPE
DOI-NOT-SUPPORTED
SITUATION-NOT-SUPPORTED
INVALID-COOKIE
INVALID-MAJOR-VERSION
INVALID-MINOR-VERSION
INVALID-EXCHANGE-TYPE
INVALID-FLAGS
INVALID-MESSAGE-ID
INVALID-PROTOCOL-ID
INVALID-SPI
INVALID-TRANSFORM-ID
ATTRIBUTES-NOT-SUPPORTED
NO-PROPOSAL-CHOSEN
BAD-PROPOSAL-SYNTAX
PAYLOAD-MALFORMED
INVALID-KEY-INFORMATION
INVALID-ID-INFORMATION
INVALID-CERT-ENCODING
UNKNOWN-ERROR
INVALID-CERTIFICATE
CERT-TYPE-UNSUPPORTED
INVALID-CERT-AUTHORITY
INVALID-HASH-INFORMATION
AUTHENTICATION-FAILED
INVALID-SIGNATURE
ADDRESS-NOTIFICATION
NOTIFY-SA-LIFETIME
CERTIFICATE-UNAVAILABLE
UNSUPPORTED-EXCHANGE-TYPE
UNEQUAL-PAYLOAD-LENGTHS
SERVER-TIMEOUT
XAUTH-FAIL
EMPTY-CONFIG
CANNOT-IDENTIFY-OURSELVES
DELETE_SA_PAYLOAD
Reserved#2
Reserved#3
Reserved#4

If a PC user clicks '(Menu) Audit record view,' Wiz Stick userAgent reads and displays the following audit data stored in Wiz Stick Portable.

- *Related SFR : FAU_SAR.1*

Table 24. List of Audit Data That Can Be Output in Wiz Stick userAgent -1

Audit Data Type	Phase Definition	Description Format
VPN	VPN Connection Started	-
	VPN Negotiation	Initiate Negotiation Phase1 Negotiation Complete - ISAKMP SA Established
	VPN Connection Succeeded	Phase2 Negotiation Complete - IPsec SA Established
	VPN Connection Failed	Enter Wrong VPN Connection Password *[Type_of_ErrorMsg]*
	VPN Connection Terminated	Delete Connection
Security Management Activity	Product Information View	-
	Audit Record View	-
	Risk Detection/Blocking Event Check	-
	Phase Check	Check of secure internet connection service status Wiz stick connection check
System	Audit Function	Audit function start Audit function termination
	Threshold of Audit Storage Exceeded	Audit data are overwritten as audit trail exceeded the threshold capacity

If a PC user clicks '(Menu) Secure internet connection > Risk detection/blocking event check,' Wiz Stick userAgent reads and displays the following audit data stored in Wiz Stick Portable.

- *Related SFR : FAU_SAR.1*

Table 25. List of Audit Data That Can Be Output in Wiz Stick userAgent-2

Audit Data Type	Phase	Description Format
Malware	*[Block time]* Block	[Detection direction-in/outbound] Detected IP address
Pharming	*[Bypass time]* Bypass	URL, detected IP address, redirected IP address

All the above-mentioned audit data reference time value when they are generated and are expressed in the form 'yyyy/mm/dd-hh:mm:sec.'

- *Related SFR : FAU_GEN.1, FPT_STM.1*

If the number of stored audit data exceeds 999, Wiz Stick Portable recognizes that in such a situation audit trail can cause data loss and deletes the 300 oldest audit data to secure the audit trail capacity.

- *Related SFR : FAU_STG.3*

3. Cryptographic Support, TSF Protection

Wiz Stick Portable provides VPN client function based on IPsec that is defined in IETF RFC 4301 (tunnel mode ESP supported, IKEv1/2 supported). If a VPN access user requests VPN connection, Wiz Stick Portable uses a pre-registered VPN settings to create a session-key through DH group 14 operation in accordance with RFC 3526, while it encrypts information exchanged with VPN gateway during the security negotiation with a session-key. For block cryptography algorithm for the encryption, AES-CBC (128/192.256 bits) is used. VPN gateway and Wiz Stick Portable can authenticate each other by verifying hash inside the packet (hash value of preshared-key, using HMAC-SHA2) and decrypting information encrypted with a session-key. A master-key necessary for VPN tunneling is made from the authenticated preshared-key. During the cryptographic key generation and cryptographic operation used for VPN connection, a random number generator (HASH-DRBG) that complies with NIST SP 800-90 is used in order to generate safe random numbers. All cryptographic keys are zeroized safely when VPN connection is terminated.

- *Related SFR : FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FCS_IPSEC.1, FCS_RBG.1*

Wiz Stick Portable and Wiz Stick adminAgent or Wiz Stick userAgent ensure safe transmission by encrypting data in all messages with AES-CBC(256 bits) algorithm. A cryptographic key used for cryptography is a combination of variable information generated whenever Wiz Stick Device is connected to a user PC and various unique values of Wiz Stick Device. Wiz stick Portable and Wiz Stick adminAgent, or Wiz Stick Portable and Wiz Stick userAgent generate and share the same cryptographic key. The same cryptographic key is also used when decrypting encrypted data inside the messages transmitted between Wiz Stick Portable and Wiz Stick adminAgent or Wiz Stick userAgent. All cryptographic keys are zeroized safely when VPN connection is terminated.

