CA *e*Trust™ Security Command Center™ r8 SP1 with CR2 Patch

Security Target Version 1.5.3

January 25, 2007

Prepared for:
CA, Inc.
One Computer Associates Plaza,
Islandia, NY 11749

Prepared by:

CYGNACOM SOLUTIONS

an Entrust Company

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Table of Contents

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:	eTrust Security Command Center r8 SP1 with CR2 Patch
ST Title:	CA eTrust Security Command Center r8 SP1 with CR2 Patch Security Target
ST Version:	Version 1.5.3
ST Authors:	Nancy Gow
ST Date:	January 25, 2007
Assurance Level:	EAL2
Strength of Function:	SOF-Basic
Registration:	<To be filled in upon registration>
Keywords:	Security Monitor, Audit Analyzer, Event Analyzer, Security Target, Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for CA *e*Trust Security Command Center (SCC) r8 SP1 with CR2 Patch.
*e*Trust Security Command Center (SCC) is a software application that provides users the ability to manage and monitor the security of an enterprise. *e*Trust SCC allows the user to collect security event and audit data from a wide range of sources throughout an enterprise and allows the data to be analyzed and managed at a centralized location. *e*Trust SCC also provides capabilities to:

- Create and manage a centralized policy regarding the retention of audit information
- Manage remote product servers (*e*Trust SCC Clients)
- Monitor the status of network resources
- Correlate events with resources
- Provide alerts and event notifications

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 boundary of the TOE.
Section 3, TOE Security Environment, identifies assumptions about the 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, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.
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 are provided in section 9.

2 TOE DESCRIPTION

2.1 Product Type

*e*Trust Security Command Center (SCC) is a software application that provides users the ability to manage and monitor the security of an enterprise at many different levels and offers customizable views, ranging from executive-level summaries to views specially designed for network security specialists.
*e*Trust SCC allows security event data and audit data to be collected from a diverse set of systems, applications, devices and appliances and then provides the ability to analyze data, set rules for alerts based on events or correlations of events, and perform reporting. *e*Trust SCC provides capabilities to create and manage a centralized policy regarding the retention of audit information. In addition, *e*Trust SCC provides tools to monitor the status of network resources and to manage products that reside on the network. *e*Trust SCC includes *e*Trust Audit, an audit data collector and analyzer, to further enhance the ability to analyze audited events on diverse systems throughout an enterprise.
The *e*Trust SCC product consists of a set of components which are distributed across a network and are described in the following subsections.

2.2 Product Specific Terminology

The following table contains definitions of the *e*Trust SCC product specific terminology used in this document:

Table 2-1 – *e*Trust SCC Terminology

Term	Definition
audit node	A system or application from which auditing information is collected
audit policy	A specification of the audit information that should be collected from the audit nodes
audit rule	A specification of audit event matching criteria and the actions to be taken when a collected audit record matches that criteria
collector database	The relational database that stores the audit data collected from managed resources. (The central data repository)
incident	Security relevant events recorded in the audit data that are defined by the administrator through an incident filter
incident filter	A set of data field values used to categorize audit events.
node	A server that runs the products that *e*Trust SCC manages and monitors
product server	A network server that hosts one or more resources managed by *e*Trust SCC. A product server is a client of the *e*Trust SCC servers.
resource	An application, device, appliance or operating system on a network that is monitored or managed by *e*Trust SCC.
workgroup	An administrator defined group of *e*Trust SCC users who have access to the same information
workplace	An administrator created list of applications that identifies the content available to a workgroup and the organization of that content.

2.3 *e*Trust SCC Components

*e*Trust SCC is a software-only product that, as delivered to the customer, includes the components described in the following sections.

2.3.1 *e*Trust SCC Server

The *e*Trust SCC Server component provides the core functionality of the product. Security functions provided by the *e*Trust SCC Server are:

User Identification and Authentication
The *e*Trust SCC Server performs user identification and password based authentication before allowing access to management and monitoring functions.

User Interface
*e*Trust SCC provides a graphical user interface (GUI) through a comprehensive set of configuration, management, and monitoring web applications. A user accesses the *e*Trust SCC GUI through a standard web browser from any workstation on the local area network that connects the SCC, Audit and product servers (*e*Trust SCC Clients). A user's access to security data and functions can be restricted. The appearance of the user interface can be customized by both the administrator and the user.

Event Monitoring
Several methods of monitoring security relevant events are provided. Audit data is collected from network resources and stored in a database in the IT Environment that is used as a central data repository. User defined audit policies and incident filters determine which data is collected and designated as significant. Various event viewers allow a user to display, sort, and filter the collected data. The *e*Trust SCC Server component also provides several methods of alerting responsible personnel when a security relevant event occurs.

Status Monitoring
*e*Trust SCC monitors and discovers services, processes, and daemons running on the managed product servers (*e*Trust SCC Client machines) on the network. The status monitoring functions of the *e*Trust SCC Server lets the users create customized views of the status of security in an enterprise. These views can be organized by application or by area of responsibility.

Product Administration
Products residing on the network servers may be managed through the *e*Trust SCC user interface. This functionality is provided both by running product utilities and by access to a product's native administrative and management interfaces through the web based *e*Trust SCC GUI described previously.

The *e*Trust SCC Server component is supported by two third-party relational databases which are used as common object repositories: The TNG Core database used to store status information and the Portal Database used to store viewing characteristics, URL information, user accounts, workgroups, workplaces and other management objects.

2.3.2 *e*Trust Audit Policy Manager

The *e*Trust Audit Policy Manager provides the functionality that allows the creation, implementation and distribution of an organization's audit policies. Audit polices specify

the event data to be collected from resources residing across the network. Audit policies also assign patterns to events so that a security relevant event can be designated through policy rules. This component also provides for the analysis of the collected audit data so that actions and alerts can be automatically triggered when a significant event occurs.

2.3.3 *e*Trust Audit Data Tools

The *e*Trust Audit Data Tools component supplies the functionality that manages the collector database. The collector database is a third-party relational database in the IT Environment that acts as the central repository for audit data collected from the network resources. The *e*Trust Data Tools component also provides support for the event viewing functions of the *e*Trust SCC GUI.

2.3.4 *e*Trust Audit Client

The *e*Trust Audit client components gather and process event information from the network resources that are managed by *e*Trust SCC. A number of product specific *e*Trust Audit client components are provided with on the *e*Trust SCC installation media and users may also develop custom components to collect audit data from other applications. Multiple versions of the *e*Trust Audit client components may reside on a single host machine. The *e*Trust Audit client must also be installed on the *e*Trust SCC server for generation of audit records for the events produced by *e*Trust SCC itself. (Therefore the *e*Trust SCC Server machine may be considered a client of the *e*Trust Audit Servers.)

2.3.5 *e*Trust SCC Agent

*e*Trust SCC Agent components also reside on the product servers (*e*Trust SCC Clients) managed by *e*Trust SCC. The *e*Trust SCC Agents consist of system-specific sub-components that monitor services, process and daemons operating on the product servers (*e*Trust SCC Clients) and provide status information to the *e*Trust SCC server.

2.3.6 Product Integration Kits (PIKs)

Product Integration Kits (PIKs) are product specific software developed to provide access to the content, monitoring and management interfaces of the resources managed by *e*Trust SCC. A PIK consists of a server-side sub-component that resides on the *e*Trust SCC Server host and an agent-side sub-component that is installed on a network product server (*e*Trust SCC Client) . PIKs developed by CA, Inc. for a number of products are provided with *e*Trust SCC. A user also has the option to create custom PIKs to integrate additional products and applications. As with the *e*Trust Audit client, multiple PIKs may reside on a single product server (*e*Trust SCC Client) .

