

Persona 5.0 Security Target



ST Version 1.0
December 31, 2002

Prepared for:

Esker, Inc.
465 Science Drive
P.O. Box 44953
Madison, WI 53744-4953

Prepared By:



7125 Gateway Drive
Columbia, MD 21046

Table of Contents

<u>1.</u>	<u>SECURITY TARGET INTRODUCTION</u>	1
<u>1.1</u>	<u>Security Target, TOE and CC Identification</u>	1
<u>1.2</u>	<u>CC Conformance Claims</u>	1
<u>1.3</u>	<u>Strength of Environment</u>	1
<u>1.4</u>	<u>Conventions, Terminology, Acronyms</u>	1
<u>1.4.1</u>	<u>Conventions</u>	1
<u>1.4.2</u>	<u>Terminology</u>	2
<u>1.4.3</u>	<u>Acronyms</u>	2
<u>1.5</u>	<u>Security Target Overview and Organization</u>	2
<u>2.</u>	<u>TOE DESCRIPTION</u>	3
<u>2.1</u>	<u>Product Type</u>	3
<u>2.2</u>	<u>Product Description</u>	3
<u>2.3</u>	<u>Security Functions</u>	3
<u>2.4</u>	<u>TOE Boundary</u>	3
<u>2.4.1</u>	<u>Physical Boundaries</u>	4
<u>2.4.2</u>	<u>Logical Boundaries</u>	4
<u>3.</u>	<u>SECURITY ENVIRONMENT</u>	8
<u>3.1</u>	<u>Threats to Security</u>	8
<u>3.2</u>	<u>Organization Security Policies</u>	9
<u>3.3</u>	<u>Secure Usage Assumptions</u>	9
<u>3.3.1</u>	<u>Personnel Assumptions</u>	9
<u>3.3.2</u>	<u>Physical Assumptions</u>	9
<u>3.3.3</u>	<u>Underlying System Assumptions</u>	9
<u>4.</u>	<u>SECURITY OBJECTIVES</u>	11
<u>4.1</u>	<u>Security Objectives for the TOE</u>	11
<u>4.2</u>	<u>Security Objectives for the Environment</u>	11
<u>4.2.1</u>	<u>Non-IT security objectives for the environment</u>	11
<u>4.2.2</u>	<u>IT security objectives for the environment</u>	12
<u>5.</u>	<u>IT SECURITY REQUIREMENTS</u>	13
<u>5.1</u>	<u>TOE Security Functional Requirements</u>	13
<u>5.1.1</u>	<u>Cryptographic support (FCS)</u>	13

5.1.2	User Data Protection (FDP)	13
5.1.3	Identification and authentication (FIA)	14
5.1.4	Security management (FMT)	14
5.1.5	Protection of the TSF (FPT)	14
5.1.6	Trusted Path/Channels (FTP)	15
5.2	Security Functional Requirements for the IT Environment	15
5.2.1	User Data Protection (FDP)	15
5.2.2	Identification and authentication (FIA)	16
5.2.3	Security management (FMT)	16
5.2.4	Protection of the TSF (FPT)	17
5.3	TOE Security Assurance Requirements	17
5.3.1	Configuration Management (ACM)	18
5.3.2	Delivery and Operation (ADO)	19
5.3.3	Development (ADV)	19
5.3.4	Guidance Documents (AGD)	20
5.3.5	Life Cycle Support (ALC)	22
5.3.6	Security Testing (ATE)	22
5.3.7	Vulnerability Assessment (VLA)	23
6.	TOE SUMMARY SPECIFICATION	25
6.1	TOE Security Functions	25
6.1.1	Cryptographic Support	25
6.1.2	Identification and Authentication	25
6.1.3	Information Flow Control	25
6.1.4	Security Management	26
6.1.5	Protection of the TSF	26
6.2	TOE Security Assurance Measures	26
6.2.1	6.2.1 Process Assurance	27
6.2.2	Delivery and Guidance	27
6.2.3	Design Documentation	27
6.2.4	Tests	27
6.2.5	Vulnerability Assessment	28
7.	PROTECTION PROFILE CLAIMS	28
8.	RATIONALE	29
8.1	Security Objectives Rationale	29
8.2	Security Requirements Rationale	34
8.2.1	Security Functional Requirements Rationale	34
8.2.2	Security Functional Requirements for the IT Environment Rationale	36
8.2.3	Security Assurance Requirements Rationale	37
8.2.4	Requirement Dependency Rationale	37
8.2.5	Explicitly Stated Requirements Rationale	38
8.2.6	Internal Consistency Rationale	39
8.2.7	Strength of Function Rationale	39
8.2.8	Security Functional Requirements Rationale	39

<u>9.</u>	<u>GLOSSARY OF TERMS</u>	42
<u>10.</u>	<u>ACRONYMS</u>	43

1. Security Target Introduction

This section presents the following information:

- Identifies the Security Target (ST) and Target of Evaluation (TOE);
- Specifies the ST conventions and ST conformance claims; and
- Describes the ST organization.

1.1 Security Target, TOE and CC Identification

ST Title – Esker Persona 5.0 Security Target

ST Version – Version 1.0

ST Date – December 31, 2002

TOE Identification – Esker Persona 5.0

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

Keywords – Esker, Persona, security target, Persona Toolbox, EAL3, Terminal Emulation, Remote Access

1.2 CC Conformance Claims

This TOE conforms to the following specifications:

Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.

- Part 2 conformant

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.

- Part 3 conformant

1.3 Strength of Environment

The TOE has been developed for an environment with a moderate level of risk to identified assets. The assurance requirements of EAL3 and the minimum strength of function of *SOF-medium* were chosen to be consistent with that level of risk.

1.4 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.4.1 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.
- 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 in parenthesis placed at the end of the component. For example FDP_ACC.1 (a) and FDP_ACC.1 (b) 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 in cases where a selection operation is combined with an assignment operation and the assignment is null, the assignment operation is simply deleted leaving on the completed selection to identify the combination of operations.
- 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 ...").

The conventions for the assignment, selection and refinement operations are described in section 5.

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

1.4.2 Terminology

See section 9 (Glossary of Terms).

1.4.3 Acronyms

See section 10 (Acronyms) – Acronym List.

1.5 Security Target Overview and Organization

The Security Target contains the following additional sections:

- TOE Description (Section 2): Provides an overview of the TOE security functions and boundary.
- Security Environment (Section 3): Describes the threats, organizational security policies and assumptions that pertain to the TOE.
- Security Objectives (Section 4): Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- IT Security Requirements (Section 5): Presents the security functional and assurance requirements met by the TOE.
- TOE Summary Specification (Section 6): Describes the security functions provided by the TOE to satisfy the security functional requirements and objectives.
- Protection Profile Claims (Section 7): Presents the rationale concerning compliance of the ST with any Protection Profiles (PPs).
- Rationale (Section 8): Presents the rationale for the security objectives, requirements, and TOE summary specifications as to their consistency, completeness and suitability.
- Glossary of Terms (Section 9)
- Acronyms (Section 10).

2. TOE Description

2.1 Product Type

Persona is a client/server application that provides users secure access to host mainframe system applications through a website. The product makes possible Java-enabled web browser interfaces to host mainframe system applications from traditional PC, Macintosh, or Unix workstations. The TOE employs a level of DES key encryption for data security that includes DES as well as 3DES.

