Computer Associates

eTrust™ Single Sign-On V7.0

Security Target V2.0

October 20, 2005

Suite 5200 West♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0985

TABLE OF CONTENTS

SECTION **PAGE**

1 SECURITY TARGET INTRODUCTION 1

1.1 SECURITY TARGET IDENTIFICATION 1
1.2 SECURITY TARGET OVERVIEW 1
1.3 COMMON CRITERIA CONFORMANCE 1
1.4 DOCUMENT ORGANIZATION 1

2 TOE DESCRIPTION 3

2.1 PRODUCT TYPE 3
2.2 ETRUST SSO COMPONENTS 3
2.3 TSF BOUNDARY AND SCOPE OF THE EVALUATION 4
2.4 TOE FUNCTIONALITY 6
2.5 IT ENVIRONMENT 7

3 TOE SECURITY ENVIRONMENT 9

3.1 ASSUMPTIONS 9
3.2 THREATS 9

4 SECURITY OBJECTIVES 11

4.1 SECURITY OBJECTIVES FOR THE TOE 11
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 11
4.2.1 Security Objectives for the IT Environment 11
4.2.2 Non-IT Security Objectives 12

5 IT SECURITY REQUIREMENTS 13

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 13
5.1.1 Class FAU: Security Audit 14
5.1.2 Class FIA: Identification and Authentication 14
5.1.3 Class FMT: Security Management 16
5.1.4 Class FTA: TOE Access 16
5.1.5 Strength of Function 16
5.2 SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT 16
5.2.1 Class FAU: Audit 17
5.2.2 Class FIA: Identification and Authentication 17
5.2.3 Class FMT: Security Management 18
5.2.4 Class FPT: Protection of the TSF 19
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 20

6 TOE SUMMARY SPECIFICATION 21

6.1 IT SECURITY FUNCTIONS 21
6.1.1 Overview 21
6.1.2 Primary Authentication 21
6.1.3 Application Authentication 22
6.1.4 Passwords 23
6.1.5 Auditing 24
6.1.6 TOE Access 24
6.1.7 SOF Claims 24
6.2 ASSURANCE MEASURES 25

7 PP CLAIMS 26

8 RATIONALE 27

8.1 SECURITY OBJECTIVES RATIONALE 27
8.1.1 Threats to Security 27
8.1.2 Assumptions 30
8.2 SECURITY REQUIREMENTS RATIONALE 31
8.2.1 Functional Requirements 31
8.2.2 Requirements for the IT Environment 33
8.2.3 Dependencies 34
8.2.4 Strength of Function 35
8.2.5 Assurance Requirements 35
8.2.6 Rationale that IT Security Requirements are Internally Consistent 35
8.2.7 Rationale for Explicitly Stated Requirements 36
8.3 TOE SUMMARY SPECIFICATION RATIONALE 36
8.3.1 IT Security Functions 36
8.3.2 Assurance Measures 38
8.4 PP CLAIMS RATIONALE 40

9 ACRONYMS 41

10 REFERENCES 42

Table Of Tables and Figures

Table or Figure **Page**

FIGURE 2-1 – ETRUST SINGLE SIGN-ON COMPONENTS 4
FIGURE 2-2 -TOE BOUNDARY 6
FIGURE 2-3 LOGICAL VIEW OF TOE INTERFACES 7
TABLE 5-1 – SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE 13
TABLE 5-2 – SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT 16
TABLE 5-3 – MANAGEMENT OF TSF DATA 18
TABLE 5-4 – EAL2 ASSURANCE COMPONENTS 20
TABLE 8.1 – ALL THREATS TO SECURITY COUNTERED 27
TABLE 8.2 – ALL ASSUMPTIONS ADDRESSED 30
TABLE 8.3 - ALL OBJECTIVES MET BY FUNCTIONAL COMPONENTS 31
TABLE 8.5 - ALL OBJECTIVES FOR THE IT ENVIRONMENT MET BY REQUIREMENTS 33
TABLE 8.4 - ALL DEPENDENCIES SATISFIED 34
TABLE 8.6 – MAPPING OF FUNCTIONAL REQUIREMENTS TO TOE SUMMARY SPECIFICATION 36
TABLE 8.7 – ASSURANCE MEASURES RATIONALE 38

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:	Computer Associates eTrust™ Single Sign-On V7.0 with patch QO67747
ST Title:	Computer Associates eTrust™ Single Sign-On V7.0 Security Target
ST Version:	Version 2.0
ST Author:	CygnaCom Solutions, Inc.
ST Date:	October 20, 2005
Assurance level:	EAL2
Registration:	<To be filled in upon registration>
Keywords:	Single Sign-On, Network Security, Identification, Authentication, Access Control, Tickets, and Security Target

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Computer Associates (CA) eTrust™ Single Sign-On. eTrust Single Sign-On is a distributed security software product that manages passwords and other authentication mechanisms for logging into multiple applications and hosts on a network. Single Sign-On automates the login process and eliminates a user's need to keep track of multiple user IDs and passwords.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5 specifies the TOE Security Requirements. The TOE security requirements are made up of Functional Requirements and Assurance Requirements. This section also includes Security Requirements for the IT Environment.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Acronym definitions and references are provided in the Appendices.

2 TOE DESCRIPTION

2.1 Product Type

eTrust Single Sign-on (SSO) is a distributed security software product that manages passwords and other authentication mechanisms for logging into multiple applications and hosts on a network. eTrust SSO automates the login process and eliminates a user's need to keep track of multiple user IDs and passwords.

2.2 eTrust SSO Components

eTrust SSO features a central administration interface that provides central control of all SSO-enabled user and application profiles. The eTrust SSO product consists of the following components: Policy Server, Policy Manager, Authentication Agent(s) and SSO Clients. Figure 2.1 provides an overview of how these components are integrated.

The **Policy Server** is a process that runs on a server host. The Policy Server is the heart of eTrust SSO. It controls eTrust SSO functions and maintains communications between the various eTrust SSO components and the secure applications that the users invoke. It also updates audit logs.

The eTrust Access Control and eTrust Directory data repositories reside on the Policy Manager host. However, these products are being separately evaluated and are part of the IT environment. eTrust Access Control is used primarily to store information about resources, applications, and access-control rules. eTrust Directory stores information about users, user groups, and logon information in an LDAP repository.

The **Policy Manager** is GUI application that is used to manage the information stored in the Policy Server. It is installed on an administrator's Windows workstation with TCP/IP communication to the Policy Server.

Authentication Agents are processes that run, generally, on an authentication host server and verifies user credentials with the authentication host (e.g., Windows AD domain controller or a Mainframe server). Once verified, the Auth Agent creates an SSO ticket which is passed back to the SSO Client and the SSO Client uses this ticket in any subsequent communications with the Policy Server – the ticket verifies the authenticity of the user using the SSO Client.

An **SSO Client** is a GUI application that runs on every user workstation. It provides a flexible and intuitive interface to the end user to enter their primary login credentials and once verified, provides automatic access to their SSO enabled applications without need to re-enter their application credentials.

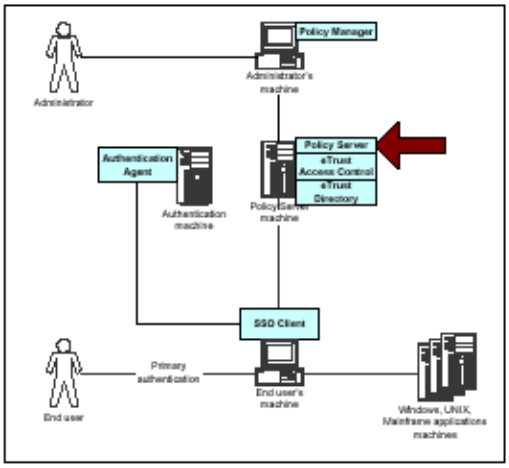

Figure 2-1 – eTrust Single Sign-On Components

2.3 TSF Boundary and Scope of the Evaluation

The TOE includes the following Software Components:

The TOE will be installed to its evaluated configuration as shown in Figure 2.2. The evaluated configuration will be on 4 separate machines which include the following:

- Server 1: Policy Server and Policy Manger running on one machine with Windows 2000 Server SP4.
- Server 2: Authentication agent running on Windows 2000 Server SP4
- Workstation 1: Policy Manager and SSO Client running on one machine with Windows 2000 SP4.
- Workstation 2: SSO Client running on Windows 2000 SP4.

