Passlogix V-GO Sign-On Platform Product Suite
Version 6.0
Security Target

Version 1.0
December 16, 2008

Prepared for:

Passlogix, Inc.
160 Pearl Street, 4th floor
New York, NY 10005 USA

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the Passlogix V-GO Sign-On Platform Product Suite provided by Passlogix, Inc. The TOE is also known under the other brand name: the Oracle Enterprise Single Sign-on Suite (ESSO). The TOE is a middleware product that allows the user to authenticate once, with subsequent automatic detection and handling by the TOE of requests for user credentials from other applications. The TOE also provides features for password reset, suspending or closing inactive sessions, and bridging strong authentication using a variety of different authentication mechanisms to applications within the enterprise.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment and the threats that are countered by the TOE and IT environment.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL3 augmented with Basic flaw remediation (ALC_FLR.1).
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

Security Target, TOE and CC Identification

ST Title – Passlogix V-GO Sign-On Platform Product Suite Version 6.0 Security Target

ST Version – Version 0.9

ST Date – September 24, 2008

TOE Identification – V-GO Sign-On Platform Product Suite version 6.0, also know as the Oracle Enterprise Single Sign-on Suite, including:

- V-GO Single Sign-On (SSO), version 6.0
- V-GO Authentication Manager (AM), version 6.0
- V-GO Provisioning Manager (PM), version 6.0
- V-GO Session Manager (SM), version 6.0
- V-G0 Self-Service Password Reset (SSPR), version 6.0

The component names for the individually branded components are as follows:

PASSLOGIX	**ORACLE**
AM 6.0 ROLLUP D	ESSO Authentication Manager 10.1.403
PM 6.0 ROLLUP D	ESSO Provisioning Gateway 10.1.403
SM 6.0 ROLLUP E	ESSO Kiosk Manager 10.1.403
SSO 6.0 ROLLUP E	ESSO Logon Manager 10.1.403
SSPR 6.0 ROLLUP D	ESSO Password Reset 10.1.403

TOE Developer – Passlogix, Inc.

Evaluation Sponsor – Passlogix, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
  - Part 3 Conformant
  - Assurance Level: EAL 3 Augmented ALC_FLR.1 Basic flaw remediation
  - Strength of Function Claim: SOF-Basic

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: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an

assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).

- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2.TOE Description

The TOE consists of five Passlogix V-GO Products that make up the Sign-On Platform, version 6.0. The TOE is also sold under the following brand name: Oracle Enterprise Single Sign-on Suite. The products are identical and are all manufactured by Passlogix; only the brand name is different.

The main product is V-GO SSO, which responds to requests for user credentials from any Windows, Web or Mainframe/Host application. SSO allows the user to authenticate once, with subsequent automatic detection and handling by SSO of requests for user credentials from other applications. The remaining four products in the V-GO Sign-On Platform are add-ons to SSO, including: V-GO AM, which enables organizations to bridge strong authentication to all of their applications, including smart cards, biometrics and Entrust authenticators; V-GO PM, which provides the ability for an administrator to automatically provision V-GO SSO with a user's ID and password by using a provisioning system; V-GO Session Manager (SM), which provides a solution that addresses the needs of traditional Single Sign-Off in a kiosk environment by suspending or closing inactive sessions; and V-GO Self Service Password Reset (SSPR), which enables users to reset their own Windows domain passwords without the intervention of administrative or help-desk personnel. The TOE consists entirely of the software applications described above.

TOE Overview

The TOE is a set of interrelated software applications that run in an MS Windows environment that can be described in terms of the following components:

- V-GO SSO, which responds to requests for user credentials from any Windows, Web or Mainframe/Host application. SSO provides allows the user to authenticate once, with subsequent automatic detection and handling by the TOE of requests for user credentials from other applications. The remaining four products in the V-GO Sign-On Platform are add-ons to SSO.
- V-GO AM enables organizations to bridge strong authentication to all of their applications, including smart cards, biometrics and Entrust authenticators. Users can employ different authenticators at different times and with different applications.
- V-GO PM provides the ability for an administrator to automatically provision V-GO SSO with a user's ID and password by using a provisioning system. An administrator is able to add, modify and delete IDs and passwords for particular applications within the provisioning system and have the changes reflected in V-GO SSO.
- V-GO Session Manager (SM) provides a solution that addresses the needs of traditional Single Sign-Off in a kiosk environment. V-GO SM has a client-side agent that suspends or closes inactive sessions and seamlessly shuts down all applications.
- V-GO Self Service Password Reset (SSPR) enables users to reset their own Windows domain passwords without the intervention of administrative or help-desk personnel. It provides end users

with an alternative means of authenticating themselves by taking a quiz comprising a series of passphrase questions.

TOE Architecture

The TOE is a suite of five products, as described above. The TOE runs in an MS Windows environment. The TOE architecture is described below for each of the five components. The primary emphasis is on SSO, since this is the main product, with the other four components being add-ons to SSO. Note that all cryptographic functionality is performed by Microsoft Cryptographic Application Programming Interface (MS CAPI) in the IT environment; the TOE makes use of cryptography to protect user credentials and TSF data, but all cryptography is performed by the IT Environment, specifically by MS CAPI.

V-GO SSO

V-GO SSO supports single sign-on by introducing a secure middle layer that collects authentication credentials once from the user and then automatically detects and handles subsequent application or system requests for user credentials. Specifically, v-GO SSO collects user credentials, stores them in an encrypted form with encryption performed by MS CAPI, and responds to requests for user credentials (username/ID, password) from any Windows, Web, or Mainframe/Host application. V-GO SSO's architecture consists of seven areas, which are depicted in Figure 1 below: (1) User Authentication; (2) Encryption; (3) Application Sign-On; (4) Core (including Storage); (5) Synchronization; (6) Event Logging; and (7) Admin Control.

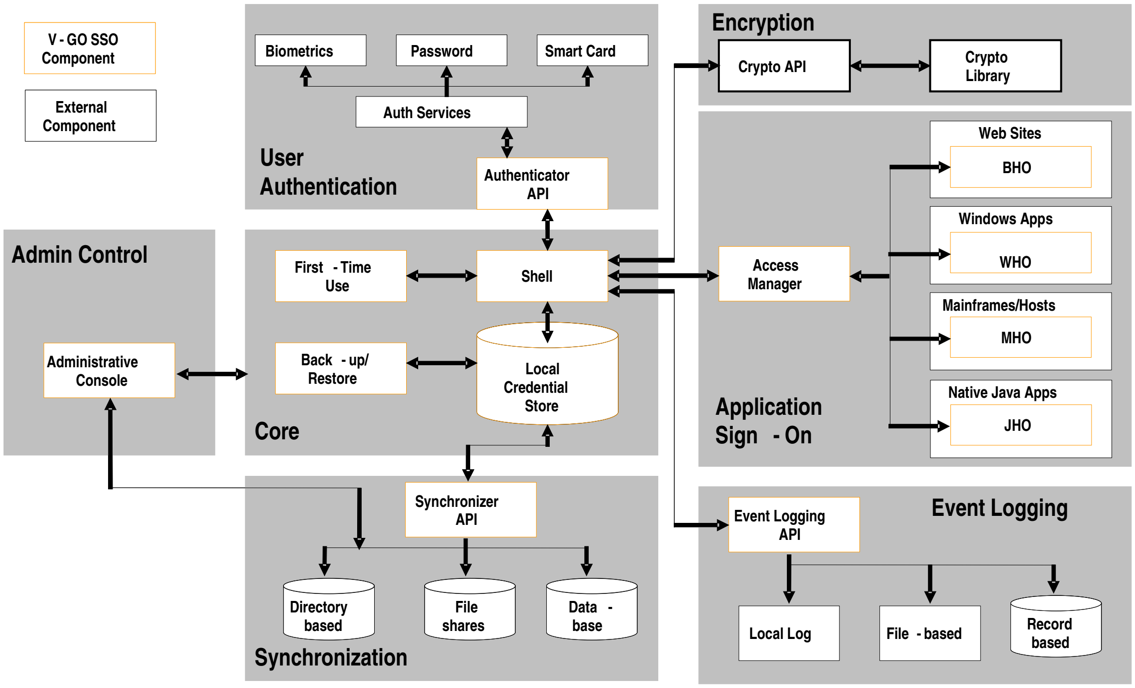

Figure 1 SSO Software Components

User authentication is the method used by the TOE, with support from the IT Environment, to validate users so they can gain access to v-GO SSO and logically behind it, applications and systems that require authentication. Each time that a user attempts a logon to the TOE, the user enters authentication information and the information is passed to an authentication service (configured by the administrator) in the IT Environment. The authentication service validates the credentials. If validated, it passes the validation to the Authenticator API within v-GO SSO. v-GO SSO ships with six authentication services:

Windows (Domain) Smart Card Logon (passphrase and certificate based), LDAP, Entrust PKI, and enhanced versions of the Windows and LDAP authenticators that support passphrase challenge. All of these authentication services are outside the TOE boundary and are in the IT environment.

Core
The Core connects all of v-GO SSO. It consists of the Local Credential Storage, v-GO Shell, First-Time Use, and Registration Wizard components.

- Local Credential Storage is an encrypted database containing all the user's credentials. Encryption is performed outside the TOE, using MS CAPI. Local Credential Storage is a Jet database file that includes user data and security attributes including each set of user credentials, user settings, and configuration information relevant to the user, i.e., authentication service(s).

- v-GO Shell receives user validation from the Authenticator API. It calls MS CAPI to encrypt data for and decrypt data from Local Credential Storage. It can then supply the credentials to the Application Sign-On Components in the IT Environment, notify the Event Logging API, and trigger Credential Synchronization as needed.

- The First-Time Use component calls MS CAPI to perform generation of user-specific keys and to gather security attributes from the user.

Encryption
MS CAPI Triple-DES or AES Encryption in the IT Environment secures user credentials in the v-GO SSO local data store. V-GO Shell requests that credentials be encrypted/decrypted by MS CAPI. By default, v-GO SSO uses the Triple-DES symmetric key encryption algorithm supplied by MS CAPI that is FIPS 140-2 certified. The administrator may specify MS CAPI AES encryption instead of Triple-DES during product installation.

V-GO SSO uses MS CAPI SHA-1 in the IT Environment to hash and verify user authentication information. Upon first-time use by an SSO user, v-GO SSO generates and maintains a cryptographically unique "primary authentication key" that is Authenticator independent and requires successful completion of the authentication process in order to be useable. Upon successful authentication, this key becomes available internally to v-GO and is then used to decrypt and access user credentials. Each credential is only decrypted on an as-needed basis and is never stored or cached in the clear.

MS CAPI in the IT Environment provides the Random Number Generation for generating the primary authentication key which is a symmetric key; the Intel Hardware RNG and RSA CSPs included in MS CAPI, selectable by the administrator at system install, are utilized.

Intelligent response and Application Sign-On
When an application presents a request for credentials, V-GO SSO detects this event, determines the appropriate action, and responds with the correct credentials. v-GO SSO detects requests for credentials in a variety of ways, depending on application type (Web, Windows, Mainframe/Host). v-GO SSO determines whether the event is a password change or logon request. If the dialog is a password-change dialog, v-GO SSO prompts the user to enter a new password. v-GO SSO then submits the old password (if required), new password, and new password again (if required) to the requesting client application.

If the event is a logon request v-GO SSO determines whether it has all necessary information or needs to request information from the user. If user credentials are not present, v-GO SSO prompts the user for credentials. When the user provides credentials to v-GO SSO, v-GO Shell stores the credentials in the Local Credential Storage. v-GO SSO Access Manager retrieves the credentials from the Local Credential Store and submits them to the client application. This intelligent response and application sign-on function is the single sign-on functionality that SSO performs.

Synchronization

While V-GO SSO stores user credentials and settings locally, it can synchronize the credentials and settings with remote network shares, directories, and devices in the IT Environment. The synchronization is triggered by a change to the Local Credential Storage or settings.

Event Logging

V-GO SSO can log all events, including credential use, credential changes, global credential events, v-GO SSO events, and v-GO SSO feature use. Event logging is also performed for all events associated with SSO add-on components included in the TOE. V-GO SSO can log the fields that administrators specify. V-GO SSO can log events locally or to any external destination through the Event Logging API.

Specifically, v-GO SSO can log:

- Credential use events: logons, manual password changes, automatic password changes;
- Credential changes: add credentials, delete credentials, change credentials, and copy credentials;
- Global credential events: backup, restore, synchronize;
- V-GO SSO events: startup and shutdown;
- V-GO SSO feature use, e.g., Logon Manager, Settings, Help, About; and,
- Modification of administrator-specified fields, e.g., Domain, Windows username, system username, Application name, Application username, event storage location.

Events can be logged to any desired destination, e.g., Local XML storage, SNMP service, Windows Event log, directory server, and Tivoli. For the evaluated configuration, events are logged to the Windows Event log.

Admin Control

Administrators are responsible for installing and maintaining the V-GO SSO system using the Admin Console. The Admin Console is accessible to Administrative users. The administrator console allows the administrator to control event logging, user authentication options, user access, and system configuration.

V-GO Authentication Manager (AM)

V-GO Authentication Manager is an add-on module to V-GO SSO. It enables organizations to seamlessly bridge strong authentication to all of their applications, including smart cards, biometrics and entrust authenticators. Users can employ different authenticators at different times and application access can be controlled based upon the authenticator used. V-GO AM adds three capabilities to V-GO SSO as follows.

- Strong authentication support from a variety of strong authenticators, including smart cards and biometric devices, for all authentication events: initial authentication, re-authentication and forced authentication.
- Multiple Authenticator support allows multiple logon methods to be used to authenticate an end-user and provides an authenticator that is capable of supporting graded authentication as well as alternative logon methods. This allows end-users the ability to mix and match multiple logon methods on-the-fly.
- Administrators can define “grades” or levels to authentication methods and to applications. This provides the ability to control what functions of V-GO AM users can execute based upon the type of authenticator presented.

V-GO Provisioning Manager (PM)

V-GO Provisioning Manager (PM) provides the ability for an administrator to automatically provision V-GO SSO with a user's ID and password by using a provisioning system. An administrator is able to add, modify and delete IDs and passwords for particular applications within the provisioning system and have the changes reflected in V-GO SSO. From the provisioning system, all usernames and passwords inside of V-GO SSO can also be deleted so that a user's access to all protected applications is eliminated. V-GO PM is installed as an add-on component to V-GO Single Sign-On (V-GO SSO).

V-GO Session Manager (SM)

V-GO Session Manager (SM) provides a solution that addresses the needs of traditional Single Sign-Off in a kiosk environment. V-GO SM has a client-side agent that suspends or closes inactive sessions and seamlessly shuts down all applications. This solution provides user identification to the kiosk by prompting users to login with a Windows password or any supported primary authenticator. V-GO SM has a client-side agent that suspends or closes inactive sessions and seamlessly shuts down all applications. V-GO SM is installed as an add-on component to V-GO Single Sign-On (V-GO SSO). V-GO SSO must be installed prior to installing V-GO SM. V-GO SSO automatically recognizes V-GO SM once it is installed.

V-GO Self Service Password Reset (SSPR)

V-GO Self Service Password Reset (SSPR) enables users to reset their own Windows domain passwords without the intervention of administrative or help-desk personnel. It provides end users with the ability to take a quiz comprised of a series of questions.

Each question is weighted with point-values. As the end user answers the quiz questions, V-GO SSPR keeps a running score**.** Points are added to the score for each correct response and points are deducted for each incorrect response. When the end user accumulates sufficient points to meet an administrator set "confidence level," V-GO SSPR permits the end user to select a new password. If the end user's score does not achieve the required confidence level after all questions have been presented, or if it falls below a preset negative value, the quiz ends and the end user is not permitted to reset the password. The reset service is available to each end user after completing a one-time enrollment interview to record passphrase answers.

SSPR allows a user to attempt a password reset three times. If on the third try the user is unsuccessful, the user is locked out of the TOE for 24 hours. Note that SSPR only allows password reset; once password reset has occurred, the user must login using the new password. SSPR operations including attempts to reset the password and password reset are logged.

TOE Environment

The intended environment of the TOE can be summarized as follows:

V-GO Single Sign-On (SSO)

SSO Client Agent

- Microsoft® Windows® 2000, XP, 2003 Server , Vista
- 100 MHz Pentium processor and 64 MB RAM
- Disk Space: ~2.5 MB for the installed program and data; a complete installation requires ~7 MB; ~25 MB available on hard disk for installer
- Internet Explorer 5.5 SP2 or higher with 128-bit encryption
- Citrix MetaFrame support requires MetaFrame 1.8 or higher
- Installation via MSI package requires Windows Installer 2.0

SSO Administrative Console & Server

- Microsoft® Windows® 2000, XP, 2003 Server, Vista
- 100 MHz Pentium-compatible processor and 64 MB RAM
- .NET Framework 1.0
- Windows Installer 2.0 or higher
- Disk Space: ~4 MB for MSI installer; ~31 MB for EXE installer, overall ~15 MB for the installed program and data
- Directory requirements Active Directory, Sun Java System Directory 5.1 or higher, Novell eDirectory 8.5 or higher, or other LDAP v2/v3 compliant directory

V-GO Authentication Manager (AM)

AM Client Agent

- Microsoft® Windows® 2000 (SP1+), XP (SP1 or SP2), Server 2003, Vista
- 120 MHz Pentium processor and 64 MB RAM
- Disk Space: a complete Installation requires ~1 MB
- Internet Explorer 6.0 or higher with 128-bit encryption
- Citrix MetaFrame support requires MetaFrame 1.8 or higher
- Installation via MSI package requires Windows Installer 2.0 or higher
- Strong authenticators likely have their own system requirements, which may differ from V-GO AM's requirements. Please refer to the strong authenticator's documentation to review the system requirements.

AM Administrative Console

- Microsoft® Windows® 2000 (SP1+), XP (SP1 or SP2), Server 2003, Vista
- 400 MHz Pentium 2 processor and 96 MB RAM
- .NET Framework 1.1
- Windows Installer 2.0 or higher
- Disk Space: a complete installation requires ~1 MB
- Directory requirements: Active Directory, Sun Java System Directory 5.1 or higher, Novell eDirectory 8.5 or higher, or other LDAP v2/v3 compliant directory

V-GO Provisioning Manager (PM)

PM Client Agent

- V-GO SSO 5.03
- Additional Disk Space: < 1 MB

PM Server

- Microsoft® Windows® 2000 Server, Windows Server 2003, Vista
- Microsoft Internet Information Server 5.x or 6.x (6.x recommended)
- Microsoft .NET Framework 1.1
- Microsoft Active Directory®, Microsoft ADAM, Sun One Directory
- Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine (MSDE 2000)
- Internet Explorer 6.0 or higher with 128-bit encryption
- Disk Space: a complete Installation requires ~3MB
- Pentium III class processor at 900MHz
- 512MB RAM

V-GO Session Manager

- Microsoft® Windows® 2000 (SP1+), Windows XP SP2, Windows Server 2003, Vista
- Microsoft .NET 1.1
- Internet Explorer 6.0 or higher with 128-bit encryption
- Pentium III 733 MHz
- 128 MB RAM
- ~ 3 MB disk space
- V-GO SSO 5.03

V-GO Self-Service Password Reset (SSPR)

General Access

- Windows 2000, Windows XP, Windows Server 2003, Vista
- Internet Explorer 5.5 SP2 or later

SSPR Server Requirements

- Windows 2000 Server, Windows Server 2003
- Microsoft Internet Information Server 5.0 or 6.0
- Microsoft .NET 1.1
- Microsoft Active Directory®, Microsoft ADAM, Microsoft SQL or Oracle® database

Physical Boundaries

The components that make up the TOE are:

- V-GO Single Sign-On (SSO) version 6.0,
- V-GO Authentication Manager (AM) version 6.0,
- V-GO Provisioning Manager (PM) version 6.0,
- V-GO Session Manager (SM) version 6.0, and
- V-G0 Self-Service Password Reset (SSPR) version 6.0.

The TOE depends on the following:

- Operating system: Microsoft® Windows® 2000 (SP1+), XP (SP1 or SP2), Server 2003, Vista to provide the OS platform for the TOE software.
- Virtual machines: Microsoft .NET Framework 1.1 to support the TOE software.
- Authentication servers: Any one of: Microsoft Windows Server 2000 SP4 or Microsoft Windows Server 2003 SP1 Active Directory; tokens that are interoperable with X9.9; RSA 5100, 5200, 6100 to perform user authentication or alternatively one of the directories listed in the next bullet (note that multiple authentication methods are supported by the TOE).
- Directory requirements: Active Directory, Sun Java System Directory 5.1 or higher, Novell eDirectory 8.5 or higher, or other LDAP v2/v3 compliant directory to perform user authentication or alternatively one of the authentication servers listed in the bullet above (note that multiple authentication methods are supported by the TOE).
- Web server: Microsoft Internet Information Services (IIS) 5.0 or 6.0 with ASP.NET installed to support TOE software.
- Web browser: Microsoft Internet Explorer 6.0 to support user and administrator access to the TOE.

Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit,
- Identification and authentication,
- Security management,
- Protection of the TSF, and
- TOE Access.

2.1.1.1Security audit

The TOE generates audit records for an unspecified level of audit. The operating system is relied on to provide reliable time stamps for use in audit records. Audit records are stored in the IT environment and can be reviewed in the IT Environment in audit file or databases selected by the administrator. Note that each of the components logs a separate set of events and that only events specified by the administrator during system installation or as configured by the administrator after installation are logged. The TOE can log events locally or to any external destination through the Event Logging API, however for the evaluated configuration the logged events are stored locally in the Windows Event Log

2.1.1.2User data protection

The TOE implements an access control policy that controls client application access to user credentials that are managed by the TOE. Windows, mainframe/host, and Web-based applications that are configured with the SSO component of the TOE may request user credentials. The TOE will provide the appropriate user credentials if the access control policy rules are met. The TOE exports user credentials in accordance with the access control policy to authorized applications when the TOE senses a request for credentials.

2.1.1.3Identification and authentication

The TOE maintains security attributes associated with each user including SSPR question responses associated with each user and keys associated with each user for encrypting and decrypting user credentials. In addition, the TOE stores user credentials encrypted using MS CAPI..

2.1.1.4Security management

The TOE provides security management functionality to allow the administrator to modify TOE behaviour and to initialize and modify user and TSF data. The TOE provides security management functionality through a set of MS Windows snap-ins to allow the administrator to modify TOE behavior. The SSO and SM components share an administrator GUI. The SSPR, PM, and AM components each have their own GUI administrator interface that is used to install and maintain the TOE component.

2.1.1.5Protection of the TSF

The TOE provides non-bypassability by restricting access to TOE functions through identification and authentication. Administrators and users cannot bypass TOE functions because they are required to log in before the requested operation is allowed

2.1.1.6TOE Access

The TOE provides the capability to terminate a session after an administrator configurable time if there is no session activity.

TOE Documentation

Passlogix offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6.2 for information about these and other documentation to meet Common Criteria requirements. TOE documentation includes the following:

- V-GO Single Sign-On Installation and Setup Guide, version 6.00
- V-GO Authentication Manager Installation and Setup Guide, version 6.0
- V-GO Provisioning Manager Installation and Setup Guide, version 6.0
- V-GO Session Manager Installation and Setup Guide, version 6.00
- V-GO Self-Service Password Reset Client Installation and Setup Guide, version 6.00
- V-GO Single Sign-On User Guide, version 6.00
- V-GO Authentication Manager User Guide, version 6.0
- V-GO Provisioning Manager Administrator Guide, version 6.00
- V-GO Session Manager Administrator Guide, version 6.00
- V-GO Session Manager Agent User Guide, version 6.00
- V-GO SSPR Management Console Guide, version 6.00

3.Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. The assets to be protected comprise the information stored, processed, or transmitted by the TOE. The term “information” is used here to refer to all data held or processed within the TOE, including data in transit between TOE components. It is assumed that an attacker is either an unauthorized user of the TOE, or an authorized user of the TOE who has been granted rights to access the information or resources held by the TOE.The threat agents are assumed to originate from a well-managed user community in a non-hostile working environment, and hence the product protects against threats of security vulnerabilities that might be exploited in the intended environment for the TOE. The TOE, in accordance with the strength of function claimed, protects against obvious breach of TOE security.

Threats

T.ACCOUNTABILITY A user may not be held accountable for their actions, *malicious or unintentional, that cause loss or misuse of application resources.*

T.ADMIN_ERROR An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.BAD_REQUEST A attacker may masquerade as an authorized client application in order to attempt to request and receive user credential information.

T.CRED_COMPROMISE An attacker may attempt to access stored user credential information stored by the TOE in order to gain unauthorized access to applications and potentially cause loss or misuse of application resources.

T.CRED_REQUEST An attacker may subvert TOE functions, causing the TOE to not provide authorized user credentials when requested by an authorized client application, thereby locking an authorized user out of the application.

T.IMPERSONATE An attacker may attempt to impersonate an authorized user in order to gain unauthorized access to protected application resources.

T.LOG_OUT A user may fail to log out of an application and walk away, allowing another person to have unauthorized access to the application.

T.TSF_COMPROMISE An attacker may access TSF data and modify or delete that data, causing the TOE to operate in an manner that is not secure.

Assumptions

A.LOCATE The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.NETWORK The IT Environment will protect network communication to and from the TOE from unauthorized disclosure or modification.

A.NO_EVIL The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation by administrators who are well trained and not hostile.

4.Security Objectives

This section summarizes the security objectives for the TOE and its environment.

Security Objectives for the TOE

O.AUDIT_GENERATION The TOE will provide the capability to create records of administrator selected security relevant events associated with users.

O.ACCESS The TOE will control access to user credential information so that only authorized client applications may receive user credentials.

O.CREDENTIAL The TOE will export authorized user credential information to authorized client applications when it detects a request for the user credentials.

O.LOG_OUT The TOE will log-out users after an administrator defined time period of inactivity to prevent access by unauthorized users.

O.MANAGE The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.RESET The TOE will provide a capability to allow users to safely reset that user’s own password without administrator assistance.

O.TOE_PROTECTION The TOE will ensure that its functions cannot be bypassed, i.e., the TOE will ensure that its security functions are invoked and succeed before any other function is allowed to proceed.

O.USER_AUTH_STORE The TOE will maintain user attributes and the attributes will be used to identify credentials for export to authorized client applications.

O.USER_IDENTIFICATION The TOE will uniquely identify users.

Security Objectives for the IT Environment

OE.ADMIN_ROLE The IT Environment will provide authorized administrator roles to isolate administrative actions.

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.AUDIT_REVIEW The IT Environment will provide the capability to view audit information.

OE.CRYPTO The IT Environment will provide cryptographic functionality to generate symmetric keys, perform symmetric encryption and decryption, and perform hashing to protect TOE TSF and user data.

OE.NETWORK The IT Environment will protect network communication to and from the TOE from unauthorized disclosure or modification.

OE.TIME_STAMPS The IT Environment will provide reliable time stamps for its own and for TOE use.

OE.USER_AUTHENTICATION The IT Environment will verify the claimed identity of users.

OE.USER_IDENTIFICATION The IT Environment will uniquely identify users.

OE.TOE_PROTECTION: The IT Environment will protect the TOE and its assets from external interference or tampering.

Security Objectives for the Non-IT Environment

OE.CONFIG The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and administrators will be competent, well trained, and not hostile.

OE.PHYCAL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

5.IT Security Requirements

This section defines the Common Criteria security functional requirements for the TOE and the IT Environment and the Common Criteria Assurance requirements for the TOE.

TOE Security Functional Requirements

The following table lists the Security Functional Requirements from Part 2 of the Common Criteria that have been identified for the Target of Evaluation. The requirement text is included below the table.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SEL.1: Selective audit
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
	FDP_ETC.1: Export of user data without security attributes
FIA: Identification and authentication	FIA_ATD.1a: User attribute definition (SSPR)
	FIA_UID.2a: User identification before any action
FMT: Security management	FMT_MOF.1a: Management of security functions behaviour
	FMT_MOF.1b: Management of security functions behaviour
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialisation
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management functions
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
FTA: TOE Access	FTA_SSL.3: TSF-initiated termination

Table 1 Security Functional Requirements for the TOE

Security audit (FAU)

5.1.1.1Audit data generation (FAU_GEN.1)

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) [**the following additional events as configured by the administrator:**

- **Credential use events: logons, manual password changes, automatic password changes**
- **Credential changes: add credentials, delete credentials, change credentials, copy credentials.**
- **Global credential events: backup, restore, synchronize.**
- **V-GO SSO events: startup and shutdown.**

- **V-GO SSO feature use, e.g., Logon Manager, Settings, Help, About.**
- **Modification of administrator-specified fields: Domain, Windows username, system username, Application name, Application username, event storage location.**
- **Authentication grade and type when a user authenticates (for V-GO AM only).**
- **Successful user logon events (including logon and logoff).**
- **Beginning of an SSPR enrollment session, cancellation of enrollment session, completion of enrollment session, success of password reset session, failure of password reset attempt, user lock-out due to too many failed password reset attempts.**

].

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, 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, **[no additional information]**.

5.1.1.2User identity association (FAU_GEN.2)

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [***event type***], b) [**no additional attributes**].

User data protection (FDP)

5.1.1.4Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**User Credential Access Control SFP**] on [**subjects: client applications; objects: user credentials; operations: requests for user credentials from client applications**].

5.1.1.5Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**User Credential Access Control SFP**] to objects based on the following: [

subjects: client applications with security attributes as follows -

- **For Windows-based client applications security attributes: application name, window name, the control ID of the input field.**
- **For mainframe/host-based client applications security attributes: window title, blocks of text at specific coordinates for Mainframe applications, username/password field text**
- **For web-based applications that are pop-up dialogs security attributes: realm and site.**
- **For web-based applications that are forms security attributes: URL, frame name, form name, specific blocks of text on the page, username/password field text, and password fields.**

Objects: user credentials with the security attributes Primary authentication key, authentication methods].

.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**the TOE will respond to client application requests for user credentials if the following is true for the type of client application making the request:**

- **For Windows-based client applications: the security attributes application name, window name, the control ID of the input field in the request match the security attributes in the applist.ini and entlist.ini files.**
- **For mainframe/host-based client applications: the security attributes window title, blocks of text at specific coordinates for Mainframe applications, username/password field text included in the request match the security attributes stored for the application in the entlist.ini file.**
- **For web-based applications that are pop-up dialogs: the security attributes realm and site included in the request match the security attributes stored for the application in the applist.ini and entlist.ini files.**
- **For web-based applications that are forms: the security attributes URL, frame name, form name, specific blocks of text on the page, username/password field text, and password fields included in the request match the security attributes stored for the application in the applist.ini and entlist.ini files.**

].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**no additional rules**].

5.1.1.6Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1 The TSF shall enforce the [**User Credential Access Control SFP**] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Identification and authentication (FIA)

5.1.1.7User attribute definition (FIA_ATD.1a) (SSPR)

FIA_ATD.1a.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user initialized responses to SSPR questions**].

Application note: FIA_ATD.1a defines the security attributes that SSPR maintains for each user. The security attributes are user defined unique responses to a set of SSPR questions. The responses are maintained, encrypted by MS CAPI with either 3DES or AES (as set by the

Administrator). SSPR will allow a user to authenticate with matching responses to the previously defined responses to the set of SSPR questions. The user is required to match the stored responses and once authenticated with the matching responses, is allowed to change the password for the user's primary authentication method stored by SSO. Note that not all SSO users may also use SSPR; SSPR must be initialized with user defined responses to the set of SSPR questions before SSPR will allow the user to authenticate and reset the password.

5.1.1.8User identification before any action (FIA_UID.2a)

FIA_UID.2a.1 The TSF shall require each user identify itself before allowing any other TSF-mediated actions on behalf of that user.

Security Management (FMT)

5.1.1.9Management of security functions behaviour (FMT_MOF.1a)

FMT_MOF.1a.1 The TSF shall restrict the ability to [***modify the behaviour of***] the functions [**default encryption algorithm for protecting user credentials (MS CAPI AES or 3DES), time interval for session termination through Session Manager Agent**] to [**Administrators**].

5.1.1.10Management of security functions behaviour (FMT_MOF.1b)

FMT_MOF.1b.1 The TSF shall restrict the ability to [***enable***] the functions [**SSPR enabled password reset**] to [**individual users who have initialized SSPR with responses to SSPR questions**].

Application Note: FMT_MOF.1b provides a security functional requirement for the initialization of SSPR responses by individual users. Individual users take an SSPR "quiz," providing specific responses to a set of pre-defined questions. The responses are stored by the TOE in encrypted form. The user may then perform an unassisted password reset if that user forgets the existing password by correctly answering SSPR questions.

5.1.1.11Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**User Credential Access Control SFP**] to restrict the ability to [***change_default, modify, delete***] the security attributes [

- **For Windows-based client applications security attributes: application name, window name, the control ID of the input field.**
- **For mainframe/host-based client applications security attributes: window title, blocks of text at specific coordinates for Mainframe applications, username/password field text**
- **For web-based applications that are pop-up dialogs security attributes: realm and site.**
- **For web-based applications that are forms security attributes: URL, frame name, form name, specific blocks of text on the page, username/password field text, and password fields.**

] to [**the administrator**].

5.1.1.12Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**User Credential Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.1.13Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify, delete***] the [**authentication methods, primary authentication user credentials**] to [**administrators**].

5.1.1.14Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**set user authentication methods, set the encryption algorithm used for protecting user credentials (MS CAPI 3DES or AES), set the time interval for session termination through Session Manager Agent, modify and delete user credentials for the primary authentication method, add, modify and delete IDs and passwords for particular applications through PM, and perform password reset through SSPR**].

Protection of the TSF (FPT)

5.1.1.15Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

TOE access (FTA)

5.1.1.16TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**administrator specified time interval**].

Security Functional Requirements for the IT Environment

The following table lists the Security Functional Requirements from Part 2 of the Common Criteria for the IT Environment. The requirement text is included below the table.

Requirement Class	Requirement Component
FAU: Security audit	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1a: Cryptographic operation (encrypt/decrypt)
	FCS_COP.1b: Cryptographic operation (hashing)

FIA: Identification and authentication	FIA_ATD.1b: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.2b: User identification before any action
FMT: Security management	FMT_MSA.2: Secure security attributes
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 2 Security Functional Requirements for the IT Environment

Security audit (SAR)

5.1.1.17Audit review (FAU_SAR.1)

FAU_SAR.1.1 The ~~TSF~~ **IT Environment** shall provide [**Administrators**] with the capability to read [**all audit information**] from the audit records.

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

5.1.1.18Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorized deletion.

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

Cryptographic support (FCS)

5.1.1.19Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The ~~TSF~~ **IT Environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**random number generator**] and specified cryptographic key sizes [**168 bits for 3DES or 256 bits for AES for the authentication key, 512 bits for the primary user key**] that meet the following: [**US FIPS-183, Appendix 3**].

5.1.1.20Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The ~~TSF~~ **IT Environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroize**] that meets the following: [**US FIPS 140-2 key zeroize requirement**].

5.1.1.21Cryptographic operation (FCS_CKM.1a) (symmetric encrypt/decrypt)

FCS_COP.1a.1 The ~~TSF~~ **IT Environment** perform [**encrypt and decrypt**] in accordance with a specified cryptographic algorithm [**3DES CBC mode or AES CBC mode as selected by the Administrator**] and cryptographic key sizes [**168 bits for 3DES and 256 bits for AES**] that meet the following: [**US FIPS-46-3 for 3DES and US FIPS-197 for AES**].

5.1.1.22Cryptographic operation (FCS_CKM.1b) (hashing)

FCS_COP.1b.1 The ~~TSF~~ **IT Environment** perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**not applicable**] that meet the following: [**US FIPS-180-2**].

Identification and authentication (FIA)

5.1.1.23User attribute definition (FIA_ATD.1b) (authenticators in the IT Environment)

FIA_ATD.1b.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: [**user credentials**].

Application note: FIA_ATD.1c defines the security attributes that the external authenticator(s) maintains for the use. The user credentials will vary, depending upon the authenticator.

5.1.1.24Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The ~~TSF~~ **IT Environment** shall allow [**password reset through SSPR password reset mechnism**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.25Multiple authentication mechanisms (FIA_UAU.5b)

FIA_UAU.5b.1 The ~~TSF~~ **IT Environment** shall provide [**one or more of the following authentication mechanisms:**

- **Windows password**
- **LDAP password**
- **Smart Card authenticator logon information**
- **Entrust authenticator logon information**
- **SAFLINK authenticator logon information**
- **DigitalPersona authenticator logon information**
- **Xyloc authenticator logon information**

] to support user authentication.

FIA_UAU.5b.2 The ~~TSF~~ **IT Environment** shall authenticate any user's claimed identity according to the [**primary logon method and other logon method(s) defined by the user and managed by the TOE**].

5.1.1.26User identification before any action (FIA_UID.2b)

FIA_UID.2b.1 The ~~TSF~~ **IT Environment** shall require each user identify itself before allowing any other TSF-mediated actions on behalf of that user.

Security management (FMT)

5.1.1.27Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The ~~TSF~~ **IT Environment** shall ensure that only secure values are accepted for security attributes.

5.1.1.28Security roles (FMT_SMR.1)

FMT_SMR.1.1 The ~~TSF~~ **IT Environment** shall maintain the roles [

- **Administrator**
- **User**

].

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

Protection of the TSF (FPT)

5.1.1.29Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The ~~TSF~~ **IT Environment** shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE **and the IT Environment**.

5.1.1.30TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own **and TOE** execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

5.1.1.31Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

TOE Security Assurance Requirements

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorisation controls
	ACM_SCP.1: TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security enforcing high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_FLR.1: Basic flaw remediation
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 TOE Security Assurance Requirements

Configuration management (ACM)

5.1.1.32Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.1.33TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.

ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

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

Delivery and operation (ADO)

5.1.1.34Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2d The developer shall use the delivery procedures.

ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

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

5.1.1.35Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

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

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Development (ADV)

5.1.1.36Informal functional specification (ADV_FSP.1)

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

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

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 TOE security functional requirements.

5.1.1.37Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.1.1.38Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

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

Guidance documents (AGD)

5.1.1.39Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

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

5.1.1.40User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

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

Life cycle support (ALC)

5.1.1.41Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

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

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.1.1.42Basic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1d The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

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

Tests (ATE)

5.1.1.43Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.1.44Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

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

5.1.1.45Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

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

5.1.1.46Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Vulnerability assessment (AVA)

5.1.1.47Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.

AVA_MSU.1.1c The guidance documentation 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.

AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

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

AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.1.1.48Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

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

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.1.1.49Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

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

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6.TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

TOE Security Functions

This section defines the security functions provided by the TOE and references the security functional requirements that are met by the security functions. In addition, at the end of this section a table is provided that maps particular components within the TOE to security functional requirements.

The TOE security functions are:

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

The subsections below define how the TOE performs each of these functions.

Security audit

The V-GO Sign-On Platform generates audit records by logging events as configured by the administrator. Each of the components logs a separate set of events and all events logged are stored by the IT Environment.

The V-GO Single Sign-on Platform can log all events, including credential use, credential changes, global credential events, TOE events, and TOE feature use. Only the events specified by the administrator during system installation or as configured by the administrator after installation are logged. The TOE can log events locally or to any external destination through the Event Logging API, however for the evaluated configuration the logged events are stored locally in the Windows Event Log.

Specifically, V-GO Sign-On Platform can log:

- Credential use events: logons, manual password changes, automatic password changes
- Credential changes: add credentials, delete credentials, change credentials, copy credentials.
- Global credential events: backup, restore, synchronize.
- V-GO SSO events: startup and shutdown.
- V-GO SSO feature use, e.g., Logon Manager, Settings, Help, About.
- Modification of administrator-specified fields: Domain, Windows username, system username, Application name, Application username, default encryption algorithm, event storage location.
- Authentication grade and type when a user authenticates (for V-GO AM only).
- Successful user logon events (including logon and logoff).

- Beginning of an SSPR enrollment session, cancellation of enrollment session, completion of enrollment session, success of password reset session, failure of password reset attempt, user lock-out due to too many failed password reset attempts.

Events can be logged to any desired destination, e.g., Local XML storage, SNMP service, Windows Event log, directory server, and Tivoli. For the evaluated configuration, events are logged locally to the Windows Event log in the IT Environment on the platform where the component is installed.

Within each audit record, the TOE records the date and time of the event (with the time provided by the OS in the IT Environment), type of event, subject identity, and the outcome (success or failure) of the event. The operating system is relied on to provide reliable time stamps for use in audit records. Audit records are stored in the IT environment and can be reviewed in the IT Environment in the Windows Event Log.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for an unspecified level of audit. The IT Environment is relied on to store audit records generated by the TOE.
- FAU_GEN.2: The TOE associates audit events with the user who caused the event.
- FAU_SEL.1: The TOE allows the administrator to select events that are audited during system installation and through the administrator interface to the TOE.

Note that the IT Environment meets the requirements of FAU_STG.1 by securely storing audit records and preventing unauthorized modifications to the audit records. The IT Environment also restricts access to audit records to administrators. A reliable timestamp is provided by the IT Environment for audit records, meeting FPT_STM.1.

User data protection

v-GO SSO performs user data protection when responding to client-side events, specifically, requests for user credentials. When an application presents a request for credentials, v-GO SSO detects this event, determines the appropriate action, and responds with the correct credentials. v-GO SSO responds to requests for user credentials slightly differently, depending on whether the request is from a Windows application, a Mainframe/Host application, or a Web Site. The user data protection function is described for each of these different types of requesting clients below.

Windows application client request

v-GO SSO responds to any and all requests for user credentials from Windows applications. All credential requests in Windows have the following attributes: application name, window name, and the control ID of the input field. v-GO SSO looks for the specific attributes of each application’s logon and password-change dialogs and responds accordingly. The attributes are stored in the basic **applist.ini** and administrative **entlist.ini** configuration files within v-GO SSO (See the v-GO SSO Administrative Console help system for additional information on these files).

The v-GO hook (**vgohook.dll**) component captures standard, OS-level Windows messages and sends them to the v-GO Shell and Access Manager components. When a specified application creates a dialog, v-GO SSO looks at the window title. If v-GO SSO recognizes the window title, it searches for the appropriate control ID(s).

v-GO SSO submits credentials to most Windows applications via secure, standard, OS-level Windows messages. Thus, keyboard-sniffing utilities cannot intercept the credentials. Furthermore, since v-GO SSO does not use scripts or keystrokes, users cannot confuse the response by selecting and working in another application.

Mainframe/Host applications

v-GO SSO responds to any and all requests for user credentials from Mainframe/Host applications.

All requests for credentials in Mainframe/Host applications have specific attributes: window title and various blocks of text (at specific coordinates for Mainframe applications), and username/password field text. v-GO SSO looks for the specific attributes of each application's logon and password-change screens and responds accordingly. The attributes are stored in the administrative **entlist.ini** configuration file (See the v-GO SSO Administrative Console help system for additional information on this file). The v-GO SSO Mainframe Helper Object monitors the Mainframe/Host, looking for the defined matches. When a new screen is presented, v-GO SSO reviews the text for matching fields. If all strings match, v-GO SSO uses the Mainframe Helper Object to submit user credentials.
v-GO SSO submits credentials via HLLAPI. Thus, keyboard-sniffing utilities cannot intercept these credentials. Furthermore, since v-GO SSO does not use scripts or keystrokes for these emulators, users cannot confuse the response by selecting and working in another application.

Web applications
v-GO SSO responds to any and all requests for user credentials from Web applications, whether in a form or via a pop-up dialog. All credential requests in Web applications are either in forms or in pop-up dialogs. The v-GO SSO Browser Helper Object (BHO) and Event Manager respond to the specific events of a web dialog popping up or of a web page rendering.
There is one BHO for Citrix/Terminal Services environments and another for standard Windows environments. Both BHOs detect events from the browser and are able to directly interact with the internals of the browser engine. The standard BHO also supports IE embedded within Lotus Notes. Since v-GO SSO does not use scripts or keystrokes for IE, users cannot confuse the response by selecting and working in another application.
v-GO SSO handles the two types of Web application credential requests similarly, as follows:
Pop-up dialogs have specific attributes: realm, and site. V-GO understands the specific attributes of each application's logon and password-change screens and responds accordingly. The attributes are stored in the basic **applist.ini** and administrative **entlist.ini** files. (Please refer to the v-GO SSO Administrative Console help system for additional information on these files). When a new pop-up dialog is created, v-GO reviews the dialog, requests credentials from v-GO Shell, then submits them to the pop-up dialog.
Forms have specific attributes: URL (including domain), frame name, form name, specific blocks of text on the page, and username/password field text, password fields (HTML <Input type=password>). v-GO SSO looks for the specific attributes of each application's logon and password-change screens and responds accordingly. The attributes are stored in the basic **applist.ini** and administrative **entlist.ini** files. (See the v-GO SSO Administrative Console help system for additional information on these files). When a new page is fully rendered, the BHO reviews the page for matching criteria. If at least a password field is present, the BHO requests credentials from v-GO Shell, then injects them into the browser.

The administrator is also responsible for initializing client application security attributes during the installation of client applications serviced by the SSO middleware. Administrators may change the default, modify, and delete the security attributes associated with client applications. The security attributes are configured during the initial configuration of the client application with SSO and may be modified or deleted by the administrator. The security attributes are:

- For Windows-based client applications security attributes: application name, window name, the control ID of the input field.
- For mainframe/host-based client applications security attributes: window title, blocks of text at specific coordinates for Mainframe applications, username/password field text
- For web-based applications that are pop-up dialogs security attributes: realm and site.
- For web-based applications that are forms security attributes: URL, frame name, form name, specific blocks of text on the page, username/password field text, and password fields.

The default upon SSO installation is that no client applications are configured for use with SSO. The administrator must specifically configure each application and its security attributes; the default values for the security attributes at system install is no installed client applications and therefore no security attributes.

Summary

SSO implements the User Credential Information Flow SFP to respond to client requests for user credentials. Depending upon the type of client, i.e., Windows, Mainframe/Host, or Web application, SSO checks the relevant security attributes within the request and if the attributes match those configured within the applist.ini and entlist.ini files, then SSO responds to the request with the user's credentials.

The User Data Protection function meets the following security functional requirements:

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1: The TOE implements the User Credential Access Control SFP to control access to user credentials by client applications.
- FDP_ACF.1: The TOE provides rules for client applications to access user credentials depending on the type of client application, i.e., Windows, Mainframe/host, or Web application. Credentials are passed to client applications if security attributes match attributes stored by the TOE.
- FDP_ETC.1: The TOE exports user credentials without security attributes to authorized applications requesting the credentials.
- FMT_MSA.1: The ability to change the default, modify, and delete the client application security attributes within the TOE is limited to the administrator. This supporting function is a security management function, but is critical to support the User data protection function.
- FMT_MSA.3: The TOE implements restrictive default values for security attributes so that no client application access is the default. The administrator may change default values. This supporting function is a security management function, but is critical to support the User data protection function.

Identification and authentication

The TOE SSO component supports identification and authentication of each user by the IT Environment before any other action may be performed by that user except password reset through SSPR. The user authenticates to an authenticator in IT Environment through the TOE SSO component, which passes user credentials from the user to the authenticator in the IT Environment. User credentials are stored encrypted using the Primary Authentication Key which is generated through MS CAPI in the IT Environment. Note that all cryptographic functions, including key generation, hashing, encryption and decryption is performed by the IT Environment using MS CAPI.

The TOE SSO may be configured to work with a number of different authenticators in the IT Environment. V-GO SSO uses MS CAPI cryptography in the IT Environment to securely store user credential data. Note that the IT Environment maintains user roles and identifies administrators to the TOE, i.e., to access the administrator interface, a user must be a Windows Administrator.

SSPR allows the user to reset their password without supplying their existing password by correctly answering a set of questions set up by the user previously. The user is allowed three tries to reset the password through SSPR. With three unsuccessful tries, SSPR causes the user to be locked out of the TOE for 24 hours. The number of correctly answered questions must meet an administrator controlled confidence level. SSPR questions and correct user responses are stored in the IT environment encrypted by MS CAPI by the TOE.

Summary

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1a: The TOE SSPR component maintains security attributes associated with each user, specifically answers to questions set up by the user previously.
- FIA_UID.2a: The TOE identifies users before allowing any other actions on the part of that user.

Note that the IT Environment maintains user attributes, provides multiple authentication mechanisms, and performs user authentication and identification before any action except password reset through SSPR.

Security management

The TOE provides security management functionality through a set of MS Windows snap-ins to allow the administrator to modify TOE behavior. The SSO and SM components share an administrator GUI. The SSPR, PM, and AM components each have their own GUI administrator interface that is used to install and maintain the TOE component. The administrator role is defined through MS Windows and only Windows administrators with appropriate privileges as configured at installation are allowed access to the TOE component administrator interfaces.

The TOE administrator interface allows administrators to:

- Set user authentication methods,
- Set the encryption algorithm used for TSF data transfer (MS CAPI 3DES or AES),
- Set the time interval in seconds for session termination through Session Manager Agent,
- Modify and delete user IDs and passwords for particular applications within a provisioning system through PM,
- Set a confidence level for user reset of password through SSPR.

The administrator is also responsible for initializing client application security attributes during the installation of client applications serviced by the SSO middleware. This functionality is described as part of the User data protection security function, above, where the security management functions directly support the access control SFP implemented by the SSO component of the TOE.

The user may enable the ability to perform an unassisted password reset when that user has forgotten his or her password by responding to a set of questions for SSPR. SSPR allows the user to reset their password without supplying their existing password by correctly answering a set of questions set up by the user through this enabling function, i.e., entering responses into the SSPR "quiz."

The Security Management function is designed the following security functional requirements:

- FMT_MOF.1a: The TOE restricts the ability to modify the behavior of the TOE, including modifying the default encryption algorithm for TSF Data, and modifying the time interval for session termination through the SM component.
- FMT_MOF.1b: The TOE allows users to enable the SSPR password reset capability for that user's individual login account by providing the capability for the user to give responses to a pre-defined set of questions.
- FMT_MSA.1: Which is a security management function that provides support for the User data protection function; the TOE enforces the User Credential Access Control SFP by restricting the ability to change the default, modify, and delete security attributes of client applications to the administrator.
- FMT_MSA.3: Which is a security management function that provides support for the User data protection function; the default is for the TOE to have no client applications; the administrator must configure client applications and their security attributes, therefore the TOE provides restrictive default values for the security attributes.

- FMT_MTD.1: The TOE restricts the ability to modify and delete authentication methods, user IDs and passwords for particular applications within a provisioning system to administrators.
- FMT_SMF.1: The TOE provides security management functions as defined above.

Note that the administrator role is determined and controlled by the IT Environment, i.e., MS Windows administrators with appropriate privileges.

Protection of the TSF

The TOE provides non-bypassability of the TSP by restricting access to TOE functions through identification and authentication.
The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: Administrators and users cannot bypass TOE functions because they are required to log in before the requested operation is allowed.

Note that the IT Environment is relied upon to maintain a security domain for its own execution as welll as protection of the TOE from interference and tampering by untrusted subjects. Both the TOE and the underlying operating system operate in their own space. The IT environment also provides reliable time stamp to support auditing. The IT Environment meets FPT_SEP.1, FPT_ITT.1, and FPT_STM.1.

TOE Access

The TOE provides the capability to terminate a session after an administrator configurable time interval through SM and can deny user access when the user attempts a password reset through SSPR and fails to answer sufficient predefined questions correctly to meet the administrator defined confidence level.

The TOE monitors login sessions and if a session is inactive for more than an administrator configured time period (defined by the administrator in seconds), then the TOE suspends or closes the inactive session and shuts down any active applications, as configured by the administrator.

The TOE Access function is designed to meet the following security functional requirements;

- FTA_SSL.3: The TOE shuts down an inactive user login session after an administrator defined time has passed.

TOE Security Assurance Measures

Configuration management

The configuration management measures applied by Passlogix ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Passlogix ensures changes to the implementation representation are controlled. Passlogix performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- Passlogix – Configuration Management Plan
- Passlogix QA/QC Policies and Procedures, 5/01/01

The Configuration management assurance measure satisfies the following EAL 3 assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

Delivery and operation

Passlogix provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Passlogix's delivery procedures describe all applicable procedures to be used to prevent inappropriate access to the TOE. Passlogix also provides documentation that describes the steps necessary to install Passlogix in accordance with the evaluated configuration.

These activities are documented in:

- V-GO Single Sign-On Installation and Setup Guide, version 6.00
- V-GO Authentication Manager Installation and Setup Guide, version 6.0
- V-GO Provisioning Manager Installation and Setup Guide, version 6.0
- V-GO Session Manager Installation and Setup Guide, version 6.00
- V-GO Self-Service Password Reset Client Installation and Setup Guide, version 6.00

The Delivery and operation assurance measure satisfies the following EAL 3 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

Development

Passlogix has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- Passlogix - Functional Specification
- Passlogix - High-level Design
- Passlogix - Design Correspondence Analysis

The Development assurance measure satisfies the following EAL 3 assurance requirements:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

Guidance documents

Passlogix provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- V-GO Single Sign-On User Guide, version 6.00
- V-GO Authentication Manager User Guide, version 6.0
- V-GO Provisioning Manager Administrator Guide, version 6.00
- V-GO Session Manager Administrator Guide, version 6.00
- V-GO Session Manager Agent User Guide, version 6.00
- V-GO SSPR Management Console Guide, version 6.00

The Guidance documents assurance measure satisfies the following EAL 3 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

Life cycle support

Passlogix ensures the adequacy of the procedures used during the development and maintenance of the TOE through its life-cycle. Passlogix includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. In addition, Passlogix identifies and tracks reported flaws, ensuring that they are addressed and corrections and corrective measures are made available as applicable.

These activities are documented in:

- Passlogix - Life-cycle Plan

The Life cycle support assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_DVS.1
- ALC_FLR.1

Tests

Passlogix has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. Passlogix has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- Passlogix - Test Plan
- Passlogix - Test Coverage Analysis
- Passlogix - Test Results

The Tests assurance measure satisfies the following EAL 3 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. Furthermore, Passlogix has conducted a misuse analysis demonstrating that the provided guidance is complete.

Passlogix has conducted a SOF analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the SOF claim: SOF-Basic. . A description of this and attack potential is included in sections 8.3 and 8.4; please see those sections for more information.

Passlogix performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Passlogix - Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL 3 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7.Protection Profile Claims

There is no protection profile claim.

8.Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies; and
- TOE Summary Specification.

Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats and usage assumptions by the security objectives.

	O.AUDIT_GENERATION	O.ACCESS	O.CREDENTIAL	O.LOG_OUT	O.MANAGE	O.RESET	O.TOE_PROTECTION	O.USER_AUTH_STORE	O.USER_IDENTIFICATION	OE.ADMIN_ROLE	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.CRYPTO	OE.NETWORK	OE.TIME_STAMPS	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TOE_PROTECTION	OE.CONFIG	OE.PHYCAL
T.ACCOUNTABILITY	X										X	X			X					
T.ADMIN_ERROR					X					X										
T.BAD_REQUEST		X			X	X														
T.CRED_COMPROMISE						X		X					X							
T.CRED_REQUEST			X					X												
T.IMPERSONATE								X	X							X	X			
T.LOG_OUT				X																
T.TSF_COMPROMISE							X											X		
A.LOCATE																				X
A.NETWORK														X						
A.NO_EVIL																			X	

Table 4 Threat to Objective Mapping

8.1.1.1T.ACCOUNTABILITY

A user may not be held accountable for their actions, malicious or unintentional, that cause loss or misuse of application resources.

This Threat is countered by ensuring that:

- O.AUDIT_GENERATION: The TOE will provide the capability create records of administrator selected security relevant events associated with users.
- OE.AUDIT_PROTECTION: The IT Environment will provide the capability to protect audit information.
- OE.AUDIT_REVIEW: The IT Environment will provide the capability to view audit information.
- OE.TIME_STAMPS: The IT Environment will provide reliable time stamps for its own and TOE use.

8.1.1.2T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is countered by ensuring that:

- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
- OE.ADMIN_ROLE: The TOE will provide authorized administrator roles to isolate administrative actions.

8.1.1.3T.BAD_REQUEST

An attacker may masquerade as an authorized client application in order to attempt to request and receive user credential information.

This Threat is countered by ensuring that:

- O.ACCESS: The TOE will control access to user credential information so that only authorized client applications may receive credentials.
- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that ony authorized administrators are able to access such functionality.
- O.RESET: The TOE will provide a capability to allow users to safely reset that user’s own password without administrator assistance.

8.1.1.4T.CRED_COMPROMISE

An attacker may attempt to access stored user credential information stored by the TOE in order to gain unauthorized access to applications and potentially cause loss or misuse of application resources.

This Threat is countered by:

- O.USER_AUTH_STORE: The TOE will maintain user credentials and attributes and the attributes will be used to identify credentials for export to authorized client applications.
- O.RESET: The TOE will provide a capability to allow users to safely reset that user's own password without administrator assistance.
- OE.CRYPTO: The IT Environment will provide cryptographic functionality to generate symmetric keys, perform symmetric encryption and decryption, and perform hashing to protect TOE TSF and user data.

8.1.1.5T.CRED_REQUEST

An attacker may subvert TOE functions, causing the TOE to not provide authorized user credentials when requested by an authorized client application, thereby locking an authorized user out of the application.

This threat is countered by:

- O.USER_AUTH_STORE: The TOE will maintain user credentials and attributes and the attributes will be used to identify credentials for export to authorized client applications
- O.CREDENTIAL: The TOE will export authorized user credential information to authorized client applications when it detects a request for the user credentials

8.1.1.6T.IMPERSONATE

An attacker may attempt to impersonate an authorized user in order to gain unauthorized access to protected application resources.

This Threat is countered by ensuring that:

- O.USER_AUTH_STORE: The TOE will maintain user attributes and the attributes will be used to identify credentials for export to authorized client applications.
- O.USER_IDENTIFICATION: The TOE will uniquely identify users.
- OE.USER_AUTHENTICATION: The IT Environment will verify the claimed identity of users.
- OE.USER_IDENTIFICATION: The IT Environment will uniquely identify users.

8.1.1.7T.LOG_OUT

A user may fail to log out of an application and walk away, allowing another person to have unauthorized access to the application..

This Threat is countered by ensuring that:

- O.LOG_OUT: The TOE will log-out users after an administrator defined time period of inactivity to prevent access by unauthorized users

8.1.1.8T.TSF_COMPROMISE

An attacker may access TSF data and modify or delete that data, causing the TOE to operate in an manner that is not secure..

This Threat is countered by ensuring that:

- O.TOE_PROTECTION: The TOE will ensure that its functions cannot be bypassed, i.e., the TOE will ensure that its security functions are invoked and succeed before any other function is allowed to proceed.
- OE.TOE_PROTECTION: The IT Environment will protect the TOE and its assets from external interference or tampering.

8.1.1.9A.LOCATE

The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

8.1.1.10A.NETWORK

The IT Environment will protect network communication to and from the TOE from unauthorized disclosure or modification.

This Assumption is satisfied by ensuring that:

- OE.NETWORK: The IT Environment will protect network communication to and from the TOE from unauthorized disclosure or modification.

8.1.1.11A. NO_EVIL

The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation by administrators who are well trained and not hostile.

This Assumption is satisfied by ensuring that:

- OE.CONFIG: The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation by administrators who are competent, well trained and not hostile.

Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target.

Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy. Note that the table below indicates the requirements that effectively satisfy the individual objectives. Rationale for each objective is provided following the table.

	O.AUDIT_GNEERATION	O.ACCESS	O.CREDENTIAL	O.LOG_OUT	O.MANAGE	O.RESET	O.TOE_PROTECTION	O.USER_AUTH_STORE	O.USER_IDENTIFICATION	OE.ADMIN_ROLE	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.CRYPTO	OE.TIME_STAMPS	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TOE_PROTECTION
FAU_GEN.1	X																
FAU_GEN.2	X																
FAU_SEL.1	X																
FAU_SAR.1												X					
FAU_STG.1											X						
FCS_CKM.1													X				
FCS_CKM.4													X				
FCS_COP.1a													X				
FCS_COP.1b													X				
FDP_ACC.1		X															
FDP_ACF.1		X															
FDP_ETC.1			X														
FIA_ATD.1a								X									
FIA_ATD.1b															X		
FIA_UAU.1															X		
FIA_UAU.5															X		
FIA_UID.2a									X								
FIA_UID.2b																X	
FMT_MOF.1a					X												
FMT_MOF.1b						X											
FMT_MSA.1		X			X												
FMT_MSA.2													X				
FMT_MSA.3		X			X												
FMT_MTD.1					X												
FMT_SMF.1					X	X											
FMT_SMR.1										X							
FPT_RVM.1							X										
FTA_SSL.3				X													
FPT_ITT.1																	X
FPT_SEP.1																	X
FPT_STM.1														X			

Table 5 Objective to Requirement Correspondence

8.1.1.12O.AUDIT_GENERATION

The TOE will provide the capability create records of administrator selected security relevant events associated with users.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE generates audit events for an unspecified level of audit.
- FAU_GEN.2: The TOE will identify users who caused the auditable event.
- FAU_SEL.1: The TOE will allow the administrator to select events to be audited.

8.1.1.13O.ACCESS

The TOE will control access to user credential information so that only authorized client applications may receive user credentials.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: The TOE implements a User Credential Access Control SFP that controls client application access to user credentials.
- FAU_ACF.1: The TOE implements a User Credential Access Control SFP that defines rules for client access to user credentials where defined security attributes must match those configured within the TOE.
- FMT_MSA.1: The ability to change the default, modify, and delete the client application security attributes within the TOE is limited to the administrator.
- FMT_MSA.3: The TOE implements restrictive default values for security attributes so that no client application access is the default. The administrator may change default values.

8.1.1.14O.CREDENTIAL

The TOE will export authorized user credential information to authorized client applications when it detects a request for the user credentials.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ETC.1: The TOE will export user credentials in accordance with the User Credential Access Control SFP. The user credentials will be exported without security attributes.

8.1.1.15O.LOG_OUT

The TOE will log-out users after an administrator defined time period of inactivity to prevent access by unauthorized users.

This TOE Security Objective is satisfied by ensuring that:

- FTA_SSL.3: The TOE will terminate a user session after an administrator specified period of inactivity.

8.1.1.16O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1a: The TOE restricts the ability to modify the behavior of the TOE, including modifying the default encryption algorithm protecting user credentials, modifying the time interval for session termination through the SM component, and modifying the default confidence level in SSPR, to the administrator.
- FMT_MSA.1: The ability to change the default, modify, and delete the client application security attributes within the TOE is limited to the administrator.
- FMT_MSA.3: The TOE implements restrictive default values for security attributes so that no client application access is the default. The administrator may change default values.
- FMT_MTD.1: The TOE restricts the ability to modify and delete authentication methods, user IDs and passwords for particular applications within a provisioning system to administrators.
- FMT_SMR.1: The TOE provides security management functions to set user authentication methods, set the encryption algorithm used for protecting user credentials (MS CAPI 3DES or AES), set the time interval for session termination through Session Manager Agent, modify and delete user IDs and passwords for particular applications within a provisioning system, set a confidence level for user reset of password through SSPR.

8.1.1.17O.RESET

The TOE will provide a capability to allow users to safely reset that user's own password without administrator assistance.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1b: The TOE will allow a user to enable the unassisted password reset function by providing responses to an SSPR quiz..
- FMT_SMF.1: The TOE provides security management functions to allow users to set up unassisted password reset for that user's own login account through SSPR.

8.1.1.18O.TOE_PROTECTION

The TOE will ensure that its functions cannot be bypassed, i.e., the TOE will ensure that its security functions are invoked and succeed before any other function is allowed to proceed.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: Administrators and users cannot bypass TOE functions because they are required to log in before the requested operation is allowed.

8.1.1.19O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_UID.2a: All users must be identified before any other action is allowed.

8.1.1.20O.USER_AUTH_STORE

The TOE will maintain user attributes and the attributes will be used to identify credentials for export to authorized client applications.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1a: The TOE maintains security attributes associated with users within the SSPR component.

8.1.1.21OE.ADMIN_ROLE

The IT Environment will provide authorized administrator roles to isolate administrative actions.

This Security Objective is satisfied by ensuring that:

FMT_SMR.1: The IT Environment maintains administrative roles.

8.1.1.22OE.AUDIT_PROTECTION

The IT Environment will provide the capability to protect audit information.

This Security Objective is satisfied by ensuring that:

- FAU_STG.1: IT Environment is relied on to store audit records generated by the TOE.

8.1.1.23OE.AUDIT_REVIEW

The IT Environment will provide the capability to view audit information.

This Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The IT Environment is also relied on to provide interfaces to read from the audit trail.

8.1.1.24OE.CRYPTO

The IT Environment will provide cryptographic functionality to generated symmetric keys, perform symmetric encryption and decryption, and perform hashing to protect TOE TSF and user data..

This Security Objective is satisfied by ensuring that:

- FCS_CKM.1: The IT Environment will generate cryptographic symmetric keys through its random number generator.
- FCS_CKM.4: The IT Environment will destroy cryptographic keys through zeroization.
- FCS_COP.1, iterations a and b: The IT Environment will provide symmetric encryption and decryption and hashing cryptographic functions.
- FMT_MSA.2: The IT Environment will ensure that only secure security values are accepted to support cryptographic functions.

8.1.1.25OE.TIME_STAMPS

The IT Environment will provide reliable time stamps for its own and for TOE use.

This Security Objective is satisfied by ensuring that:

- FPT_STM.1: The IT Environment provides time stamps for its own and for TOE use.

8.1.1.26OE.USER_AUTHENTICATION

The IT Environment will verify the claimed identity of users.

This Security Objective is satisfied by ensuring that:

- FIA_ATD.1b: The IT Environment maintains security attributes associated with users. The user credentials are dependent upon the authentication mechanism.
- FIA_UAU.1: The IT Environment offers no TSF-mediated functions until the user is authenticated except password reset through SSPR.
- FIA_UAU.5: The IT environment will provide multiple authentication methods to support the TOE authentication mechanism.

8.1.1.27OE.USER_IDENTIFICATION

The IT Environment will uniquely identify users.

This Security Objective is satisfied by ensuring that:

- FIA_UID.2.b: The IT Environment offers no TSF-mediated functions until the user is identified.

8.1.1.28OE.TOE_PROTECTION

The IT Environment will protect the TOE and its assets from external interference or tampering.

This Security Objective is satisfied by ensuring that:

- FPT_ITT.1: The IT Environment will ensure that TOE data is protected from disclosure and modification when it is transmitted between separate parts of the TOE and the IT Environment.
- FPT_SEP.1: The IT Environment will maintain a security domain for its own and TOE execution through the Windows operating system (OS). The OS will enforce separation of the security domains of the TOE and any other processes.

Security Assurance Requirements Rationale

EAL3 augmented was selected as the assurance level because the TOE is a commercial product whose users require a moderate to high level of independently assured security. The TOE is intended to provide a reasonable level of protection comparable to the protection provided by most commercial-off-the-shelf products. This is reflected in the definition of the TOE environment in chapter 2 and the security objectives for the TOE in chapter 4 of this ST.

The assurance level EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

ALC_FLR.1 was selected to exceed EAL3 assurance objectives in order to ensure that identified flaws are addressed. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. The attack potential is considered to be low, since users will have public knowledge of the TOE and have no access to the TOE except through identification and authentication mechanisms in the IT Environment and through SSPR for password reset. Analysis of the IT Environment security measures is outside the scope of the ST and the attack potential for SSPR is low since users are locked out for 24 hours after three failed attempts to change a password. As such, EAL3 and SOF Basic are appropriate for the environment in which the TOE will be installed and used.

Strength of Functions Rationale

The security target includes a probabilistic or permutational function of password reset assisted by SSPR. The list of relevant security functions and security functional requirements includes:

- Security Management
  - FMT_MOF.1b
  - FMT_SMF.1

The security functional requirement FMT_MOF.1b, with support from FMT_SMF.1 is met by the by the v-G0 Self-Service Password Reset (SSPR) subsystem in conjunction with authentication mechanisms in the IT Environment. SOF analysis is provided for the SSPR password reset function at SOF-Basic. The TOE must protect against obvious vulnerabilities, and SOF-Basic is appropriate for this level of protection.

Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2 (hierarchical to FIA_UID.1)
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	FAU_GEN.1 and FMT_MTD.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA2	FCS_CKM.1, FMT_MSA.2
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_ETC.1	FDP_ACC.1	FDP_ACC.1
FIA_ATD.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	none
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_MTD.1	FMT_SMR.1 and FMT_MTD.1
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	FDP_ACC.1, FMT_SMR.1, FMT_MSA.1, ADV_SPM.1	FDP_ACC.1, FMT_SMR.1, FMT_MSA.1, see rationale below for not including ADV_SPM.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2

FPT_ITT.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
FTA_SSL.3	none	none
ACM_CAP.3	ALC_DVS.1	ALC_DVS.1
ACM_SCP.1	ACM_CAP.3	ACM_CAP.3
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_DVS.1	none	none
ALC_FLR.2	none	none
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.2 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_MSU.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.2
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.2 and AGD_ADM.1 and AGD_USR.1

Table 6 Requirement Dependency Analysis

Assurance requirement ADV_SPM.1 is a dependency to FMT_MSA.2, related to the cryptographic support (FCS) requirements included in the ST. The rationale for not including this dependency in the ST is CC Part 2 paragraph 1020 states that if the developer provided a clear definition of the secure values and the reason why they should be considered secure, the dependency from FMT_MSA.2 Secure security attributes to ADV_SPM.1 Informal TOE security policy model can be argued away. In the case of this TOE, there are no secure security values entered into the TOE; the IT Environment generates symmetric keys using a random number generator and destroys keys by zeorizing the generated key. No values are entered by the administrator, therefore this requirement is not applicable.

Explicitly Stated Requirements Rationale

There are no explicitly stated requirements.

TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The table below demonstrates the relationship between security requirements and security functions.

	Security audit	User data protection	authentication Identification and	Security management	Protection of the TSF	TOE Access
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SEL.1	X					
FDP_ACC.1		X				
FDP_ACF.1		X				
FIA_ATD.1a			X			
FIA_UID.2a			X			
FMT_MOF.1a				X		
FMT_MOF.1b						
FMT_MSA.1		X		X		
FMT_MSA.3		X		X		
FMT_MTD.1				X		
FMT_SMF.1				X		
FPT_RVM.1					X	
FTA_SSL.3						X

Table 7 Security Functions vs. Requirements Mapping

PP Claims Rationale

See Section 7, Protection Profile Claims.