2.2 Product Description

The Persona 5.0 product (henceforth called Persona) is a client/server application that provides access between client applications and host mainframe system computers from client platforms communicating through the Persona Server. Persona provides secure access to host mainframe system data and applications through thin clients including Java applet, Java application, and native Windows clients. Persona resides on a Windows 2000 or Windows XP Professional web server and offers centralized and remote administration. Persona delivers precise terminal emulation to IBM mainframe, IBM AS/400, Unix, Digital, and Data General host systems. Persona's three-tier architecture enables high-level security encoding capabilities, including SSL, SSH, DES, and Triple DES to safeguard display and report data transmitted between one or more Persona client workstations through the Persona server to a host mainframe system computer.

2.3 Security Functions

The TOE implements the following security functions:

Cryptographic Support - The Target of Evaluation Security Functions (TSF) uses the secure sockets layer (SSL) protocol to enforce the two-step encryption information flow policy from the client to the Persona server and SSL or the Secure Shell (SSH) protocol to enforce the information flow policy between the Persona server and the host. Cryptographic operations are performed on all data sent between the client and the host.

Information Flow - The flow of information is controlled from the client to the host in accordance with the two-step encryption information flow control policy. Operations that would change the security attributes of information are not permitted, as this would be in violation of an information flow control SFP.

Identification & Authentication - For remote administration, administrators are identified and authenticated by the TSF. Authentication is through a password.

Security Management - One administrative role is supported. A Remote Administrator monitors and can terminate session connections.

Self Protection - The TOE environment ensures all information from a client to a host or a host to a client goes through the TSF. The TSF ensures that all information must flow through the policy enforcement mechanisms. This is enforced by two-step encryption. In order for a client to access a host, the client must use PKI technology between the client and the TSF. Once this connection has been established, the TSF establishes a separate encrypted communication session between the TSF and the host.

2.4 TOE Boundary

The TOE is version 5.0 of the Persona product composed of client, server, and configuration components. Persona requires a physically protected web server running Windows 2000 or Windows XP Professional on which the server and configuration components of the TOE are installed.

The TOE resides within the Application layer of the OSI network model. The TOE adds an extra layer of protection by using the SSL (Secure Socket Layer) or the Secure Shell (SSH) protocols when it sends or

receives information from a host mainframe system and the SSL protocol when the TOE sends or receives information from a client. The TOE uses cryptography to establish a secure session between the Persona server and one or more Persona clients. It also allows the server to authenticate itself to the client via a server certificate.

The TOE uses public/private key encryption when a Persona client connects with the Persona server through the SSL protocol. Once that connection is secured, DES or 3DES secret key encryption ensures that the information in the session is transmitted safely and with minimal risk from attack. In addition to the SSL protocol, Persona uses its own proprietary transfer protocol that runs over SSL or SSH for communication between the Persona client and the Persona server.

The TOE is composed entirely of software and the boundaries are described below.

2.4.1 Physical Boundaries

Physically, the TOE is composed of a server component and a client component. The server component (Persona Server) is installed on a platform operating as a web server and located in an environment protected by a firewall. The client component runs on a client computer from which a person using that computer wishes to communicate to a host mainframe computer. Persona Server provides a connection between client and host mainframe computers. The client cannot reside on the same server machine as the Persona service, while the host computers are also located in an environment protected by a firewall. Communication between clients and host computers must pass through the Persona server. The Persona server runs on a Windows 2000 or Windows XP Professional web server with a minimum processor based on the operating system specifications. The TSF are provided by the Persona 5.0 server.

Two environmental requirements for the Persona Server are that the operating system is Microsoft Windows 2000 or Windows XP Professional and that a web server is installed, Microsoft Internet Information Server (IIS).

Persona makes host sessions available through the client workstation's web browser, or through Windows or Java Application Thin Client interfaces with or without a browser. The client workstation requires a workstation with Java Virtual Machine (JVM) that supports Java Runtime Environment (JRE) 1.1 or 1.3 for Java-based clients or a 32-bit Windows platform, excluding Windows NT 3.5x, for the Windows thin client.

2.4.2 Logical Boundaries

Persona 5.0 includes 3 components: the Client Component, Server Component and the Configuration Component.

Client Component

A request to connect to a host mainframe computer from a client workstation is generated at the Client component. This component includes two subcomponents: the "Session Client" and the "Remote Administration Client." The Session Client is downloaded from the Web Server to the client workstation as a Java Applet, a Java application, or a Windows thin client. The Session Client is not part of the TOE Security Functions (TSF) because the abstraction of "user" as a person does not participate in the information flow policy enforced by the TSF. The Remote Administration Client is downloaded as a digitally signed Java Applet and provides an interface for remote administration of server sessions from a remote client.

Server Component

The Server component includes the Persona Server, Persona Session Processes, and the PRAText. The Persona Server provides public/private key encryption to ensure a secure connection when the Persona client makes a request. Once the connection is made, Persona Server spawns an appropriate Persona Session Process. The Persona Session Process(es), one for each client-to-host communication session, performs two encryption steps, one between the Session Client and the Persona Session Process, and one

between the Persona Session Process and the host mainframe. The Persona Session Process also provides the terminal emulation required by a host to communicate with a client.

Persona provides remote administration through the PRAText.exe subcomponent via the Administrator interface. An administrator is required to be identified and authenticated using a password. Once the administrator has been successfully validated, the PRAText.exe subcomponent provides the ability to monitor, terminate, and send messages to established Persona Session processes.

Configuration Component

The Configuration Component has two subcomponents: the Persona Service Manager and the Persona Toolbox. Persona Toolbox is a local application that executes on the server. Persona Toolbox is only available to a configuration manager¹ and is used to create host session files. Host session files are host files created by a configuration manager that are later accessed when clients attempt to connect to hosts. Entries in the host session files are used to determine the hosts with which clients can connect.

Persona Service Manager is a dialog-based application available only to the configuration manager. This program allows modification to a wide range of Persona-specific settings that are stored in the Windows Registry and used during the execution of Persona Server.

While this component is managed entirely by the IT environment, it is included in the description since all information flow policy decisions are based upon the settings resulting from the use of the Configuration Component.

¹ Configuration Manager is a term used to describe the operating system administrator.

