National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Computer Associates
eTrust™ Single Sign-On V7.0

Report Number: **CCEVS-VR-05-0124**
Dated: October 24, 2005
Version 1.0

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

ACKNOWLEDGEMENTS

Validation Team

James E Brosey
Catalina Gomolka
Mitretek Systems, Inc.
Falls Church, VA

Olin Sibert
Orion Security Solutions, Inc.
McLean, VA

Common Criteria Testing Laboratory

Debra Baker
Peter Kukura
Clifton Morgan
CygnaCom Solutions (an Entrust Company)
McLean, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of the Computer Associates International, Inc. product eTrust™ Single Sign-On V7.0 was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 30 August 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.2, Part 2 and Part 3, Evaluation Assurance Level (EAL 2), and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met. This Validation Report is not an endorsement of the Computer Associates International, Inc product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by CygnaCom Solutions.

The Target of Evaluation (TOE) is eTrust™ Single Sign-On (SSO) V7.0, which consists of:

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

- 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 an 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.

For this evaluation, the operating system and the hardware platform on which the software components are running are in the IT environment. Therefore, the operating system and the hardware platform have not been evaluated or tested. The TOE relies on the IT environment to provide Protected Audit Trail Storage, User attribute definition, Management of security function behavior, Management of TSF data, Management of expiration time, Specification of management functions, Security roles, Non-Bypassability of the TSP, Domain separation and Reliable time stamps.

1.1 EVALUATION DETAILS

Evaluated Product: eTrust™ Single Sign-On V7.0 with patch QO67747
Developer: Computer Associates International, Inc., One Computer Associates Plaza, Islandia, NY 11749
CCTL: CygnaCom Solutions, 7925 Jones Branch Dr., Suite 5200 West, McLean, VA 22102-3321.
Validation Team: James E Brosey, Mitretek Systems, Inc., 3150 Fairview Park South, Falls Church, VA 22042-4519.
EAL: EAL2
Completion Date: 30 August 2005.

1.2 INTERPRETATIONS

The Evaluation Team performed an analysis of the international and national interpretations regarding the CC and the CEM and determined NIAP Interpretations are optional and are not considered for this product in order to ensure acceptance internationally.

The Evaluation Team determined that the following CCIMB interpretations were applicable to this evaluation:

Final Interpretation for RI # 137 - Rules governing binding should be specifiable.

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 THREATS TO SECURITY

The Security Target identified the following threats that the evaluated product addresses:

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.ForgeAuth	An attacker may attempt to forge or copy authentication information, in order to gain unauthorized access to resources protected by the TOE.
T.Impersonate	An attacker may attempt to impersonate another user, in order to gain unauthorized access to protected resources.
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.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.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.Reuse An attacker may attempt to reuse authentication data, allowing the attacker to gain unauthorized access to resources protected by the TOE.

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.

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

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.

2 IDENTIFICATION

2.1 SECURITY TARGET AND TOE IDENTIFICATION

Security Target – *eTrust™ Single Sign-On V7.0 Security Target V2.0*, dated October 20, 2005.

TOE Identification – eTrust™ Single Sign-On V7.0 with patch QO67747

The Evaluated Configuration of the TOE is software only and includes the following Software Component running on separate machines running Windows 2000 Server SP4s machines:

- Server 1: Policy server
- Server 2: Authentication agent
- Workstation 1: Policy Manager
- Workstation 2: SSO Client

CC Identification – *Common Criteria for Information Technology Security Evaluatio*n, Version 2.2, January 2004, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Securit*y, Version 2.2, Revision 256, January 2004.

Assurance Level - This ST is Common Criteria Version 2.2, Part 2 extended and Part 3 conformant, at Evaluation Assurance Level 2

Keywords - Single Sign-On, Network Security, Policy Server, Identification, Authentication, Agent and Tickets.

2.2 IT SECURITY ENVIRONMENT

The eTrust SSO ST levies requirements on the TOE as well as the IT Environment. In the case of this TOE, the IT Environment includes the Operating System as well as other eTrust products (eTrust Access Control, eTrust Directory, eTrust Audit), LDAP, SSL implementation, encrypted communication, third party applications and the underlying hardware platforms.