In the evaluated configuration, LDAP authentication for primary authentication is used.

The TOE is software-only and includes the Policy Server, Authentication Agent, Policy Manager, and SSO client software components.

The TOE does not include the following IT Environment Components:

- Underlying Hardware platform(s)
- Underlying Operating System platform(s): Windows 2000 Server SP4 for all product components
- eTrust Access Control v5.2
- eTrust Directory 8.0
- LDAP implementation
- LDAP client used to connect to LDAP directory
- SSL implementation
- Cryptographic modules
- Domain Controller used to provide a physically protected local area network.

- Applications

Copies of eTrust Access Control v5.2 and eTrust Directory v8.0 are embedded in the Policy Server. However, these products are being separately evaluated and are outside the scope of this evaluation.

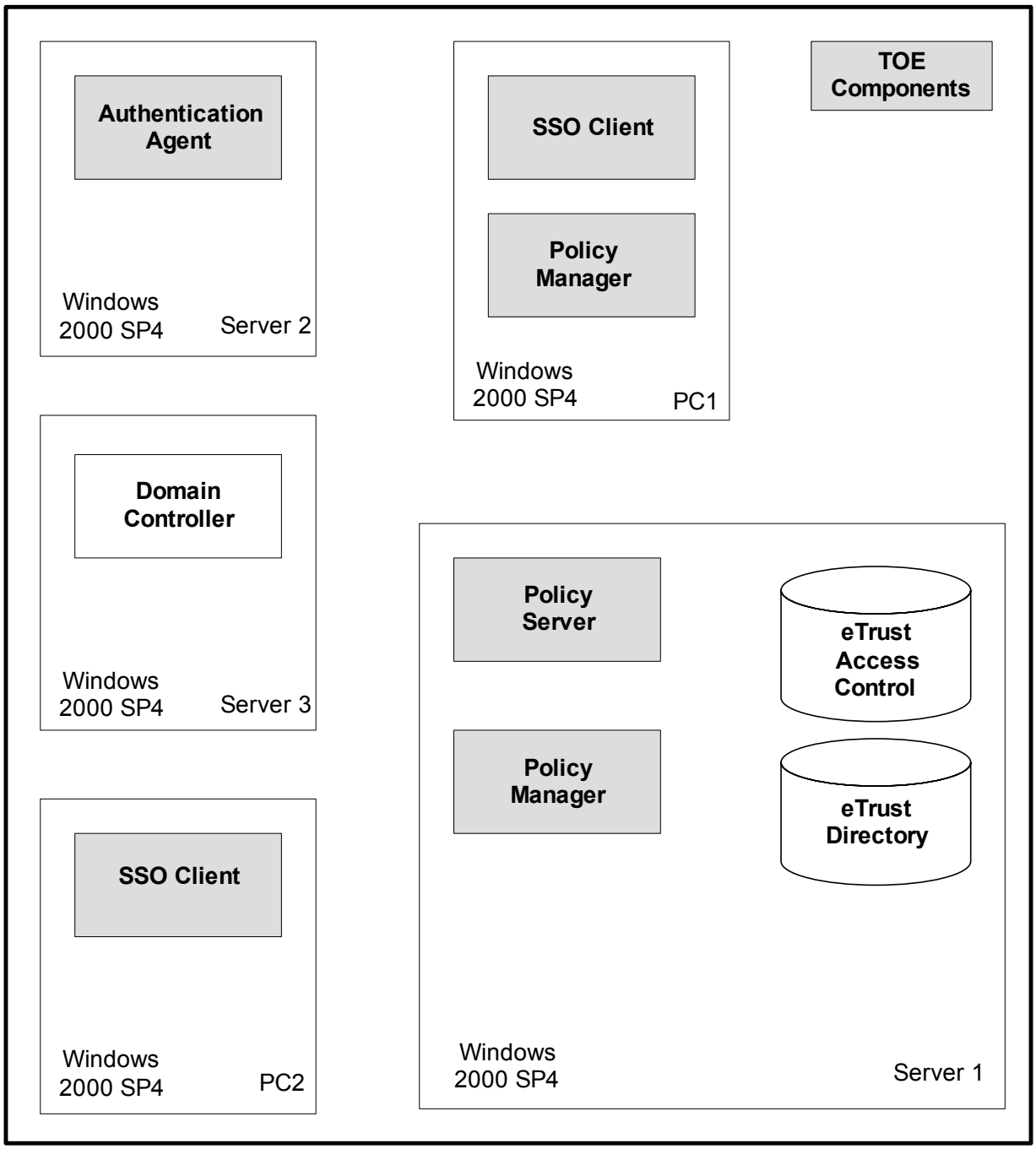

Figure 2-2 -TOE Boundary

2.4 TOE Functionality

The TOE provides the following security functionality: identification and authentication, audit, secure management of TOE security functions and data, session establishment, and protection of TOE security functions. The main security service provided by eTrust SSO is to manage authentication information securely. eTrust SSO manages passwords and other authentication information for logging into multiple applications and hosts on a network. There are two steps of the authentication process: **primary authentication** and **application authentication**.

Primary authentication is the process by which the end user is authorized to use eTrust SSO. The host that performs primary authentication is called the authentication host. Primary authentication is performed by an Authentication Agent running on the authentication host.

The Authentication Agent verifies the credentials that the SSO Client provides, and if they are valid sends an SSO ticket back to the SSO Client. The SSO Client caches the ticket and sends the ticket to the Policy Server as proof that the end user has been authenticated. . An SSO ticket is valid for a predetermined period of time.

Once the end user is successfully authenticated, the SSO Client requests an application list. The end user selects an application. The SSO Client sends the SSO ticket that it has cached on behalf of the user to the Policy Server to obtain the necessary information to login to the application. If the end user is authorized to login to the application at the time, the Policy Server sends the information to login to the application to the SSO Client. The SSO Client authenticates the end user to the application.

eTrust SSO provides the capability for users to create or generate passwords either for primary authentication when authenticating to the SSO client or for authentication to the application. ETrust can enforce its password policy at the time that the passwords are created by the user or generated.

eTrust SSO provides the capability of auditing the following events: primary authentication, end user request for an application list, end user request for login variables,

eTrust SSO can control the number of sessions a user can have open.

Figure 2-3~~Figure 2-3~~ shows a logical view of the eTrust SSO components and interfaces.