- *Related SFR : FCS_CKM.1, FCS_CKM.4, FCS_COP.1. FPT_ITT.1*

Wiz Stick Portable encrypts all the data transmitted to an external update server by using SHA2 (256 bits) and RSAES-OAEP (2048 bits). A cryptographic key used for RSAES-OAEP cryptography is a public key of the update server, which is loaded in the storage of Wiz Stick Device for distribution. Data transmitted to the external update server by Wiz Stick Portable contains a cryptographic key that is randomly generated by combining various unique values of Wiz Stick Device. This cryptographic key is used when the update server encrypts data transmitted to Wiz

Stick Portable with AES-CBC (128 bits) algorithm. When encrypted data are sent from the external update server, Wiz Stick Portable deciphers them by using AES-CBC (128 bits) algorithm with the key same as the one previously sent to the update server, and verifies the integrity with SHA2(256 bits) algorithm.

Regarding all cryptographic keys used for cryptography of the data transmitted with the external update server, Wiz Stick Portable zeroized them safely after data cryptography is complete.

- *Related SFR : FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPT_ITC.1, FPT_ITI.1*

When TSF data are stored inside Wiz Stick Portable, it encrypts data with ASE-CBC (128 bits) algorithm for safe storage. All cryptographic keys used for cryptography are generated with a combination of various unique values of Wiz Stick Device and stored in a safe location, and zeroized safely after data cryptography is complete.

- *Related SFR : FCS_CKM.1, FCS_CKM.4, FCS_COP.1*

4. Detection and Blocking of Access to Harmful Sites

Wiz Stick Portable provides the SFP that detects access from a user PC to harmful sites (malicious code distribution site, C&C server, etc. defined by the developer KT Corp.) and blocks access to harmful sites based on the detection result.

Wiz Stick Portable analyzes the header and payload (URL, IP information) of the packet inside the traffic that passes through the TOE by using the Snort and detects access to a harmful site. The detected result is recorded as audit log, while IP address, protocol and port information of the detected harmful site are set as ACL referenced by iptables, thereby blocking access to a harmful site.

The rule used for detection and blocking of access to harmful sites is updated on a regular basis by the Update Server operated by the developer, KT Corp, so that it maintains the up-to-date security status.

- *Related SFR : FDP_IFC.2(1), FDP_IFF.1(1)*

5. Detection and Blocking of Access to Pharming Sites

Wiz Stick Portable provides the SFP that detects access by a user PC to pharming sites and blocks access to pharming sites based on the detection result.

Wiz Stick Portable forwards DNS query packet (TCP/UDP 53 port) generated from a user PC to the Secure DNS server operated by KT Corp. to receive normal DNS information, and then use Snort to carry out comparison to check if URL and IP of the site the user tries to access match accurate URL and IP information of banking sites and portal sites that have been affected by pharming in the past. Wiz Stick Portable sets IP address, protocol and port information of the detected pharming site as the policy referenced by iptables, thereby redirecting access to a pharming site towards a normal site in order to block the user's access to the pharming site. The rule used for detection and blocking of access to pharming sites is updated on a regular basis by the Update Server operated by the developer, KT Corp, so that it maintains the up-to-date security status.

- *Related SFR : FDP_IFC.2(2), FDP_IFF.1(2)*

6. IPsec VPN Client

Wiz Stick Portable the VPN SFP that passes data by performing cryptography/hashing for data transmitted through the TOE from external IT entities, or performing deciphering/integrity check/data transmission to external IP entities. Wiz Stick Portable refers to IP address of an external IT entity to determine if it is a communication partner. It creates a security channel or uses an existing security channel based on ESP header information in order to process the origin and destination IP address of the information transmitted from the communication partner and IPsec protocol. It neither calls a security mechanism nor creates a security channel for outbound and inbound traffic to/from an external IT entity other than the communication partner. In addition, any inbound packet without header information such as ESP that is necessary for IPsec protocol processing shall be denied.

- *Related SFR : FDP_IFC.1, FDP_IFF.1(3)*

7. VPN Access User Authentication

When an administrator registers a VPN security policy through Wiz Stick adminAgent, VPN access password is also entered and stored in Wiz Stick Portable. VPN access password requires a complicated combination rule as below to ensure a high level of confidentiality.

- *Related SFR : FIA_SOS.1*

Table 26. Quality Metric of VPN Access Password and Combination Rule

Category	Quality Metric	
Allowable Characters	English Capital/Small Letter	A-Z, a-z
	Number	0-9
	Special Character	!@#$%^&*()_-+=
Combination Rule	Min/Max Length	9-16 digits
	Password shall be a combination of all the allowable characters (English capital/small letters, numbers and special characters).	

A PC user clicks the VPN Connection button in Wiz Stick Device to request VPN connection, and enters VPN connection password set by an administrator to be authorised as a VPN connection user. The TOE shall allow all the actions mediated by the TSF other than VPN connection before the VPN connection user is successfully authenticated. The attribute "VPN connection authorised" is maintained for the authorised VPN connection user until VPN connection is terminated.

- *Related SFR : FIA_ATD.1, FIA_UAU.1*

8. Security Management Function

A PC user can perform the following management functions for security functions and TSF data through Wiz Stick userAgent:

- *Related SFR : FMT_SMF.1*

Table 27. List of Security Management Functions Provided by Wiz Stick userAgent

Category	Management Function
Security Function Management	Stop/start VPN
TSF Data Management	Check Wiz Stick product information, check safe internet access service operation status, check Wiz Stick connection

An administrator can perform the following management functions for inquiry, modification and deletion of security attributes of VPN connection SFP and parts of TSF data.

- *Related SFR : FMT_SMF.1*

Table 28. List of Security Management Functions Provided by Wiz Stick adminAgent

Category	Management Function
Security Function Management	Stop/start VPN
Security Attribute Management	Inquire, modify, delete VPN SFP security attribute
TSF Data Management	Check Wiz Stick product information