Figure 1: Persona Subsystems

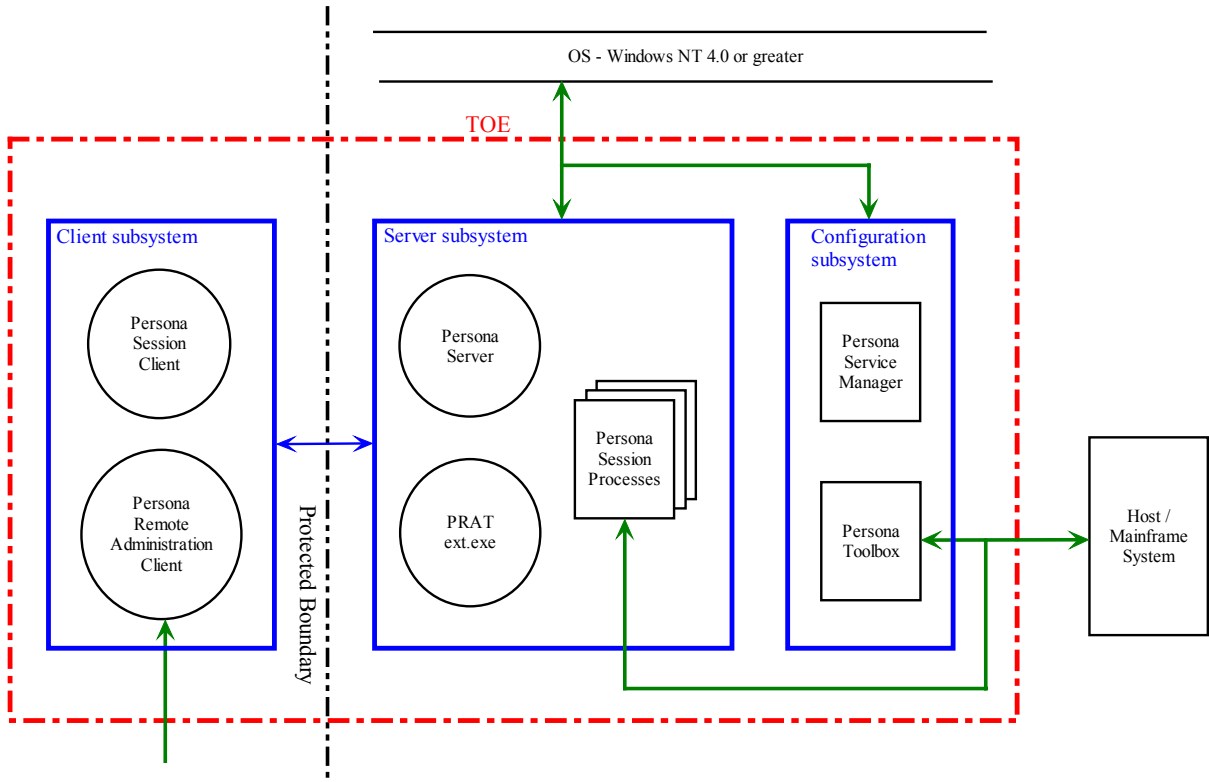


Figure 1: Esker Persona 5.0 Architecture

3. Security Environment

This section includes the following:

- Threats to security,
- Organizational security policies, and
- Secure usage assumptions.

This information provides the basis for the Security Objectives specified in Section 4, the security functional requirements for the TOE and environment specified in Sections 5.1 and 5.2, and the TOE Security Assurance Requirements specified in Section 5.3.

3.1 Threats to Security

Threats are undesirable events and are characterized in terms of a threat agent, a presumed attack method, vulnerabilities that are the foundation for the attack, and identification of the asset under attack.

Threat agents can be categorized as either individuals who have not been granted the right to access the system (unauthorized users) or authorized users of the TOE that have been granted the right to access the system, but may attempt to access assets protected by the system to which they do not have permission to access.

Assets comprise the information stored, processed or transmitted by the TOE. The term “information” is used here to refer to all data held within a system, including data in transit between separate parts of the TOE.

In general, the **threat agents** are assumed to have an attack potential of **medium**. As a result, the TOE has been developed with the assumption that a potential attacker would have a medium level of expertise, access to a medium level of resources, and also have a medium level of motivation.

Following are the threats countered by the TOE:

T.ADMIN_ERROR_OMMISION	Administrators fail to perform some function essential to security.
T.DISCLOSURE_OF_MESSAGE_CONTENT	The contents of a message may be read by a subject other than the client and host that are the sender and recipient of the message.
T.DISCLOSURE_OF_PRIVATE_KEYS	A private or secret key is improperly disclosed to a network node (host or client) through a protocol failure.
T.INTEGRITY	A process that can gain access to the client or host port address used to communicate through the TOE can modify message content by adding, deleting, or changing message contents.
T.MODIFICATION_OF_PRIVATE_KEYS	A private key is modified by a process executing in a network node that has no valid reason for viewing or modifying the key whereby the process gained access to the key through a protocol failure.
T.SENDER DENIES SENDING INFORMATION	The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

3.2 Organization Security Policies

An organizational security policy is a set of rules, practices and procedures imposed by an organization to address its security needs. The following are the Organizational Security Policies enforced by the TOE:

P.MANAGE	The TOE must provide authorized administrators with utilities to effectively manage security functions of the TOE.
P.TRANSIT	The TOE must have the ability to protect system data in transmission between distributed parts of the network in which the TOE operates.

3.3 Secure Usage Assumptions

This section describes the aspects of the operating environment in which the TOE is intended to be used—including personnel and physical assumptions of the environment. The TOE is assured of providing effective security measures in its intended environment only if it has been delivered, installed, and administered as intended.

The operational environment must be managed in accordance with the user and administration guidance documentation.

3.3.1 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL	The TOE administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.TRAINED_STAFF	Authorized TOE administrators are trusted to follow the guidance provided for the secure operation of the TOE.

3.3.2 Physical Assumptions

A.PHYSICAL_PROTECTION	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.
A.DEDICATED	The server platform must be a dedicated server only available to the Persona Configuration Manager (that person responsible for the installation and configuration of Persona).
A.CLIENTS	The client cannot reside on the same server machine as the Persona service.

3.3.3 Underlying System Assumptions

A.FILES	All of the TOE Security Functions (TSF) related files and directories (including executables, run-time libraries, audit logs) are protected from unauthorized access by the system control mechanisms
A.I&A	Users of the underlying system are identified and authenticated.
A.SEP	The underlying system will provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed.

[A.WINDOWS_ADMIN](#)

Access to all TOE configuration tools, the Persona Service and the TSF data saved in OS data structures is restricted to members of the Windows administrator group.

[A.FWALL](#)

All connection requests from a client to connect to a host mainframe will be directed through the Persona Server through a firewall.

4. Security Objectives

This section includes the security objectives including security objectives for the TOE, security objectives for the environment, and security objectives for both the TOE and environment.

4.1 Security Objectives for the TOE

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

O.AUTHORIZATION	The TSF must ensure that only an authorized administrator gains access to the TOE and its resources by uniquely authenticating their claimed identity before granting access to the TOE and its resources.
O.CLIENT2HOST_CONFIDENTIALITY	Message content cannot be read by a subject other than at the communication end-points; client and host.
O.CLIENT2HOST_INTEGRITY	Message content cannot be modified by a subject other than by the sender and receiver at the communication end-points; client and host.
O.ENCRYPTION	The content of every message that passes through the TOE is fully encrypted.
O.NON_REPUDIATION	The TSF must be able to prevent the denial that a message was sent from a specific client or host.
O.REMOTE_ADMINISTRATION	An identified and authorized remote administrator may manage identified TSF entities from a remote client.

4.2 Security Objectives for the Environment

This section specifies the security objectives for the environment.

4.2.1 Non-IT security objectives for the environment

OE.AUTH	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected in a manner that maintains IT security objectives.
OE.MANAGE	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.
OE.PHYSICAL_PROTECTION	The TOE hardware, software, and firmware critical to security policy enforcement are protected from unauthorized physical modification.
OE.ALWAYS_INVOKED	All session communication between a client and a host mainframe that required TSF mediation shall pass through the TSF.

4.2.2 IT security objectives for the environment

OE.ACCESS	The system on which the Persona Server is installed shall provide the access control mechanisms required to protect the TOE's data and system files.
OE.I&A	The system on which the Persona Server is installed shall identify and authenticate users prior to providing access to any TOE data and system files.
OE.ADMIN	The operating environment must include a set of functions that allow effective management of its functions and data.
OE.PROTOCOL_IMP	All operating environments (client, server, and host mainframe) shall provide an implementation of the SSL and SSH protocols whereby each session is managed in its own process domain.
OE.SEP	The system on which the Persona Server is implemented shall provide mechanisms to isolate the TOE Security Functions (TSF).

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. This section organizes the SFRs by CC class. Throughout this section, when the term user is presented, it is interpreted to be a client network address, since the user abstraction is unknown to the TOE.