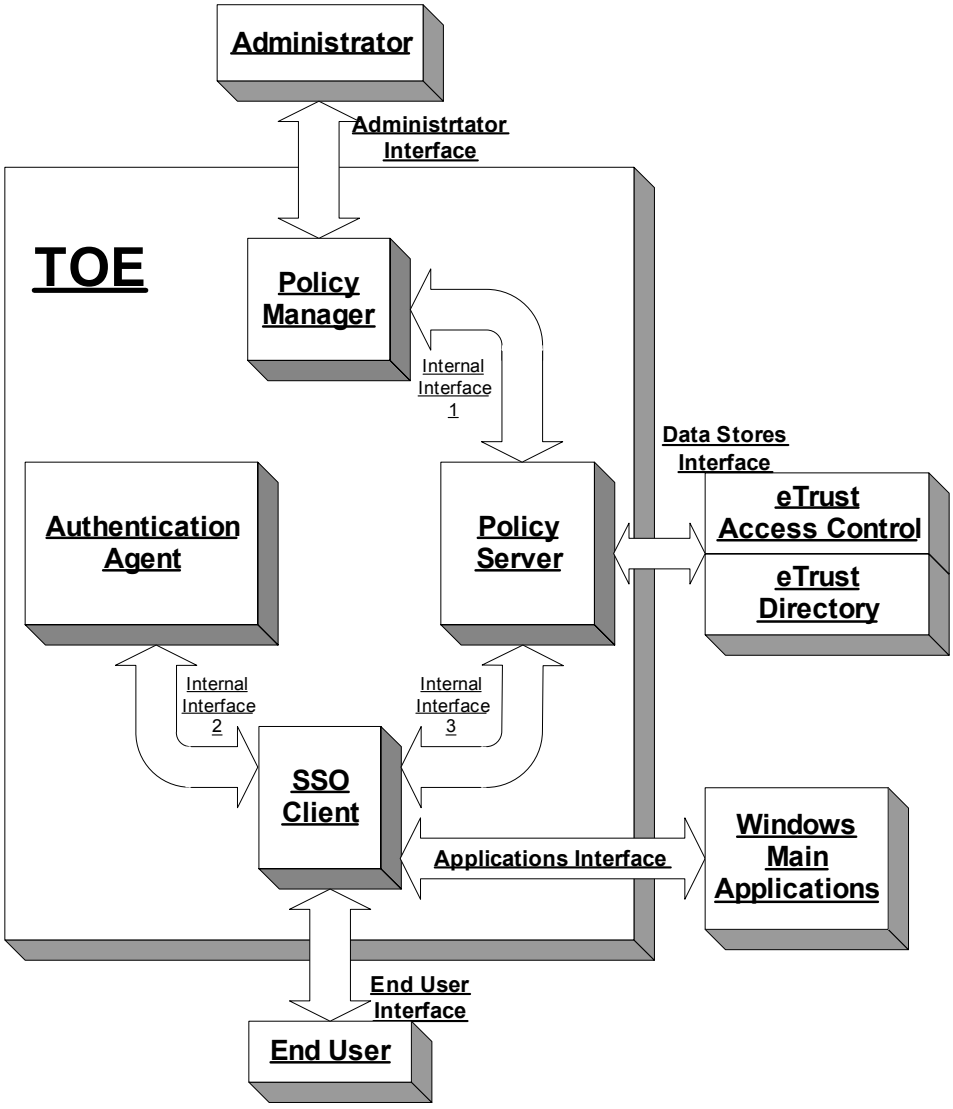

Figure 2-3 Logical View of TOE Interfaces

2.5 IT Environment

It is assumed that there will be no untrusted users or software on the Policy Server and Authentication Host servers. It is assumed that the TOE components communicate over a physically protected Local Area Network.

eTrust SSO relies upon the underlying operating system on both the Authentication Hosts and Policy Server machines providing reliable and consistent time stamps. This is because tickets generated by Authentication Hosts are only valid for a designated time interval, which is configurable. The administrator is responsible for ensuring that the Policy Server and Authentication Host servers' clocks are synchronized.

eTrust Access Control and eTrust Directory are also part of the IT environment. They provide the data repository and security management functions.

Audit records are stored in the IT environment.

All communication between SSO components uses industry standard 3-DES or El Gamal 128 key encryption. The eTrust SSO ticket, used for authentication, is encrypted using a secret key that both the Authentication Agent and the Policy Server know. Encryption is not in the scope of the TOE and therefore, was not tested.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

The secure usage assumptions are as follows:

Item	Assumption ID	Assumption Description
1	A.Admin	The administrator is trusted to correctly configure the TOE.
2	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the Policy Server host.
3	A.TrustedLAN	It is assumed that the TOE components communicate over a physically protected Local Area Network.
4	A.Users	It is assumed that users will protect their authentication data.

3.2 Threats

The TOE must counter the following threats to security:

Item	Threat ID	Threat Description
1	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.
2	T.ForgeAuth	An attacker may attempt to forge or copy authentication information, in order to gain unauthorized access to resources protected by the TOE.
3	T.Impersonate	An attacker may attempt to impersonate another user, in order to gain unauthorized access to protected resources.
4	T.Mismanage	Administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
5	T.NoAttributes	The TSF may not be able to correctly enforce its security policy with respect to identification and authentication or TOE access due to not maintaining user security attributes.
6	T.OffHours	An attacker may attempt to login as an authorized user and gain unauthorized access to resources protected by the TOE. The attacker may login multiple times, thus locking out the authorized user.
7	T.Reuse	An attacker may attempt to reuse authentication data, allowing the attacker to gain unauthorized access to resources protected by the TOE.

Item	Threat ID	Threat Description
8	T.TSF_Compromise	A user or process may cause, through an unsophisticated attack, TSF date, or executable code to be inappropriately viewed, modified, or deleted.
9	T.Undetect	Attempts by an attacker to violate the security policy and tamper with TSF data may go undetected.
10	T.Walkaway	A logged-in user may leave a workstation without logging out, which could enable an unauthorized user to gain access to the resources protected by the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Item	Objective ID	Objective description
1	O.Audit	The TOE must be able to audit primary authentication attempts, end user requests for application lists and login information, and access to eTrust SSO records.
2	O.AuthPrim	The TOE must identify and authenticate all users before providing them with application authentication information.
3	O.DenySession	The TOE must be able to deny session establishment based the maximum number of sessions a user can have open simultaneously and an idle time-out.
4	O.Expire	The TOE must associate an expiration date with authentication information.
5	O.PasswordGen	The TOE must support automatic generation of passwords.
6	O.PasswordQual	The TOE must be able to specify password quality parameters such as minimum and maximum interval between password changes, minimum length, and numbers of types of characters.
7	O.Reauthenticate	The TOE must be able to require the user to be reauthenticated under specified conditions.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objective for the IT environment is as follows:

Item	Objective ID	Objective description
1E	OE.Admin	The IT environment must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.
2E	OE.Attributes	The IT environment must maintain user attributes.
3E	OE.AuditStore	The IT environment must store audit data.
4E	OE.Manage	The IT environment must be able to store and maintain properties of users and resources.
5E	OE.Roles	The IT environment must support multiple administrative roles.

Item	Objective ID	Objective description
6E	OE.Self_Protection	The IT environment will maintain a domain for the execution of the TSF that protects the TSF and its resources from external interference, tampering, or unauthorized disclosure.
7E	OE.Time	The underlying operating system must provide reliable time stamps to support the audit function.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are as follows:

Item	Objective ID	Objective description
1N	ON.Install	Those responsible for the TOE must ensure that the TOE is delivered and installed on a physically protected Local Area Network in a manner that maintains IT security.
2N	ON.NoUntrusted	The administrator must ensure that there are no untrusted users and no untrusted software on the Policy Server host.
3N	ON.Operations	There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner.
4N	ON.ProtectAuth	The users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, and CCIMB Final Interpretations.

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. Iterations are not included in this ST and are not discussed further. These operations are defined in Common Criteria, Part 1, section 4.4.1.3.2 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5.1. . All except FMT_SAE_EXP.1 are taken from Part 2 of the Common Criteria. FMT_SAE_EXP.1 is an explicitly stated requirement which is derived in part from CC Part 2.

Table 5-1 – Security Functional Requirements for the TOE

Item	Component	Component Name
1	FAU_GEN.1	Audit data generation
2	FIA_SOS.1	Verification of secrets
3	FIA_SOS.2	TSF Generation of secrets
4	FIA_UAU.2	User authentication before any action [Primary Authentication]
5	FIA_UAU.6	Re-authenticating [Primary Authentication]
6	FIA_UID.2	User identification before any action [Primary Authentication]
7	FMT_SAE_EXP.1	Enforcement of time-limited authorization
8	FTA_TSE.1	TOE session establishment

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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

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

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

c) [the following* auditable events*:

- ***Primary authentication, and***
- ***End user request for login variables.]***

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[none]***

Dependencies: FPT_STM.1 Reliable time stamps

5.1.2 Class FIA: Identification and Authentication

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***[the rules of the password policy:***

- ***Minimum length of 8,***
- ***At least one special character,***
- ***At least one numeric character,***
- ***At least one uppercase and one lowercase character***
- ***30 day expiration date***
- ***Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as "password").]***

]

Dependencies: No dependencies.

Application note: SSO enforces the password policy for passwords created on SSO at the time that the user creates the password. The password policy rules are stored in the data store. The administrator must configure a password policy that meets the minimum requirements for the evaluated configuration as specified in the Administrator Guide. These rules are specified in Section 6.1.4.

FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet ***[the rules of the password policy:***

- ***Minimum length of 8,***
- ***At least one special character,***
- ***At least one numeric character,***
- ***At least one uppercase and one lowercase character***
- ***30 day expiration date***
- ***Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as "password")]***

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for ***[Application and Primary Authentication].***

Dependencies: No dependencies.

