VirtualEye Version 5.0

Security Target (EAL1)

Version 6.7

28 October 2010

Prepared by:
Viewtech International Sdn Bhd
(***formerly known as I-Pocket Solution Sdn Bhd***)

DOCUMENT HISTORY

Version Number	Version Date	Change Details
Version 1.0	10 December 2009	First Draft
Version 2.0	19 January 2010	Added in SFRs, amended logical scope and physical cope, updated diagrams, included more descriptions.
Version 3.0	28 January 2010	Correct SFR syntax and statements, corrected diagrams, and corrected spelling errors, added in tables.
Version 4.0	10th February 2010	Correct SFR syntax and statements, corrected diagrams, and corrected spelling errors, added in tables, add and corrected dependencies, spelling error corrected, updated table of contents.
Version 5.0	21st April 2010	Amended the physical scope of TOE figure based on comments in ERR, ensured that mapping of TSF is correct, reviewed and revised the relevant SFRs.
Version 6.0	17th May 2010	Amended the physical and logical scope of the TOE, the list of security features for the TOE, and revised the relevant SFR's.
Version 6.1	07th June 2010	Included the process for authentication and streaming to the TOE description. Amended the logical scope of the TOE to include the secure communication via https, as well as the TOE summary specification.
Version 6.2	24th June 2010	Reviewed and revised SFR's. Added SFR's for https and CAPTCHA. Amended the logical scope to exclude the GSM network type of connectivity.
Version 6.3	05th August 2010	Added the definition for ARPG. Added a figure to explain the logical scope better. Reviewed and revised the SFR's,

		TSS, and logical scope.
Version 6.4	18th August 2010	Revised the following items based on comments from evaluators. • Logical scope of the TOE • SFR's • TSS
Version 6.5	03rd September 2010	Revised the following items based on comments from evaluators. • Logical scope of the TOE • SFR's • TSS • Appendix A-1
Version 6.6	30th September 2010	Revised the following items based on comments from evaluators. • Strength of passwords via changing of colors.
Version 6.7	28th October 2010	Revised the following items based comments from evaluators: • FAU_SAA.3 – removed the word "all" in the assignment for FAU_SAA.3.2 • Specified the fields/forms for input validation in TSS • Revised the SFR for audit log generated

Table of Contents

1 Document introduction

1.1 DOCUMENT CONVENTIONS

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.

1. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of additional security requirements is denoted by **bold underline text** in red color font. Refinement for taking out a security requirement within the SFR's is denoted by ~~**bold strikethrough text**~~ in red color font.

2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*] in red color font.

3. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value] in red color font.

4. The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number) in red color font.

1.2 TERMINOLOGY

Acronym	Meaning
3G	3rd Generation which is a family of standards for mobile telecommunications fulfilling specifications by the International Telecommunication Union
ARPG	Automated Random Password Generator
CC	Common Criteria
DVR	Digital Video Recorder
EAL	Evaluation Assurance Level
EDGE	Enhanced Data for Global Evolution is a third-generation, high-speed, mobile data and Internet access technology
FIPS PUB	Federal Information Processing Standards Publication
GB	Giga Bytes

GHz	Giga Hertz
GPRS	General packet radio service (GPRS) is a packet oriented mobile data service available to users
HSDPA	High-Speed Downlink Packet Access
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server.
IP	Internet Protocol. An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication
LAN	Local Area Network
MB	Mega Bytes
MHz	Mega Hertz
NTP	Network Time Protocol (a protocol used to synchronize the clocks of computers to sometime reference)
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SQL	Structured Query Language
SQL Injection	SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application
SSL	Secure Socket Layer (also known as TLS). SSL are cryptographic protocols that provide security for communications over networks such as the Internet
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
Triple DES	Triple Data Encryption Standard (DES) where it applies the DES cipher algorithm three times to each data block
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
URL	Uniform Resource Locator (The best-known example of a URL is the "address" of a web page on the World Wide Web)
VE5	VirtualEye Version 5.0
Wi-Fi	Wireless networking technology to provide wireless internet and network connections.

The following terminology is used in the ST:

- Authorized Subscribers / Users – an entity that has been properly identified and authenticated, as well as have subscribed to the TOE. These users are considered to be legitimate users of the TOE.
- Authorized administrator/Administrator – A user in the administrator role is an authorized user who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given them. The term authorized administrator is taken from the CC and is used in the ST in those sections that are derived from the CC directly. Otherwise, the term administrator is used. These terms are used interchangeably.
- Security-Relevant TSF data – Data used by the TSF that which defines, controls or monitors the configuration of the security features of the system. This data includes system security configuration information, audit records, user security attributes, authentication data, and access control policy information.

1.3 REFERENCES

- Common Criteria Part 1 Version 3.1 Revision 3
- Common Criteria Part 2 Version 3.1 Revision 3
- Common Criteria Part 3 Version 3.1 Revision 3
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 3

1.4 DOCUMENT ORGANIZATION

This ST contains:

- **ST Reference & TOE Reference:** the ST reference and the TOE reference, which provide identification material for the ST and the TOE that the ST refers to.
- **TOE Overview:** briefly describes the usage of the TOE and its major security features, identifies the TOE type and identifies any major non-TOE hardware/software/firmware required by the TOE.
- **TOE Description:** Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- **TOE Security Objectives:** Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- **TOE Security Functional Requirements:** Presents the Security Functional Requirements (SFRs) met by the TOE.
- **TOE Security Assurance Requirement:** Presents the Security Assurance Requirements (SARs) met by the TOE.
- **TOE Summary Specification:** Describes the security functions provided by the TOE to satisfy the security requirements and objectives.

