National Information Assurance Partnership

Common Criteria Evaluation and Valiation Scheme

Validation Report

Esker Persona 5.0

Report Number： CCEVS-VR-02-0033
Dated: 31 December 2002
Version: 1.3

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

1. Executive Summary

An evaluation of the Esker Persona 5.0 was begun 26 September 2002 and completed 31 December 2002. The evaluation was for the Evaluation Assurance Level 3 (EAL3). The Persona 5.0 product (henceforth called Persona) is a client/server application that provides secure access from client workstations to host platform system computers through the Persona server. The TOE employs a level of DES key encryption for data security that includes DES as well as 3DES. Persona 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. The TOE is an all software TOE and includes no hardware. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The evaluation was performed by Science Applications International Corporation (SAIC) in the United States. The evaluation was carried out in accordance with requirements drawn from the Common Criteria CCv2.1, Part 3 for EAL3 [CC_PART3] and Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology [CEM_PART2]. The assurance activities at EAL3 offer confidence that the Esker Software, Persona Version 5.0 (with documentation and software deliverables as defined in sections 6. and 8., respectively) contains requirements that are:

- Justifiably included to counter stated threats and meet realistic security objectives,
- Internally consistent and coherent
- Technically sound and
- Free from vulnerabilities associated with obvious and known threats.

SAIC, the Common Criteria Testing Laboratory [CCTL], is accredited by the National Voluntary Laboratory Accreditation Program [NVLAP] and approved by the NIAP validation body to conduct security evaluations.. The CCTL has presented CEM work units and rationale that are consistent with the CC, the CEM and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories [CCEVS_PUB 4]. The CCTL team concluded that the requirements of the EAL 3 have been met. Therefore, a **pass** verdict has been issued, by the CCTL, for the Esker software, Persona 5.0.

The information contained in this Validation Report is not an endorsement of the Esker Persona product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

1.1. Evaluation Highlights

Dates of Evaluation: 26 September 2002 – 31 December 2002
Evaluated Product: Esker Persona 5.0
Developer: Esker, Inc., 465 Science Drive, P.O. Box 44953, Madison, WI 53744-4953
CCTL: Science Applications International Corporation, Common Criteria Testing Laboratory, 7125 Columbia Gateway Drive, Suite 300, Columbia, MD 21046
Evaluation Class: EAL3
PPs Claimed: None.
Validation Team: William R. Simpson, Institute for Defense Analyses
Margaret T. Webster-Butler, National Security Agency
Version of CC: Common Criteria version 2.1, August 1999
Version of CEM: Common Evaluation Methodology 1.0, August 1999
Effective Date for Interpretations: All interpretations as of 27 September 2002

2. Product Identification

The Target of Evaluation (TOE) is Esker Persona 5.0. It consists of the following components:

- Client Component
- Server Component
- Configuration Component.

The TOE as delivered is all software and includes no hardware. Further, the operating system, web server software and firewall are required to be in the environment, but are not supplied as part of the TOE. The product must run on a dedicated web server that has installed either Windows 2000, or Windows XP Professional, and is protected by a firewall configuration. The configuration of the environment required software is covered in the Administrative Guidance for Esker Persona 5.0 and must be adhered to strictly to maintain the security of the software. The TOE has been tested on a Windows 2000 platform.

Note that the evaluated configuration is a specific configuration that, after purchase, must be installed and configured using the administrative guidance provided by the vendor.

3. Security Policy

The TOE with support from its IT environment provides the following security functions:

- Cryptographic Support.
- Information Flow.

- Identification & Authentication.
- Security Management.
- Self Protection.

In addition, the following organization security policies are 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.

The ST defines this in greater detail.

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following assumptions for the TOE were made:

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.
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.

4.2 Environmental Assumptions

Since the operating system, web server, and firewall are not included in the evaluation, they must be separately secured.

4.3 Clarification of Scope

None

4.3.1 Interpretations

The evaluation team performed an analysis of the international and national interpretations and identified those that are applicable and had impact to the TOE evaluation. The interpretations identified to have impact on the evaluation were applied by the evaluation team as the CEM work units were applied.