2.4 TOE Physical Boundary

The Target of Evaluation includes the following components of the *e*Trust SCC product:

- *e*Trust SCC Server
- *e*Trust Audit Policy Manager
- *e*Trust Audit Data Tools

The TOE does not include:

- *e*Trust Audit Client and *e*Trust SCC Agent components

- Product Integration Kits (PIKs)
- Collector Database
- Common Object Repository Databases
- Operating System of the *e*Trust SCC servers
- User Console (the workstation used to access the *e*Trust SCC user interface)

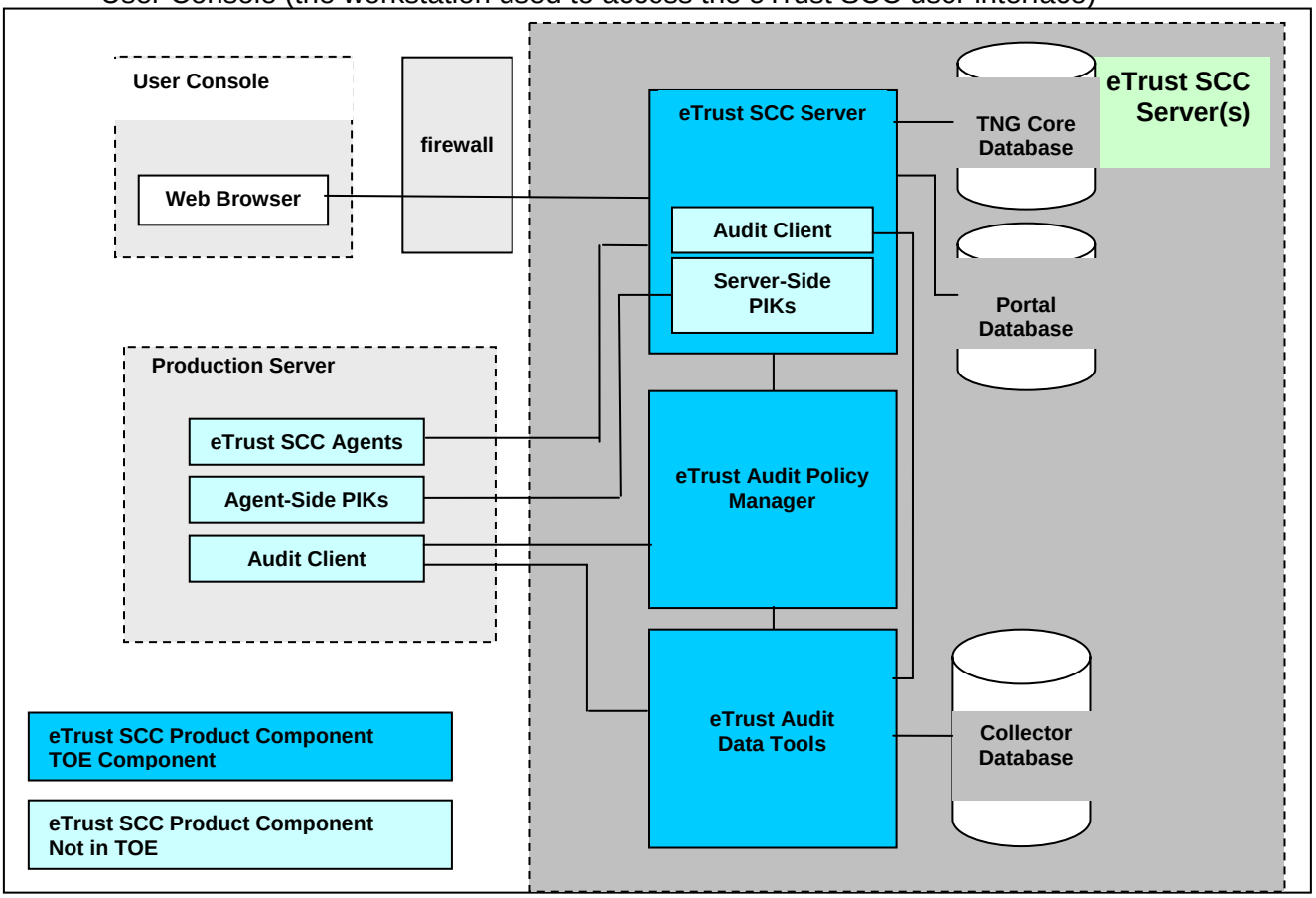

Figure 1 - *e*Trust SCC Components

2.5 TOE Logical Boundary and TOE Security Functions

The logical boundary of the TOE is defined by the security functionality provided by *e*Trust SCC. This includes:

- **Security Audit:** *e*Trust SCC has the following security auditing functions:
  - Collects audit information from its managed resources
  - Generates audit records of its own use
  - Takes administrator defined actions when a security relevant event is detected in a resource's audit data or when the status of a resource becomes critical.
  - Provides the administrators with rule and filter based specification of security significant events.
  - Provides users with audit record viewing capabilities

- **Identification and Authentication:** *e*Trust SCC provides user identification through user accounts and password-based authentication.
- **Security Management:** *e*Trust SCC provides security management through the use of the administration capabilities of the web-based user interface. Access to management functions and data is controlled through the use of administrator roles.
- **Partial Protection of the TSF**: *e*Trust SCC protects its security functions and data from interference and tampering through its own interfaces in conjunction with protection from the IT environment.

2.6 IT Environment and Evaluated Configuration

The evaluated configuration consists of three servers running the Windows 2003 SP1 operating system: two are SCC Servers and will be installed with the TOE component software, the third is the product server (*e*Trust SCC Client) that will be managed and monitored by the TOE. The evaluated configuration is shown below in Figure 2.

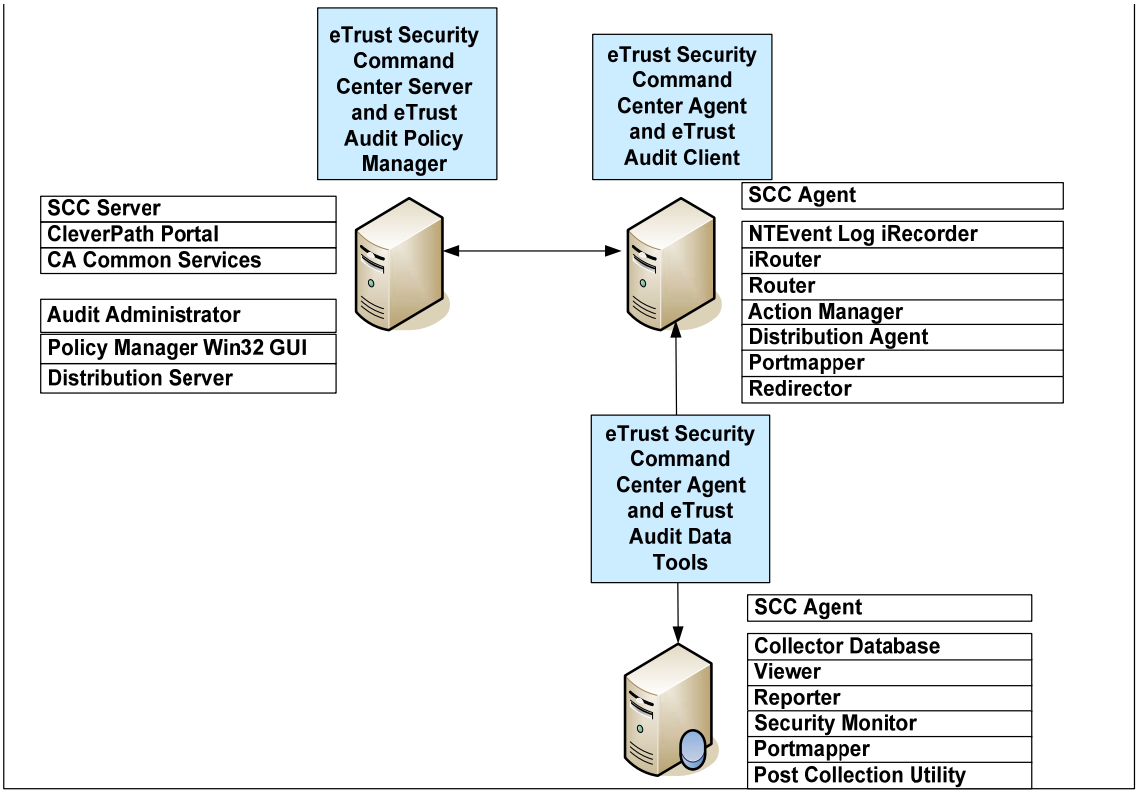

Figure 2 - *e*Trust SCC Evaluated Configuration

The following tables specify the hardware, operating systems, and software which are in the IT Environment of the evaluated configuration. The second column lists the minimum requirements and versions of the software and hardware on which the TOE is compliant, the third column specifies the tested configuration that was used for the evaluation.