Table 1 TOE Functional Security Requirements

Security Functional Class	Security Functional Components
Cryptographic support (FCS)	FCS_COP.1 Cryptographic Operation
User Data Protection (FDP)	FDP_IFC.2 Complete information flow control
	FDP_IFF.1 Simple security attributes
	FDP_ITC.1 Import of user data without security attributes
Identification and authentication (FIA)	FIA_UAU.1 Timing of authentication
Security management (FMT)	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_RVM.1 Non-bypassability of the TSP
Trusted Path/Channels (FTP)	FTP_ITC.1 Inter-TSF channel
	FTP_TRP.1 Trusted Path

5.1.1 Cryptographic support (FCS)

5.1.1.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[encryption and decryption]** in accordance with a specified cryptographic algorithm **[DES or Triple DES]** and cryptographic key sizes **[56 bits (DES) and 168 bits (Triple DES)]** that meet the following: **[The DES and Triple DES algorithms as implemented by Esker]**.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the **[two-step encryption information flow control]** on **[clients and communication packets]** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.2.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1-NIAP-0417 The TSF shall enforce the **[two-step encryption information flow control SFP]** based on the following types of subject and information security attributes: **[SSL or SSH session keys]**.

FDP_IFF.1.2-NIAP-0417 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. If the SSL session keys can be successfully negotiated between the client and TSF, then communication packets are permitted to flow.
2. If the SSH session keys can be successfully negotiated between the client and TSF, then communication packets are permitted to flow.

FDP_IFF.1.3-NIAP-0417 The TSF shall enforce the [*no additional information control SFP rules*].

FDP_IFF.1.4-NIAP-0417 The TSF shall provide the following [*no additional SFP capabilities*].

FDP_IFF.1.5-NIAP-0417 The TSF shall explicitly authorize an information flow based on the following rules: [*no explicit authorization rules*].

FDP_IFF.1.6-NIAP-0417 The TSF shall explicitly deny an information flow based on the following rules: [*no explicit denial rules*].

5.1.2.3 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [**two-step encryption information flow control SFP**] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [*no additional rules*].

5.1.3 Identification and authentication (FIA)

5.1.3.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [**remote administration login prompt**] on behalf of the user to be performed before the user is authenticated.

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

5.1.4 Security management (FMT)

5.1.4.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Remote Administrator**].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_RVM.1 Non-bypassability of the TSP

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.

5.1.6 Trusted Path/Channels (FTP)

5.1.6.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**all communications with the remote trusted IT product**].

5.1.6.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**all connection requests**].

5.2 Security Functional Requirements for the IT Environment

The following security functional requirements (SFRs) are intended to be satisfied by the IT environment rather than the TOE itself. Many of these SFRs are the same requirement that is satisfied by the TOE; however in the context of the IT security environment the context (e.g., user abstractions, objects protected) is different. When the IT environment is referenced below, it is referencing the part of the IT environment that must be trusted and not part of the TOE.

All SFRs were drawn from Part 2 of the Common Criteria.

Security Functional Class	Security Functional Components
User Data Protection (FDP)	FDP_ACC.1 Subset access control
	FDP_ITT.1 Basic internal transfer protection
Identification and Authentication (FIA)	FIA_UAU.1 Timing of authentication
	FIA_UID.1 Timing of identification
Security Management (FMT)	FMT_MSA.1 Management of Security Attributes
	FMT_MSA.3 Static attribute initialization
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_SEP.1 TSF domain separation

Table 2: Security Functional Components for the IT Environment

5.2.1 User Data Protection (FDP)

5.2.1.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The IT environment shall enforce the **Discretionary Access Control Policy** on [**subjects - processes**] **acting on the behalf of users, [Person Service, host files, Person Tool Box, Persona Service Manager, and operations among subjects and objects covered**

by the SFP]; and all operations among subjects and objects covered by the DAC policy. The DAC policy shall be able to control access to users and groups of users.

5.2.1.2 FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The IT environment shall enforce the [the SSL and SSH protocols are implemented and operate correctly] to prevent the [disclosure of key material] of user data when it is transmitted between physically-separated parts of the TOE.

Note: It is expected that each SSL and SSH session running in the client and the host mainframe operates in a separate process and then when a session terminates, the process terminates.

5.2.2 Identification and authentication (FIA)

5.2.2.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The IT environment shall allow [access to other objects except the Persona Service] on behalf of the user to be performed before the user is authenticated.

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

Note: Windows administrators must be authenticated before being granted access to the Persona Service.

5.2.2.2 FIA_UID.1 Timing of identification

FIA_UID.1.1 The IT environment shall allow [access to other objects except the Persona Service] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The IT environment shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Note: Windows administrators must be authenticated before being granted access to the Persona Service.

5.2.3 Security management (FMT)

5.2.3.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The IT environment shall enforce the [two-step encryption information flow control SFP] to restrict the ability to [modify] the security attributes [protocol selection, SSL or SSH] to [the Administrator]².

5.2.3.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1-NIAP-0409 The IT environment shall enforce the [two-step encryption information flow control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP

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

² The IT environment role named *Administrator* is referred to elsewhere as the Configuration Manager to avoid confusion with the Remote Administrator role of the TOE.

5.2.3.3 FMT_SMR.1 Security roles

FMT_SMR.1.1 The IT environment shall maintain the roles [**Configuration Manager**].

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

Note: The IT environment recognizes only one role, that of the Configuration Manager. The Configuration Manager creates host session files and provides administrative functions from the Persona server machine. The TOE recognizes only one role, that of the Remote Administrator. The Remote Administrator can monitor and terminate connected Persona session processes.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 FPT_SEP.1 TSF domain separation

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

FPT_SEP.1.2 The IT environment shall enforce separation between the security domains of subjects in the TSC.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 3: EAL 3 Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.3 Authorization controls
	ACM_SCP.1 TOE CM coverage
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support (ALC)	ALC_DVS.1 Identification of security measures
Tests (ATE)	ATE_COV.2 Analysis of Coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	AVA_MSU.1 Examination of guidance

	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.3.1 Configuration Management (ACM)

ACM_CAP.3 Authorization Controls

- 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 labeled with its reference.
- ACM_CAP.3.3C_RI-003** The configuration list shall uniquely identify all configuration items that comprise the TOE.
- ACM_CAP.3.4C** The configuration list shall describe the configuration items that comprise the TOE.
- ACM_CAP.3.5C** The CM documentation shall describe the method used to uniquely identify the configuration items.
- ACM_CAP.3.6C** The CM system shall uniquely identify all configuration items.
- ACM_CAP.3.7C** The CM plan shall describe how the CM system is used.
- ACM_CAP.3.8C** The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
- ACM_CAP.3.9C** The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
- ACM_CAP.3.10C** The CM system shall provide measures such that only authorized 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.

ACM_SCP.1 TOE CM Coverage

- ACM_SCP.1.1D_RI-004** The developer shall provide a list of configuration items for the TOE.
- ACM_SCP.1.1C_RI-004** 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.1.2C** The CM documentation shall describe how configuration items are tracked by the CM system.

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

5.3.2 Delivery and Operation (ADO)

ADO_DEL.1 Delivery Procedures

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.

ADO_IGS.1 Installation, generation, and start-up procedures

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 **_RI-051** 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 examine the provided installation, generation, and start-up procedures to determine that they describe the steps necessary for secure installation, generation, and start-up of the TOE.

5.3.3 Development (ADV)

Informal 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.

ADV_HLD.2 Security enforcing high-level design

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.

ADV_RCR.1 Informal correspondence demonstration

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.