Application Note: SSO can be used to generate passwords both for use on SSO and applications. When SSO generates a password, it meets the rules specified by the password policy. The password policy rules are stored in the data store. The administrator must configure a password policy that meets the minimum requirements for the evaluated configuration as specified in the Administrator Guide. These rules are specified in Section 6.1.4.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions

- ***[When the SSO Ticket expires;***
- ***When the SSO Client's workstation is locked using the eTrust SSO StationLock option; and***
- ***When accessing specific applications designated as "sensitive" that require reauthentication at frequent intervals.].***

Dependencies: No dependencies.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.1.3 Class FMT: Security Management

FMT_SAE_EXP.1 Enforcement of time-limited authorisation

Hierarchical to: No other components.

FMT_SAE_EXP.1.1 For each of these security attributes, the TSF shall be able to [***disallow authentication***] after the expiration time for the indicated security attribute has passed.

Dependencies:

FPT_STM.1 Reliable time stamps

5.1.4 Class FTA: TOE Access

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on ***[the maximum number of sessions a user can have open simultaneously; an idle time-out for locking a session]***

Dependencies: No dependencies

5.1.5 Strength of Function

The overall strength of function requirement is SOF-Basic. The strength of function requirement applies to FIA_SOS.1 and FIA_SOS.2. The SOF claim for FIA_SOS.1 and FIA_SOS.2 is SOF-Basic.

5.2 Security Functional Requirements for the IT Environment

The security functional requirements for the IT environment are listed in Table 5.2. All except FMT_SAE_ENV.1 are taken from Part 2 of the Common Criteria. FMT_SAE_ENV.1 is an explicitly stated requirement which is derived in part from CC Part 2.

Table 5-2 – Security Functional Requirements for the IT Environment

Item	Component	Component Name
1	FAU_STG.1	Protected Audit Trail Storage
2	FIA_ATD.1	User attribute definition
3	FMT_MOF.1	Management of security function behavior

Item	Component	Component Name
4	FMT_MTD.1	Management of TSF data
5	FMT_SAE_ENV.1	Management of expiration time
6	FMT_SMF.1	Specification of management functions
7	FMT_SMR.1	Security roles
8	FPT_RVM.1	Non-Bypassability of the TSP
9	FPT_SEP.1	Domain separation
10	FPT_STM.1	Reliable time stamps

5.2.1 Class FAU: Audit

Audit records are stored in the IT environment.

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 **Refinement:** The ***IT environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 **Refinement:** The ***IT environment*** shall be able to ***[prevent***] unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FIA: Identification and Authentication

User attributes are stored and managed in the IT environment.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 **Refinement:** The ***IT Environment*** shall maintain the following list of security attributes belonging to individual users:

- ***[User name;***
- ***Method used for authenticating this user;***
- ***Administrative role(s) the user can assume (administrator; auditor; operator, password manager);***
- ***Applications that the user is authorized to access;***
- ***Login information for the various applications that the user is authorized to access;***
- ***Terminal identifier(s) for the user's current SSO sessions(s);***
- ***Metaframe Application identifiers for the user's current Metaframe Application sessions;***
- ***Date and time of the user's last login;***

- ***Day and time restrictions on the user's logins;***
- ***Date(s) and time(s) of the user's last password update(s), if the method used for authenticating this user involves one or more passwords ;***
- ***Date, if any, on which the user's account was suspended;***
- ***Date, if any, on which the user's account was reinstated.***
- ***Expiration date for the user's account;]***

Dependencies: No dependencies.

5.2.3 Class FMT: Security Management

These functions are provided by the eTrust Access Control and eTrust Directory in the IT environment.

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 **Refinement:** The ***IT Environment*** shall restrict the ability to **[determine the behaviour]** the functions **[*audit*]** to **[*Auditor*].**

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 **Refinem**

ent*:* The ***IT Environment*** shall restrict the ability to ***[change_default, query or modify as specified in Table 5.3***] the ***[TSF Data as specified in Table 5.3)***] to ***[the role as specified in Table 5.3].***

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

Table 5-3 – Management of TSF Data

Role	Allowed Operations on TSF Data
Administrator	The administrator can add, read or modify user, group, application, authentication hosts records including authentication and login information. The administrator cannot select auditable events or review the audit log.
Auditor	The auditor can select auditable events and review the audit log.
Password Manager	The password manager can change another user's password.
End User	If eTrust SSO is configured to allow users to change their passwords, as opposed to requiring that their passwords be automatically generated, an End User can change his or her own password.

FMT_SAE_ENV.1 Management of expiration time

Hierarchical to: No other components.

FMT_SAE_ENV.1.1 The TSF shall restrict the capability to specify an expiration time for [***tickets***] to [***Administrators***].

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

FMT_SMF.1.1 **Refinement:** The ***IT Environment*** shall be capable of performing the following security management functions [***Management of TSF data as specified in Table 5.3***.]

Dependencies: No dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 **Refinement:** The ***IT Environment*** shall maintain the roles [

- ***Administrator,***
- ***Auditor,***
- ***Password Manager,***
- ***End User].***

FMT_SMR.1.2 **Refinement:** The ***IT Environment*** shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.2.4 Class FPT: Protection of the TSF

This function is provided by the underlying operating system.

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 **Refinement:** The ***IT Environment*** shall ensure that ***IT Environment security policy*** enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1 Domain separation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT Environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The EAL2 assurance components are listed in Table 5.3.

Table 5-4 – EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

eTrust SSO is a distributed system that provides a single sign-on capability. The SSO Client runs on each end user's workstation and interacts with the eTrust SSO Client, which in turn interacts with an Authentication Agent running on an authentication host to verify the user credentials entered by the user in the SSO Client. Once these primary credentials are verified by the Authentication Agent, the Authentication Host returns a SSO ticket to the SSO Client which the SSO Client uses in turn to verify the user to the Policy Server. The SSO Client automatically interacts with the Policy Server to retrieve the list of SSO enabled applications that the user is defined to access. The SSO Client displays this list of applications to the end user. Once the end user launches any of these applications, the Policy Server, upon verifying the identity of the end-user (by verifying the information passed in the encrypted ticket from the Client, provides the eTrust SSO Client with a login script and the user's login credentials for that application. The SSO Client then uses the login script (a TCL script) and the user's login credentials to launch the application and populate the applications login dialog.

The main security service provided by eTrust SSO is to manage authentication information securely. The two steps involved in an eTrust SSO authentication session are **Primary Authentication** and **Application Authentication.**

6.1.2 Primary Authentication

IAPRI-1 Primary Authentication

Primary Authentication is the way that eTrust SSO users prove their identities. Once users have proved their identities, these users are entitled to obtain their application login information. eTrust SSO performs no actions on behalf of the user without authenticating the user.

During primary authentication, the eTrust SSO Client executing on the user's workstation provides the user's authentication information to an Authentication Agent running on an Authentication Host. The Authentication Agent uses the capabilities of the Authentication Host, which can include things such as reading biometric data or smartcards, to authenticate the user. In the evaluated configuration, LDAP authentication is to be used (username/password). Thus, the Authentication will be partially provided by eTrust Directory which is outside the TOE Boundary. After the user is authenticated, the Authentication Agent creates an SSO Ticket and sends it to the SSO Client, which caches it. An SSO Ticket is valid for a predetermined period of time set by the Administrator through an MS Windows interface in the IT environment. Once primary authentication is carried out, the eTrust SSO Client automatically requests an application list and this list is displayed on the end user's workstation.

When the end user requests to log into one of their SSO enabled application, the SSO Client sends the SSO ticket that it has cached, to the Policy Server. If the SSO Ticket has not expired and the Policy Server verifies the authenticity of the SSO ticket, the Policy Server sends the login variables and the application script to the SSO Client. If the SSO ticket has expired, the Policy Server informs the eTrust SSO Client that the SSO ticket is invalid and tells it to re-authenticate the user by performing primary authentication again.

IAPRI-2 Primary Authentication Options

eTrust SSO supports the following evaluated Authentication method:

- LDAP (any LDAP compliant repository.)

IAPRI-3 Tickets for Primary Authentication

The SSO ticket is an encrypted string containing the information needed for authenticating the user to the Policy Server. When the SSO Client starts up, it requests authentication from its designated Authentication Agent. The Authentication Agent works with an Authentication Host to verify the user's credentials provided by the SSO Client, and if they are valid sends an SSO Ticket to the eTrust SSO Client. The SSO Client then subsequently sends the SSO ticket to the Policy Server for any requests for data as proof that the end user has been authenticated.