The TOE relies on the environment to provide

- Protected Audit Trail Storage;
- User attribute definition;
- Management of security function behavior;
- Management of TSF data;
- Specification of management functions;
- Security roles;
- Non-Bypassability of the TSP;
- Domain separation; and
- Reliable time stamps

The TOE was evaluated with the Microsoft Windows 2000 operating system in the TOE IT environment.

2.3 OPERATING SYSTEM

The TOE was evaluated on the Microsoft Windows 2000 Server operating system with Service Pack 4

2.4 HARDWARE PLATFORM

The Computer Associates eTrust SSO product was evaluated using the hardware platform as described in section 8 of this document.

3 SECURITY POLICY

The eTrust Single Sign-on TOE provides these security services:

- Primary Authentication
- Application Authentication
- Passwords

- Auditing
- TOE Access

Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

3.1 PRIMARY AUTHENTICATION POLICY

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. 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

The eTrust SSO supports the following evaluated Primary Authentication methods:

LDAP (any LDAP compliant repository.)

eTrust SSO also supports other non-evaluated Primary Authentication methods. Each eTrust SSO end user is associated with one or more Primary Authentication methods.

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.

The IT environment provides the SSO Ticket encryption, using a combination of ElGamal Public Key and Triple DES encryption.

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 every five minutes.

3.2 APPLICATION AUTHENTICATION POLICY

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.

3.3 PASSWORD POLICY

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.

3.4 AUDITING POLICY

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.

3.5 TOE ACCESS POLICY

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.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 USAGE ASSUMPTIONS

A.Admin	The administrator is trusted to correctly 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.TrustedLAN	It is assumed that the TOE components communicate over a physically protected Local Area Network.
A.Users	It is assumed that users will protect their authentication data.

4.2 ENVIRONMENTAL OBJECTIVES

OE.Admin	The IT environment must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.
OE.Attributes	The IT environment must maintain user attributes.
OE.AuditStore	The IT environment must store audit data.
OE.Manage	The IT environment must be able to store and maintain properties of users and resources.
OE.Roles	The IT environment must support 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.Time	The underlying operating system must provide reliable time stamps to support the audit function.

4.3 CLARIFICATION OF SCOPE

The product that a customer would purchase can include more than the evaluated TOE, eTrust Single Sign-on, version 7.0. It can also be bundled with other eTrust applications that are not part of this evaluation. The additional Computer Associates (CA) applications that may be bundled with this product are treated in this evaluation as part of the IT Environment.

Some requirements were placed upon the configuration of the IT Environment to support the analysis and conclusions reached by this evaluation. To use this product in the evaluated configuration, the IT environment requirements need to be addressed by the TOE administrator. Since the eTrust Single Sign-on TOE supports configurations that are outside the scope of this evaluation, the TOE administrator must remember that only the functions addressed by the Security Target were evaluated. For example, although eTrust SSO supports the multiple Authentication methods, only LDAP was evaluated.

5 ARCHITECTURAL INFORMATION

The TOE 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.

The eTrust Single Sign-on TOE is software only. The TOE includes the following Software Components:

- The Policy Server
- The Authentication Agent
- The Policy Manager
- The SSO Client

All the software components run on Windows 2000 with Service Pack 4. Although multiple instantiations of each software component can be used, the evaluation team chose to include one Policy Server, two Policy Managers, one Authentication Agent, and two SSO clients in the evaluated configuration (see section 8) for simplicity. Each software component may reside on a separate machine as in a large distributed network, or several software components can reside on the same machine as in a small network. The evaluated configuration (see Figure 4) shows the arrangement of software components for this evaluation.

In the evaluated configuration, LDAP authentication is used for primary authentication (username/password). Thus, the Authentication is partially provided by eTrust Directory which is outside the TOE Boundary.

5.1 GENERAL TOE FUNCTIONALITY

The TOE provides the following security functionality:

- Audit data generation;
- Verification of secrets;
- TSF Generation of secrets;
- User authentication before any action [Primary Authentication];
- Re-authenticating [Primary Authentication];
- User identification before any action [Primary Authentication];
- Time-limited authorization; and
- TOE session establishment.