Table 2-2 – *e*Trust SCC Server Configuration

	Requirements	**Tested Configuration**
SCC Product Components:	*e*Trust SCC Server *e*Trust Audit Policy Manager *e*Trust Audit Client Server-Side PIKs	*e*Trust SCC Server *e*Trust Audit Policy Manager *e*Trust Audit Client Server-Side PIKs
Windows System Requirements:	Windows 2000 Server with SP4. Windows 2003 Server EE with SP1	Windows 2000 Server with SP4
Minimum Hardware Requirements:		
Processor:	Pentium-III or higher, 1.4 GHz processor or higher	Intel® Xeon™ 3.00 GHz processor
Memory:	1 GB RAM minimum	2 GB
Disk Space:	Greater than 6 GB	33.8 GB
Other Hardware:	None required	DVD Drive
Database Requirements:	Microsoft SQL Server 2000 with Service Pack 3 (with Dictionary order, case-sensitive, for use with 1252 Character Set)	Microsoft SQL Server 2000 Enterprise Edition
Software:	TCP/IP installed Microsoft Internet Explorer 6.0 or higher	TCP/IP installed Microsoft Internet Explorer 6.0 SP1

Table 2-3 – *e*Trust Data Tools Server Configuration

	Requirements	**Tested Configuration**
SCC Product Components:	*e*Trust Audit Data Tools *e*Trust SCC Agent	*e*Trust Audit Data Tools *e*Trust SCC Agent
Windows System Requirements:	Windows 2000 Server with SP4. Windows 2003 Server EE with SP1	Windows 2000 Server with SP4.
Minimum Hardware Requirements:		
Processor:	Pentium-III or higher, 1.4 GHz processor or higher	Intel® Xeon™ 3.00 GHz processor
Memory:	1 GB RAM minimum	2 GB
Disk Space:	Greater than 6 GB	33.8 GB
Other Hardware:	None required	DVD Drive
Database Requirements:	Microsoft SQL Server 2000 with Service Pack 3 (with Dictionary order, case-sensitive, for use with 1252 Character	Microsoft SQL Server 2000 Enterprise Edition (with Dictionary order, case-sensitive, for use with

	Set)	1252 Character Set)
Software:	TCP/IP installed	TCP/IP

Table 2-4 – Product Server (*e*Trust SCC Client) Configuration

	Requirements	**Tested Configuration**
SCC Product Components:	*e*Trust SCC Agent *e*Trust Audit Client Agent-Side PIKs	*e*Trust SCC Agent *e*Trust Audit Client Agent-Side PIKs
Windows System Requirements:	Windows 2000 Windows 2003 Windows XP	Windows XP 2002 Professional with SP2
Minimum Hardware Requirements:		
Processor:	Pentium II 400 MHz	Pentium III 498MHz
Memory:	128 MB	640 MB
Disk Space:	100 MB	18 GB
Other Hardware:	None	DVD +/-R Drive
Database Requirements:	None	None
Software:	TCP/IP installed Microsoft Internet Explorer 6.0 or higher	TCP/IP installed Microsoft Internet Explorer 6.0

3 TOE Security Environment

3.1 Assumptions

This section contains secure usage assumptions regarding the IT security environment.

Table 3-1 – Secure Use Assumptions

Assumption ID	Assumption Description
A.NoEvil	It is assumed that the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation to install and manage the TOE securely
A.NoUntrusted	It is assumed that there will be no untrusted software on the TOE servers.
A.Password	It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data
A.Physical	It is assumed that the TOE server hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

In any organization, there are critical software applications (e.g. a database server or anti-virus application) and critical platforms (e.g., mail server host). The resources protected by the TOE are applications and platforms identified as critical.
The TOE provides security monitoring and management services. Hence, the threats relevant to this specification are threats that can be mitigated through detection and appropriate response. Threats mitigated by the TOE are listed in Table 3-2.
The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

Table 3-2 – Security Threats

Threat ID	Threat Description
T.Attack	Unauthorized accesses and activity indicative of misuse on IT system resources the TOE monitors may not be identified or associated with other suspicious events thereby allowing the resource to be compromised by an attacker.
T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TOE security functions and data.
T.MisManage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 - Security Objectives for TOE

Objective ID	Objective Description
O.Admin	The TOE shall include a set of functions that allow effective management of TOE security functions and data.
O.Analyze	The TOE shall apply analytical processes to information collected from the monitored resources in order to identify potential security violations.
O.Audit	The TOE shall generate audit records for access to the TOE's user interface and creation, deletion and changes to administrative objects.
O.Collect	The TOE shall collect information about events that are indicative of potential security violations of critical resources.
O.I&A	The TOE shall provide functionality to require identification and authentication for all users of the *e*Trust SCC user interface.
O.PartialProtect	The TSF shall provide protection for itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
O.Respond	The TOE shall notify administrative personnel to potential security violations of critical resources.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

The security objectives for the IT environment are as follows:

Table 4-2 - Security Objectives for IT Environment

Objective ID	Objective Description
OE.AuditProtection	The IT Environment shall provide the capability to protect the collected audit information.
OE.AuditResource	The IT Environment shall provide the capability to generate records of events that are indicative of potential security violations of critical resources.
OE.PartialProtect	The IT Environment shall provide protection for the TOE and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
OE.Time	The underlying operating systems shall provide reliable time stamps.

4.2.2 Non-IT Security Objectives

The security objectives for the Non-IT environment are as follows:

Table 4-3 – Non-IT Security Objectives

Objective ID	Objective Description
ON.NoUntrusted	There shall be no untrusted software on the *e*Trust SCC Server and *e*Trust Audit hosts.
ON.Personnel	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE and they shall ensure that the TOE is installed, managed and operated in a manner which is consistent with the TOE guidance documentation.
ON.Physical	Those responsible for the TOE shall ensure that the TOE servers are protected from any physical attack.
ON.PwdProtect	Users of the TOE shall ensure that they choose strong passwords and that they protect their authentication data as instructed by the administrator guidance.

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, explicitly stated requirements based on 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. 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
- iteration: allows a component to be used more than once with varying operations.

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.***
- Iterations are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations.
- Explicitly Stated Requirements will be noted with a "_EXP" added to the component name.

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1. They are all taken from or, in the case of explicitly stated requirements, based on components from Part 2 of the Common Criteria.

Table 5-1 - Functional Components

Class	Component	Component Name
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1-1	Audit data generation
	FAU_GEN_EXP.1	Audit data collection
	FAU_SAA.3	Simple attack heuristics
	FAU_SAR.1-1	Audit review
	FAU_SAR.1-2	Audit review
	FAU_SAR.3	Selectable audit review
Identification & Authentication	FIA_UAU.2	User authentication before any action

Class	Component	Component Name
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_RVM_EXP_TOE.1	Partial non-bypassability of the TSP: TOE
	FPT_SEP_EXP_TOE.1	Partial TSF domain separation: TOE

5.1.1 Class FAU: Security Audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take **[*the actions specified by an SCC Administrator, where the possible actions are:***

1. ***Execute a designated program***
2. ***Send an email notification to a designated recipient***
3. ***Send the event data to the collector database***
4. ***Execute an assigned workflow***
5. ***Visually indicate a critical status of a resource on the SCC GUI.***

] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_GEN.1-1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1-1.1 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 events:***

a. eTrust SCC logon

b. eTrust SCC logoff

c. Create, Deletion and Modification of:

- ***Menu Profiles***
- ***Status Monitor Profiles***
- ***Product Interface Profiles***

- ***Status Monitor Configuration Items***
- ***iTicker Profiles***
- ***Presentation Profiles***
- ***Table Collector Definitions***
- ***Incident Management Items***

]

FAU_GEN.1-1.2 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 ST:

[

for all events:

- ***subject's computer id***

for operations on objects:

- ***SCC Object Class***
- ***SCC Object Name***
- ***Operation on SCC Object***

].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN_EXP.1 Audit data collection

Hierarchical to: No other components.