5.3.4 Guidance Documents (AGD)

AGD_ADM.1 Administrator Guidance

- 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 behavior 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 on 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.

AGD_USR.1 User Guidance

- 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 behavior 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 on 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.

5.3.5 Life Cycle Support (ALC)

ALC_DVS.1 Identification of security measures

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.

5.3.6 Security Testing (ATE)

ATE_COV.2 Analysis of coverage

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.

ATE_DPT.1 Testing: high-level design

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.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

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.
ATE_IND.2 Independent testing	
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.

5.3.7 Vulnerability Assessment (VLA)

AVA_MSU.1 Examination of Guidance

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.

AVA_SOF.1 Strength of TOE security functions

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.

AVA_VLA.1 Developer Vulnerability Analysis

AVA_VLA.1.1D_RI-051 The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D_RI-051 The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1C_RI-051 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_RI-051 The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C_RI-051 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.

6.1 TOE Security Functions

6.1.1 Cryptographic Support

The TSF uses public key and secret key technology to enforce the information flow policy from the client to the TOE using the Secure Socket Layer (SSL) protocol from the client to the Persona Server and the SSL or the Secure Shell (SSH) protocol to enforce the information flow policy between the Persona Server and a host mainframe. Cryptographic operations are performed on every packet communicated through the TSF. The Persona session management performs encryption between the client and Persona Server and the Persona Server and the remote trusted host. This two-step encryption ensures that the TOE is communicating with the actual identified client as well as the actual identified host to provide a trusted communication path from the client through to the host.

The server certificate contains the public key to help ensure data security. The TOE includes a default generic test certificate.. The Persona Service Manager provides an interface to change the default certificate to the customer's specific certificate.

All packets that are communicated between a client and a host mainframe during one session pass through the TSF with full-packet encryption occurring twice; once between the client and the Persona Server and once between the Persona Server and the host mainframe. Encryption is performed using the 3DES algorithm with a key size of 168 bits or DES with a key size of 56 bits. All data imported into the TOE over this encrypted channel is imported without security attributes.

All successful client requests to the Persona Server initiate a trusted path that encrypts data between the client and the Persona Server. Each connection between the client and the Persona Server is distinct from other connections. Likewise, all requests between the Persona Server and the host are encrypted to prevent modification and deletion. A remote host is deemed trusted when the administrator establishes the remote host as a valid connection target for Persona clients.

The Cryptographic Support security function satisfies the following security requirements:

FCS_COP.1

FDP_ITC.1

FTP_TRP.1

FTP_ITC.1

6.1.2 Identification and Authentication

For remote administration, a Remote Administrator is identified and authenticated by the TSF. Authentication is through a Remote Administrator name and password. A Remote Administrator is required to enter the correct Admin name and password.

The Identification and Authentication security function satisfies the following security requirements:

FIA_UAU.1

6.1.3 Information Flow Control

The flow of information is controlled from the client to the host and the host to the client in accordance with the two-step encrypted information flow control policy. Operations that would change the security

attributes of information are not permitted, as this would be in violation of an information flow control SFP.

The Information Flow Control security function satisfies the following security requirements:

FDP_IFC.2

FDP_IFF.1

6.1.4 Security Management

Security Management is provided when the TOE is installed through set-up options and a different security management interface is provided while the TOE is in execution. During setup a configuration manager with access to the Persona service will establish host session files.

One administrative role is supported while the TOE is in execution. The Remote Administrator is the only logon permitted to Persona and is the only recognized user. The Remote Administrator manages the active session in that the sessions can be monitored and/or terminated remotely through the Administrator interface and PRAText.exe server component. Session termination by the Remote Administrator effectively destroys all session keys, since session keys do not persist beyond the session for which they were created.

The Security Management security function satisfies the following security requirements:

FMT_SMR.1

6.1.5 Protection of the TSF

The TOE environment ensures all information from a client to a host or a host to a client goes through the TSF. The TSF ensures that all information must flow through the policy enforcement mechanisms. This is enforced by two-step encryption. In order for a client to access a host, the client must use PKI technology between the client and the TSF. Once this connection has been established, the TSF establishes a separate encrypted communication session between the TSF and the host. The TSF creates a separate process, unique to the specific client and host, to mediate all communication between the client and the host. There is no communication path that passes the client information directly to the host except through the Persona Session Process dedicated to the specific session.

The Protection security function satisfies the following security requirements:

FPT_RVM.1

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL 3 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and,
- Vulnerability Assessment.

6.2.1 6.2.1 Process Assurance

6.1.1.1 Configuration Management

Esker has a separate Quality Assurance organization. Visual SourceSafe is used for version control and document control. The *Esker Configuration Manual* describes the configuration system including the following information:

- Identification of configuration items,
- Assignment of configuration control numbers,
- Tracking configuration items,
- Version control, and
- Build control that includes the code module versions, administrative guidance, and design documentation applicable to a single build.

Assurance Requirements: ACM_CAP.3, ACM_SCP.1.

6.1.1.2 Life-Cycle Support

The *Esker Life-cycle Support Manual* describes 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. This documentation provides evidence that these security measures are followed during the development and maintenance of the TOE.

Assurance Requirements: ALC_DVS.1

6.2.2 Delivery and Guidance

Esker provided a *Persona 5.0 Administrator's Getting Started Guide*. This manual is directed at the administrator, as Persona provides on-line help files for the user connecting to the host. This manual provides appropriate installation information and describes how to configure the various environmental products as well.

Assurance Requirements: AGD_ADM.1, AGD_USR.1.

6.2.3 Design Documentation

The *Persona Design Document* describes all of the external interfaces of the TOE that are used by the security functions. The *Persona Design Document* describes TOE decomposition into subsystems and the TOE Security Functions (TSF) performed by each subsystem is identified and the external interfaces of the TSF provided by each subsystem are identified.

The Correspondence Matrix provided a mapping between the functional specification and the TSS, and the high level design and the functional specification.

Assurance Requirements: ADV_FSP.1, ADV_HLD.2, ADV_RCR.1.

6.2.4 Tests

The Persona test documentation describes how each security function is tested. Indeed all security tests are mapped to security functions to ensure that the security function is completely tested, Persona test documentation also describes the test setup, and expected results for each test. Esker provided test documentation and test matrices to SAIC. Test documentation included the following:

- Persona Test Plan
- Persona Test Setup
- Persona Testing Methodology
- Persona Actual Test Results
- Persona Session Process Test Cases
- Persona Toolbox Test Cases

- Persona Service Test Cases
- Persona Service Manager Test Cases
- Persona Remote Admin Tool Test Cases
- Persona Remote Admin Ext Tool Test Cases
- Persona Windows Thin Client Test Cases
- Persona Java Application Client Test Cases
- Persona Java Client Test Cases

Assurance Requirements: ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2.

6.2.5 Vulnerability Assessment

The *Persona Vulnerability Assessment Methodology* document describes Eskers methodology for searching public domain information in search for possible problem areas reported that might be germane to Persona. The individuals responsible for vulnerability analysis also perform penetration testing by trying to use interfaces in unintended ways to determine their effect.

Another aspect of the vulnerability assessment determines if the administrative guidance is consistent with the design information.

Persona Vulnerability Assessment Methodology document also provides the Strength of Function (SOF) Analysis for the remote administrator Admin Name and password to determine the randomness of the password and mapped this to the SOF-level medium discussed in the Common Criteria.

Persona Vulnerability Assessment Methodology document demonstrates an understanding of the vulnerability assessment documentation requirements for consistency between administrative guidance and design documentation, SOF calculations, and how Esker has determined that the TOE does not have obvious exploitable flaws.