Tickets have an expiration time and the Policy Sever checks whether or not the ticket has expired. SSO tickets are time stamped. The time stamp, provided by the IT environment, is used by the Policy Server to verify whether or not the ticket has expired. An expired ticket will require the user to reauthenticate before being allowed access to the applications.

SSO Ticket encryption is provided by a combination of ElGamal Public Key and Triple DES encryption in the IT environment.

IAPRI-4 Reauthentication

There are three cases for which the end user will have to be re-authenticated:

- When the SSO ticket expires;
- When the eTrust SSO Client's workstation is locked using the eTrust SSO StationLock option. This option locks the end user out of the workstation after the workstation is idle for a specified period and displays the appropriate login box depending on what primary authentication mechanism the user is defined to be able to use. Once the required data is entered, the eTrust SSO Client attempts reauthentication with the primary authentication agent. If reauthentication is successful, the eTrust SSO Client unlocks the workstation; and
- When accessing specific applications designated as "sensitive" that require reauthentication at frequent intervals, such as five minutes.

6.1.3 Application Authentication

IAAPP-1 Application Login Information

The Policy Server retrieves from the embedded eTrust Access Control* repository a list of applications that the user is authorized to use and sends the list to the eTrust SSO Client. When the end user selects an application from the application list displayed on the workstation, the eTrust SSO Client sends the SSO Ticket and the application identifier to the Policy Server. The Policy Server checks the SSO Ticket and if it is valid, the Policy Server sends the login script (a TCL script) and the login information to the eTrust SSO Client. The eTrust SSO Client then automatically begins to execute the login script. First, the login script starts up the application. Then it carries out application authentication by populating the user's application credentials in the applications login dialog.

eTrust SSO supports the following mechanisms to log users into applications: Password, One Time Password (OTP), and Ticket. Only the Password mechanism is included in the evaluated configuration.

eTrust Directory and eTrust Access Control are part of the IT Environment.

IAAPP-2 Application Password Authentication

If the application uses a password for login, then the eTrust SSO Client executes the login script on the workstation, simulating a normal end user login. The eTrust SSO Client invokes the application and then enters the login information sent from the Policy Server into the proper fields in the application's login window or screen.

The first time a user invokes one of their SSO enabled applications, they will be prompted to enter their application credentials. The credentials are sent to the Policy Server which stores them in the embedded eTrust Directory or eTrust Access Control repositories. This process on the SSO Client is termed "Learn Mode". Subsequently, when a user invokes the same application, the Policy Server fetches the user's username and password for the selected application from the embedded eTrust Directory or eTrust Access Control product repository and sends it to the eTrust SSO Client so that the user is automatically allowed access without manual intervention.

eTrust Directory and eTrust Access Control are part of the IT Environment.

6.1.4 Passwords

PWD-1 Password Policy

A password policy is a set of rules for checking the validity of a new password and for defining when a password expires. SSO has the capability of specifying the following password attributes:

- The minimum length of the password;
- The minimum number of alphanumeric, alphabetic, uppercase, lowercase, numeric, and/or special characters.
- For how many days, maximum and minimum, each password is to remain usable.
- How many previous passwords to retain as unusable. Up to 8 previous passwords can be defined as unusable.

Password policies are a class in the eTrust Single Sign-On Data Store (refer to Table 6-1). Password policies apply to both user-selected and automatically generated passwords.

The Administrator Guide requires that passwords in the evaluated configuration meet the following minimum requirements:

- Minimum length of 8,
- At least one special character,
- At least one numeric character,
- At least one uppercase and one lowercase character
- 30 day expiration date
- Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as "password").

PWD-2 Password Generation

Single Sign-On supports automatic generation of passwords. The administrator can require the automatic generation of passwords using the PWD_AUTOGEN property in the USER class record. Automatically generated passwords must meet the same password policy rules as user-selected passwords.

6.1.5 Auditing

AUDIT-1 Audit Generation

The eTrust Single Sign-On Policy Server generates the following types of audit events:

- Primary authentication,
- End user request for login variable

AUDIT-2 Audit Record Contents

The following information is recorded for all events:

- User issuing the request,
- Type of event,
- Date and time of event, and
- Success or failure of event.

When login variables are requested, the application name is recorded.

6.1.6 TOE Access

TA-1 Session Establishment

The eTrust Single Sign-On Administrator uses the following to control a user's session:

- Limiting the maximum number of sessions a user can have open simultaneously
- Defining what happens when a user attempts to exceed the number of open sessions:
    - Terminate the oldest session
    - Terminate the newest session
    - Terminate all sessions
    - Ask the user which of their sessions they want to terminate
    - Reject the registration of the new session – the user is denied log-on
- Set the idle time-out for locking a session.

6.1.7 SOF Claims

The following IT Security Functions are realized by probabilistic or permutational mechanisms:

- PWD-1 Password Policy
- PWD-2 Password Generation

The SOF claim for this IT security function is SOF-Basic.

6.2 Assurance Measures

The eTrust Single Sign-On Policy Server satisfies the assurance requirements for Evaluation Assurance Level EAL2.

The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Item	Assurance Requirement	Evaluation Evidence
1	ACM_CAP.2	Configuration Item List
2	ADO_DEL.1	Distribution Centers Procedures Manual 2004Mar01 (DCPM) Product Submission Form (2003Dec18) Product Submission Form Process Flow.doc (2003Dec18) Preservation of Product 1Apr2004
3	ADO_IGS	Computer Associates, *eTrust™ Single Sign-on Getting Started* Computer Associates, eTrust™ *Single Sign-on Administrator's Guide 7.0*
4	ADV_FSP.1	Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0* Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0*
5	ADV_HLD.1	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0*
6	ADV_RCR.1	Computer Associates eTrust SSO Client version 7.0.1 Common Criteria Evaluation Development Specification 0.8, 26 January 2005
7	AGD_ADM.1	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0* Computer Associates, *eTrust™ Single Sign-on User's Guide for the Assistant 7.0* Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0*
8	AGD_USR.1	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0* Computer Associates, *eTrust™ Single Sign-on User's Guide for the Assistant 7.0* Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0*
9	ATE_COV.1	*Test coverage analysis, eTrust™ Single Sign-on,* Version 1.2
10	ATE_FUN.1	Test scripts provide by the vendor
11	ATE_IND.2	TOE for Testing
12	AVA_SOF.1	*Computer Associates eTrust Single Sign-on Strength of Function Analysis,* Version 1.1
13	AVA_VLA.1	*Computer Associates Single Sign-on Vulnerability Analysis,* Version 1.1

7 PP Claims

The eTrust Single Sign-On Policy Server Security Target was not written to address any existing Protection Profile.

8 RATIONALE

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8.1 shows that all the identified threats to security are countered by Security Objectives for the TOE.

Table 8.1 – All Threats to Security Countered

Item	Threat Name	Threat Description	Security Objective
1	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.	5 - O.PasswordGen 6 - O.PasswordQual
2	T.ForgeAuth	An attacker may attempt to forge or copy authentication information, in order to gain unauthorized access to resources protected by the TOE.	4 - O.Expire 7 - O.Reauthenticate
3	T.Impersonate	An attacker may attempt to impersonate another user, in order to gain unauthorized access to protected resources.	2 - O.AuthPrim 4 - O.Expire 6 - O.PasswordQual
4	T.Mismanage	Administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	1E - OE.Admin 4E - OE.Manage 5E - OE.Roles
5	T.NoAttributes	The TSF may not be able to correctly enforce its security policy with respect to identification and authentication or TOE access due to not maintaining user security attributes.	2E - OE.Attributes
6	T.OffHours	An attacker may attempt to login as an authorized user and gain unauthorized access to resources protected by the TOE. The attacker may login multiple times, thus locking out the authorized user.	3 - O.DenySession
7	T.Reuse	An attacker may attempt to reuse authentication data, allowing them to gain unauthorized access to resources protected by the TOE.	4 - O.Expire 7 - O.Reauthenticate
8	T.TSF_Compromise	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately viewed, modified, or deleted.	6E - OE.Self_Protection
9	T.Undetect	Attempts by an attacker to violate the security policy and tamper with TSF data may go undetected.	1 - O.Audit 3E - OE.AuditStore 7E - OE.Time

Item	Threat Name	Threat Description	Security Objective
10	T.Walkaway	A user may leave the workstation without logging out, which could enable an unauthorized user to gain access to the resources protected by the TOE.	7 - O.Reauthenticate 3 - O.DenySession

T.BadPassword: Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE. T.BadPassword is countered by:

- O.PasswordGen: The TOE must support automatic generation of passwords. This objective eliminates the need for users to select their own passwords.
- O.PasswordQual: The TOE must be able to specify password quality parameters such as minimum and maximum interval between password changes, minimum length, and numbers of types of characters. This objective ensures the quality of passwords selected by users and enables the administrator to specify checks for bad password qualities.

T.ForgeAuth: An attacker may attempt to forge or copy authentication information, in order to gain unauthorized access to resources protected by the TOE. T.ForgeAuth is countered by:

- O.Expire: The TOE must associate an expiration date with authentication information. This objective mitigates the risk of attackers gaining access to resources using forged or copied authentication information. If an expiration date is associated with the authentication data, the attacker will have a reduced opportunity to reuse it.
- O.Reauthenticate: The TOE must be able to require the user to be reauthenticated under specified conditions. This objective prevents an attacker from walking up to an unattended workstation and performing activities using the identity of the user who left the workstation unattended.

T.Impersonate: An attacker may attempt to impersonate another user, in order to gain unauthorized access to protected resources. T.Impersonate is countered by:

- O.AuthPrim: The TOE must identify and authenticate all users before providing them with application authentication information. This objective prevents the attacker from falsely claiming the identity of an authorized user.
- O.Expire: The TOE must associate an expiration date with authentication information. This objective reduces the opportunity for an attacker to use forged or copied authentication information to impersonate an authorized user.
- O.PasswordQual: The TOE must be able to specify password quality parameters such as minimum and maximum interval between password changes, minimum length, and numbers of types of characters. This objective makes it more difficult for attackers to guess passwords and impersonate an authorized user.

T.Mismanage: Administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- OE.Admin: The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. This objective provides for assistance to administrators to correctly manage the TOE.
- OE.Manage: The TOE must be able to store and maintain properties of users and resources. This objective provides assistance to the administrators in managing the TOE.

- OE.Roles: The TOE must support multiple administrative roles. Multiple administrative roles can be used to enforce separation of duty, so that one administrator can catch errors made by another administrator.

T.NoAttributes: The TSF may not be able to correctly enforce its security policy with respect to identification and authentication or TOE access due to not maintaining user security attributes. T.NoAttributes is countered by:

- OE.Attributes: The IT environment must maintain user attributes. This objective directly addresses the threat of incorrect security policy enforcement by the TSF if user security attributes are not maintained.

T.OffHours: An attacker may attempt to login as an authorized user and gain unauthorized access to resources protected by the TOE. The attacker may login multiple times, thus locking out the authorized user. T.OffHours is countered by:

- O.DenySession: based the maximum number of sessions a user can have open simultaneously and an idle time-out. This objective limits the conditions under which a user can login.

T.Reuse: An attacker may attempt to reuse authentication data, allowing them to gain unauthorized access to resources protected by the TOE. T.Reuse is countered by:

- O.Expire: The TOE must associate an expiration date with authentication information. This objective reduces the opportunity for an attacker to reuse forged or copied authentication information.
- O.Reauthenticate: The TOE must be able to require the user to be reauthenticated under specified conditions. This objective prevents an attacker from walking up to an unattended workstation and performing activities using the identity of the user who left the workstation unattended.

T.TSF_Compromise: A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately viewed, modified, or deleted. T.TSF_Compromise is countered by:

- OE.Self_Protection: The IT environment will maintain a domain for the execution of the TSF that protects the TSF and its resources from external interference, tampering, or unauthorized disclosure. This objective prevents unauthorized user or process from inappropriate disclosure of or tampering with TSF or executable code.

T.Undetect: Attempts by an attacker to violate the security policy and tamper with TSF data may go undetected. T.Undetect is countered by:

- O.Audit: The TOE must be able to audit primary authentication attempts, end user requests for application lists and login information, and access to eTrust SSO records. This objective provides for the detection of attempts to violate the security policy.
- OE.AuditStore: The IT environment must provide for the storage of audit data. This objective provides for the storage of audit data.
- OE.Time: The underlying the operating system must provide reliable time stamps to support the audit function. This objective provides for reliable time stamps to support the audit function.

T.Walkaway: A user may leave the workstation without logging out, which could enable an unauthorized user to gain access to the resources protected by the TOE. T.Walkaway is countered by:

- O.Reauthenticate: The TOE must be able to require the user to be reauthenticated under specified conditions. This objective prevents an attacker from walking up to an unattended workstation and performing activities using the identity of the user who left the workstation unattended.
- O.DenySession: The TOE must be able to deny session establishment based the maximum number of sessions a user can have open simultaneously and an idle time-out. This objective limits the conditions under which a user can login.

8.1.2 Assumptions

Table 8.2 shows that all of the secure usage assumptions are addressed by either security objectives for the IT environment or Non-IT security objectives.

Table 8.2 – All Assumptions Addressed

Item	Name	Assumption	Objective
1	A.Admin	The administrator is trusted to correctly configure the TOE.	1N - ON.Install 3N - ON.Operations
2	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the Policy Server host.	2N - ON.NoUntrusted
3	A.TrustedLAN	It is assumed that the TOE components communicate over a physically protected Local Area Network.	1N - ON.Install
4	A.Users	It is assumed that users will protect their authentication data.	4N - ON.ProtectAuth

A.Admin: The administrator is trusted to correctly configure the TOE. A.Admin is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed on a physically protected Local Area Network in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE.
- ON.Operations: There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner. The procedures will provide guidance to the administrator on how to configure the TOE.

A.NoUntrusted: It is assumed that there will be no untrusted users and no untrusted software on the Policy Server host. A.NoUntrusted is covered by:

- ON.NoUntrusted: The administrator must ensure that there are no untrusted users and no untrusted software on the Policy Server host. This objective corresponds directly to the assumption.

A.TrustedLAN: It is assumed that the TOE components communicate over a physically protected Local Area Network. A.TrustedLAN is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed on a physically protected Local Area Network in a manner that maintains IT security. This objective states that the TOE will be installed on a physically protected Local Area Network.

A.Users: It is assumed that users will protect their authentication data. A.Users is covered by:

- ON.ProtectAuth: The users must ensure that their authentication data is held securely and not disclosed to unauthorized persons. This objective corresponds directly to the assumption.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8.3 shows that all of the security objectives of the TOE are satisfied.

Table 8.3 - All Objectives Met by Functional Components

Item	Objective	Objective Description	Security Functional Requirement
1	O.Audit	The TOE must be able to audit primary authentication attempts, end user requests for application lists and login information, and access to Single Sign-On Data Store records.	FAU_GEN.1 Audit data generation
2	O.AuthPrim	The TOE must identify and authenticate all users before providing them with application authentication information.	FIA_UAU.2 User authentication before any action FIA_UID.2 User authentication before any action
3	O.DenySession	The TOE must be able to deny session establishment based the maximum number of sessions a user can have open simultaneously and an idle time-out.	FTA_TSE.1 TOE session establishment
4	O.Expire	The TOE must detect forging or copying of another user's authentication information.	FMT_SAE_EXP.1 Enforcement of time-limited authorisation FIA_UAU.6 Re-authenticating
5	O.PasswordGen	The TOE must support automatic generation of passwords.	FIA_SOS.2 TSF generation of secrets
6	O.PasswordQual	The TOE must be able to specify password quality parameters such as minimum and maximum interval between password changes, minimum length, and numbers of types of characters.	FIA_SOS.1 Verification of secrets FIA_SOS.2 TSF generation of secrets
7	O.Reauthenticate	The TOE must be able to require the user to be reauthenticated under specified conditions.	FIA_UAU.6 Re-authenticating

O.Audit: The TOE must be able to audit primary authentication attempts, end user requests for application lists and login information, and access to Single Sign-On Data Store records. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events

O.AuthPrim: The TOE must identify and authenticate all users before providing them with application authentication information. O.AuthPrim is addressed by:

- FIA_UAU.2 User authentication before any action, which requires that users be authenticated before allowing any TSF-mediated actions such as access to protected data.
- FIA_UID.2 User identification before any action, which requires that users be identified before allowing any TSF-mediated actions such as access to protected data.