The following sections provide the number and title of the applicable interpretations and the CEM class in which they were considered.

Applicable National Interpretations

1. Configuration Management List (0412) - ASE
2. Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (0418) - ASE
3. Association Of Information Flow Attributes W/Subjects And Information (0417) - ASE
4. Empty Assignments (0407) – ASE
5. Management of Security Attributes (0409) - ASE
6. Identification of Standards (0427) - ASE

Applicable International Interpretations

1. Unique Configuration of CIs (03) – ASE
2. Scope of the Configuration Item List (04) – ASE
3. Content of Evidence (051) - ASE
4. Separate objectives for TOE and environment (084) – ASE
5. Strength of Function and Requirements (085) - ASE

4.3.2 Threats

Specific threats to IT security that should be countered by the Esker software Persona 5.0, and include threats against the host as well as 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 though 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.

5. Architectural Information

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 for communication between the Persona client and the Persona server. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

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

5.1 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 Persona 5.0 server provides the TSF. Three restrictions on the environment software for the Persona Server are that the operating system is Microsoft Windows 2000 or Windows XP Professional, a web server is installed, Microsoft Internet Information Server (IIS) and that the server be protected by a firewall. 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.

5.2 Logical Boundaries

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

5.2.1 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.

5.2.2 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.

5.2.3 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 manager[1] 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

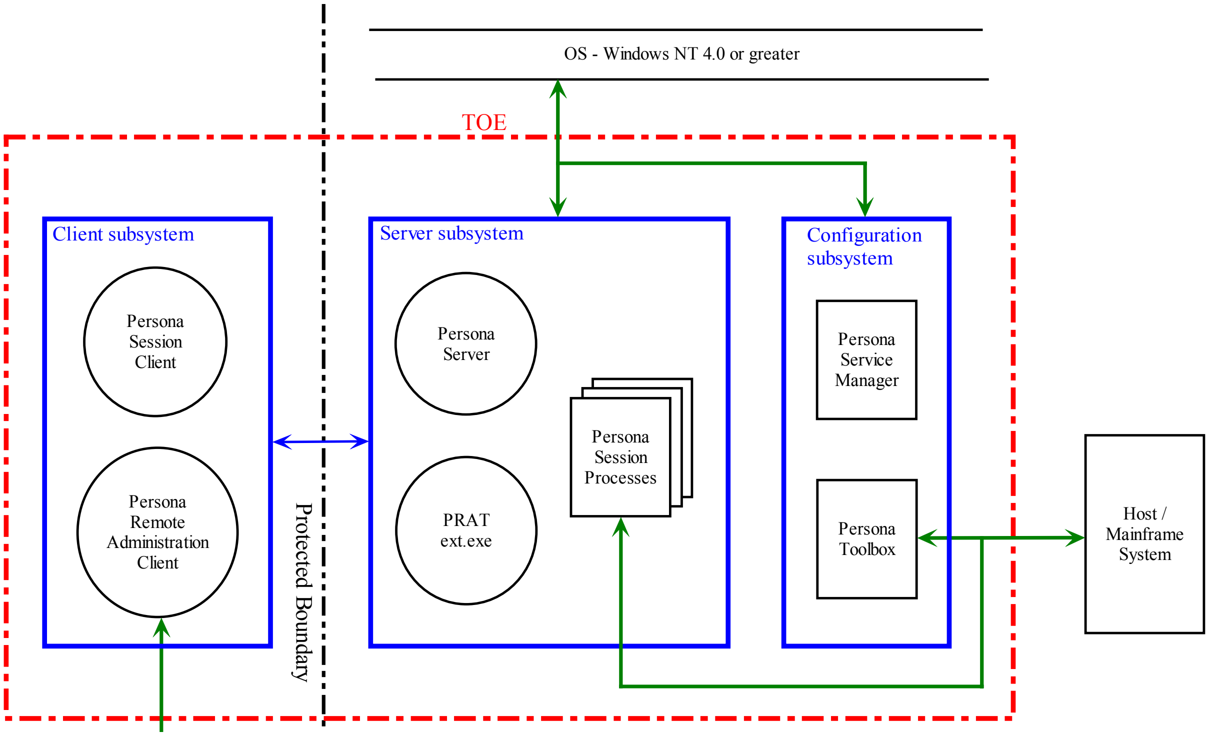

Figure 1: Esker Persona 5.0 Architecture

6. Delivered Product

The delivered product consists of the following items:

1. A CD labeled "Persona 5.0" (contains the TOE software - the help files are part of the GUI after installation)
2. A document titled "Esker Persona 5.0 Administrator's Getting Started Guide, Issued December 30, 2002"
3. A document titled "Important Delivery Information About your Persona 5.0 solution" (one page document to inform user of how the product was delivered to ensure safe arrival and content of box).
4. A Packing Slip
5. Software License Agreement

For a longer list of the major pieces of evidence examined during the evaluation, see section 14 of this report.

7. IT Product Testing

7.1 Examination of Vendor Tests

The vendor provided test plans, procedures, test results and a test coverage document. The evaluator examined the test coverage analysis and found that the vendor provided a correspondence between the tests provided for evaluation and the functional specification.

The evaluator was able to complete a sample of tests that represents approximately 75% of the vendor's test suite. The evaluator found this sufficient to verify the basic functionality of the TOE and the proper execution of the security functions.

The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSF was appropriate for this EAL3 evaluation. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.2 Evaluator Independent Tests

The evaluation team used the same test configuration used to perform the vendor test subset to perform the independent tests. The evaluation team also used the same test tools such as the packet sniffers documented in the vendor test documentation and used to perform the vendor test subset.

Independent testing was pursued to demonstrate the five security functions. As with the vendor test, for each test case, test were developed to include test steps, expected results, and actual results.

Note: when a vendor test case was discovered that was applicable to the team test description, the vendor test case was used but modified accordingly.

The evaluators found no obvious vulnerabilities during testing of the TOE.

7.3 Strength of Function

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim. The overall SOF claim for the TOE made in ST is expressed as an SOF rating, SOF-medium. The vendor provided calculations supporting their claim that the TOE met this rating. The evaluation team believed that the vendor calculations and assumptions were applicable and supported the rating of SOF-Medium. The SOF analysis (documented in "Persona Vulnerability Assessment Methodology" considered 3 cases - layman, proficient, and expert. In all case, the attacker had public knowledge of the TOE. In all cases the attacker required more than a Medium attack potential.

7.4 Vulnerability Analysis

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

The evaluation team examined the vendor's vulnerability analysis ["Persona Vulnerability Assessment Methodology"] and found that the vendor considered external resources and all of the evaluation deliverables: the ST, functional specification, high-level design, user guidance, administrator guidance, secure installation, generation, and start-up procedures, vulnerability analysis, and the strength of function claims analysis when developing ["Persona Vulnerability Assessment Methodology"].

The evaluation team devised a penetration test plan based upon the vendor's vulnerability assessment.

The evaluators did not identify a vulnerability that violated the TOE security policy given its environment and threats. Therefore, the evaluators determined that the product met the criteria of EAL3 for vulnerability analysis (in particular, that "The purpose of the vulnerability assessment activity is to determine the existence and exploitability of flaws or weaknesses in the TOE in the intended environment. This determination is based upon analysis performed by the developer and the evaluator, and is supported by evaluator testing.").

8. Evaluated Configuration

The environment configuration used to test the TOE by the evaluation team is described as follows:

Persona Server:

Persona 5.0 Server:	Windows 2000, sp3 with IIS 5

Persona Client:

Persona 5.0 Windows Thin Client:	Windows NT 4.0 SP6a
Persona 5.0 Java Application Client:	Windows NT 4.0 SP6a
Persona 5.0 Java Client:	Windows NT 4.0 SP6a (using IE 5.x)

Host:

IBM AS/400 host platform

Firewall Usage

A VPN configuration was utilized to connect to the host platform using Sonic Wall's Virtual Private Network (VPN) product. Additionally, IP Filtering on the server was enabled appropriately to protect the server and the host. Therefore, all client connection requests to connect to a host computer were directed through the Persona Server.

Tools Required:

The following test tools needed by the developer test suite are identified in the Persona Test Plan. These tools are also used in the Evaluation Independent Test Configuration.

CommView(Packet Sniffer Utility)

Windows 2000 Event Log

SonicWall Host firewall

9. Results of the Evaluation

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures [CCEVS_PUB 3]. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology [CEM], and the CCEVS. The validation team therefore concludes that the evaluation and its results of **pass** are complete.

9.1 Assurance Content

The evaluation provides for Assurance at the EAL 3 level without augmentation. Therefore, this includes the assurance components as shown in the table below:

EAL3 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

10.Validator Comments/Recommendations

As with any evaluation, this evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The product has been evaluated at the assurance level of EAL 3 and it has been determined that it meets its functional claims. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The validator observed that the evaluation and all of its activities were in accordance with the CC the CEM, and CCEVS practices; and that the CCTL presented appropriate CEM work units and rationale. The validation team therefore concludes that the evaluation, and its results of **pass,** are complete and correct.

11. Annexes

None, the remainder of this page is blank.

12. Security Target

The Security Target is provided separately; it is Version 1.0, December 31, 2002.

13. List Of Acronyms And Glossary Of Terms

The following acronyms are provided for reference:

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

The following terms are provided for reference:

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 others).

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 cipher text data,
- The transformation of cipher text 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.

14. Documentation

The evidence used in this evaluation is based upon the product and the following documentation:

Design documentation

RCR_Correspondence Matrix_11/21/2002_6:46 PM

DES_Persona Design_2002/12/16_0811

FS_Persona WTP Protocol Specification_12/02_0751

Delivery and Operation

DEL_Persona 5.0 U.S. Delivery Information_2002/11/18_1521

DEL_Persona 5.0 European Delivery Information_2002/11/18_1646
Esker Persona 5.0 Administrator's Getting Started Guide, Issued December 30, 2002

Guidance documentation
Esker Persona 5.0 Administrator's Getting Started Guide, Issued December 30, 2002

Configuration Management

TD_Beta Process_2002/10/185_1614

CM_Creating Patches and Specials_2002/11/22_1021

CM_Development Cycle_2002/11/22_1022

CM_Esker Policy Configuration List_2002/12/31_1032

CM_Host Access Configuration Management Plan_ 2002/12/13_1354

CM_Host Access Life Cycle Support_ 2002/12/18_1421

CM_The Nightly Build_2002/11/22_1029

CM_Persona 5.0 Configuration Item List.xls_11/23/2002_4:02 PM

CM_Post-Mastering Activities _2002/11/22_1025

CM_Releasing a Build to QA _2002/11/22_1025

CM_SmarTerm/Persona Builder Setup _2002/11/22_1028

CM_Tip-Toe Mode _2002/11/22_1039

Life Cycle

CM_Host Access Configuration Management Plan_2002/13/13_1354

Host Access Life Cycle Support: CM_Host Access Life Cycle Support_2002/12/18_1421

Test documentation

TD_Persona High Level Acceptance Testing Checklist_2003-02-06

TD_Persona Java Application Client Test Cases_2003-02-06

TD_Persona Java Client Test Cases_2003-02-06

TD_Persona Remote Admin Ext Test Cases_2002/12/18_0945

TD_Persona Remote Admin Tool Test Cases _2002/12/06_1136

TD_Persona Service Manager Test Cases _2002/12/06_1154

TD_Persona Service Test Cases_2002/12/18_1011

TD_Persona Sessions Process Test Cases _2002/12/18_0943

TD_Testing Methodology _2002/12/11_1206

TD_Persona Test Plan_2002/12/16_0945

TD_Persona Test Setup_2002/12/17_1557

TD_Persona Toolbox Test Cases_2002/12/18_0947

TD_Persona Windows Thin Client Test Cases _ 2002/12/17_1611

Actual Test Results, 12/12/02

Vulnerability Assessment
TD_Persona Vulnerability Assessment Methodology _ 2002/12/10_1747

Security Target
Esker Persona 5.0 Security Target, version 1.0, 12/31/02

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB 1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS_PUB 2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000

[CCEVS_PUB 3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 1.0, January 2002.

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.