A logical diagram of the eTrust SSO TOE and the environment in which it exists is provided in Figure 1. A physical diagram of the TOE in its environment in shown in Figure 4.

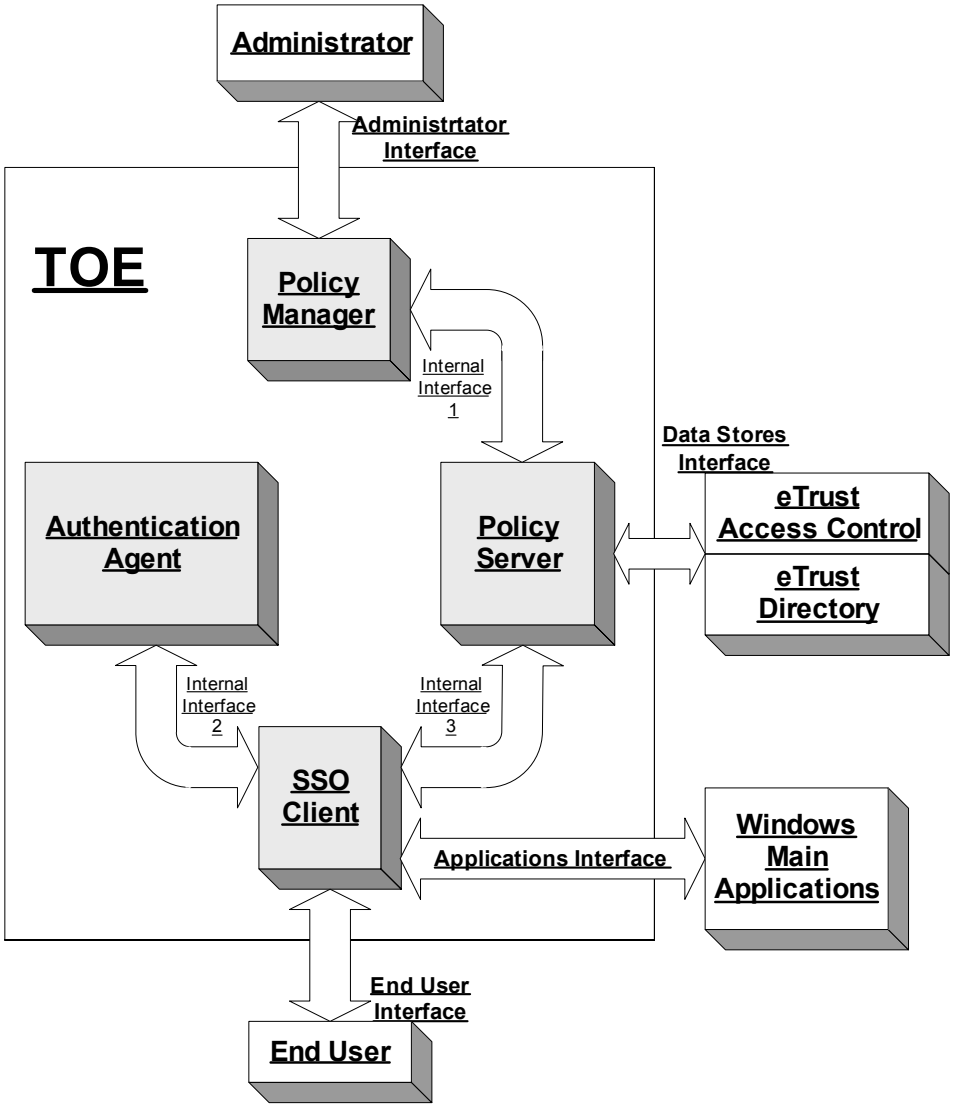

Figure 1: TOE Boundary

5.2 TOE INTERFACES

All the external interfaces to eTrust SSO were all GUI interfaces, whether they were accessible by an administrator or an end user.

The internal interfaces are not part of the TOE. They are private, encrypted network protocol interfaces between the TOE components. The communications between the components is encrypted using a system based on a combination of ElGamal Public Key and Triple DES encryption. These interfaces were not tested.

Figure 1 shows the external and internal interfaces of the TOE.