FAU_GEN_EXP.1.1 The TSF shall be able to collect audit information from any resource that has an *e*Trust Audit agent installed and configured to gather the event data it generates.

FAU_GEN_EXP.1.2 The TSF shall collect at least the following information:

a) Event time stamp, computer name, domain name, log name, event id, username, source and event category.

Dependencies: FAU_GEN.1 Audit data generation

FPT_STM.1 Reliable time stamps

FAU_SAA.3 Simple attack heuristics

Hierarchical to: FAU_SAA.1

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events **[**

a. An audit event specified in a defined audit policy

b. An accumulation or combination of audit events specified in a defined audit policy

c. An audit event specified in a defined incident filter

] that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of **[*the audit data collected from a resource*].**

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Dependencies: No dependencies

FAU_SAR.1-1 Audit review

Hierarchical to: No other components.

FAU_SAR.1-1.1 The TSF shall provide **[*the Portal Administrator*]** with the capability to read **[*all audit information specified in FAU_GEN.1*]** from the audit records.

FAU_SAR.1-1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1-2 Audit review

Hierarchical to: No other components.

FAU_SAR.1-2.1 The TSF shall provide **[*an SCC user assigned to a workplace*]** with the capability to read **[*all audit information for resources assigned to the same workplace*]** from the audit records.

FAU_SAR.1-2.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches, sorting, and ordering*]** of audit data based on **[*any audit data field displayed to the user according to the user's role and workplace assignment*]**.

Dependencies: FAU_SAR.1 Audit review

5.1.2 Class FIA: Identification & Authentication

FIA_UAU.2 User Authentication before any action

Hierarchical to: FIA_UAU.1 Timing of Authentication

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.7 Protected authentication feedback

Hierarchical to:	No other components.
FIA_UAU.7.1	The TSF shall provide only **[*a confirmation of user name and asterisks for password for password-based authentication*]** to the user while the authentication is in progress.
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_UID.2 User Identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

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_MTD.1 Management of TSF data

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to **[*Security Management Functions as specified in Table 5-2*]** the **[*TSF Data as specified in Table 5-2*]** to **[*the Administrative Role as specified Table 5-2*].**
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: **[*as specified in Table 5-2*]**.
Dependencies:	No dependencies

Table 5-2 – Management of TSF Data: *e*Trust SCC

Administrative Role	Security Management Functions	TSF Data Objects
SCC Administrator	create, edit, and delete	audit nodes and audit node groups audit rules audit actions
	create, activate, edit, and delete	audit policies
	create, modify and delete	applications and application groups event views incident groups and workflow policies status views
Portal Administrator	create, modify and delete	nodes and node groups users and workgroups workplaces
	assign users to workplaces	users and workplaces
	create, edit, and delete	audit nodes and audit node groups audit rules audit actions
	create, activate, edit, and delete	audit policies
	create, modify and delete	applications and application groups event views incident groups and workflow policies status views
	view TOE generated audit and event data	TOE generated audit and event data
	view collected audit and event data	audit and event data collected from all resources
SCC User (workplace administrator)	view status view audit and event data execute product utilities execute product administration interfaces	audit and event data collected from resources in the user's assigned workplace

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*SCC Administrator, Portal Administrator, SCC User*].**

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

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TSF

FPT_RVM_EXP_TOE.1 Partial non-bypassability of the TSP: TOE

Hierarchical to: No other components.

FPT_RVM_EXP_TOE.1.1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP_TOE.1 Partial TSF domain separation: TOE

Hierarchical to: No other components.

FPT_SEP_ EXP_TOE.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_ EXP_TOE.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2 Security Functional Requirements for the IT Environment

The IT Environment security functional requirements are listed in Table 5-3 - Functional Components for the IT environment. They are all taken from or, in the case of explicitly stated requirements, based on components from Part 2 of the Common Criteria.

Table 5-3 - Functional Components for the IT environment

Class	Component	Component Name
Security Audit	FAU_GEN.1-2	Audit data generation
	FAU_STG.1	Protected audit trail storage
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM_EXP_IT.1	Partial non-bypassability: IT Environment
	FPT_SEP_EXP_IT.1	Partial domain separation: IT Environment
	FPT_STM.1	Reliable time stamps

5.2.1 Class FAU: Security Audit

FAU_GEN.1-2 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1-2.1 **Refinement**: The ***resources*** 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) **[*no other events*].**

FAU_GEN.1-2.2 **Refinement**: The ***resources and eTrust Audit agent components*** 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 ST: **[*resource id, domain name, event ID, source, category, event description*].**

Dependencies: FPT_STM.1 Reliable time stamps

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

FAU_STG.1.1 **Refinement:** The ***TOE Server OS and DBMS*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 **Refinement**: The ***TOE Server OS and DBMS*** 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 FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

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

Dependencies: No dependencies.

FPT_RVM_EXP_IT.1 Partial non-bypassability: IT Environment

Hierarchical to: No other components.

FPT_RVM_EXP_IT.1.1 The security functions of the TOE server OS shall ensure that TOE server OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the TOE server OS is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP_IT.1-2 Partial domain separation: IT Environment

Hierarchical to: No other components.

FPT_SEP_EXP_IT.1.1 The security functions of the TOE server OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the TOE server OS.

FPT_SEP_EXP_IT.1.2 The security functions of the TOE server OS shall enforce separation between the security domains of subjects in the scope of control of the TOE server OS.

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 ***use by the TOE***.

Dependencies: No dependencies

5.3 Strength of Function

There is an overall strength of function claim of SOF-Basic. The strength of function requirement applies to the password mechanism (FIA_UAU.2) which is probabilistic. A policy for selecting a strong password for user authentication to meet this claim is described in the administrator guidance.

5.4 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 are refined. The assurance components are listed in Table 5-4 - Assurance Requirements: EAL2.

Table 5-4 - Assurance Requirements: EAL2

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

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

The following sections describe the IT Security Functions of the *e*Trust SCC Components.

Table 6-1 - Security Functional Requirements mapped to Security Functions

Security Function	Sub-Function		SFR
Security Audit	AU-1	Security Alarms	FAU_ARP.1
	AU-2	Audit Data Generation: TOE	FAU_GEN.1-1
	AU-3	Audit Data Collection	FAU_GEN_EXP.1
	AU-4	Simple Attack Heuristics	FAU_SAA.3
	AU-5	Audit Review: TOE Audit Data	FAU_SAR.1-1
	AU-6	Audit Review: Collected Audit Data	FAU_SAR.1-2
	AU-7	Selectable Audit Review	FAU_SAR.3
Identification & Authentication	IA-1	User Authentication before any Action	FIA_UAU.2
	IA-2	Protected Authentication Feedback	FIA_UAU.7
	IA-3	User Identification before any Action	FIA_UID.2
Security Management	SM-1	Management of Security Functions Behavior	FMT_MTD.1
	SM-2	Specification of Management Functions	FMT_SMF.1
	SM-3	Security Roles	FMT_SMR.1
Protection of the TSF	PT-1	Partial Non-bypassability of the TSP: TOE	FPT_RVM_EXP_TOE.1
	PT-2	Partial TSF Domain Separation: TOE	FPT_SEP_EXP_TOE.1

6.1.1 Security Audit

6.1.1.1 AU-1 Security Alarms (FAU_ARP.1)

Security alarms can be set through either the definition of an audit policy or an incident filter:

When the TOE detects a potential security violation as indicated by an event that meets a defined audit policy, it can:

- Execute a program
- Send an email notification to responsible personnel
- Send the event to the central audit data repository (the collector database)

The action taken depends on the audit policy defined by the administrator. This functionality is provided by the *e*Trust Audit components of the TOE. Audit policies are further described in AU-4.