O.DenySession: The TOE must be able to deny session establishment based the maximum number of sessions a user can have open simultaneously and an idle time-out. O.DenySession is addressed by:

- FTA_TSE.1 TOE session establishment, which requires that the TSF be able to deny session establishment based on day and time restrictions, holiday access, user record suspended, and user record expired.

O.Expire: The TOE must associate an expiration date with authentication information. O.Expire is addressed by:

- FMT_SAE_EXP.1 Enforcement of time-limited authorisation, which requires that the TSF not allow authentication after a user's ticket has expired.
- FIA_UAU.6 Re-authenticating, which requires that the TSF reauthenticate the user under the specified conditions.

O.PasswordGen: The TOE must support automatic generation of passwords. O.PasswordGen is addressed by:

- FIA_SOS.2 TSF generation of secrets, which requires that the TSF provide a mechanism to generate passwords.

O.PasswordQual: The TOE must be able to specify password quality parameters such as minimum and maximum interval between password changes, minimum length, and numbers of types of characters. O.PasswordQual is addressed by:

- FIA_SOS.1 Verification of secrets, which requires that the TSF provide a mechanism to verify that passwords meet the rules of the password policy.
- FIA_SOS.2 TSF generation of secrets, which requires that the TSF be able to enforce the use of generated passwords that meet the rules of the password policy.

O.Reauthenticate: The TOE must be able to require the user to be reauthenticated under specified conditions. O.Reauthenticate is addressed by:

- FIA_UAU.6 Re-authenticating, which requires that the TSF reauthenticate the user under the specified conditions.

8.2.2 Requirements for the IT Environment

Table 8.5 shows that all of the security objectives for the IT environment are satisfied.

Table 8.5 - All Objectives for the IT Environment Met by Requirements

Objective	Objective Description	Security Functional Requirement
OE.Admin	The IT environment must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.	FMT_MOF.1 Management of security functions behavior FMT_MTD.1 Management of TSF data FMT_SAE_ENV.1 Management of expiration time
OE.Attributes	The TSF must maintain user attributes.	FIA_ATD.1 User attribute definition
OE.AuditStore	The IT environment must provide for the storage of audit data.	FAU_STG.1 Protected audit trail storage
OE.Manage	The IT environment must be able to store and maintain properties of users and resources.	FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions
OE.Roles	The IT environment must support multiple administrative roles.	FMT_SMR.1 Security roles
OE.Self_Protection	The IT environment will maintain a domain for the execution of the TSF that protects the TSF and its resources from external interference, tampering, or unauthorized disclosure.	FPT_RVM.1 Non-bypassability of the TSP FPT_SEP.1 Domain Separation
OE.Time	The underlying the operating system must provide reliable time stamps to support the audit function.	FMT_STM.1 Reliable time stamps

OE.Admin: The IT environment must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. OE.Admin is addressed by:

- FMT_MOF.1 Management of security functions behaviour, which requires that the auditor be able to manage the behavior of the audit tools.
- FMT_MTD.1 Management of TSF Data, which specifies the TSF Data Management functions that must be provided.
- FMT_SAE_ENV.1 Management of expiration time, which specifies that administrators can set the expiration time.

OE.Attributes: The IT environment must maintain user attributes. OE.Attributes is addressed by:

- FIA_ATD.1 User attribute definition, which requires that the **IT environment** maintain security attributes of user.

OE.AuditStore: The IT environment must store audit data. OE.AuditStore is addressed by

- FAU_STG.1 Protected audit trail storage.

OE.Manage: The IT environment must be able to store and maintain properties of users and resources. OE.Manage is addressed by:

- FMT_MTD.1 Management of TSF data, which requires that the administrator be able to manage application and host authentication records. Applications and hosts are resources.
- FMT_SMF.1 Specification of management functions, which requires that the IT environment perform security management functions to support roles and data access control.

OE.Roles: The IT environment must support multiple administrative roles. OE.Roles is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple administrative roles.

OE.Self_Protection: The IT environment will maintain a domain for the execution of the TSF that protects the TSF and its resources from external interference, tampering, or unauthorized disclosure. OE.Self_Protection is addressed by:

- FPT_RVM.1 Non-bypassability of the TSP**,** which requires that the security policy enforcement functions be invoked and succeed before each function within the TSC is allowed to proceed.
- FPT_SEP.1 Domain Separation, which requires that the IT environment maintain a security domain for the execution of the TSF that protects it from interference and tampering by untrusted subjects.

OE.Time underlying the operating system must provide reliable time stamps to support the audit function. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that times stamps be provided by the IT environment.

8.2.3 Dependencies

Table 8.4 shows the dependencies between the functional requirements. All dependencies are satisfied. FIA_UAU.2, and FMT_SMR.1require FIA_UID.1. This dependency is satisfied, since FIA_UID.2 is included and FIA_UID.2 is hierarchical to FIA_UID.1. This is denoted by an *(H)* following the dependency reference.

Table 8.4 - All Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
		TOE		
1	FAU_GEN.1	Audit data generation	FPT_STM.1	10E
2	FIA_SOS.1	Verification of secrets	None	None
3	FIA_SOS.2	TSF Generation of secrets	None	None

No.	Component	Component Name	Dependencies	Reference
4	FIA_UAU.2	User authentication before any action [Primary Authentication]	FIA_UID.1	6(H)
5	FIA_UAU.6	Re-authenticating [Primary Authentication]	None	None
6	FIA_UID.2	User identification before any action [Primary Authentication]	None	None
7	FMT_SAE_EXP.1	Enforcement of time-limited authorisation	FPT_STM.1	10E
8	FTA_TSE.1	TOE session establishment	None	None
		IT Environment		
1E	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
2E	FIA_ATD.1	User attribute definition	None	None
3E	FMT_MOF.1	Management of TSF function behaviour	FMT_SMF.1 FMT_SMR.1	6E 7E
4E	FMT_MTD.1	Management of TSF data	FMT_SMF.1 FMT_SMR.1	6E 7E
5E	FMT_SAE_ENV.1	Management of expiration time	FMT_SMR.1	7E
6E	FMT_SMF.1	Specification of management functions	None	None
7E	FMT_SMR.1	Security roles	FIA_UID.1	6(H)
8E	FPT_RVM.1	Non-bypassability of the TSP	None	None
9E	FPT_SEP.1	Domain separation	None	None
10E	FPT_STM.1	Reliable time stamps	None	None

8.2.4 Strength of Function

The detailed SOF analysis and rationale is provided in a separate document called the Computer Associates eTrust Single Sign-on Strength of Function Analysis, Version 1.2 provides detailed rationale and analysis of Strength of Function. A strength of function level of SOF-Basic counters an attack level of low.

8.2.5 Assurance Requirements

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The main security service provided by eTrust SSO is to manage authentication information securely. To support this main security service, the SFRs: FIA_SOS.1, Verification of secrets; FIA_SOS.2, TSF Generation of secrets; FIA_UAU.2, User authentication before any action; FIA_UAU.6, Re-authenticating; FIA_UID.2, User identification before any action all support identification and authentication. Supporting identification and authentication is an audit capability, FAU_GEN.1, Generation of audit data which generates audit records based on identification and

authentication events. FMT_SAE.1, Time-limited authorization and FTA_TSE.1, TOE session establishment are included to support the secure maintenance of user logon sessions once they are established through identification and authentication.

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data, there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

8.2.7 Rationale for Explicitly Stated Requirements

The ST has two explicitly stated SFRs:

- FMT_SAE_EXP.1 Enforcement of time-limited authorisation for the TOE
- FMT_SAE_ENV.1 Management of expiration time for the IT environment

These were used in lieu of FMT_SAE.1 Time-limited authorisation, because the enforcement is provided by the TOE, whereas the expiration time is set through an interface to the IT environment.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8.6 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8.6 – Mapping of Functional Requirements to TOE Summary Specification

Functional Component	Functional Requirement	TSS Ref. No	IT Security Function
FAU_GEN.1	Audit data generation	AUDIT-1 AUDIT-2	Audit Generation Audit Record Contents
FIA_SOS.1	Verification of secrets	PWD-1	Password Policy
FIA_SOS.2	TSF Generation of secrets	PWD-1 PWD-2	Password Policy Password Generation
FIA_UAU.2	User authentication before any action [Primary Authentication]	IAPRI-1 IAPRI-2 IAAPP-2	Primary Authentication Primary Authentication Options Application Password Authentication
FIA_UAU.6	Re-authenticating [Primary Authentication]	IAPRI-4	Reauthentication
FIA_UID.2	User identification before any action [Primary Authentication]	IAPRI-1 IAPRI-2 IAAPP-1	Primary Authentication Primary Authentication Options Application Login Information
FMT_SAE_EXP.1	Enforcement of time-limited authorisation	IAPRI-3	Tickets for Primary Authentication
FTA_TSE.1	TOE session establishment	TA-1	Session Establishment

FAU_GEN.1 Audit data generation: This requirement is met by:

- AUDIT-1 Audit Generation, which specifies the types of events to be audited.
- AUDIT-2 Audit Record Contents, which specifies the information to be recorded in an audit record.

FIA_SOS.1 Verification of secrets: This requirement is met by:

- PWD-1 Password Policy, which identifies the password policy rules that can be specified.

FIA_SOS.2 TSF Generation of secrets: This requirement is met by:

- PWD-1 Password Policy, which identifies the password policy rules that can be specified.
- PWD-2 Password Generation, which states the PWD_AUTOGEN property in the user record can be used to require the automatic generation of passwords.

FIA_UAU.2 User authentication before any action [Primary Authentication]: This requirement is met by:

- IAPRI-1 Primary Authentication, which describes how primary authentication is performed.
- IAPRI-2 Primary Authentication Options, which describes the types of primary authentication allowed in the evaluated configuration and specifies that the “None” option is not allowed in the evaluated configuration.
- IAAPP-2 Application Password Authentication executes the application login script simulating normal end user login.

FIA_UAU.6 Re-authenticating [Primary Authentication]: This requirement is met by:

- IAPRI-4 Reauthentication, which specifies the conditions under which reauthentication is required.

FIA_UID.2 User identification before any action [Primary Authentication]: This requirement is met by:

- IAPRI-1 Primary Authentication, which describes how primary authentication is performed.
- IAPRI-2 Primary Authentication Options, which describes the types of primary authentication allowed in the evaluated configuration and specifies that the “None” option is not allowed in the evaluated configuration.
- Application Login Information which describes the how a user’s application login information is retrieved and communicated to the application authentication method via the Policy Server and SSO Client.

FMT_SAE_EXP.1 Enforcement of time-limited authorisation: This requirement is met by:

- IAPRI-3 Tickets for Primary Authentication, which describes the ticket mechanism and specifies that tickets expire and the TSF checks for ticket expiration.

FTA_TSE.1 TOE session establishment: This requirement is met by:

- TA-1 Session Establishment, which identifies the properties in the USER class record used to control session establishment.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements were satisfied. The rationale is provided in Table 8.7.

Table 8.7 – Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.2	CM Documentation	Configuration Item List	Multiple extracts from the CVS and VSS configuration management systems were provided to show version of the product source code (stored in CVS) and the product documentation (stored in VSS)
2	ADO_DEL.1	Delivery Procedures	Distribution Centers Procedures Manual 2004Mar01 (DCPM) Product Submission Form (2003Dec18) Product Submission Form Process Flow.doc (2003Dec18) Preservation of Product 1Apr2004	Packing, storage, and distribution Allows developers to submit product information for Master Media into CA's distribution channels through the Distribution Control Center (DCC) application. Internal procedures used for Product Submission Form process mentioned in 3. Handling, storage, packaging, preservation and delivery of CA software.
3	ADO_IGS.1	Installation, generation, and start-up procedures	Computer Associates, *eTrust™ Single Sign-on Getting Started* Computer Associates, eTrust™ *Single Sign-on Administrator's Guide 7.0* Computer Associates, *eTrust™ Common Criteria Supplement to the Guidance Documentation V1.0*	Provides detailed instructions on how to install SSO. Provides guidance on installing SSO in a security configuration.
4	ADV_FSP.1	Functional Specification	Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0* Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0*	Describes the TSF interfaces Describes the TOE functionality
5	ADV_HLD.1	High-Level Design	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0*	Describes the TOE subsystems and their associated security functionality
6	ADV_RCR.1	Representation Correspondence	Computer Associates eTrust SSO Client version 7.0.1 Common Criteria Evaluation Development Specification 0.8,	Provides a mapping of TOE functions from this ST to the functional specification and the high level design

Item	Component	Evidence Requirements	How Satisfied	Rationale
			26 January 2005	
7	AGD_ADM.1	Administrator Guidance	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0* Computer Associates, *eTrust™ Single Sign-on User's Guide for the Assistant 7.0* Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0* Computer Associates, *eTrust™ Common Criteria Supplement to the Guidance Documentation V1.0*	Describes how to administer the TOE securely. Describes how to use a tool for managing the TOE Describes the administrative interfaces
8	AGD_USR.1	User Guidance	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0* Computer Associates, *eTrust™ Single Sign-on User's Guide for the Assistant 7.0* Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0* Computer Associates, *eTrust™ Common Criteria Supplement to the Guidance Documentation V1.0*	Describes how to use the TOE securely
9	ATE_COV.1	Test Coverage Analysis	*Test coverage analysis, eTrust™ Single Sign-on,* Version 1.2	Provides an analysis of test coverage for functional tests provided.
10	ATE_FUN.1	Test Documentation	Test scripts provide by the vendor	Provides test scripts including test setup, procedures, expected, and actual results for vendor functional tests
11	ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
12	AVA_SOF.1	SOF Analysis	*Computer Associates eTrust Single Sign-on Strength of Function Analysis,* Version 1.2 Computer Associates, *eTrust™ Common Criteria Supplement to the Guidance Documentation V1.0*	Provides analysis of the SOF-basic rating claimed in this Security Target
13	AVA_VLA.1	Vulnerability Analysis	*Computer Associates Single Sign-on Vulnerability Analysis,* Version 1.2	Provides analysis of obvious vulnerabilities and how the product mitigates them.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 ACRONYMS

CC	Common Criteria [for IT Security Evaluation]
COTS	Commercial Off The Shelf
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
OTP	One Time Password
SDI	Security Dynamics Incorporated
Single Sign-On	Signal Sign On
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

10 References

CCITSE	*Common Criteria for Information Technology Security Evaluation*, CCIB-98-026, Version 2.0, May 1998.
Single Sign-On-ADM	Computer Associates, *eTrust™ Single Sign-on Administrator's Guide 7.0*
Single Sign-On-AST	Computer Associates, *eTrust™ Single Sign-on User's Guide for the Policy Manager 7.0*
Single Sign-On-ENT	Computer Associates, *eTrust™ Single Sign-on Agent for Entrust 7.0*
Single Sign-On-GSG	Computer Associates, *eTrust™ Single Sign-on Getting Started*
Single Sign-On-REF	Computer Associates, *eTrust™ Single Sign-on Command Reference 7.0*
Single Sign-On-SCPT	Computer Associates, *eTrust™ Single Sign-on Scripting: Guide and Reference 7.0*
Single Sign-On-SID	Computer Associates, *eTrust™ Single Sign-Agent for SecureID 7.0*
Single Sign-On-SW	Computer Associates, *eTrust™ Single Sign-on Agent for SafeWord 7.0*
Single Sign-On-WEB	Computer Associates, *eTrust™ Single Sign-on eTrust Single Sign-On for Web 7.0*
ACU-COMREF	Computer Associates, *eTrust™ Access Control for Unix Command Reference Version 5.0*
ACU-INSTALL	Computer Associates, *eTrust™ Access Control for Unix Installation and Getting Started Guide Version 5.0*
ACU-TOOLS1	Computer Associates, *eTrust™ Access Control for Unix Administration Tools 1 Security Administrator, Seaudit, SecMon Version 5.0*
ACU-TOOLS2	Computer Associates, *eTrust™ Access Control for Unix Administration Tools 2 eTrust Admin for Access Control Version 5.0*
ACU-USERG	Computer Associates, *eTrust™ Access Control for Unix User's Guide Version 5.0*
ACU-UTILS	Computer Associates, *eTrust™ Access Control for Unix Utilities Guide Version 5.0*
AUD-GSG	Computer Associates, *eTrust™ Audit Getting Started*