5.3 TSF SUBSYSTEMS AND FUNCTIONALITY

The TOE 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 subsystems: Policy Server, Policy Manager, Authentication Agent(s) and SSO Clients. Figure 1 provides an overview of how these components are integrated.

5.3.1 Policy Manager Subsystem

The Policy Manager provides the following functionality:

- Allows administrators to associate users with an authentication method used to validate user credentials prior to allowing user action.
- Allows administrators to establish ticket expiration times, time for each user's session, and designate sensitive applications which require re-authentication by a user.
- Allows administrators to Add, delete, and link applications to users
- Allows administrators to Add, delete, and link password policies to applications
- Allows administrator to set password length, character types, password expiration date, and the number of previous passwords that are unusable
- Allows administrator to set the PWD_AUTOGEN property in a user's class record
- Provides audit generation for Administrator logon
- Updates changes to primary authentication

5.3.2 Policy Server Subsystem

The Policy Server provides the following functionality:

- Verifies SSO Ticket and application ID for each user. If the ticket and application ID is valid, the Policy Server sends the login script and login information to the SSO Client. Invalid tickets prevent user from performing TSF actions.
- Records user, event, date, time, result, application name, and targeted user into audit record

5.3.3 Authentication Agent Subsystem

The Authentication Agent provides the following functionality:

- Verifies user credentials with an Authentication Host which includes
    - creates the SSO ticket
    - sends the SSO ticket to SSO Client if user credentials are valid
    - otherwise prevents user from performing any action.
- Performs authentication functions when user attempts to unlock a workstation, open a sensitive application, or user attempts to logon after SSO ticket expires.

5.3.4 SSO Client Subsystem

The SSO Client provides the following functionality:

- For Primary Authentication:
  - Checks authentication method prompts user for logon credentials, send credentials to Authentication Agent for verification prior to allowing user to perform other actions.
  - Obtains SSO ticket
  - Sends SSO Ticket to the policy server and caches it.
- Requires user to re-authenticate when ticket expires, workstation is unlocked, or sensitive application is accessed.
- For Application Login:
  - Obtains user application list.
  - Sends SSO ticket and application ID to Policy Server.
  - Obtains login script from Policy Server
  - Executes the login script which simulates normal user login. Executes "Learn Mode" for first time invoked applications.
- Audits Primary authentication, request for application list, and request for login variables. Audit Records User ID and application name.

6 DOCUMENTATION

Purchasers of a product containing the eTrust SSO receive the following TOE documentation:

- Computer Associates, *eTrust™ Single Sign-on Getting Started*
- *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™ Single Sign-On V7.0 Common Criteria Supplement to the Guidance Documentation, V1.0*

7 IT PRODUCT TESTING

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the Evaluation Team.

All of the testing was conducted in a test lab at the developer's site at:

Computer Associates
2291 Wood Oak Drive
Herndon, VA 20171-2823

The testing was performed in four parts over three business days. Installation Testing was performed the first day. Developer testing was performed the on all three days. Independent and Penetration testing was performed on the third day of testing.

The test plan and results, as well as the evaluation team's review of the testing in the Evaluation Technical Report, well written and complete.

7.1 INSTALLATION TESTING

The installation was performed by Computer Associates personnel while being observed and recorded by the Evaluator. The Target of Evaluation was installed following the procedures defined in the following documents:

- *eTrust Single Sign-On Getting Started 7.0*, contained in the installation package, and
- *eTrust Single Sign-On Implementation Guide 7.0.*
- *Computer Associates eTrust™ Single Sign-On V7.0 Common Criteria Supplement to the Guidance Documentation, V1.0*

The guidance documentation includes a patch that was downloaded from the Computer Associates web site and installed separately.

The installation was done in four stages, one for each of the installed TOE component machines.

The Minimum hardware requirements for installing eTrust Single Sign-On are:

Component	Minimum Hardware Requirements
SSO Client 7.0	Pentium 266 MHz or greater 128 MB of RAM or greater 100 MB of Disk Space
Policy Server 7.0	Pentium 400MHz or greater 256 MB of RAM or greater 600MB of disk space
Policy Manager 7.0	Pentium 266 MHz or greater 128 MB of RAM or greater 20 MB of disk space
Authentication Agent 7.0	Pentium 400MHz or greater 256 MB of RAM or greater 50 MB of disk space

Figure 2: TOE Developer Test Results

The test installation resulted in a successful installation of eTrust SSO in the evaluated configuration. Only minor changes to configuration parameters in the Windows registry and initialization files and the installation of test scripts were necessary to run the functional and independent tests. These changes are detailed in the prerequisites of the individual tests.

The standard user guidance does not describe the procedures used to download the latest patches to the eTrust SSO components from the Computer Associates Website. These should be included as an addendum to the standard installation package.

7.2 DEVELOPER TESTING

The evaluation team selected to run the entire set of tests provided by the developer. The evaluation team mapped the test cases to the TOE Security Functions (TSFs) and to the TSFIs and determined that at least one test is provided for every function and for every interface.

The evaluation team performed all the test cases provided by the developer. All of the test cases included a purpose, explicit test steps, and an expected result. Once again, the testing was performed by Computer Associates personnel while being observed and recorded by the Evaluator. Since all of the external interfaces are GUI interfaces, all of the testing involved exercising the GUI interfaces. There were no automatic test scripts or test tools.

During the course of testing, the evaluation team observed that some of the original test cases failed. The evaluation team determined that the developer had provided test cases for eTrust Single Sign-on version 8.0. These test cases for eTrust Single Sign-on version 8.0 did not run successfully, because that functionality did not exist in eTrust Single Sign-on version 7.0. All of the developer test cases that verified functionality in eTrust version 7.0 ran successfully.

In Section 4 of *Evaluation Technical Report for a Target of Evaluation, eTrust Single Sign-on v7.0, ETR version 2.4, dated October 13, 2005*, the Evaluation Team reported that the evaluator examined the test results and determined that the developer testing was a success. The developer's tests run by the evaluation team completed successfully and all test results were archived in *Test Plan and Report, EAL 2 Evaluation, Computer Associates eTrust™ Single Sign-On V7.0, Version 1.1, July 12, 2005.* The Evaluation Team reported that the actual test results from the developer's tests matched the developer's expected results. A list of final test cases and their actual results are shown below:

Security Function	Function Title	Test Case for Function	Success/Failure
IAPRI-1	Primary Authentication	IAPRI-1-2_LDAP _Authentication	**Success**
IAPRI-2	Primary Authentication Options	IAPRI-1-2_LDAP _Authentication	**Success**
IAPRI-3	Tickets for Primary Authentication	IAPRI-3-4_Ticket_Expiration	**Success**
IAPRI-4	Re-authentication	IAPRI-3-4_Ticket_Expiration	**Success**
		IAPRI-4_SharedWorkstation	**Success**
		IAPRI-4_SensitiveExpiration	**Success**
IAAPP-1	Application Login Information	IAAPP-1-2_PWD-2_App_Login	**Success**
IAAPP-2	Application Password Authentication	IAAPP-1-2_PWD-2_App_Login	**Success**
PWD-1	Password Policy	PWD-1_PasswordPolicy	**Success**
PWD-2	Password Generation	IAAPP-1-2_PWD-2_App_Login	**Success**
AUDIT-1	Audit Generation	AUDIT-1-2_Audit_Generation	**Success**
AUDIT-2	Audit Record Contents	AUDIT-1-2_Audit_Generation	**Success**
TA-1	Session Establishment	TA-1_SessionEstablishment	**Success**

Figure 3: TOE Developer Test Results

7.3 EVALUATION TEAM INDEPENDENT TESTING

The evaluator devised a test subset for independent testing. The test subset consisted of functions not tested by the developer. All of the test cases included a purpose, explicit test steps, and an expected result. The evaluator produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible. This time the testing was performed by the evaluator, with the Computer Associates personnel and the Validator observing. The Validator only observed the independent and penetration testing.

The Evaluator-Team-Defined Test cases were executed after the TOE was installed in the evaluated configuration consistent with the Security Target. The evaluator selected tests to be enhanced during the testing of the entire Developer's Functional test suite. The identification of tests mainly included, but was not limited to, Security Audit, Identification and Authentication, and TOE Access. Since all of the

external interfaces are GUI interfaces, all of the testing involved exercising the GUI interfaces. There were no automatic test scripts or test tools.