The TOE also enforces policies to detect a potential security violation as indicated by an event that meets a defined incident. Incident definitions are based on events recorded in the audit data that are tagged by the administrator during the creation of an incident filter. Incident data is incident filter's attributes: owner of the incident, priority of execution of a workflow, identification number for the incident workflow, associated workflow policy, and status of the workflow. Incident Groups organize associated incidents, or events that need special attention.

When an incident filter is triggered the TOE can execute a workflow that is associated with the incident. Workflows are time-based programs that can perform activities such as override incident data (such as assign an incident not acted upon to another administrator), set status on nodes, notify personnel of the incident, and perform other commands specified by the administrator. Each incident workflow can precede or follow another in sequence based on the time the event occurred, so that the sum of these time-based workflows makes up a workflow policy.

The SCC user can configure a view through the GUI so that it visually indicates when a monitored resource has a critical status. This functionality is provided through the *e*Trust SCC server status monitoring capability that was described in Section 2.3.1.

6.1.1.2 AU-2 Audit Data Generation: TOE (FAU_GEN.1-1)

This sub-function refers to the functionality provided by *e*Trust SCC Server component and refers to the logging of events generated by *e*Trust SCC itself.
*e*Trust SCC will generate audit records for the following events:

- Start-up and shutdown of the audit functions;
- *e*Trust SCC logon
- *e*Trust SCC logoff
- Creation, Deletion and Modification of:
    - Menu Profiles
    - Status Monitor Profiles
    - Product Interface Profiles
    - Status Monitor Configuration Items
    - iTicker Profiles
    - Presentation Profiles
    - Table Collector Definitions
    - Incident Management Items

Each audit record contains the following information:

- Event Timestamp
- Event Type
- Subject Identity (User ID)
- Event Result
- Subject's Computer ID (ID of the computer used to access the *e*Trust SCC GUI)

For events that are operations on TSF data objects, the audit records also include the fields:

- SCC Object Class (e.g.: iTicker Profile)
- SCC Object Name (e.g.: ETest)
- Operation on SCC Object (e.g.: Create)

6.1.1.3 AU-3 Audit Data Collection (FAU_GEN_EXP.1)

This sub-function refers to the functionality provided by the *e*Trust Audit component of the TOE. Collection is meant to mean gathering or extracting audit events from a number of sources. The TOE is open-ended to the types of events that are collected from the product servers (*e*Trust SCC Clients). The events collected are defined through the central audit policies and can be collected from any operating system or application that produces an audit log. There must be a corresponding *e*Trust Audit Client component installed on the product server (*e*Trust SCC Client) for this to occur. The Audit Agent components that collect the data add identifying information to the events captured such as computer name, domain name, log name and other fields as required. The audit data generated by the TOE itself, described previously in AU-2, is collected by the same mechanism; i.e. the *e*Trust Audit Client must be installed on the *e*Trust SCC Server and an audit policy defined for the *e*Trust SCC events.
This functionality depends on FAU_GEN.1-1 and on FAU_GEN.1-2 which is in the IT Environment.

6.1.1.4 AU-4 Simple Attack Heuristics (FAU_SAA.3)

As described in AU-1 and AU-2 above, the administrator can define an audit event to be security relevant either through audit policies or incident filters. When the TOE detects a match between its internal definition and the data collected from the audit records of resources, appropriate action can be taken as previously described in AU-1.

Incident filters have been previously described in AU-1.

The administrator is able to define the central audit policy through the *e*Trust Audit Policy Manager GUI, and to manage the *e*Trust Audit Clients. The TOE is permissive in the sense that no auditing events are collected by the *e*Trust Audit Client until the central audit policy has been defined and distributed to the *e*Trust Audit Client. Through the *e*Trust Audit Policy Manager GUI the administrator is able to define a set of filters for detecting a potential violation of the TSP. This capability is accomplished through defining

1. what audit events should trigger an alarm and
2. what form the alarm should take.

*e*Trust Audit is installed with a set of predefined filters (rules) resident on the *e*Trust Audit Policy Manger, which can be edited and augmented by the *e*Trust SCC user/administrator through the *e*Trust Audit Policy Manager GUI (available through the eTrust SCC Client GUI) prior to distribution to the *e*Trust Audit Clients. Through the *e*Trust Audit Policy Manager GUI (available through the eTrust SCC Client GUI) the administrator can define an accumulation or combination of audit events based on

specified criteria (a rule or filter) that *e*Trust Audit Client uses to determine which events are subject to the action described in the filter known to indicate a potential security violation.

Audit events that do not meet a filter are dropped. Through this interface the administrator can also manage the *e*Trust Audit Clients through the iRecorder subcomponent of each installation The iRecorder Manager component is used to view status, configuration, and supported data model information for selected recorders.

6.1.1.5 AU-5 Audit Review: TOE Audit Data (FAU_SAR.1-1)

Only the Portal Administrator has the capability to read the audit information generated by *e*Trust SCC Itself. This audit information was previously described in AU-2.

The *e*Trust SCC Server component is supported by two third-party relational databases which are used as common object repositories: The TNG Core database used to store status information and the Portal Database used to store viewing characteristics, URL information, user accounts, workgroups, workplaces and other management objects. All login and logoff events to the SCC server are audited and are stored in the Portal Database. Any Portal Database transactions are audited by the SCC Server. The SCC Server stores the date and time when the event occurred, the type of the event, the computer from where the change was made. For changes made to objects, the SCC Server audits the objects class, object name and the operation made on the object.

The *e*Trust SCC Server component restricts access to the data in the Portal Database and TNG Core database by user role. The user role is associated with a user when they login to the *e*Trust SCC GUI and are identified and authenticated by user name and password.

6.1.1.6 AU-6 Audit Review: Collected Audit Data (FAU_SAR.1-2)

This function refers to the ability to view the audit records produced by the resources on the product servers (*e*Trust SCC Clients) through the *e*Trust SCC GUI. An *e*Trust SCC user will be able to view the audit records only if the user has been assigned to the same workplace that contains the resources that generated those audit records.

6.1.1.7 AU-7 Selectable Audit Review (FAU_SAR.3)

The TOE provides searches, sorting and ordering of the collected audit data through the event and audit record viewing capabilities of the *e*Trust SCC GUI. The audit records that are displayed are restricted by user role. For example, only the Portal Administrator can view records pertaining to user logons and logoffs (*e*Trust SCC generated audit data); only a user assigned to a workplace can view audit records generated by the resources in that workplace (collected audit data). The exact fields of the audit records that are displayed on the *e*Trust SCC GUI can be defined by the administrator or the users themselves through the *e*Trust SCC GUI. In this way only the data fields of most significance to a particular user will be displayed. The data once displayed, can be searched, sorted and ordered by any audit record field that is displayed to the user

through standard GUI functions; i.e. clicking on the column header representing an audit data field will sort the records by that field.

6.1.2 Identification & Authentication

6.1.2.1 IA-1 User Authentication before any Action (FIA_UAU.2)

This requirement refers to the functionality provided by the *e*Trust SCC Server component of the TOE for authentication of the user before allowing TSF access through the browser based *e*Trust SCC GUI. Authentication is through a user password configured by the administrator. A policy to ensure a hard-to-guess password is specified in the administrator guidance.
The TOE compares the entered user name and password with the attributes of the user account objects stored in the object repository database for its authentication and identification of users.

6.1.2.2 IA-2 Protected Authentication Feedback (FIA_UAU.7)

This requirement refers to the functionality provided by the *e*Trust SCC Server component of the TOE to mask user authentication data. Only asterisks are displayed on the login screen of the *e*Trust SCC GUI when the user password is entered.