2 INTRODUCTION

2.1 ST AND TOE REFERENCE

ST Title	**VirtualEye Version 5.0 Security Target (EAL1)**
ST Version	**Version 6.7, 28 October 2010**
TOE Identification	**VirtualEye Version 5.0**
CC Identification	**CC Version 3.1 Revision 3**
Assurance Level	**EAL1**
ST Author	**Prabha Sivam, Ros Yusoff**
Keyword	**Virtual Eye, VE5**

2.2 TOE OVERVIEW

The TOE is part of the entire application system known as Virtual Eye. Virtual Eye is a web based and mobile video surveillance service that offers a carrier-grade mobile streaming system to provide high quality video streaming over the Internet. It is designed to enable users to access live video camera feed or playback recorded video clips from the web portal or mobile devices. VE5 uses streaming technology like h.264 and mjpeg for live streaming via the VE5 portal and mobile respectively, supporting the standard communication protocols such as GPRS, EDGE, 3G, and HSDPA.

VE5 provides an interface between users' DVR(s), IP camera(s) and user's mobile phone, enabling images from the user's web cam to be captured, converted, transmitted and delivered to the user's mobile phone or even via online through VE5 portal. VE5 is accessed through the Internet via a web based browser (e.g. Internet Explorer) on a user computer and enables the user to set up a mobile access to remote IP cameras via a centralized hosted web site via the VE5 web server.

It is worth noting that all recorded videos and pictures are given unique filenames via a random filename generator that resides in the application server. These recorded items will then be stored in the recording server but referenced in the database server.

The scope of the TOE covers the following components of VE5:

1. Web portal available for authorized subscribers and administrators.
2. Mobile device application available for authorized subscribers. The TOE only covers those subscribers who are connected to the web portal via a Wi-Fi connectivity.

The above scope of the TOE provides the following security features that are described in Section 2.3.2. Briefly, the security features introduced by the TOE are:

1. Security audit
2. User Data Protection
3. Identification and authentication
4. Security management
5. TOE access

2.2.1 TOE Type

VE5 is a Microsoft.NET and JAVA web-based application built for authorized subscribers to log in and view their IP based video and images. The TOE itself comprises of the following scope:

1. Web portal available for authorized subscribers and administrators. This web portal application is built using Microsoft.NET and JAVA. Authorized subscribers and administrators access the web portal through their web browser over the Internet or within the LAN (for authorized administrators only). Live and recorded streaming of videos for subscribers are not part of the TOE. Please refer to Section 2.3.2 for details.
2. Mobile device application available for authorized subscribers. This mobile application is built using JAVA. Authorized subscribers access the mobile application using a Wi-Fi connection. The subscribers can authenticate themselves using username and password through the mobile device application. The live stream of videos is not part of the TOE. Please refer to Section 2.3.2 for details.

2.2.2 Required non-TOE Hardware and Software

Below are the requirements for the hardware and software to run the TOE:

Hardware	**Application & Web Server;** **Recording & Streaming Server** • Intel(R) Xeon(R) Processor 3.0GHz/2M,800MHz • DIMM Memory 2GB (4x512), • DDR-2 400MHz ECC 2R Memory • SCSI Hard Drives 73GB Ultra320 (10K RPM, 80-pin) • Integrated Dual Intel Gigabit Network Card
	Database Server • Intel(R) Dual Core Processor 3.4GHz/2M,800MHz • Operating System Windows Server 2003 • DIMM Memory 2GB (4x512), • DDR-2 400MHz ECC 2R Memory • 5x SCSI Hard Drives 173GB Ultra320 (10K RPM, 80-pin) • Integrated Dual Intel Gigabit Network Card
	Authorized subscriber's & administrator's computer

	• A standard PC with Operating System: Windows 98,2000,NT,XP,Vista (For evaluation purpose, Windows XP was used) • CPU: At least 1Ghz with 32 bit processor • RAM: At least 512 MB • Disk space: Very minimal (less than 1GB) • 1 USB 2.0 port available (for the web cam)
	Authorized subscriber's mobile phone • Java-supported mobile phones that are Wi-Fi enabled
	Digital Video Recorder • Megavision DVR series (for testing purposes)
	IP Camera • Vivotek IP Camera series (for testing purposes)
	Email Server
Software	**Servers** • Windows 2003 Server OS including IIS 6.0 for the web and application server • Apache Server version 2.3 for the web and application server • mySQL Server 5.0 Database for the database server • Proprietary Recording and Streaming software for the Recording and Streaming server (developed by the vendor)
	Authorized subscriber's & administrator's Computer • Operating System: Windows 98,2000,NT,XP, Vista (For evaluation purpose, Windows XP was used) • Internet Explorer 7
	Authorized subscriber's mobile phone • JAVA enabled mobile phones • Wi-Fi enabled mobile phones (For evaluation purpose, Nokia N95, ASUS GARMIN M20 and Nokia N73 were used)

The TOE is to be installed on a computer that acts as a server which has a minimum hardware and software requirements as stated in the table above.

The TOE is accessed via a web portal (for the authorized subscribers and administrators), as well as a mobile application (for the authorized subscribers) with the minimum hardware and software requirements stated in the table above.

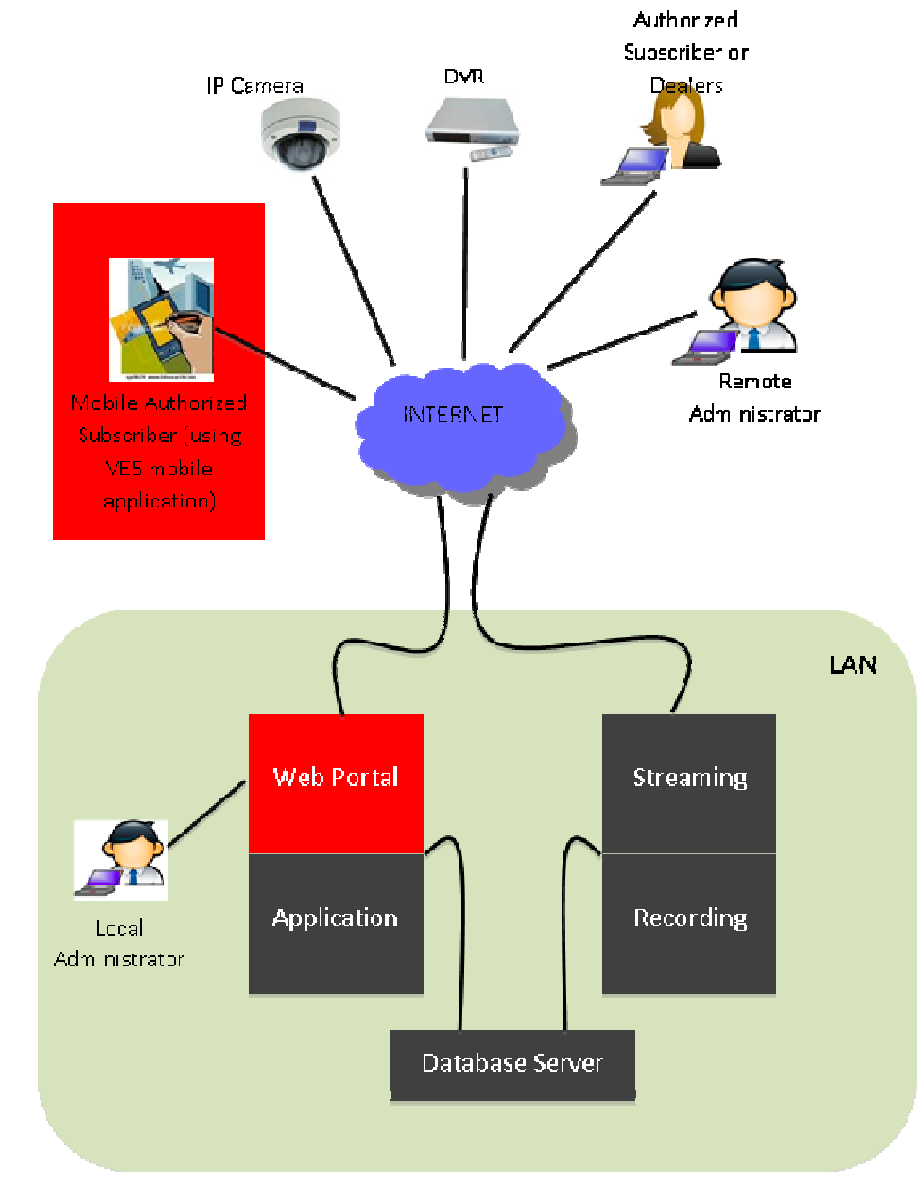
Notes:

1. The mentioned hardware and software requirements are not part of the TOE.
2. All mentioned 3rd party software is not part of the TOE.
3. Live and recorded streaming of videos from the IP cameras and streaming / recording server are not part of the TOE. Note however that all users must be identified and authenticated via the web portal before they can access the videos. Moreover, their sessions are managed by the VE5 web portal (TOE) using session timeouts.

Authorized administrators can access the TOE from the Internet or within the LAN.
Authorized subscribers can access the TOE from the Internet.

2.3 TOE DESCRIPTION

2.3.1 Physical Scope of the TOE



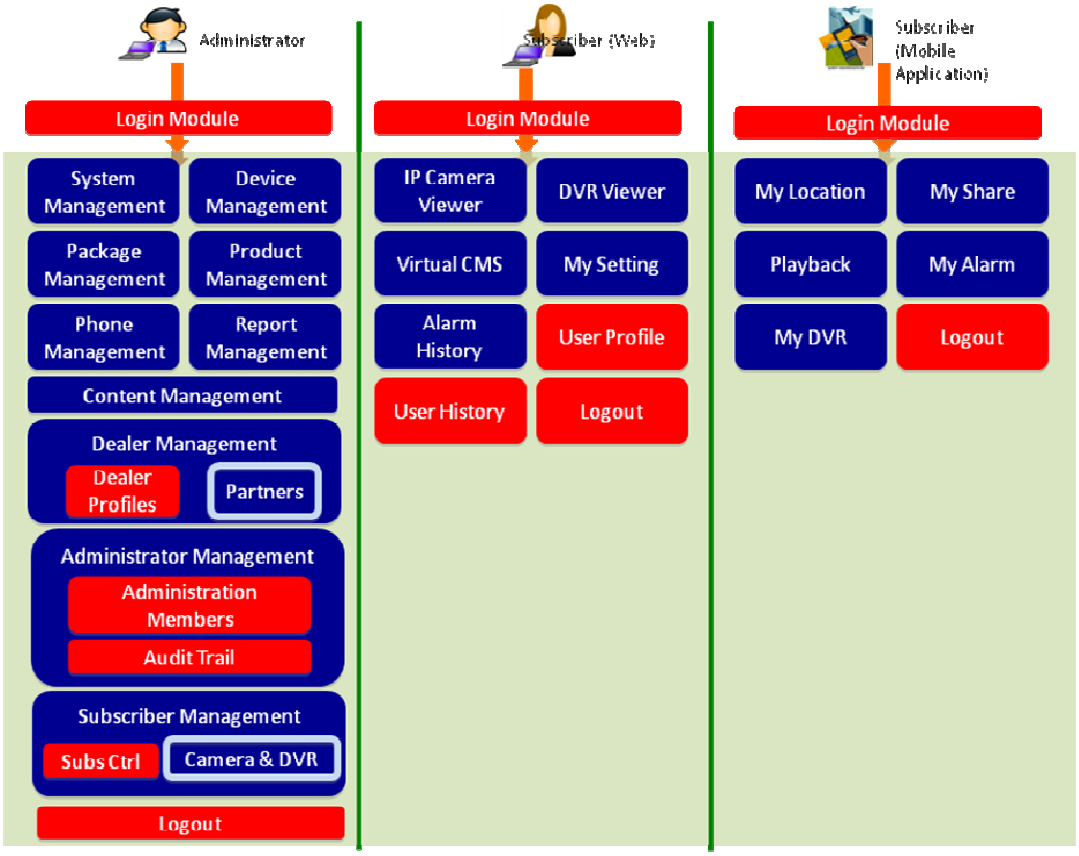
TOE

The TOE consists of the VE5 web portal and mobile application (the software). The pieces of hardware used are not part of the TOE.

Please refer to the section below (Section 2.3.2) for the detail description on the process flows of the identification / authentication of users before the live or recorded streaming of videos can be performed.

2.3.2 Logical Scope of the TOE

The figure below depicts the logical scope of the TOE:



TOE

Functions / Modules for Authorized Administrators:

An authorized administrator has access to the following functions or modules within VE5 through the web portal:

1) **System Management:** Module to manage system configuration (such as email addresses and email login) and monitor the status of the server.
2) **Administrator Management:** Module to manage list of administrator users. The list of users will only able to use the modules available in the administration area, not the main portal.
3) **Subscriber Management:** Module to manage list of subscribers, subscribers' IP camera and subscribers' DVR. This module will also manage subscriber logins to main portal.
4) **Package Management:** Module to manage package to offer to customers.
5) **Product Management:** Module to manage list of current products available. The products will be listed in the main portal page.
6) **Device Management:** Module to manage list of hardware devices currently used by the customers.
7) **Phone Management:** Module to manage list of supported phones, list of phone manufacturers and list of available phone drivers (to stream video on the phone).
8) **Dealer Management:** Module to manage list of dealers for I-Pocket. This will also manage the logins for the dealers, to access Dealer Area where they can manage their own subscribers.
9) **Content Management:** Module to manage items displayed on the portal front page, such as section title and image.
10) **Report Management:** Module that consists of a list of available reports, such as subscriber listing, package listing and user listing.
11) **Logout:** Disconnects the user, ends the session and clears the cookies/cache.

Functions / Modules for Authorized Subscribers Using Web Browsers:

Among the functions or modules that can be accessed by the authorized subscriber has within VE5 through the web portal are:

1) **IP Camera Viewer:** Module to view life stream videos fed by the installed IP cameras through the web portal.
2) **DVR Viewer:** Module to view life stream videos from DVR's.
3) **Alarm History:** View recorded events triggered for example an object missing event and the time that it occurred
4) **Virtual CMS:** Monitor, arm, disarm, and handle the panic button for a specified site (with the list of zones, alarm descriptions and event status)
5) **My Setting:** Module to manage the IP cameras and DVR's.
6) **User Profile:** Module to manage update personal information about the authorized subscriber.
7) **User History:** Module to view the audit trail of activities by that specific authorized subscriber.
8) **Logout:** Disconnects the user, ends the session

Functions / Modules for Authorized Subscribers Using Mobile Application:

Authorized subscribers can also view live stream videos fed by the installed IP cameras through their registered mobile phones via a Wi-Fi connection. However, the viewing of videos is not part of the TOE.

Among the functions or modules that can be accessed by the authorized subscriber has within VE5 through the mobile application are:

1) **My Location:** Displays the list of all location and the respective list of cameras
2) **My Share:** Displays the list of shared cameras
3) **Playback:** Displays the playback files
4) **My Alarm:** List alarms that are recorded by cameras due to motion detection
5) **My DVR:** Displays the cameras that attached to the digital video server
6) **Logout:** Disconnects the user, ends the session

Below is the TOE scope description for the identified security functions. The details can be found in the TSS section.

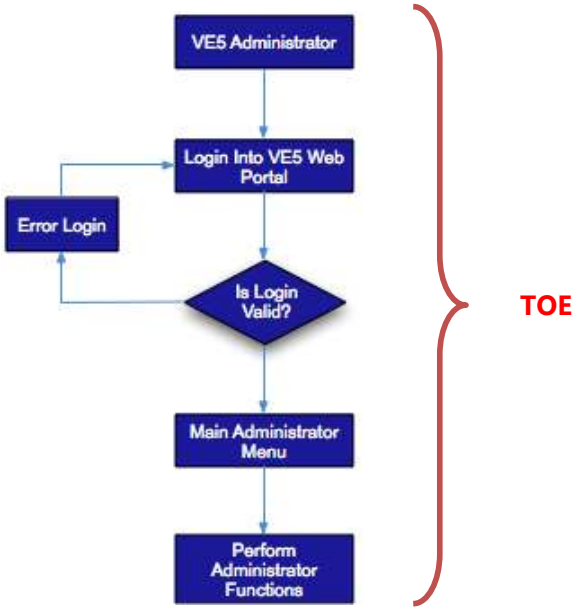
Security Function	TOE Scope Description
Security Audit	The TSF generates audit logs that consist of various auditable events or actions. Authorized administrators have the capability to read and view all the recorded logs for administrative accounts through the web portal. The audit trail generated is able to relate activities and events taken place to the specific usernames which then can be traced to the specific defined roles. The recorded logs are available in the Audit Trail sub-module. Authorized subscribers can view their own history of activities via a web browser in the User History sub-module within the Web Portal. They are able to view the event ID, task category, detail task, date / time, and the IP address. Neither the administrators nor the subscribers can delete the logs.
User Data Protection	Input validation checks are performed at the application level for interactive forms within VE5 web portal for a protection against SQL injections.