The environment and configuration for the Team-Defined testing was the same as that for the Developer Functional testing. No hardware test tools were used during the testing. No general test setup procedures were performed prior to the Team-Defined testing. Setup steps and pre-requisites specific to individual tests are described in the individual test case documents.

Specifically, one of the independent tests determined that an end user could only access an application, which was on the SSO application list, through the SSO interface. The end user could not by-pass the SSO interface to access this application separately.

The Validation Team observed the Evaluation Team's independent testing effort and concluded that the testing was successful.

7.4 EVALUATION TEAM PENETRATION TESTING

For its penetration tests, the Evaluation Team evaluated the developer's vulnerability analysis document, the independent test plan, the guidance documentation and the TOE design to identify potential penetration test cases. Penetration tests were selected based on the Evaluation Team's experience with evaluating the developer's design, guidance, test, and vulnerability assessment documentation.

The evaluator created a penetration test plan. All of the test cases included a purpose, explicit test steps, and an expected result. There were no automatic test scripts or test tools.

The testing was performed by the evaluator, with the Computer Associates personnel and the Validator observing. The Validator only observed the independent and penetration testing.

The penetration tests evaluated:

- Unauthorized User Access
- Vulnerabilities Related to Guessing the Password
- Unauthorized Access of a Logged in Account or Multiple Unauthorized Logins
- Administrator Incorrectly Configures the TOE
- Attack on Policy Server, Policy Manager, and/or Authentication Agent to cause a Denial of Service

Since all the external interfaces are GUI interfaces, the penetration testing was limited. The penetration testing only exercised the external interfaces and not the internal interfaces. There were not any tests to check whether the network traffic between machines could be intercepted or corrupted.
Also, the penetration tests did not thoroughly evaluate the "out of bounds" or "negative" parameters for external TOE interfaces to attempt to "break" the interface allowing a hacker access to the network.

The Validation Team observed the Evaluation Team's penetration testing and concluded that the testing was successful.

8 EVALUATED CONFIGURATION

In Section 4 of *Evaluation Technical Report for a Target of Evaluation, eTrust Single Sign-on v7.0, ETR version 2.0, dated August 25, 2005*, the Evaluation Team reported that the test configuration was consistent with the evaluated configuration in the Security Target.

The TOE, Computer Associates eTrust Single Sign-on v7.0, was evaluated with other Computer Associates Applications (eTrust Access Control and eTrust Directory) in the IT Environment. The evaluator verified the installation Procedures and Delivery procedures during installation of the TOE for testing. The testing activity confirmed that the installation, generation, and start-up procedures result in a secure configuration.

The TOE was tested using the following configuration:

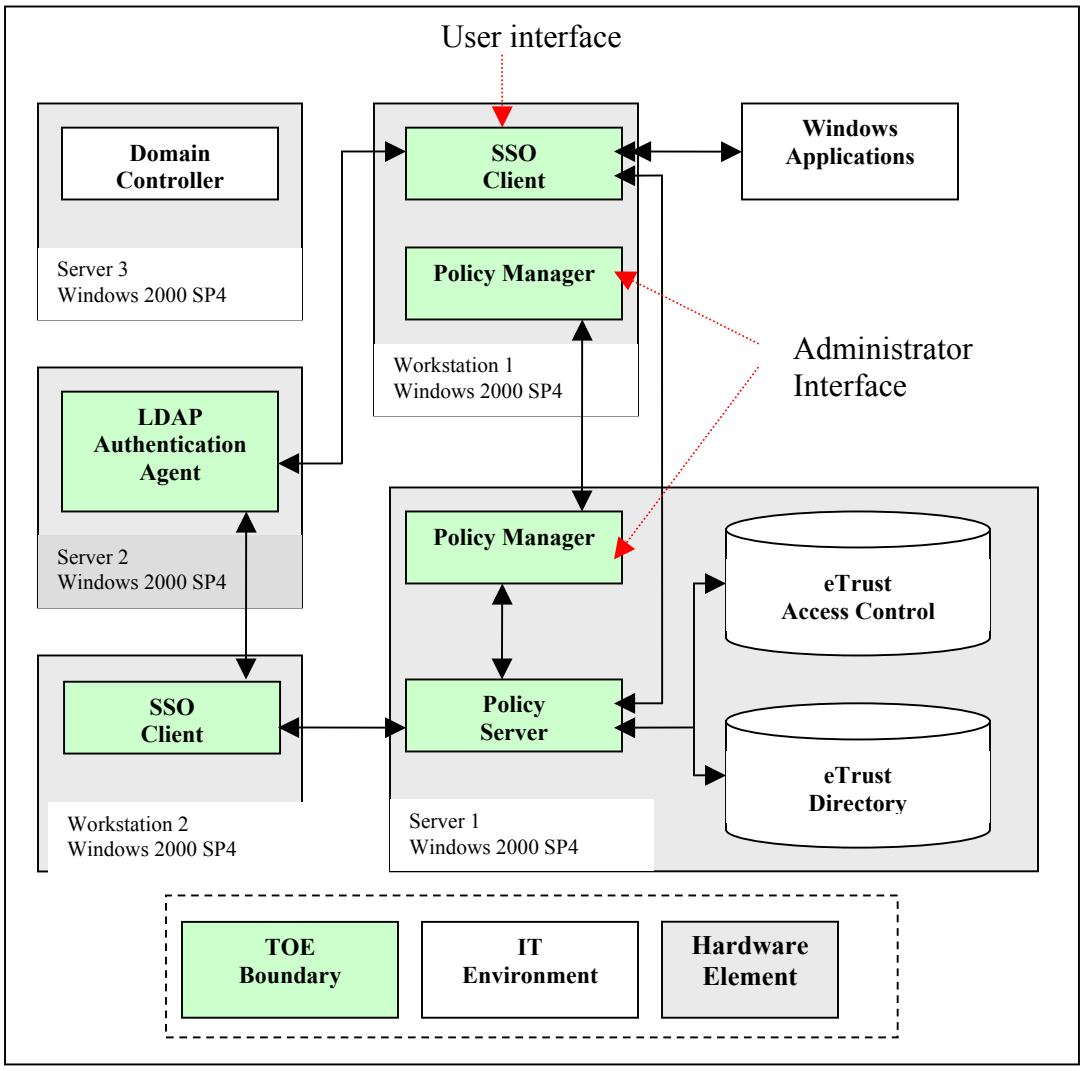

Figure 4: TOE Test Configuration

The eTrust SSO TOE was installed and tested as follows:

Server 1 software:

- Windows 2000, SP4
- eTrust SSO Policy Server 7.0 GA
- eTrust SSO Policy Manager 7.0 GA
- eTrust Access Control v5.2 (Embedded within SSO 7.0 installed on Server 1)
- eTrust Directory 4.0 (Embedded within SSO 7.0 installed on Server 1)

Server 1 hardware:

- Pentium 1 GHz processor
- 256 MB RAM
- 1 GB Hard Drive

Server 2 software:

- Windows 2000, SP4
- LDAP Authentication Agent 7.0.2.382

Server 2 hardware:

- Pentium 1 GHz processor
- 256 MB RAM
- 300 MB Hard Drive

Workstation 1 software:

- Windows 2000, SP4
- eTrust SSO Policy Manager 7.0
- eTrust SSO Client 7.0.2.384

Workstation 1 hardware:

- Pentium 1 GHz processor
- 256 MB RAM
- 100 MB Hard Drive

Workstation 2 software:

- Windows 2000, SP4
- eTrust SSO Client 7.0.2.384

Workstation 2 hardware:

- Pentium 1 GHz processor
- 256 MB RAM
- 100 MB Hard Drive

A fifth machine running Windows 2000, SP4 was used as the Domain Controller for the tested configuration and to run the Telnet simulator used in testing. This machine is not part of the TOE.

The evaluation team chose the following evaluated configuration because it included all the components of the TOE in one of its simplest forms. This configuration has two Policy Managers and SSO clients to show that the client software is extensible. The evaluation team did not test the limits of the number of SSO clients that might be installed, due to the limits in the lab environment.