6.1.2.3 IA-3 User Identification before any Action (FIA_UID.2)

This requirement refers to the functionality provided by the *e*Trust SCC Server component of the TOE for identification of the user before allowing TSF access through the *e*Trust SCC GUI. Identification is through a user name configured by the administrator.

6.1.3 Security Management

6.1.3.1 SM-1 Management of TSF data (FMT_MTD.1)

*e*Trust SCC is intended to be used by the security manager and security operators of an enterprise. Therefore management of TSF data is restricted by user role as specified in Table 5-2.

As mentioned in AU-5 the user role is associated with a user when they are identified and authenticated at login by the *e*Trust SCC Server using the entered name and password.

General configuration and modification of the TSF data is constrained to the SCC Administrator and Portal Administrator roles. Only the Portal Administrator has access to the TSF data that is stored in the Portal Database as explained in AU-5. Therefore only the Portal Administrator can use the management functions that act on this data, such as the functions to define a new user. The SCC Administrator has access to the administration workplace which allows use of the functions that act on the TSF data such as audit policies. The Portal Administrator also has access to the administration workplace, and therefore can perform all the functions available to the SCC Administrator.

The SCC User role is normally that of an administrator (security operator) of one or more of the security products that are integrated into the *e*Trust SCC. Users having the SCC User role are only allowed to monitor and manage the products in their assigned workplace.

See Table 5-2 for details of the data and functions each role may access.

6.1.3.2 SM-2 Specification of Management Functions (FMT_SMF.1)

This sub-function specifies the management functions available through the *e*Trust SCC user interface. The *e*Trust SCC user interface is a GUI available through a web-browser to any workstation on the same network as the TOE components. The interface is handled by the embedded web server technology and content management services of the *e*Trust SCC Server component of the TOE.

6.1.3.3 SM-3 Security Roles (FMT_SMR.1)

This sub-function defines the roles that are used to limit access to the management functions of the *e*Trust SCC GUI. There are three roles: SCC Administrator, Portal Administrator and SCC User. All roles have administration capabilities. An SCC User assigned to a workplace has access to monitoring and management functions for the resources in that same workplace. The SCC Administrator has access to the administration workplace. The Portal Administrator can be thought of as the *e*Trust SCC System Administrator since they have access to all TOE functions and data. A user may have more than one role. The user roles and the management functions allowed for each role are specified in Table 5-2 – Management of TSF Data: *eTrust* SCC.

6.1.4 Protection of the TSF

6.1.4.1 PT-1 Partial Non-bypassability of the TSP: TOE (FPT_RVM_EXP_TOE.1)

The TSF ensures that TOE security functions are non-bypassable. Since this is a distributed, software-only TOE, it also relies on the underlying operating system to provide non-bypassability. The TSF ensures that security protection enforcement functions are invoked and succeed before each function within the TOE's scope of control is allowed to proceed. All management user operations are conducted in the context of an associated management session. This management session is allocated only after successful authentication into the TOE. User operations are checked for conformance to the granted level of access (implemented by user role and workplace assignment), and rejected if not conformant. The management session is destroyed when the corresponding user logs out of that session.

6.1.4.2 PT-2 Partial TSF Domain Separation: TOE (FPT_SEP_EXP_TOE.1)

The TSF has well defined external interfaces with its users and its interface to the IT environment on which it depends. Supplementing this, *e*Trust SCC relies on Microsoft

SQL Server to manage the Collector database and the databases used as its common object repositories.
Since the TOE is software only, it relies partially on the operating system of the TOE server(s) to provide file protections and process separation. In addition, the underlying assumption regarding the operation of TOE is that the server components are maintained in a physically secure environment.

6.2 SOF Claims

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

IA-1 User Authentication before any Action

Within IA-1, the methods used to provide difficult-to-guess passwords are probabilistic and based on the password policy that is defined in the administrative guidance. The SOF claim for this IT security function in SOF-basic.

6.3 Assurance Measures

*e*Trust SCC satisfies the assurance requirements for Evaluation Assurance Level EAL2. See Table 8-8 - Assurance Measures Rationale for the items provided as evaluation evidence to satisfy the EAL2 assurance requirements.

7 PP Claims

This Security Target is 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

Threat ID	Threat Description	Objective ID	Rationale
T.Attack	Unauthorized accesses and activity indicative of misuse on IT system resources the TOE monitors may not be identified or associated with other suspicious events thereby allowing the resource to be compromised by an attacker.	O.Analyze O.Collect O.Respond OE.AuditResource OE.Time	O.Collect specifies the collection of event data generated by the managed resources (OE.AuditResource supported by OE.Time). O.Analyze will process the collected event information to see if any of the data matches an audit policy or incident filter that signifies an unauthorized user had access to a critical resource (e.g. an unauthorized user name in the audit records generated by a critical process) or signifies an attack such as the disabling of a critical resource (e.g. an event code that designates a change to the file permissions of a resource). O.Respond will take action to notify responsible personnel of the event indicating the unauthorized access or misuse of the resource. O.Respond can also indicate a critical status of a resource that corresponds to a disabled resource.

Threat ID	Threat Description	Objective ID	Rationale
T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TOE security functions and data.	O.Audit O.I&A O.PartialProtect OE.AuditProtection OE.PartialProtect OE.Time	O.Audit generates audit records that will report any access to the TOE's user interface and the creation, deletion and changes to administrative objects. (Supported by OE.Time for reliable time stamps). O.I&A requires identification and authentication for all users before allowing access to the *e*Trust SCC user interface. O.PartialProtect specifies how the TOE protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. (Supported by OE.AuditProtection which protects the Collector Database and OE.PartialProtect which specifies the protection provided by the TOE server(s) OS and the DBMS of the common object repositories).
T.MisManage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	O.Admin	O.Admin specifies the controlled set of functions that allow effective management of TOE security functions and data.

8.1.2 Assumptions

Table 8-2 shows that all of the secure usage assumptions are addressed by Non-IT security objectives.

Table 8-2 - All Secure Use Assumptions Addressed

Assumption ID	Assumption Description	Objective ID & Rationale
A.NoEvil	It is assumed that the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation to install and manage the TOE securely	ON.Personnel ON.Personnel specifies that those working as authorized administrators shall be carefully selected. It also ensures that the administrators will be properly trained so that the TOE is installed, managed and operated according to the TOE guidance documentation.

Assumption ID	Assumption Description	Objective ID & Rationale
A.NoUntrusted	IT is assumed that there will be no untrusted software on the TOE servers.	ON.NoUntrusted ON.NoUntrusted ensures that there shall be no untrusted software installed on the server(s) that host the *e*Trust SCC Server and *e*Trust Audit components of the TOE.
A.Password	It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data	ON.PwdProtect ON.PwdProtect ensures that users of the TOE shall be instructed by the administrator guidance to choose strong passwords in accordance with the documented password policy and to protect their authentication data.
A.Physical	It is assumed that the TOE server hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	ON.Physical ON.Physical specifies that those responsible for the TOE shall ensure that the server(s) that host the *e*Trust SCC Server and *e*Trust Audit components of the TOE are protected from any physical attack by being located in a secure environment.

8.1.3 Organizational Security Policies

There are no organizational security policies that must be met by the TOE.

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 for the TOE

Objective	Objective Description	SFR and Rationale
O.Admin	The TOE shall include a set of functions that allow effective management of TOE security functions and data.	FAU_SAR.1-1: Audit review The TOE provides the functionality for the Portal Administrator to read all audit information generated by *e*Trust SCC itself. FAU_SAR.1-2: Audit review The TOE provides the functionality for an SCC User (workplace administrator) to read all audit information generated by the resources assigned to the same workplace. FAU_SAR.3: Selectable audit review The TOE provides the ability for the user to sort, search and order the display of audit data by any audit data fields on the display. FMT_SMF.1: Specification of management functions The TOE provides a comprehensive set of management functions to allow administrators to manage its security functions and data.