Security Function	TOE Scope Description
Identification and Authentication	The TOE requires each user to be identified and authenticated (using username and password) prior to performing any authenticated functions. This is done in the login module. Authorized subscribers can only view their own data, not others. Authorized subscribers with mobile application can only authenticate themselves and view the live stream of videos from the installed IP cameras. The full functions area available to the authorized subscribers through the web portal. A minimum of 6 and a maximum of 12 characters is required for the passwords. Status of strength is shown by color code from grey-light blue-light grey-blue-dark blue by the password strength indicator utility through the web portal. The password strength indicator utility calculates the number of characters with the length and will indicate the usage of at least one character that is case-sensitive. It will indicate the compulsory requirement for the password. The TOE also provides ARPG and CAPTCHA functions as detailed out in Section 7 (TOE Summary Specifications).
Security Management	The TOE handles the identification and authentication of authorized subscribers and administrators. The access rights given will be based on these 2 defined roles. Authorized administrators can add, edit, change passwords and / or delete administrative accounts in the Administration Members sub-module; edit and / or delete subscribers' accounts in the Subscriber Control (Subs Ctrl) sub-module; add, edit, and / or delete dealers' accounts in the Dealer Profiles sub-module; and, view administrative logs in the Audit Trail sub-module. Authorized web-based subscribers can change own password in the User Profile sub-module; reset password via the usage of ARPG; and, view own user history or logs in the User History sub-module. Details of the functions allowed to be performed by these 2 defined roles are in Section 7 (TOE Summary Specifications).

Security Function	TOE Scope Description
TOE Access	The default session timeout is 10 minutes. After inactivity during a session of 9 minutes 30 seconds, a prompt will appear to click OK to continue session. If the subscriber clicks OK within 30 seconds, the session continues, else the session will auto log out. The authorized subscribers are then returned to the main page of the VE5 web portal. This security function is only available for the sessions established via the web portal, not the mobile application. The TOE assumes that the operational environment of the VE5 web portal provides a reliable time stamp source.

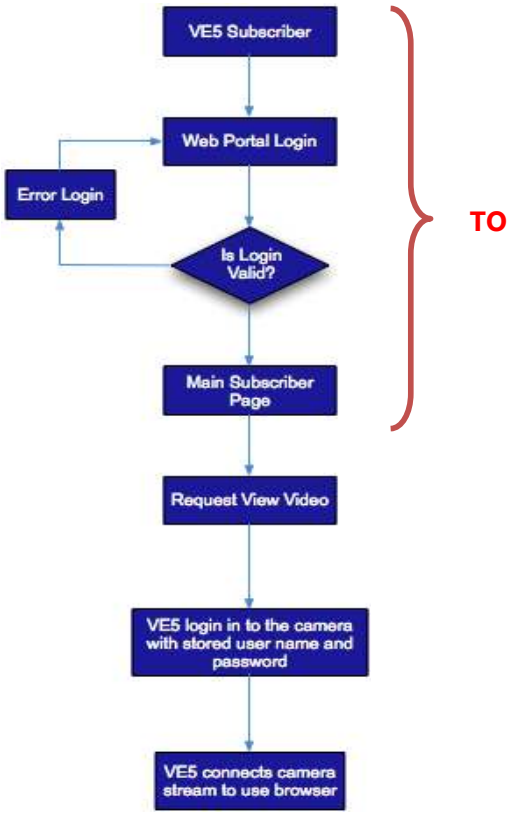
An authorized subscriber or administrator needs to log in to the TOE with a unique username and password to access any of the modules or functions in VE5.

Below is the process flow for the administrator authentication via a web browser on his / her computer:



The administrators are authenticated on the VE5 web portal via https channel.

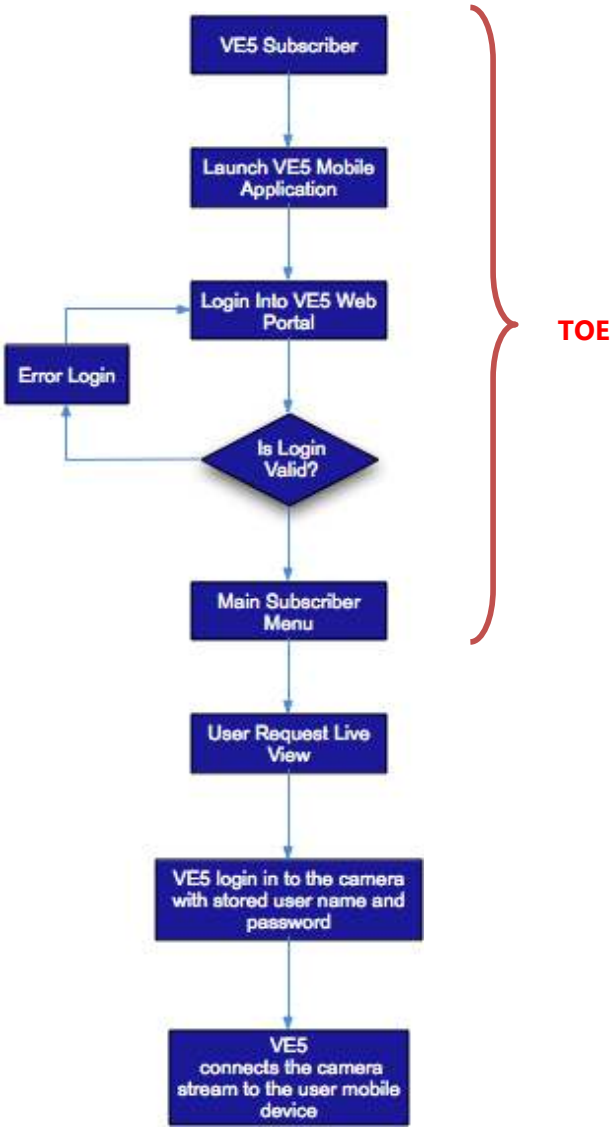
Below is the process flow for the subscriber authentication and request for viewing of videos via a web browser on his / her computer:



Subscribers are authenticated on the VE5 web portal via https channel using their web browsers. Once they are authenticated and a session is established, the subscribers are connected to the IP cameras, DVR's or streaming server directly (streaming directly from these devices to the subscribers' web browsers). Note that the streaming function is not part of the TOE.

Authorized subscribers can also view life stream videos fed by the installed IP cameras through their registered mobile phones via a Wi-Fi connection. However, the viewing of videos is not part of the TOE.

Below is the process flow for the subscriber authentication and request for viewing of videos via a mobile application on his / her JAVA enabled mobile phones:



Subscribers are authenticated on the VE5 web portal via https channel using the mobile application on their JAVA enabled mobile phones. Once they are authenticated and a session is established, the subscribers are connected to the IP cameras and DVR's (streaming directly from these devices to the subscribers' mobile application on their mobile phones). Note that the streaming function is not part of the TOE.

3 CONFORMANCE CLAIMS

3.1 COMMON CRITERIA CLAIMS

The following conformance claims are made for the TOE and ST:

- **CCv3.1 Rev.3 conformant**. The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 3.
- **Part 2 extended**. The ST is Common Criteria Part 2 extended.
- **Part 3 conformant**. The ST is Common Criteria Part 3 conformant.
- **Package conformant**. The ST package is conformant to Evaluation Assurance Level (EAL) 1.
- TOE and ST does not conform **Protection Profiles**.

4 TOE SECURITY OBJECTIVES

This section defines the security objectives for the supporting environment of the TOE.

4.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Certain objectives with respect to the general operating environment must be met for the TOE to meet its security functional requirements. Those objectives are:

Security Objective	Description
OE.TIME	The operational environment must provide a reliable time stamp source.
OE.NOEVIL	Administrators and subscribers are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance.
OE.INSTALL	Those responsible for the TOE (administrators and subscribers) must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the organization's IT security objectives.
OE.RELIABLE	All hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns. All supporting components' performance is monitored and maintained by administrators.
OE.PHYSICAL	The operational environment of the TOE restricts the physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel.
OE.CREDEN	Those responsible for the TOE (administrators and subscribers) must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with the organizational policies and procedures disallowing disclosure of user credential information) in a manner, which maintains the organization's IT security objectives.

OE.MOBLOGOUT	The authorized subscribers that are accessing through the mobile application via their mobile phones (via a Wi-Fi connection) must ensure that they log out of the mobile application by clicking on the logout option.
OE.CHANNEL	The operational environment of the TOE must protect the transmitted information to the Web Portal via usage of HTTPS using a server based SSL.

5 EXTENDED COMPONENTS DEFINITION

The table below contains the extended security functional requirements for the TOE:

Security Function Class	Security Function Component
FPT: Protection of the TSF	FPT_STM_EXT.1 Reliable time stamps

FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data.

The above component is a member of FPT_STM, an existing CC Part 2 family. The following extended requirement for the FPT class has been included in this ST because the operational environment is capable of providing reliable time stamps for TSF functions that is not covered in CC Part 2.

Reliable time stamps (FPT_STM_EXT.1)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM_EXT.1.1:	The operational environment shall be able to provide reliable time stamps for the TSF functions.
Application Note:	*Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU_GEN.1 and FMT_SAE.1 security functions. The TOE does not have a feature to generate time stamps independently. The underlying operating system needs to provide reliable time stamps from the system clock for use by the TOE. The date and time stamps provided by the underlying operating system can be manually configured by administrators or fed by NTP servers.*

6 SECURITY REQUIREMENTS

This section specifies the requirements for the TOE.

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This sub-section specifies the SFRs for the TOE. It organizes the SFRs by the CC classes.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_SAA.3: Simple Attack Heuristics
	FAU_SAR.1: Audit Review
	FAU_STG.1: Protected Audit Trail Storage
FDP: User Data Protection	FDP_ACC.1: Subset Access Control
	FDP_ACF.1: Security Attribute Based Access Control
FIA: Identification and Authentication	FIA_ATD.1: User Attribute Definition
	FIA_SOS.1: Verification of Secrets
	FIA_SOS.2: TSF Generation of Secrets
	FIA_UAU.2: User Authentication Before Any Action
	FIA_UID.2: User Identification Before Any Action
	FIA_USB.1 User-subject Binding
FMT: Security Management	FMT_MSA.1: Management of Security Attributes
	FMT_MTD.1: Management of TSF Data
	FMT_SAE.1: Time-limited Authorization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FTA: TOE Access	FTA_SSL.3: TSF-initiated Termination

6.1.1 Security Audit

6.1.1.1 Audit Data Generation (FAU_GEN.1)

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 functions;**~~
b) All auditable events for the [*not specified*] level of audit and

c) [

Role	Recorded Event
Administrator	• Authentication successful and unsuccessful • Add, edit and delete record successful and unsuccessful • Invalid username or password • Maximum failed login attempts • Search record • Logout
Subscriber (web-based)	• Authentication successful • Changes related to camera setting • Logout

].

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 identity, outcome (success or failure) of the event; and
b) For audit event type, based on the auditable event definitions of the functional components included in the ST, [originated IP address and modules accessed by the administrators and subscribers].

Application Note: *Please refer to Section 8 for the rationale for not addressing the FPT_STM.1 as a dependency of FAU_GEN.1.*
The TOE is more restrictive as it does not allow the administrators or subscribers to start-up and shutdown the audit functions. The audit functions are always on.

6.1.1.2 User Identity Association (FAU_GEN.2)

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit Data Generation
FIA_UID.1 Timing of Identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: *Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.*

6.1.1.3 Simple Attack Heuristics (FAU_SAA.3)

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FAU_SAA.3.1	The TSF shall be able to maintain an internal representation of the following signature events [SQL injections] that may indicate a violation of the enforcement of the SFRs.
FAU_SAA.3.2	The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [inputs by validating data input/interactive forms in the Web Portal].
FAU_SAA.3.3	The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

6.1.1.4 Audit Review (FAU_SAR.1)

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1	The TSF shall provide [authorized administrators and subscribers] with the capability to read [recorded audit information] 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.

6.1.1.5 Protected Audit Trail Storage (FAU_STG.1)

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit Data Generation

FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

6.1.2 User Data Protection

6.1.2.1 Subset Access Control (FDP_ACC.1)

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [access control SFP] on [authorized administrators and subscribers for the following functions or operations:

Role	Function
Administrator	• Login as an administrator • Logout as an administrator • Add, edit, change passwords and delete administrative accounts • Edit and delete subscriber accounts • Add, edit, and delete dealers accounts • View audit logs for the administrative accounts
Subscriber (web-based)	• Login as a subscriber • Logout as a subscriber • Change own password • Reset password via the usage of ARPG • View own user history or logs
Subscriber (mobile application)	• Login as a subscriber • Logout as a subscriber

].

6.1.2.2 Security Attribute Based Access Control (FDP_ACF.1)

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset Access Control
FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [usernames and user roles].

FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [administrators and subscribers are explicitly granted access to a function or resource if he/she belongs to a user role which has been granted access].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].
.	
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].
Application Note:	*The TOE does not have any default value for passwords for both the administrators and subscribers. Hence, there is no dependency to FMT_MSA.3.*

6.1.3 Identification and Authentication

6.1.3.1 User Attribute Definition (FIA_ATD.1)

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 users: [CAPTCHA image and CAPTCHA code entered by subscribers].

6.1.3.2 Verification of Secrets (FIA_SOS.1)

Hierarchical to:	No other components
Dependencies:	No dependencies

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [a minimum of 6 characters to a maximum of 12 characters for authorized subscribers]. *(refer to Appendix A-1)

6.1.3.3 TSF Generation of Secrets (FIA_SOS.2)

Hierarchical to:	No other components
Dependencies:	No dependencies

FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet [a minimum of 6 characters to a maximum of 12 characters for authorized subscribers].
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [a forgotten password via the usage of ARPG].

6.1.3.4 User Authentication Before Any Action (FIA_UAU.2)

Hierarchical to:	FIA_UAU.1 Timing of Authentication
Dependencies:	FIA_UID.1 Timing of Identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Application Note:	*Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.*

6.1.3.5 User Identification Before Any Action (FIA_UID.2)

Hierarchical to:	FIA_UID.1 Timing of Identification
Dependencies:	No dependencies
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.6 User-subject Binding (FIA_USB.1)

Hierarchical to:	NO other components
Dependencies:	FIA_ATD.1 User Attribute Definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [CAPTCHA image and CAPTCHA code entered by subscribers].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [CAPTCHA code entered must match CAPTCHA image for the following activities: a) Subscribers filling in the Forgot Password form, or b) Subscribers editing their profiles].

FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [none].

6.1.4 Security Management

6.1.4.1 Management of Security Attributes (FMT_MSA.1)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MSA.1.1:	The TSF shall enforce the [access control policy] to restrict the ability to [*change*] the security attributes [passwords] to [authorized subscribers and administrators].

6.1.4.2 Management of TSF data (FMT_MTD.1)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1:	The TSF shall restrict the ability to [*view*] the [auditable data] to [authorized administrators and subscribers].

6.1.4.3 Time-limited Authorisation (FMT_SAE.1)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps
FMT_SAE.1.1:	The TSF shall restrict the capability to specify an expiration time for [authorized subscribers' sessions in the web portal] to [none].
FMT_SAE.1.2:	For each of these security attributes, the TSF shall be able to [log out the associated authorized user account for the web portal] after the expiration time for the indicated security attribute has passed.

Application Note: *Please refer to Section 8 for the rationale for not addressing the FPT_STM.1 as a dependency of FMT_SAE.1.*

6.1.4.4 Specification of management functions (FMT_SMF.1)

Hierarchical to: No other components.
Dependencies: No dependencies

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [

Role	Function
Administrator	• Add, edit, change passwords and delete administrative accounts • Edit and delete subscriber accounts • Add, edit, and delete dealers accounts • View audit logs for the administrative accounts
Subscriber (web-based)	• Change own password • Reset password via the usage of ARPG • View own user history or logs

].

6.1.4.5 Security Roles (FMT_SMR.1)

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrators and subscribers].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 TOE Access

6.1.5.1 TSF-initiated Termination (FTA_SSL.3)

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1:	The TSF shall terminate an interactive session after [a specified time interval of user inactivity (default value is 10 minutes) for subscribers].

6.2 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE meets the security assurance requirements for EAL1. The following table is the summary for the requirements:

Assurance Class	Assurance Components
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 Operational User Guidance AGD_PRE.1 Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1 Labeling of the TOE ALC_CMS.1 TOE CM Coverage
ASE: 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
ATE: Tests	ATE_IND.1 Independence Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability Survey

7 TOE SUMMARY SPECIFICATIONS

The TOE Summary Specification (TSS) enables evaluators and potential consumers to gain a general understanding of how the TOE is implemented. The below table summarizes the TSFs matching the SFRs.

	FIA_ATD.1	FIA_SOS.1	FIA_SOS.2	FIA_UID.2	FIA_UAU.2	FIA_USB.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.3	FAU_SAR.1	FAU_STG.1	FPT_STM_EXT.1	FTA_SSL.3	FMT_MSA.1	FMT_MTD.1	FMT_SAE.1	FMT_SMR.1	FMT_SMF.1	FDP_ACC.1	FDP_ACF.1
Security Audit							√	√		√	√	√			√					
User Data Protection									√											
Identification and Authentication	√	√	√	√	√	√														
Security Management														√			√	√	√	√
TOE Access												√	√			√				

Security Function	TOE Scope Description
Security Audit	The TSF generates audit logs that consist of various auditable events or actions. Date and time of events, IP addresses, usernames, modules accessed, and events or actions taken by the authorized users are recorded. Authorized administrators have the capability to read and view all the recorded logs for administrative accounts through the web portal. The audit trail generated is able to relate activities and events taken place to the specific usernames which then can be traced to the specific defined roles. The recorded logs are available in the Audit Trail sub-module Authorized subscribers can view their own history of activities via a web browser in the User History sub-module within the Web Portal. They are able to view the event ID, task category, detail task, date / time, and the IP address. Neither the administrators nor the subscribers can delete the logs. The TOE assumes that the operational environment provides a reliable time stamp source for the accuracy of the dates and times recorded in the logs mentioned above. **Functional Requirement Satisfied:** **FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FMT_MTD.1, FPT_STM_EXT.1.**

User Data Protection	Not validating input is one of the reasons for malicious database manipulation or system crashes. User Data Protection function provides the TSF with the ability to protect user data by ensuring data sent to the Web Portal is validated prior to processing it. Input to the field available in the interactive forms in the VE5 Web Portal is validated before it is processed. The input validation is performed for the web subscriber login form (both username and password fields). If the subscriber is registered with a username or password that contains any unaccepted character (known as "black" list), then the input will not be validated. The input is validated based on the list of unacceptable characters (known as "black" list) to ensure that no malicious code is inserted into the SQL query or at least keep malicious code from being processed. **Functional Requirement Satisfied:** **FAU_SAA.3**

Identification and Authentication	The TOE requires each user to be identified and authenticated (using username and password) prior to performing any authenticated functions. The usernames and passwords for the authorized subscribers and administrators are stored in the database server encrypted using TripleDES. The encryption process itself is done at the application level. Note that the encryption is not part of the TOE (the database and application are not part of the TOE). Authorized subscribers can only view their own data, not others. Authorized subscribers with mobile application can only authenticate themselves and view the life stream of videos from the installed IP cameras. The full functions area available to the authorized subscribers through the web portal. A minimum of 6 and a maximum of 12 characters is required for the passwords. Status of strength is shown by color code from grey-light blue-light grey-blue-dark blue by the password strength indicator utility through the web portal. The password strength indicator utility calculates the number of characters with the length and will indicate the usage of at least one character that is case-sensitive. It will indicate the compulsory requirement for the password. If an authorized subscriber forgets his or her password, there is option in VE5 web portal where he or she clicks on FORGOT PASSWORD button and enters USERNAME and EMAIL ADDRESS and the system will automatically generate a password using ARPG and email it back to the authorized users. The administrator does not even know the password generated. The User Profile (for web-based subscribers to manage their profiles) and the "forget password" pages consist of a program called CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) to ensure that the forms are filled in by a human being instead of a SPYBOT. **Functional Requirement Satisfied:** **FIA_UID.2, FIA_UAU.2, FIA_SOS.1, FIA_SOS.2, FIA_ATD.1, FIA_USB.1**

Security Management	The TOE handles the identification and authentication of authorized subscribers and administrators. The access rights given will be based on these 2 defined roles. Authorized administrators can perform the following functions: 1. Add, edit, change passwords and / or delete administrative accounts in the Administration Members sub-module 2. Edit and / or delete subscribers' accounts in the Subscriber Control (Subs Ctrl) sub-module 3. Add, edit, and / or delete dealers' accounts in the Dealer Profiles sub-module 4. View administrative logs in the Audit Trail sub-module Authorized web-based subscribers can perform the following functions: 1. Change own password in the User Profile sub-module 2. Reset password via the usage of ARPG 3. View own user history or logs in the User History sub-module Subscribers and administrators are explicitly granted access to the resources or functions within VE5 based on their user role. **Functional Requirement Satisfied:** **FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_SMF.1, FMT_SMR.1.**

TOE Access	The default session timeout is 10 minutes. After inactivity during a session of 9 minutes 30 seconds, a prompt will appear to click OK to continue session. If the subscriber clicks OK within 30 seconds, the session continues, else the session will auto log out. The authorized subscribers are then returned to the main page of the VE5 web portal. This security function is only available for the sessions established via the web portal, not the mobile application. The TOE assumes that the operational environment of the VE5 web portal provides a reliable time stamp source. **Functional Requirement Satisfied:** **FTA_SSL.3, FMT_SAE.1, FPT_STM_EXT.1.**

8 SECURITY REQUIREMENTS RATIONALE

8.1 RATIONALE FOR NOT ADDRESSING ALL DEPENDENCIES

FPT_STM.1:

FPT_STM.1 is a dependency of FAU_GEN.1 and FMT_SAE.1 that has not been included. Reliable time stamps are provided by the operational environment through an interface of the TOE. The time stamps captured in the TOE is derived from the operating system of the computer on which the instance of VE5 web portal is installed and running.

9 APPENDIX A-1

Password Strength Indicator

Password strength indicator is used to convey the user the strength level of the password entered. The strength is determined by the following criteria:

a) Length of password
b) Contains alphabet characters and numbers
c) Contains both lower and uppercase characters

In order to secure the user input from SQL injection attack, other special characters (such as double quote (") and single quote (')) are not allowed.

Strength Level:

The color code describer as per below:

1. Poor - Grey color: Maximum 7 characters of lower or upper case letters, or maximum 1 numeric character
2. Weak - Light blue color: Any 2 of the below list of combinations
3. Good - Light grey color: Any 3 of the below list of combinations
4. Strong – Blue color: All 4 of the below list of combinations but contains only 8 characters
5. Excellent - Dark blue color: All 4 of the below list of combinations

List of combinations:

1. Minimum 2 characters for symbols
2. Minimum 2 upper case letters
3. Minimum 2 lower case letters
4. Minimum 2 numeric characters

Please note that the passwords can only be accepted if it meets the minimum 6 to 12 characters. If the color code is grey (poor password strength), the password cannot be saved.

10 APPENDIX A-2

Screenshot of Virtual Eye application on Java based mobile phone for userid identification and authentication.

Splash Screen of VE5 Mobile Application

=====➔

User is prompted to enter: Userid and password