9 RESULTS OF THE EVALUATION

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM
The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. In the Final ETR, all Fail or Inconclusive work unit verdicts have been resolved by the vendor and the evaluation team.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document: *Evaluation Technical Report for a Target of Evaluation, eTrust Single Sign-on v7.0, ETR version 2.3, dated October 13, 2005*, contain the verdicts of "PASS" for all the work units.

The evaluation team determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements. The rationale supporting each CEM work unit verdict is recorded in the ETR.

Therefore, when configured according to the following guidance documentation:

- Computer Associates, *eTrust™ Single Sign-on Getting Started*
- *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™ Single Sign-On V7.0 Common Criteria Supplement to the Guidance Documentation, V1.0*

The TOE eTrust Single Sign-on version 7.0 is CC compliant and satisfies the *eTrust™ Single Sign-On V7.0 Security Target V2.0*, dated October 20, 2005.

10 VALIDATION COMMENTS/RECOMMENDATIONS

10.1 VALDATION COMMENTS

The product, eTrust Single Sign-on version 7.0, passed all of the work units and all of the tests performed by the evaluation team. The validation team witnessed the testing, reviewed the

recommendations of the evaluation team, and was satisfied that the product performed the requirements necessary for EAL2.

The items included in this section are to make the user aware of the limits of the evaluation.

The TOE is distributed, but there is no functional requirement to protect TOE data between machines. Since there are no requirements to protect the TOE data between distributed components of the TOE, the evaluation team did not check whether the network traffic between TOE machines could be intercepted. The ST states that the internal network traffic is encrypted using a combination of ElGamal Public Key and Triple DES encryption, but this assertion was not tested since the encryption is in the IT environment. The customer can have no confidence, based on this evaluation, that the SSO product is capable of protecting itself from any type of threat that could have access to the communication paths between components.

The TOE contains the authentication mechanisms and the password creation rules that provide the strength of function, but does not maintain the passwords. The passwords are stored with the used id in the LDAP.

Interfaces to the user applications, the data stores, and LDAP are external interfaces to the TOE. These interfaces were not tested since they are not user or administrator accessible. The customer should be aware that LDAP stores the user id and password for eTrust SSO and is not part of the TOE. The user id and password is transferred from the LDAP over an external interface to the Policy Sever. The customer must insure that this interface is protected.

Since there is an assumption that no untrusted software will be installed on any of the hardware, the evaluation team did not check if spyware installed on the client machine could intercept TSF data.

The TOE has an optional evaluated function that allows the administrator to configure the TOE to terminate the oldest session when more that the allowable number of user sessions is attempted. This functionality needs to be used with caution. If the user is only allowed one session at a time, has valuable information open in that session, and attempts to open another session, may cause valuable information to be lost. Also, if an attacker discovers the correct user id and password for authentication, which is difficult, then the valid user session could be terminated.

eTrust SSO was not difficult to install and configure, it was easy to operate and easy to administer. All of the interfaces were GUI interfaces.

The evaluation team worked well with the validation team. The evaluation team provided all the necessary information to perform a complete and effective review of the product to the Validation team.

10.2 VALIDATION RECOMMENDATIONS

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 4 of the ETR, volume 1, and

the Conclusions presented in Section 5 of the ETR, volume 1. The Validation Team, therefore, concludes that the evaluation and Pass result for the TOE identified here is complete and correct: eTrust Single Sign-on v7.0.

11 LIST OF ACRYONYMS

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
SSO	Single-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

12 BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 1.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 2.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.2, January 2004, Part 3.
- *Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3*, Version 1.0, February 2002.
- *Common Evaluation Methodology for Information Technology Security, version 2.2, Revision 256,* January 2004.
- *eTrust™ Single Sign-On V7.0 Security Target V2.0*, dated October 20, 2005.
- *Evaluation Technical Report for a Target of Evaluation, eTrust Single Sign-on v7.0, ETR version 2.3, dated October 20, 2005*.
- *Test Plan and Report, EAL 2 Evaluation, Computer Associates eTrust™ Single Sign-On V7.0, Version 1.1, July 12, 2005*
- *Computer Associates eTrust SSO Client version 7.0.1 Common Criteria Evaluation Development Specification 2.0, dated 20 October 2005*
- *Computer Associates eTrust™ Single Sign-On V7.0 Common Criteria Supplement to the Guidance Documentation, V1.0*