Objective	Objective Description	SFR and Rationale
O.Analyze	The TOE shall apply analytical processes to information collected from the monitored resources in order to identify potential security violations.	FAU_SAA.3: Simple attack heuristics The TOE has the capability to analyze the audit data collected from its resources according to administrator defined rules, policies and filters. The TOE is able to indicate a potential security violation by applying these analytical processes.
O.Audit	The TOE shall generate audit records for access to the TOE's user interface and creation, deletion and changes to administrative objects.	FAU_GEN.1-1: Audit data generation The TOE generates audit records that provide information about the use of management functions and access of TSF data through the *e*Trust SCC user interface.
O.Collect	The TOE shall collect information about events that are indicative of potential security violations of critical resources.	FAU_GEN_EXP.1: Audit data collection The TOE collects audit data from its managed resources that provide information to indicate security relevant events.
O.I&A	The TOE shall provide functionality to require identification and authentication for all users of the *e*Trust SCC user interface.	FIA_UAU.2: User authentication before any action The TOE requires that a user be authenticated by entering a valid password before allowing access to any management functions or data. FIA_UID.2: User identification before any action The TOE requires that a user be identified by entering a valid user id before allowing access to any management functions or data.
O.PartialProtect	The TSF shall provide protection for itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.	FIA_UAU.7: Protected authentication feedback The TOE masks a user's password on entry so that it cannot be observed by untrusted personnel. FMT_MTD.1: Management of TSF data The TOE restricts access to management functions and TSF data by assigned user role. FMT_SMR.1: Security roles The TOE maintains the user roles: SCC Administrator, Portal Administrator and SCC User, to limit access to management functions and TSF data. FPT_RVM_EXP_TOE.1: Partial non-bypassability of the TSP: TOE The TOE protects itself through the operation of its own enforcement functions. FPT_SEP_EXP_TOE.1: Partial TSF domain separation: TOE The TOE protects itself by enforcing separation between code executing on behalf of difference users.
O.Respond	The TOE shall notify administrative personnel to potential security violations of critical resources.	FAU_ARP.1: Security alarms The TOE has the ability to notify administrative personnel to potential security violations of critical resources through the execution of a program, email notification, storage of data in the collector database, execution of a workflow or by visually indicating a critical status on the user's display.

8.2.2 Dependencies

Table 8-4 and Table 8-5 show the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the item number of the component that satisfies the dependency. An (E) following the item number of the component that satisfies the dependency signifies that an environment SFR meets this dependency.

Table 8-4 - TOE SFR Dependencies Satisfied

Item	Component	Dependencies	How Satisfied	
1	FAU_ARP.1	FAU_SAA.1	4 (H)	FAU_SAA.3
2	FAU_GEN.1-1	FPT_STM.1	21 (E)	FPT_STM.1
3	FAU_GEN_EXP.1	FAU_GEN.1 FPT_STM.1	2 16 (E) 21 (E)	FAU_GEN.1-1 FAU_GEN.1-2 FPT_STM.1
4	FAU_SAA.3	None	None	None
5	FAU_SAR.1-1	FAU_GEN.1	2 16 (E)	FAU_GEN.1-1 FAU_GEN.1-2
6	FAU_SAR.1-2	FAU_GEN.1	2 16 (E)	FAU_GEN.1-1 FAU_GEN.1-2
7	FAU_SAR.3	FAU_SAR.1	5 6	FAU_SAR.1-1 FAU_SAR.1-2
8	FIA_UAU.2	FIA_UID.1	10 (H)	FIA_UID.2
9	FIA_UAU.7	FIA_UAU.1	8 (H)	FIA_UAU.2
10	FIA_UID.2	None	None	None
11	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	12 13	FMT_SMF.1 FMT_SMR.1
12	FMT_SMF.1	None	None	None
13	FMT_SMR.1	FIA_UID.1	10 (H)	FIA_UID.2
14	FPT_RVM_EXP_TOE.1	None	None	None
15	FPT_SEP_EXP_TOE.1	None	None	None

Table 8-5 - IT Environment SFR Dependencies Satisfied

Item	Component	Dependencies	How Satisfied	
16	FAU_GEN.1-2	FPT_STM.1	21 (E)	FPT_STM.1
17	FAU_STG.1	FAU_GEN.1	2 16 (E)	FAU_GEN.1-1 FAU_GEN.1-2
18	FPT_ITT.1	None	None	None
19	FPT_RVM_EXP_IT.1	None	None	None
20	FPT_SEP_EXP_IT.1	None	None	None
21	FPT_STM.1	None	None	None

8.2.3 Rationale why dependencies are not met

All dependencies for both the TOE and IT SFRs have been met.

8.2.4 Strength of Function Rationale

Part 1 of the CC defines “strength of function” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this ST. SOF-basic states, “A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.”
The rationale for choosing SOF-basic was to be consistent with the assurance requirements included in this ST; namely the Environment is where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product, consistent with a Common Criteria Level of Evaluation of EAL2. Specifically, AVA_VLA.1 requires that the TOE be resistant to an attacker with a low to moderate attack potential, this is consistent with SOF-basic. Consequently, the metrics (password) chosen for inclusion in this ST for this TOE were determined to be acceptable for SOF-basic and would adequately protect information in a Basic Robustness Environment.
The one security function based on probabilistic methods is IA-1 identified in Section 6.1.2.1 and applies to FIA_UAU.2 (*see* Section 5.1.2). A policy for selecting a strong password for user authentication to meet this claim is described in the administrator guidance.

8.2.5 Assurance Rationale

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 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.

The FAU_ auditing requirements provide the main function of *e*Trust SCC, to manage and monitor the network resources. All of these requirements build upon each other. *e*Trust SCC generates its own audit trail of security events as specified in FAU_GEN.1-1. FAU_GEN_EXP.1 specifies how *e*Trust SCC collects audit event data which has been generated itself (FAU_GEN.1-1) and by the network resources that it monitors (FAU_GEN.1-2). The collected audit data is protected by a DBMS in the IT Environment (FAU_STG.1). The collected audit is analyzed through the means specified in FAU_SAA.3. When the analysis determines a potential security violation an alert is

generated as specified in FAU_ARP.1. In addition, FAU_ARP.1 also states that *e*Trust SCC can alert responsible personnel when a resource has a critical status. *e*Trust SCC also provides authorized users the ability to view the *e*Trust SCC audit data as stated in FAU_SAR.1-1, and the resource audit data as stated in FAU_SAR.1-2. The audit viewing capability is enhanced by FAU_SAR.3 which provides the ability to sort, search and order the audit information.

User login processing is described by the FIA_ requirements. FIA_UID.2 requires that a user must enter a valid user id and FIA_UAU.2 requires the entry of a valid password before the user is allowed access to the *e*Trust SCC user interface. The password is protected by being masked on data entry as described in FIA_UAU.7

Once a user is authorized by the FIA_ requirements, the management requirements of the FMT_ class describe the access to the TSF that the user is allowed. Access to the management functions described in FMT_SMF.1 is controlled by the user's assigned role(s) which are specified in FMT_SMR.1. The FMT_MTD.1 requirement details the exact operations allowed on TSF data objects that are allowed for each user role.

*e*Trust SCC protects itself through the requirements mentioned above: FAU_GEN.1-1 for security auditing, FIA_UID.2 and FIA_UAU.2 for user identification and authentication and FMT_MTD.1 for controlled access to security management functions and data. The TOE also protects itself through the TSF protection requirements of the FPT_ class. FPT_RVM_EXP_TOE.1 specifies non-bypassability of the TSP enforcement functions and FMT_SEP_EXP_TOE.1 specifies the security domain separation that *e*Trust SCC provides through its own interfaces.

Because *e*Trust SCC is a distributed, software-only TOE, it also relies on the IT Environment to provide protection. As mentioned earlier FAU_STG.1 provides protection of the collected audit data. The TOE also depends on the operating system and DBMS on the servers that host the TOE components to provide non-bypassability of security enforcement functions (FPT_RVM_EXP_IT.1) and domain separation (FPT_SEP_EXP_IT.1). The FPT_ITT.1 specifies that the environment must protect data transmitted between TOE components. *e*Trust SCC also relies on the environment to provide reliable time stamps for its audit logging (FPT_STM.1).