Assurance Requirements: AVA_MSU.1, AVA_SOF.1; AVA_VLA.1.

7. Protection Profile Claims

This TOE does not claim conformance to a Protection Profile.

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;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

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

Table 4: Mapping of TOE Security Objectives to Threats

Objectives	O.AUTHORIZATION	O.CLIENT2HOST_CONFIDENTIALITY	O.CLIENT2HOST_INTEGRITY	O.ENCRYPTION	O.NON_REPUDIATION	O.REMOTE_ADMINISTRATION	OE.ACCESS	OE.ALWAYS_INVOKED	OE.I&A	OE.ADMIN	OE.PROTOCOL_IMP	OE.SEP	OE.AUTH	OE.MANAGE	OE.PHYSICAL_PROTECTION
T.Admin error omission	X					X								X	
T.Disclosure of message content		X		X											
T.Disclosure of private keys											X				
T.Integrity			X	X											
T.Modification of private keys											X	X			
T.Sender Denies Sending Information					X										
P.Manage	X					X								X	
P.Transit		X	X												
A.Manage														X	
A.No_Evil														X	
A.Physical_Protection															X

Objectives	O.AUTHORIZATION	O.CLIENT2HOST_CONFIDENTIALITY	O.CLIENT2HOST_INTEGRITY	O.ENCRYPTION	O.NON_REPUDIATION	O.REMOTE_ADMINISTRATION	OE.ACCESS	OE.ALWAYS_INVOKED	OE.I&A	OE.ADMIN	OE.PROTOCOL_IMP	OE.SEP	OE.AUTH	OE.MANAGE	OE.PHYSICAL_PROTECTION
A.Trained_Staff														X	
A.Dedicated															X
A.Clients															X
A.Files							X								
A.Fwall								X							
A.I&A									X						
A.Sep											X	X			
A.Windows_Admin							X			X					

T.Admin error omission

Administrators fail to perform some function essential to security.

This threat is addressed because those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives (OE.Manage). Also the TSF must ensure that only an authorized administrator gains access to the TOE and its resources by uniquely identifying and authenticating their claimed identify before granting access to the TOE and its resources. (O.Authorization). The only TOE interface for authorized administrators to perform TOE functions that are essential to security is the remote administrator client interface (O.Remote_Administration).

T.Disclosure of message content

The contents of a message may be read by a subject other than the client and host that are the sender and recipient of the message.

This threat is addressed because message content cannot be read by a subject other than at the communication end-points, client and host (O.Client2host_confidentiality). The message used to protect message content is that all message content is fully encrypted (O.Encryption).

T.Disclosure of private keys

A private or secret key is improperly disclosed to a network node (host or client) through a protocol failure.

This threat is addressed because all operating environments (client, server, and host mainframe) provide an implementation of the SSL or SSH protocols whereby each session is managed in its own process domain. This prevents processes not associated with a session from seeing keys associated with another session (OE.Protocol_Imp).

T.Integrity

A process that can gain access to the client or host port address used to communicate through the TOE can modify message content by adding, deleting, or changing message contents.

This threat is addressed because the message content cannot be modified by a subject other than by the sender and receiver at the communication end-points, client and host (O.Client2host_Integrity). The method used to protect message integrity is that all message content is fully encrypted (O.Encryption).

T.Modification of private keys

A private key is modified by a process executing in a network node that has no valid reason for viewing or modifying the key whereby the process gained access to the key through a protocol failure.

This threat is addressed because all operating environments (client, server, and host mainframe) provide an implementation of the SSL and SSH protocols whereby each session is managed in its own process domain. This prevents processes not associated with a session from changing or deleting keys (OE.Protocol_Imp). Also, the system on which the Persona Server is implemented provides mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed. This ensures that packet encryption in accordance with the SSL and SSH protocols cannot be bypassed and that a client or host packet cannot tamper with keys (OE.Sep).

T.Sender Denies Sending Information

The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

This threat is addressed because the TSF prevents a sender from denying that the sender was the source of the message (O.Non_Repudiation).

P.Manage

The TOE must provide authorized administrators with utilities to effectively manage security functions of the TOE.

This policy is addressed because those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives (OE.Manage). Also the TSF must ensure that only authorized administrators gain access to the TOE and its resources by uniquely identifying them and identifying all users and authenticating their claimed identify before granting access to the TOE and its resources. (O.Authorization). The only TOE interface for authorized administrators to manage TOE functions is the remote administrator client interface (O.Remote_Administration).

P.Transit

The TOE must have the ability to protect system data in transmission between distributed parts of the network in which the TOE operates.

This policy is addressed because message content cannot be read by a subject other than at the communication end-points, client and host (O.Client2host_confidentiality), and because the message content cannot be modified by a subject other than by the sender and receiver at the communication end-points, client and host (O.Client2host_Integrity).

A.Files

All of the TOE Security Functions (TSF) related files and directories (including executables, run-time libraries, audit logs) are protected from unauthorized access by the system control mechanisms.

This assumption is consistent with the OE.Access environmental objective because the system on which the Persona Server is installed shall provide the access control mechanisms required to protect the TOE's data and system files.

A.Fwall

All connection requests from a client to connect to a host mainframe will be directed through the Persona Server through a firewall.

This assumption is consistent with the OE.Always_Invoked environmental objective that states all session communication between a client and a host mainframe that required TSF mediation shall pass through the TSF.

A.I&A

Users of the underlying system are identified and authenticated.

This assumption is consistent with the environmental objective OE.I&A that the system on which the Persona Server is installed shall identify and authenticate users prior to providing access to the TOE data and system files.

A.Sep

The underlying system will provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed. The TSF components are 1) the process address space used by the TSF, and 2) the Registry settings.

This assumption is consistent with the environmental objective OE.Protocol_Imp that states all operating environments (client, server, and host mainframe) shall provide an implementation of the SSL or SSH protocols whereby each session is managed in its own process domain. Also the system on which the Persona Server is implemented shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed (OE.Sep).

A.Windows_Admin

Access to all TOE configuration tools, the Persona Service and the TSF data saved in OS data structures is restricted to members of the Windows administrator group.

This assumption is consistent with the environmental objective OE.Access where the system on which the Persona Server is installed shall provide the access control mechanisms required to protect the TOE's data and system files. Additionally, the OE.Admin objective supports this assumption by requiring the underlying system to provide an administrator role and supporting administrative functions.

A.Manage

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is consistent with the OE.Manage environmental objective because those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.

A.Dedicated

The server platform must be a dedicated server only available to the Persona Configuration Manager (that person responsible for the installation and configuration of Persona).

This assumption is consistent with the OE.Physical_Protection environmental objective because those responsible for the TOE must ensure that the TOE is protected from physical access from untrusted users.

A.Clients

The client cannot reside on the same server machine as the Persona service.

This assumption is consistent with the OE.Physical_Protection environmental objective because those responsible for the TOE must ensure that the TOE is protected from physical access from non-administrative users.

A.No_Evil

The TOE administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

This assumption is consistent with the OE.Manage environmental objective because authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.Physical_Protection

The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

This assumption is consistent with the OE.Physical_Protection because the TOE hardware, software, and firmware critical to security policy enforcement are protected from unauthorized physical modification.

A.Trained_Staff

Authorized TOE administrators are trusted to follow the guidance provided for the secure operation of the TOE.

This assumption is consistent with the OE.Manage environmental objective because those responsible for the TOE must be knowledgeable to ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.

8.2 Security Requirements Rationale

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

8.2.1 Security Functional Requirements Rationale

Table 5 provides the correspondence mapping between security objectives for the TOE and the security functional requirements that satisfy them.

Table 5: SFRs mapped to Security Objectives

SECURITY FUNCTIONAL REQUIREMENT	O.AUTHORIZATION	O.CLIENT2HOST_CONFIDENTIALITY	O.CLIENT2HOST_INTEGRITY	O.ENCRYPTION	O.NON-REPUDIATION	O.REMOTE_ADMINISTRATION
FCS_COP.1 Cryptographic Operation		X	X	X	X	
FDP_IFC.2 Complete information flow control		X	X		X	
FDP_IFF.1 Simple security attributes				X		
FDP_ITC.1 Import of user data without security attributes				X		
FIA_UAU.1 Timing of authentication	X					
FMT_SMR.1 Security roles	X					X
FPT_RVM.1 Non-bypassability of the TSP				X		
FTP_ITC.1 Inter-TSF trusted channel		X	X			
FTP_TRP.1 Trusted Path		X	X			

8.2.1.1 O.Authorization

The TSF ensure that only authorized administrators gain access to the TOE and its resources by uniquely authenticating their claimed identify before granting access to the TOE and its resources.

This objective is satisfied by requiring that administrators must be identified and authenticated before they can use any other TSF functions (FIA_UAU.1). Also, the TSF maintains one role, the *remote administrator* who is the only authorized administrator who can access TOE resources (FMT_SMR.1)

8.2.1.2 O.Client2Host_Confidentiality

Message content cannot be read by a subject other than at the communication end-points; client and host.

This objective is satisfied by requiring the two-step encryption process on all communication packets between the client and the host (FDP_IFC.2). The TSF enforces this two-step encryption process for a process in either the client or the host to be able to receive communication data in an intelligible form. All communication encryption complies with the DES or 3DES standard (FCS_COP.1). Clients connecting to the TSF use a trusted path to ensure confidentiality of user data (FTP_TRP.1). The TSF connecting to a remote host uses a trusted path to ensure confidentiality of user data (FTP_ITC.1).

8.2.1.3 O.Client2Host_Integrity

Message content cannot be modified by a subject other than by the sender and receiver at the communication end-points; client and host.

This objective is satisfied by requiring the two-step encryption process on all communication packets between the client and the host (FDP_IFC.2). All communication encryption complies to the DES or 3DES standard (FCS_COP.1). Clients connecting to the TSF use a trusted path to ensure integrity of user data (FTP_TRP.1). The TSF connecting to a remote host uses a trusted path to ensure integrity of user data (FTP_ITC.1).

8.2.1.4 O.Encryption

The content of every message that passes through the TOE is fully encrypted.

A fundamental security function provided by the TSF is the use of encryption and key exchanges. A information flow security policy is maintained over all communication through the use of full session encryption that is provided through the exchange of cryptographic keys (FDP_IFF.1) (FCS_COP.1). Through the use of PKI technology on all session communication the confidentiality of data exchanged between the sender and receiver is assured. Session communication through SSL or SSH ensures the sender and receiver must present encryption keys as the security attribute of the session information and no information may be imported into the TSF without a private session key (FDP_ITC.1).

Each communication session from a client to a host must go through a two-step encryption process. One set of keys is used between the client and the TSF and another set of keys are used between the TSF and the host. There is no way for communication to flow between the client and the host without going through the TSF, since the client and host have no mechanism to exchange keys. First, an environmental requirement forces all client calls into the enclave to first go through a firewall to be proxied into the TOE. So, if the client had an actual host address, the client could not directly communicate with the host. Secondly, when the client selects a host from the client interface, the only address the client is presented with is the address of the TOE. The combination of the two-step encryption process and forced proxy ensures that the TSF functions are always invoked (FPT_RVM.1).

8.2.1.5 O.Non_repudiation

The TSF must be able to prevent a sender from denying that the sender was the source of the message.

This objective is satisfied by requiring the two-step encryption process on all communication packets between the client and the host (FDP_IFC.2). All communication encryption complies to the DES or 3DES standard (FCS_COP.1). Since a session is established with the Persona Server and the Persona Server establishes a connection with the host mainframe, when communication begins between the client and the host mainframe, both the client and the host have non-refutable evidence that they are communicating to the node on the other end. Since the SFP does not address the user associated with the client or the host, the “sender” is the client and the “receiver” is the host mainframe. If non-repudiation needs to be linked to a person then it is the responsibility of the host to provide user identification and authentication.

8.2.1.6 O.Remote_Administration

An identified and authorized remote administrator may administer identified TSF entities from a remote client.

The Remote Administrator is the only administrative role provided by the TSF (FMT_SMR.1). The Remote Administrator has a limited role in that the primary function is to review the status of active sessions and terminate active sessions. Nearly all security attributes and default values used by the TSF cannot be changed once they are installed and the system on which the TSF runs is rebooted.

8.2.2 Security Functional Requirements for the IT Environment Rationale

This section provides evidence supporting the internal consistency and completeness of the security functional requirements for the environment in the Security Target. **Table 6** provides the correspondence mapping between security objectives for the IT Environment for the TOE and the security functional requirements for the IT Environment that satisfies them.

Table 6: SFRs For the IT Environment mapped to Security Objectives

SECURITY FUNCTIONAL REQUIREMENT FOR THE IT ENVIRONMENT	OE.ACCESS	OE.I&A	OE.ADMIN	OE.PROTOCOL_IMP	OE.SEP
FDP_ACC.1 Subset access control	X				
FDP_ITT.1 Basic internal transfer protection				X	
FIA_UAU.1 Timing of authentication		X			
FIA_UID.1 Timing of identification		X			
FMT_MSA.1 Management of security attributes.			X		
FMT_MSA.3 Static attribute initialization			X		
FMT_SMR.1 Security roles			X		
FPT_SEP.1 TSF domain separation					X

8.2.2.1 OE.Access

The system on which the Persona Server is installed shall provide the access control mechanisms required to protect the TOE's data and system files.

The FDP_ACC.1 requirement ensures there will be a discretionary access control (DAC) mechanism present to protect files. The details of the requirement are not necessary (i.e., FDP_ACF.1) to meet the stated objective. Rather, Persona is only concerned that DAC is available and is not concerned with its implementation details such as permission bits or access control lists.

8.2.2.2 OE.I&A

The system on which the Persona Server is installed shall identify and authenticate users prior to providing access to any TOE data and system files.

The FIA_UID.1 and FIA_UAU.1 requirements ensure that the system must perform identification and authentication of all users. These requirements work together to satisfy this objective.

8.2.2.3 OE.Admin

The operating environment must include a set of functions that allow effective management of its functions and data.

The FMT_SMR.1 requirement ensures there is an administrative role. The FMT_MSA.1 requirement allows the administrator to establish parameters (i.e., SSH or SSL) for connections with remote trusted hosts. The FMT_MSA.3 requirement allows the administrator to override default values in the two-step encryption information flow policy. Together these requirements address this objective.

8.2.2.4 OE.Protocol_imp

All operating environments (client, server, and host mainframe) shall provide an implementation of the SSL or SSH protocols whereby each session is managed in its own process domain.

The FDP_ITT.1 requirement ensures that there will be a correct implementation of SSH or SSL to support TOE operations. This requirement ensures the objective is adequately addressed.

8.2.2.5 OE.Sep

The system on which the Persona Server is implemented shall provide mechanisms to isolate the TOE Security Functions (TSF).

The FPT_SEP.1 requirement provides assurance that the TOE is isolated from untrusted subjects. This requirement ensures the objective is adequately addressed.






8.2.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL 3 assurance package and is based on good rigorous commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The Security Objectives for the TOE were reviewed and EAL 3 was found to sufficiently address them.

8.2.4 Requirement Dependency Rationale

Table 7: SFRs and associated dependencies

Requirement No.	Functional Requirements	Dependencies	Dependency	Dependency Met
-----------------	-------------------------	--------------	------------	----------------

Requirement No.	Functional Requirements	Dependencies	Dependency	Dependency Met
1	FCS_COP.1	FDP_ITC.1	4	
		FMT_MSA.2		No - See rationale below
		FCS_CKM.4		No - See rationale below
2	FDP_IFC.2	FDP_IFF.1	3	
3	FDP_IFF.1	FDP_IFC.1*	2	Included in FDP_IFC.2
		FDP_MSA.3		No - See rationale below
4	FDP_ITC.1	FDP_IFC.1*	2	Included in FDP_IFC.2
		FMT_MSA.3		No - See rationale below
5	FIA_UAU.1	FIA_UID.1		No - See rationale below
6	FMT_SMR.1	FIA_UID.1		No - See rationale below
7	FPT_RVM.1	No dependencies		
8	FTP_ITC.1	No dependencies		
9	FTP_TRP.1	No dependencies		

- FDP_IFC.1 – The FDP_IFC.2 requirement, which is hierarchical to FDP_IFC.1, has been included. The inclusion of FDP_IFC.2, which provides complete information flow control, satisfies the subset information flow control requirement.
- FMT_MSA.2 – The FMT_MSA.2 requirement is a dependency of the FCS_COP.1 requirement to support the management of the cryptographic security function. In Persona, the administrator does not enter any values related to the cryptographic security function so this requirement is not applicable.
- FCS_CKM.4 – This requirement addresses key destruction. The keys associated with the DES and 3DES algorithms are automatically deleted upon disconnection. Therefore, these requirements are not necessary to satisfy the FCS_COP.1 requirement.
- FMT_MSA.3 – The configuration manager performs the management activities required to support the two-step encryption information flow policy. Hence, the FMT_MSA.3 requirement is included in the security function requirements for the IT environment.
- FIA_UID.1 – Persona has only one valid account – administrator. The administrator is required to supply a password to access the account so authentication-related requirements are applicable while identification requirements are implicit.

8.2.5 Explicitly Stated Requirements Rationale

This ST does not contain any explicitly stated functional or assurance requirements.

8.2.6 Internal Consistency Rationale

The ST includes no instance of a requirement that contradicts another requirement in the ST. In instances where different requirements apply to the same events or types of data, the requirements and the operations performed within the requirements do not contradict each other, but provide supporting functionality ensuring that the TOE is internally consistent.

The combination of several different supporting security functions, and the inclusion of dependencies as illustrated in **Table 7: SFRs and associated dependencies and the associated rationale for not including dependencies**, ensures that together the selected requirements form a mutually supportive whole. The following items also support this claim:

- Mapping and suitability of the requirements to security objectives (as justified in **Table 5** and **Table 6**);
- Inclusion of architectural requirements FPT_RVM.1 to protect the TSF;
- Inclusion of security management requirements to ensure proper configuration and control of other security functional requirements.

8.2.7 Strength of Function Rationale

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism which is used to meet the FIA_UAU.1 requirement. By requiring passwords consist of eight characters (with 95 available characters, the password space exceeds 700,000,000,000,000 available combinations), the claim exceeds the minimum claim of SOF-medium, as stated in section 1.3.

The SOF-medium strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.

8.2.8 Security Functional Requirements Rationale

Table 8: Mapping of SFRs to Security Functions

REQUIREMENT	CRYPTOGRAPHIC SUPPORT	INFORMATION FLOW	IDENTIFICATION & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION
FCS_COP.1	X				
FDP_IFC.2		X			
FDP_IFF.1		X			
FDP_ITC.1	X				
FIA_UAU.1			X		
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_SMR.1				X	
FPT_RVM.1					X
FTP_ITC.1	X				
FTP_TRP.1	X				

FCS_COP.1 Cryptographic operation

All communication encryption complies to the DES or 3DES FIPS 46-6 “Data Encryption Standard.” This claim has not been validated rather it is an assertion made by Esker.

FDP_IFC.2 Complete information flow control

A two-step encryption process is required on all communication packets between the client and the host.

FDP_IFF.1 Simple security attributes

An information flow security policy is maintained over all communication through the use of full session encryption that is provided through the exchange of cryptographic keys using PKI technology.

FDP_ITC.1 Import of user data without security attributes

Session communication through SSL or SSH ensures the sender and receiver must possess correct encryption keys as the security attribute of the session information and no information may be imported into the TSF without a session key.

FIA_UAU.1 Timing of authentication

Remote Administrators must be authenticated using a password at a login screen provided before they may perform an administrative function.

FMT_SMR.1 Security roles

A Remote Administrator role is the only administrative role provided by the TSF. The interface provided is through the Remote Administration client interface.

FPT_RVM.1 Non-bypassability of the TSP

Each communication session from a client to a host must go through a two-step encryption process. One set of keys is used between the client and the TSF and another set of keys are used between the TSF and the host. There is no way for communication to flow between the client and the host without going through the TSF, since the client and host have no mechanism to exchange keys. First, an environmental requirement forces all client calls into the enclave to first go through a firewall to be proxied into the TOE. So if the client had an actual host address, the client could not directly communicate with the host. Secondly, when the client selects a host from the client interface, the only address the client is presented is the address of the TOE. The combination of the two-step encryption process and forced proxy ensures that the TSF functions are always invoked.

FTP_ITC.1 Inter-TSF trusted channel

When Persona Server sends packets to a remote trusted host, the packets are encrypted to prevent data modification and disclosure. Any time the Persona Server makes a connection with a remote trusted host, it requests an encrypted connection. A remote host is deemed trusted when the administrator establishes the remote host as a valid connection target for Persona clients (via the Persona Server). All data is imported without security attributes.

FTP_TRP.1 Trusted path

All client requests to the Persona Server initiate a trusted path that encrypts data between the client and the Persona Server. Each client connection is separate from other client connections to prevent modification and disclosure of user data.

9. Glossary of Terms

The following definitions are used throughout this ST:

Administrator: Accounts at this level have limited authority in the administration of the TOE (according to what has been defined in the system settings). The Administrator can add, remove, and change settings.

Authentication data: Information used to verify claimed identities.

Authorized administrators: A term used to for the Administrator role defined by the TOE.

Compromise: the unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: the property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Configuration Manager: a term used to describe the operating system administrator.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines:

- The transformation of plaintext data into ciphertext data,
- The transformation of ciphertext data into plaintext data,
- A digital signature computed from data,
- A keyed hash computed from data,
- The verification of a digital signature computed from data,
- An authentication code computed from data, or
- An exchange agreement of a shared secret.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Private key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. (Public keys are not considered CSPs.)

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does not imply a classification level rather the term implies the need to protect the key from disclosure or substitution.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

10. Acronyms

ACM	Assurance Configuration Management
ADO	Assurance Delivery and Operation
AGD	Assurance Guidance Documents
ADV	Assurance Development
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
DAC	Discretionary Access Control
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
I&A	identification and authentication
ISO	International Organization for Standardization
IT	Information Technology
OS	Operating System
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
SF	Security Functions
SFR	Security Functional Requirements
SFP	Security Function Policy
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functions
TSP	TOE Security Policy