8.2.7 Explicitly Stated Requirements Rationale

FAU_GEN_EXP.1 had to be explicitly stated because the collection of the audit data generated by the managed resources, which is vital to the functioning of the product, could not be described by existing CC functional requirements. The audit data referenced in this requirement differs from the TOE audit data specified in the CC standard FAU_GEN.1 in that it is not generated by the TOE upon a security relevant event, but rather collected from an outside source (the managed resources). FAU_GEN_EXP.1 was modeled on FAU_GEN.1, and therefore has a dependency on FPT_STM.1 to supply reliable timestamps. FAU_GEN_EXP.1 also has a dependency on an instance of FAU_GEN.1 in the IT Environment to specify the generation of audit records from the managed resources.

FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FPT_RVM_EXP_IT.1, and FPT_SEP_EXP_IT.1 had to be explicitly stated because the TOE is software only and therefore can only provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. The approach used for these requirements is according to the NIAP policy requiring software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005'. As with FPT_RVM.1, and FPT_SEP.1, on which they were based, these explicit requirements have no dependencies.

8.2.8 Requirements for the IT Environment

Table 8-6 shows that all of the security objectives for the IT environment are satisfied. Rationale that all objectives are satisfied is stated in the text following the table.

Table 8-6 - All Objectives for the IT Environment Met by Requirements in the IT Environment

Objective	Objective Description	SFR and Rationale
OE.AuditProtection	The IT Environment shall provide the capability to protect the collected audit information.	FAU_STG.1: Protected audit trail storage The IT Environment protects the collected audit information through the protection functions of the operating system and the database management system that resides on the server that hosts the *e*Trust Audit Data Tools component.
OE.AuditResource	The IT Environment shall provide the capability to generate records of events that are indicative of potential security violations of critical resources.	FAU_GEN.1-2: Audit data generation The managed resources in the IT Environment can generate audit records that provide information indicative of potential security violations.
OE.PartialProtect	The IT Environment shall provide protection for the TOE and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.	FPT_ITT.1: Basic internal TSF data transfer protection The IT Environment provides a secure network that protects TSF data when it is transmitted between TOE components. FPT_RVM_EXP_IT.1: Partial non-bypassability: IT Environment The security enforcement functions of the TOE server(s) operating system protects the TOE components that reside there. FPT_SEP_EXP_IT.1: Partial domain separation: IT Environment The security functions of the TOE server(s) operating system protects the TOE by enforcing separation between code executing on behalf of difference users.
OE.Time	The underlying operating systems shall provide reliable time stamps.	FPT_STM.1: Reliable time stamps The IT Environment provides reliable time stamps for use by the TOE.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-7 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-7 - Mapping of Functional Requirements to TOE Summary Specification

SFR	TSS Security Function		Rationale
FAU_ARP.1	AU-1	Security Alarms	Specifies the actions taken by *e*Trust SCC when it detects a potential security violation.
FAU_GEN.1-1	AU-2	Audit Data Generation: TOE	Specifies the audit information generated by *e*Trust SCC itself.
FAU_GEN_EXP.1	AU-3	Audit Data Collection	Specifies how *e*Trust SCC collects audit information from its managed resources.
FAU_SAA.3	AU-4	Simple Attack Heuristics	Specifies the capabilities of *e*Trust SCC to analyze the collected audit information so that actions can be taken upon the discovery of a security relevant event.
FAU_SAR.1-1	AU-5	Audit Review: TOE Audit Data	Specifies that the *e*Trust SCC user interface allows the Portal Administrator to view the audit data generated by *e*Trust SCC itself.
FAU_SAR.1-2	AU-6	Audit Review: Collected Audit Data	Specifies that the *e*Trust SCC user interface allows SCC Users to view the audit data generated by the managed resources by workplace assignment.
FAU_SAR.3	AU-7	Selectable Audit Review	Specifies that *e*Trust SCC allows sorting, searching and ordering of the audit records by any data field displayed to the user.
FIA_UAU.2	IA-1	User Authentication before any Action	Specifies that *e*Trust SCC requires a valid user password before allowing access to any other function.
FIA_UAU.7	IA-2	Protected Authentication Feedback	Specifies that the *e*Trust SCC user interface masks the user's password upon entry.
FIA_UID.2	IA-3	User Identification before any Action	Specifies that *e*Trust SCC requires a valid user id before allowing access to any other function.
FMT_MTD.1	SM-1	Management of TSF Data	Specifies how *e*Trust SCC controls access to management functions and TSF data by the roles assigned to the users.
FMT_SMF.1	SM-2	Specification of Management Functions	Specifies the management functions provided through the *e*Trust SCC user interface.
FMT_SMR.1	SM-3	Security Roles	Specifies the user roles maintained by *e*Trust SCC that are used to control access to the management functions and TSF data.
FPT_RVM_EXP_TOE.1	PT-1	Partial Non-bypassability of the TSP: TOE	Specifies how the security enforcement functions of *e*Trust SCC enforce non-bypassability.

SFR	TSS Security Function		Rationale
FPT_SEP_EXP_TOE.1	PT-2	Partial TSF Domain Separation: TOE	Specifies how the security enforcement functions of *e*Trust SCC enforce domain separation.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-8.

Table 8-8 - Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.2 Configuration Items	CM Documentation CM Proof Configuration Item List	Configuration List	CM Proof Shows the CM system being used. Configuration Item List(s) is comprised of a list of the source code files and version numbers is comprised of a list of design documents with version numbers is comprised of test documents with version numbers user and administrator documentation with version numbers
2	ADO_DEL.1 Delivery Procedures	Delivery Procedures	Delivery Procedures	Provides a description of all procedures that are necessary to maintain security when distributing *e*Trust SCC software to the user's site. Applicable across all phases of delivery from packaging, storage, and distribution.
3	ADO_IGS.1 Installation, Generation and Startup Procedures	Installation, generation, and start-up procedures	*e*Trust SCC, Getting Started Guide v8.0 *e*Trust ™ Security Command Center™ r8 SP1 with CR2 Patch Common Criteria Supplement Guide	Getting Started Guide and CC Supplement Guide - Provides detailed instructions on how to install and configure *e*Trust SCC.
4	ADV_FSP.1 Informal Functional Specification	Functional Specification	*e*Trust SCC Development Documentation	Describes the TSF interfaces and TOE functionality.
5	ADV_HLD.1 Descriptive High-Level Design	High-Level Design	*e*Trust SCC Development Documentation	Describes the TOE subsystems and their associated security functionality.
6	ADV_RCR.1 Informal Correspondence Demonstration	Representation Correspondence	*e*Trust SCC Development Documentation	Provides the following two dimensional mappings: HLD to FSP External Interfaces to the SFRs

Item	Component	Evidence Requirements	How Satisfied	Rationale
7	AGD_ADM.1 Administrator Guidance	Administrator Guidance	*e*Trust SCC Administrator Guide v8.0 *e*Trust ™ Security Command Center™ r8 SP1 with CR2 Patch Common Criteria Supplement Guide	Describes how to administer the TOE securely.
8	AGD_USR.1 User Guidance	User Guidance	*e*Trust SCC User Guide v8.0	Describes the secure use of the TOE.
9	ATE_COV.1 Evidence of Coverage	Test Coverage Analysis	*e*Trust SCC Test Coverage	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
10	ATE_FUN.1 Functional Testing	Test Documentation	*e*Trust SCC Test Plan	Test documentation includes test plans and procedures and expected and actual results.
11	ATE_IND.2 Independent Testing – Sample	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
12	AVA_SOF.1 Strength of TOE Security Function Evaluation	SOF Analysis	*e*Trust SCC SOF Analysis	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
13	AVA_VLA.1 Developer Vulnerability Analysis	Vulnerability Analysis	*e*Trust SCC Vulnerability Analysis	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

This section is not applicable. There are no PP claims.

9 ACRONYMS

Acronym	Description
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy