BMC CONTROL-SA Security Target

Version 1.0

8 July 2005

Prepared for:
BMC Software, Inc.
2101 City West Boulevard
Houston, TX 77042

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

LIST OF TABLES

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is CONTROL-SA provided by BMC Software, Inc. CONTROL-SA is a software application that provides enterprise-wide security management of information systems. CONTROL-SA provides the Administrator with the necessary tools to manage the organization's two invaluable assets, users and information resources.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by TOE and IT environment and the organizational policy that must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL2.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – BMC CONTROL-SA Security Target

ST Version – Version 1.0

ST Date – 8 July 2005

TOE Identification – BMC CONTROL-SA composed of the following components:

- ESS v3.3 SP1
- CONTROL-SA/Solaris Agent v3.1.0
- ESS Web Console v2.1.01 SP1
- CONTROL-SA/RACF Agent v3.2.01
- ESS Console v3.8.01 SP1
- CONTROL-SA/Active Directory (AD) Agent v3.1.07 SP2

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
    - Part 3 Conformant
    - EAL 2

1.3 Conventions, Terminology, Acronyms

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

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

Account	An entity (e.g., authorized administrator) with access rights to a Managed System; a TSF data item in the context of this evaluation.
Account data	The asset managed by the TOE (part of the TSF data), including: for each Managed System account, the user permissions and credentials on each Managed System (if any), whether expressed directly or as a consequence of other data about the user (*e.g.*, group membership, profile), and for each administrator, the administrator permissions in the TOE, the list of Managed Systems, and information about their location and type

Authorized Administrator	See ESS Administrator.
DBMS	Data Base Management System
ESS	Enterprise SecurityStation
ESS Administrator	A person, who is authorized to maintain ESS data, has login rights to the ESS Console; manages ESS systems, facilities and objects. An ESS Administrator is allowed access only after successful authentication.
Managed System	A security product or module. The Managed System may be the native security of an operating system (for example, Solaris, HP-UX, Novell NetWare), an add-on security product (for example, RACF, SeOS), or any other product that requires user registration (for example, Sybase, Oracle). The Managed System may reside anywhere in the network. Its access privileges are managed via an SA-Agent platform. Each Managed System entity represents a specific Managed System connected via the appropriate SA-Agent. The TOE provides an interface (gateway) to each supported Managed System which enables the relevant agent to perform the following: (a) request that the Managed System modify account data (b) obtain from the Managed System notification that account data was locally modified on the Managed System (that is, not through the medium of the TOE)
SA-Agent	Operating as a security administration agent running on the various platforms in the enterprise (Windows, Solaris, and RACF[1]), the SA-Agent processes and transfers security commands and data between Managed System and the central Enterprise SecurityStation workstation.

2 TOE Description

The Target of Evaluation (TOE) is BMC CONTROL-SA. This section describes the TOE, its purpose, structure, and functionality.

2.1 TOE Overview

The TOE is designed to manage and maintain the enterprise-wide security of user access to information systems and resources that are distributed among numerous heterogeneous systems. It enables the automated and simplified management of all enterprise security systems from a central point of control.

The following are key features and benefits that the TOE provides:

- Enables end-to-end identity management and resource provisioning from a central location.
- Centralized user and security system administration.
- Centralized enterprise security policies management.
- Cuts operational costs with high-level automation.
- Decreases time spent on administration and training through use of a single consistent management tool.

[1] Resource Access Control Facility (RACF). A large system security program for IBM mainframes that checks passwords and prevents unauthorized users from accessing files.

- Tightens security with full accountability, auditing and reporting capabilities, which increase administrator awareness.
- Reduces help desk password reset and access-rights administration through automation capabilities.
- Simplifies password management for users by reducing the number of passwords that need to be remembered.
- Increases user productivity by providing faster automatic updates and access to resources in minutes not days.
- Decreases errors in user definitions, resulting in a decrease in the help desk work load.

The TOE is an integrated client/server solution consisting of Enterprise SecurityStation, which is the central point of control, and **SA-Agent**, which runs on any number of managed platforms or networks throughout an organization. Each SA-Agent interfaces with an access control systems, such as RACF or other applications that require user and resource administration. Each such system is referred to as a **Managed System (MS)**.

Managed Systems, while providing platform-specific security, fail to provide a multi-platform level of security control and administration. The TOE supplies that missing feature with a dedicated, synchronized security data repository and Graphical User Interface (GUI). Users can be registered or deleted, access rights can be granted, changed, or denied, and the access control policies can be set, changed, and monitored. An administrator can make global changes to all of the accounts in a single action.

The TOE maintains a central database of accounts (that is, users and their access privileges) for various Managed Systems. The TOE centralizes account data in its database, and maintains the consistency of this data with the data on the corresponding Managed Systems.

TOE administrators maintain this database using one or more of the following methods:

- The TOE's ESS Console (Windows GUI module)
- Web browser in conjunction with the TOE's Web Console module
- Command line level batch files

When a TOE administrator adds a new account to the database, the TOE administrator specifies the Managed Systems to which the account is to be granted access and the access privileges the account will have on each of these systems. The TOE generates a single password for the account for all the specified Managed Systems and updates each of the Managed Systems accordingly.

Subsequent modifications to an account's password and access privileges, including the revoking of these privileges, are automatically updated on each of the Managed Systems.

Local modifications of account passwords and access privileges (performed on the Managed System directly rather than via the TOE) are automatically posted to the TOE database so that the consistency of the TOE database and the access data as maintained in the Managed Systems' databases are maintained.

The account data on each Managed System and their protection are outside the scope of the TOE.

2.2 TOE Architecture

Security administration for the entire enterprise, regardless of number and variety of platforms, is performed from a central point of control. This central point of control, Enterprise SecurityStation, enables the security administrator to manage different environments via an advanced, easy-to-use Console.

Using Enterprise SecurityStation, the administrator can perform all key security administration tasks such as: define new entities (for example, Accounts or Groups), connect users to their organizational roles, inquire about entities, set enterprise-wide security policies and standards, and identify security alerts.

The TOE consists of the following components:

Enterprise SecurityStation (ESS) Server - is the central point of control. The ESS receives data from Open Services, ESS Console, and Command line batch update files and updates the ESS database accordingly. The ESS also instructs the gateways to communicate with the Managed Systems.

Router - directs communications among the ESS Server-gateway and SA-Agent-gateway pairs

ESS Console - The ESS Console provides comprehensive, interactive access to the ESS database. ESS Console is the administrator's primary interface to ESS data, which is maintained in the ESS database. The ESS Console displays ESS database information, collects administrator input and passes this input to ESS for execution. The ESS Console is an element of the ESS server and is a separate executable.

Web Console (GUI) - Web Console provides view and controller functionality. The Web Console enables end users to interact with Open Services, and it sends data to the end user in the form of Web pages displayed in the client browser.

Open Services - Open Services provides the CONTROL-SA system with an open, common, easy-to-use application-programming interface (API) for connecting CONTROL-SA service providers with CONTROL-SA service consumers. Open Services connects Enterprise SecurityStation, a back-end service provider to various front-end applications and clients. The Open Services component collects input from the Web Console and other clients (for example, SPML Form Generator) and passes this input to the ESS component. Open Services connects to ESS Server using the ESS-API.

Command line batch update files - The command line batch update files contain commands for ESS execution. These files are read directly by ESS. ESS Server also accepts input from a batch update file. This capability is most often used when the TOE is installed, in order to build the TOE database from existing accounts.

Application and System Gateways – The Gateways represent a process, which handles communication with one or more Managed System Agents and updates the Enterprise SecurityStation database. Gateways communicate with each other. On the Managed System, the gateway communicates with the ESS gateway on the one hand and the Managed System agent on the other. The ESS gateway is used for communication between the Managed System Gateways and the ESS Server. Application and system gateways communicate with the Managed System agents to pass commands received from ESS to the Managed System agents for execution by the Managed System and to receive notification from the Managed System agents of local modifications that affect the ESS database (for example, a change to user access permissions).

Managed System Agents - Managed System agents, residing on the Managed System receive commands from ESS for execution by the Managed System, execute the commands on the Managed System, and notify the gateway of local modifications that affect the ESS database (for example, a change to user access permissions).

The underlying operating systems that support the TOE are as follows:

TOE Component	OS Version
ESS v3.3 SP1	Solaris 9
CONTROL-SA/Solaris Agent v3.1.0	Solaris 9
ESS Web Console v2.1.01 SP1	Solaris 9
CONTROL-SA/RACF Agent v3.2.01	RACF
ESS Console v3.8.01 SP1	Windows 2000, XP, Server 2003
CONTROL-SA/Active Directory (AD) Agent v3.1.07 SP2	Windows Server 2003

In addition, the following third-party components are also required for the functioning of the TOE, and comprise the environment in which the TOE components execute.

Product	Version	Notes
WebLogic	7	J2EE Web Application Server – runs Java Runtime; includes servlet containers
WebSphere	5.0.2.3	J2EE Web Application Server – runs Java Runtime; includes servlet containers
JBoss	3.0.4	Open source J2EE Web Application Server, provided with SA-Control; does not include servlet containers
Tomcat	4.1.24	Servlet container (required only for JBoss)
Wasp		Development toolkit and runtime component; Wasp server executes Web Services requests
Sun JDK	1.4.1_02	Java runtime component
IBM JDK	On Solaris: (Sun + IBM added library)1.3.1_09	Java runtime component
JCE	7	Java encryption services
Orbix/OrbixSSL	3.3.6	CORBA standard middleware; provides session management, including secure channels between applications on different computers
Oracle	8.1.7.0 through 9.2.4	Stores the ESS data, including audit logs
Adaptive Server Enterprise (Sybase)	12.0.0.6 through 12.5.01	
TCL/Tk	8.3.4	

Notes related to Third Party Components

- WebLogic, WebSphere, and JBoss all perform the same functionality. The customer is free to choose among them.
- WebLogic and WebSphere include the functionality provided by Tomcat; JBoss does not.
- SunJDK and IBM JDK provide the same functionality, and the customer is free to choose between them.
- Oracle and Sybase provide the same functionality, and the customer is free to choose between them.

2.2.1 Physical Boundaries

Each component of the TOE is a software application that operates within a specified environment. The TOE physical boundaries are the external interfaces and the interfaces to the IT environment. The interfaces to the IT environment refer to interfaces that provide any necessary services to the TOE that are necessary for the TOE to function properly. The operating systems and third party components are not part of the TOE.

The TOE consists of the components illustrated below. These components work together to provide centralized security administration for the entire enterprise.

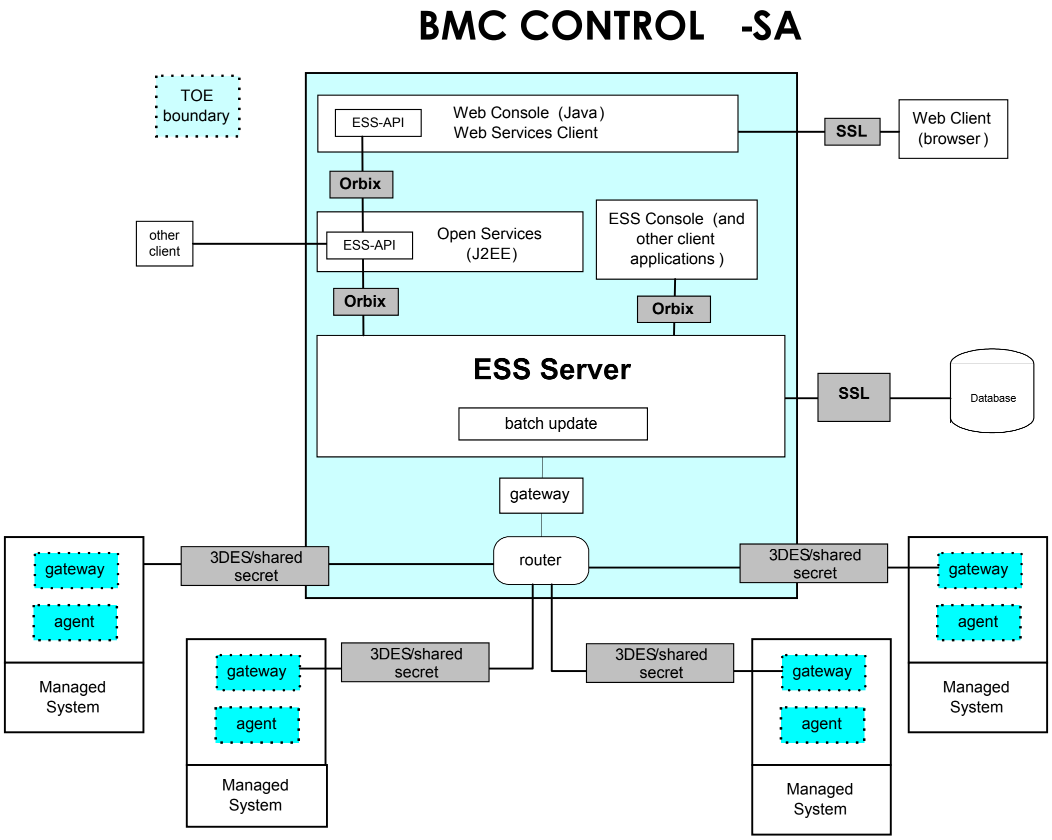

Figure 1 TOE Architecture

As illustrated in Figure 1, many SA-Agent platforms can communicate with Enterprise SecurityStation via the ESS gateways. SA-Agent does not replace the security provided by the individual Managed System. Together with the features of Enterprise SecurityStation, SA-Agent enables enterprise-wide management and security administration of multiple Managed Systems.

Interaction between SA-Agent and the Managed Systems is achieved through the USA-API. Since each Managed System has different facilities and operates using its own unique terminology, SA-Agent is provided with a dedicated USA-API for each type of Managed System supported. The use of dedicated USA-APIs enables SA-Agent to handle the unique features and operations of each Managed System.

Although the SA-Agents runs on any number of managed platforms or networks throughout an organization, the Sa-Agents included in the evaluated configuration are: CONTROL-SA/Agent for Solaris v3.1.07, CONTROL-SA/Agent for Microsoft Active Directory v3.1.07, and CONTROL-SA/Agent for RACF v3.2.01.

2.2.2 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces. The TOE logically supports the following security functions at its interfaces:

- Security Audit
- Cryptographic Support
- User Data Protection

- Identification and Authentication
- Security Management
- Protection of the TSF

2.2.2.1 Security audit

Audit records are generated when security related auditable events occur. Refer to Security audit section in the TSS for a complete list of auditable events. The information that is recorded in the audit record includes the date/time, the responsible user, the event, the outcome of the event, and if applicable, the unique identification of the Managed System. The TOE provides the functionality necessary for authorized administrators to review audit logs.

2.2.2.2 Cryptographic support

The TOE supports cryptographic operations such as data encryption/decryption of the data that is transmitted between the ESS and the Managed Systems.

2.2.2.3 User data protection

The TOE enforces an ESS Access Control policy, which restricts access to the TOE and its functions (i.e. administering attributes of Managed Systems). This protection requires that users (authorized administrator) of the TOE be identified and authenticated before any access to the Managed Systems attributes is granted. Access is granted based on privileges defined by the TOE granted to the user (authorized administrator) that allow access to specific Managed System attributes.

2.2.2.4 Identification and authentication

All users must be identified and authenticated before access to the TSF is allowed. The user is required to provide a user ID and password, if the verification is successful, access into the TOE is granted.

2.2.2.5 Security management

The TOE is managed through the Enterprise SecurityStation (ESS) Server, which is the central point of control through which administrators can perform all key security administration tasks including:

- Management of Audit Data
- Management of ESS Access Control
- Management of ESS and Managed System data

2.2.2.6 Protection of the TSF

The TOE implements a set of security mechanisms to protect the transmission and integrity of its data. The TOE uses data encryption to protect the data transmitted between components of the TOE. The TOE also ensures the consistency of TSF data when replicated between components of the TOE.

3 Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of TOE security environment defines the following:

- Threats that the product is designed to counter
- Organizational security policies with which the product is designed to comply
- Assumptions made on the operational environment and the method of use intended for the product

3.1 Threats

T.AUDIT A user may perform unauthorized actions that go undetected.

T.TRANSMIT An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing the unauthorized user to intercept and modify transmitted information.

T.SYNC An unauthorized user may cause the data (security administration data and access control permissions) on the ESS and Managed System to become unsynchronized, as a result obsolete access controls, including old authentication data may be exploited.

T.UNAUTH An unauthorized user may gain access to and/or modify the TOE data.

3.2 Organizational Security Policies

P.GEN_KEYS Cryptographic keys will be generated in accordance with requirements defined by FIPS-140-1.

P.DES_KEYS Cryptographic keys will be destroyed in accordance with requirements defined by FIPS 140-1.

P.MANAGE The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.

P.PROTECT The TOE shall be protected from unauthorized accesses and modification of TOE data and functions.

3.3 Assumptions

A.ADMIN The authorized administrators are competent, not careless, willfully negligent, or hostile and will adhere to the guidance and instructions provided in the TOE documentation. The authorized administrators are also trained for proper TOE operation.

A.BACKUP The authorized administrator follows the computer system backup and recovery procedures, to enable the computer system and product to be restored to a secure state after a failure of the computer system or product.

A.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

A.LOCATE The components of TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

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

A.OS It is assumed that the underlying operating system and associated DBMS will provide capabilities and be configured appropriately to protect TSF data and functions (logically as well as physically).

A.TIME The operating environment will provide a reliable system time.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as IT Security Objectives for the TOE, IT Security Objectives for the Environment, or Non-IT Security Objectives for the Environment. The security objectives reflect the stated intent to counter the identified threats, comply with any organizational security policies identified, and address any assumptions. All of the identified threats, organizational security policies, and assumptions are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.AUDIT The TOE shall generate audit records of the security relevant actions of the users of the TOE to ensure that users are held accountable for their actions on the TOE. The TSF must present this information in a readable and searchable format to authorized administrators and ensure that only authorized administrators are able to access this information.

O.AUTH The TOE must ensure that only authorized users gain access to the TOE and its resources by uniquely identifying and authenticating all users before granting access to the TOE and its resources.

O.MANAGE The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.TRANSMIT The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE.

O.UPDATE The TOE must ensure synchronization occurs between ESS and the Managed Systems.

4.2 Security Objectives for the IT Environment

OE.GEN_KEYS The TSF must ensure that cryptographic keys are generated in accordance with requirements defined by FIPS 140-1.

OE.DES_KEYS The TSF must ensure that cryptographic keys are destroyed in accordance with requirements defined by FIPS 140-1.

OE.TIME The IT environment shall provide a reliable time source for the TOE to provide an accurate timestamp for all audit records.

4.3 Security Objectives for the Non-IT Environment

OE.ADMIN Authorized users of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.

OE.BACKUP In the event of computer system or product failure, the authorized administrator will ensure the computer system and product will be restored to a secure state through proper adherence to procedures applicable to backup and recovery of the computer system and product.

OE.INSTALL Those responsible for the TOE must ensure that the TOE and its operating environment is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

OE.LOCATE Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack and modification that might compromise the TOE security objectives.

OE.OS The underlying operating system and associated DBMS will provide capabilities and be configured appropriately to protect TSF data and functions (logically as well as physically).

5 IT Security Requirements

This section defines the security functional and security assurance requirements for the TOE and associated Information Technology (IT) environment components. The SFR were drawn from the Part 2 Common Criteria version 2.2. The SAR were drawn from the Part 3 Common Criteria version 2.2

Note that in addition to these requirements, CONTROL-SA also satisfies a minimum strength of function 'SOF-basic'. The only applicable (i.e., probabilistic or permutational) security functional requirements are FIA_UAU.2. Note that some of the TOE security functional requirements (FCS_COP.1 and FPT_ITT.1) are based on cryptography, the strength of which is outside the scope of the Common Criteria.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by CONTROL-SA.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation FAU_SAR.1: Audit review FAU_SAR.2: Restricted audit review FAU_SAR.3: Selectable audit review
FCS: Cryptographic Support	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_ITT.3: TSF data integrity monitoring
	FPT_TRC.1: Internal TSF consistency

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.2 Audit data generation (FAU_GEN.1)

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

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

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

c) [**all modifications performed on the ESS database, aborting of a transaction upon detection of a data integrity error, success or failure of attempts to establish a connection via ESS login attempts, and successful attempts to start and stop batch jobs**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[for connection attempts: unique identification of the Managed System]**.

5.1.1.4 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**authorized administrator**] with the capability to read [**all audit information**] from the audit records.

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

5.1.1.5 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.6 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, sorting***] of audit data based on [**user ID, date/time, Managed System, and action**].

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**DES**, **3DES**] and cryptographic key sizes [**56 bits (DES) and 168 bits (Triple DES))**] that meet the following: [**The DES and Triple DES algorithms as implemented by BMC**].

5.1.2 User data protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the [**ESS Access Control**] on [

a. subjects: users (authorized administrator)
b. objects: Managed System]
and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**ESS Access Control**] to objects based on the following: [

subject: users (authorized administrator)

- **Managed System identity with associated privileges**

object: Managed Systems

- **Account**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Access is granted on requested operations based on privileges granted for the Managed System**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no explicit rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**no explicit rules**].

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user ID, password, list of Managed Systems, list of privileges granted for the Managed Systems**].

5.1.3.2 User authentication before any action (FIA_UAU.2)

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.

5.1.3.3 User identification before any action (FIA_UID.2)

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**ESS Access Control**] to restrict the ability to [***change_default, delete,*** [**add**]] the security attributes [**user ID, password, list of Managed Systems, list of privileges granted for the Managed Systems**] to [**authorized administrator**].

5.1.4.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**ESS Access Control**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query, modify, delete and*** [**update**]] the [**ESS and Managed System data**] to [**authorized administrator**].

5.1.4.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) **Management of Audit data**
b) **Management of ESS Access Control**
c) **Management of ESS and Managed System data**].

5.1.4.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**authorized administrator**].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Basic internal TSF data transfer protection (FPT_ITT.1)

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

5.1.5.2 TSF data integrity monitoring (FPT_ITT.3)

FPT_ITT.3.1 The TSF shall be able to detect [***modification of data***] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: [**abort the transaction**].

5.1.5.3 Internal TSF consistency (FPT_TRC.1)

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [**access to perform updates to the ESS and/or Managed System data**].

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by the IT environment of CONTROL-SA.

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Cryptographic support (FCS)

5.2.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**FIPS 140-1 Compliant Key Generation Algorithm**] and specified cryptographic key sizes [**56 bits (DES) and 168 bits (Triple DES)**] that meet the following: [**FIPS 140-1 Level 1, Section 4.8.1 Key Generation compatible algorithm**].

5.2.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**FIPS 140-1 Level 1, Section 4.8.5 Key Destruction compatible method**].

5.2.2 Protection of the TSF (FPT)

5.2.1.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1 Delivery and operation (ADO)

5.3.1.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.2 Development (ADV)

5.3.2.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.2.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1c The presentation of the high-level design shall be informal.
ADV_HLD.1.2c The high-level design shall be internally consistent.
ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.2.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3 Guidance documents (AGD)

5.3.3.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

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

5.3.3.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

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

5.3.4 Tests (ATE)

5.3.4.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

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

5.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.5.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE Summary Specification

This section describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE generates audit records for the following auditable events:

- Start-up and shutdown of the audit functions
- All modifications performed on the ESS database
- Aborting of a transaction upon detection of a data integrity error
- Success or failure of attempts to establish a connection via ESS login attempts
- Successful starting and stopping of batch jobs

Each audit record will include the date and time of the event which is obtained from the IT environment, type of event, user identity, and the outcome (success or failure) of the event. Additionally, for connection attempts between TOE components, the audit record will include the unique identification of the Managed System.

The audit records are presented in a readable format and can be sorted and/or searched by user ID, date/time, Managed System, and action. The TOE restricts access to the audit records to those users who have been granted explicit read-access.

The TOE logs audit information regarding all security relevant actions, such as all modifications performed on the ESS database. The entries in this log provide an audit trail of all additions, deletions, and modifications performed either in Enterprise SecurityStation or in any Managed System administered by Enterprise SecurityStation.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: Audit records are generated for the appropriate security relevant events and include the date and time of the event, type of event, user identity, and outcome of the event.
- FAU_SAR.1: The TOE provides authorized administrators with the ability to read and interpret audit data.
- FAU_SAR.2: Access to audit records is restricted to the authorized administrators.
- FAU_SAR.3: The TOE provides the ability for users to search and sort through the audit data based on any field in the audit report such as user identity or type of action.

6.1.2 Cryptographic support

The TOE uses the keys that were generated by the IT environment to encrypt and decrypt the data that is transmitted between the ESS and the Managed Systems. Each transaction sent to the SA-agent uses a different key. The transaction number and time are used with a hash function to pull the specific key. The encryption keys are selected from a pool of keys. The encryption key file can be different for each SA-agent the TOE communicates with. This key pool file is generated by the administrator for each SA-agent as part of the configuration and install process.

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_COP.1: Data encryption and decryption is performed in accordance with the Triple DES and DES cryptographic algorithms and specified cryptographic key sizes. BMC uses the commercially available source code, AFAIK, for its cryptographic operations. The Triple DES and DES conformance has not been validated rather it is an assertion made by BMC.

6.1.3 User data protection

The TOE provides ESS Server, a central point of control, and SA-Agent, which runs on any number of managed platforms or networks. Each SA-Agent interfaces with an access control system, such as RACF or other applications that require user and resource administration. Each such system is referred to as a Managed System.

The TOE enforces ESS Access control policies, which provides complete access control on users, the Managed System, and all operations between them. ESS Access Control is enforced based on the security attributes of the users and the Managed System. For users (authorized administrators)), the applicable security attribute is the Managed System identity with associated privileges. For the Managed System, the applicable security attribute is the account. The account, which is defined in Section 1, is the identification of the authorized administrator with privileges to the Managed System.

Access is granted on requested operations based on privileges granted for the Managed System. Users can be registered or deleted, by the authorized administrator. Access rights can be granted, changed, or denied, by the authorized administrator. Organizational policies can be set, changed, and monitored, by the authorized administrator. All these actions can be executed centrally and then automatically propagated to the appropriate Managed Systems.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2: The ESS Access Control policy is enforced on all users, Managed Systems and operations between them.
- FDP_ACF.1: ESS Access Control is based on the security attributes of the users and the Managed System, which are the Managed System identity with associated privileges and the Account.

6.1.4 Identification and authentication

The TOE maintains the following attributes for each user account in the TOE: user ID, authentication data (password), list of Managed Systems, and list of privileges granted to access Managed System attributes. The two types of privileges (access rights) that can be assigned are view and modify.

- The view connection privilege defines the access rights to view an entity in the Entity window or in a Properties window. For instance, to view the connections between entities, the authorized administrator must have access rights to view the two entities connected. For example, to view details of connections between Accounts and Groups, the authorized administrator must be connected to Access rules for Accounts and for Groups, with rights to view details.
- The modify connection privilege defines access rights to modify an entity. The modify access rights apply to all possible actions or to specific actions (e.g., insert, update, delete, connect).

The TOE requires users (authorized administrators) to provide unique identification (user ID) and authentication data (passwords) before access to the TOE is granted. The TOE compares the entered password to the password assigned to the account associated with the user ID entered and only allows access to the TOE if the passwords match. Therefore, no administrative actions are allowed until the TOE successfully authenticates the user.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE maintains the following list of security attributes for individual users: user identity, credential data, list of Managed Systems, list of privileges granted for the Managed Systems.
- FIA_UAU.2: The TOE requires that users be successfully authenticated before they are granted access to the TOE and any of its functions. This security function has a SOF-basic strength of function claim.
- FIA_UID.2: The TOE requires each user to identify itself before they are granted access to the TOE and any of its functions.

6.1.5 Security management

The TOE provides the ability to manage the security functions of the software through the ESS Server, which is the central point of control. These functions include the following:

- Management of Audit Data
- Management of ESS Access Control Policy
- Management of ESS and Managed System data

The TSF provides the management functions that allow the authorized administrator to view (read) the audit records. The authorized administrator can also sort and search the audit records by the following fields: userID, the date/time, the managed system, and the action or event.

The TSF provides the ability to manage the security functions of the TOE. Only the authorized administrator is permitted to perform management functions. The management functions include the ability to manage the behavior of the ESS Access Control policies, as well as change_default, delete, and add the security attributes; userID, password, list of managed systems, and the privileges granted for the managed system.

The ability to manage the ESS and Managed System data is restricted to the authorized administrator. The authorized administrator can query, modify, update, and delete the data.

The TOE supports the following role:

Authorized Administrator: A person authorized to maintain ESS and Managed System data: has login rights to the ESS Console; manages ESS systems and objects. The authorized administrator is allowed access only after successful identification and authentication. Only an authorized administrator can perform the following functions:

1. Change_default, delete and add the security attributes, which are: user ID, authentication data, list of Managed Systems and list of privileges granted for the Managed Systems.
2. Specify alternative initial values to override the default restrictive values for security attributes that are used to enforce the SFP.
3. Query, modify, delete, and update the ESS Server and Managed System data.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: Only authorized administrators have the ability to modify, delete or add security attributes.
- FMT_MSA.3: Restrictive default values are provided for security attributes that are used to enforce the SFP.
- FMT_MTD.1: Only authorized administrators can query, modify, delete, and update the ESS and Managed System data.
- FMT_SMF.1: The TOE performs the following security management functions: managing audit data, managing ESS Access Control, and management of ESS and Managed System data.
- FMT_SMR.1: The TOE maintains the role of authorized administrator and has the ability to associate users with roles.

6.1.6 Protection of the TSF

The TOE implements a set of security mechanisms to protect data from disclosure and modification during transmission. Any modification of data detected during transmission will cause the transaction to be aborted and an audit record to be issued.

Data encryption is used to ensure the security of privileged data external to the ESS database. Encryption is used to protect:

- **Transmitted data**

This consists of:

  - Data transmitted between Enterprise SecurityStation and the SA-Agent platforms.
  - Data transmitted between Enterprise SecurityStation components (for example, between the Console and ESS gateway).
  - Data transmitted between Enterprise SecurityStation and its supporting DBMS.

- **Stored data**

  This consists of:

  - Privileged data temporarily stored on an SA-Agent platform.
  - Encryption of stored data is handled automatically by SA-Agent and requires no intervention by the user.

- Inter-component communication is mainly conducted via Orbix, which provides Secure Socket Layer (SSL) authentication. SSL security is used to protect data transmitted between the Application Server and client applications. When SSL is implemented for this purpose, the necessary X.509 certificates must exist in both the Enterprise SecurityStation Server and client application installations. These certificates are installed together with Enterprise SecurityStation Server and with the client applications. Hence the SA-Agents and gateways are protected by ensuring communication is allowed when the entities have the shared secret keys. In addition, it is assumed the TOE and TOE components are placed in an access-controlled location.

In addition, local modifications of account passwords and access privileges (performed on the Managed System directly rather than via the TOE) are automatically posted to the TOE database so that the consistency of the TOE database and the access data as maintained in the Managed Systems' databases are maintained. This function ensures that obsolete access control data, to include old authentication data cannot be accessed to gain unauthorized access to the TOE and its data.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TOE protects its data from disclosure and modification when it is transmitted between separate parts of the TOE.
- FPT_ITT.3: The TOE is able to detect any modifications to data being transmitted between separate parts of the TOE and will abort the transaction upon any detection of a data integrity error. In addition, an audit record is generated to record this event.
- FPT_TRC.1: The TOE ensures the consistency of TSF data (security administration data and access control permissions) that is replicated between the ESS and the Managed Systems.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Tests
- Vulnerability Assessment

6.2.1 Configuration management

The configuration management measures applied by BMC ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. BMC ensures changes to the implementation representation are controlled. BMC performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, and configuration management documentation and all of these items are identified in the CM Plan as configuration items.

These activities are documented in:

- Identity Management BU Configuration Management Guide, Version 1.0, November 11, 2004
- Identity Management BU Configuration Management User Guide, Version 1.0, November 16, 2004
- BMC CONTROL-SA Configuration Management, Version 1.1, 11 May, 2005
- Project Configuration Management with CVS

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

BMC provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary start-up instructions. BMC delivery procedures describe all applicable procedures to be used to prevent inappropriate access to the TOE. BMC installs and configures the TOE for end users and then provides guidance necessary to securely start the TOE.

These activities are documented in:

- BMC Control-SA Secure Delivery, version 1.0, January 21 2005

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

BMC has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- BMC Control-SA Functional Specification / High Level Design / Representation Correspondence, Version 1.3, 21 March 2005

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

BMC provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- BMC CONTROL-SA Administrator and User Guidance, Version 1.0, 21 January 2005
- CONTROL-SA®/Agent for Microsoft Active Directory Administrator Guide, Version 3.1.07, March 1, 2004

- Release Notes:
  - CONTROL-SA®/Agent for Microsoft Active Directory, Version 3.1.07, April 8, 2004
  - CONTROL-SA®/Agent for Microsoft Active Directory, Version 3.1.07 Service Pack 1, August 25, 2004
  - CONTROL-SA®/Agent for Microsoft Active Directory, Version 3.1.07 Service Pack 2, December 29, 2004
  - CONTROL-SA®/Agent for RACF (version 3.2.01) Administrator Guide, December 26, 2004
- Release Notes:
  - CONTROL-SA®/Agent for RACF, Version 3.2.01, February 2, 2005
  - CONTROL-SA®/Agent for Solaris Administrator Guide, Version 3.1.07, December 31, 2003
- Release Notes:
  - CONTROL-SA®/Agent for Solaris, Version 3.1.07, December 31, 2003
  - CONTROL-SA®/Web Console (2.1.01) (Tomcat Deployment) Administrator Guide, September 20, 2004
  - CONTROL-SA Web Console® (2.1.01) User's Guide, September 20, 2004
- Release Notes:
  - CONTROL-SA®/Web Console, Version 2.1.01, September 23, 2004
  - CONTROL-SA®/Web Console, Version: 2.1.01 Service Pack 1, December 22, 2004
- Enterprise SecurityStation® (3.3.00) (Oracle Database) Installation Guide, October 20, 2004
- Enterprise SecurityStation® (3.3.00) Administration Guide, October 20, 2004
- Release Notes:
  - Enterprise SecurityStation®, Version: 3.3.00, December 2, 2004
  - Enterprise SecurityStation®, Version: 3.3.00 Service Pack 1, March 1, 2005
- Enterprise SecurityStation® Console Installation Guide, Version 3.8.01, May 10, 2004
- Enterprise SecurityStation® Console Administration Guide, Version 3.8.01, May 10, 2004
- Enterprise SecurityStation® Console User Guide, Version 3.8.01, February 26, 2004
- Release Notes:
  - Enterprise SecurityStation® Console, Version 3.8.01, June 6, 2004
  - Enterprise SecurityStation® Console, Version 3.8.01 Service Pack 1, October 3, 2004

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- BMC CONTROL-SA Test Plan, Version 1.1, 11 May 2005

- WECO.zip
- ESS Console.zip
- 26 Oct Test File.zip

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

BMC has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Basic.

BMC performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- BMC CONTROL-SA Vulnerability and Strength of Function Analysis, Version 1.0, December 26, 2004

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7 Protection Profile Claims

There are no Protection Profile claims in this Security Target.

8 Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- Explicitly Stated Requirements;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

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

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational security policies, threats, and assumptions by the security objectives.

	O.AUDIT	**O.AUTH**	**O.MANAGE**	**O.TRANSMIT**	**O.UPDATE**	**OE.GEN_KEYS**	**OE.DES_KEYS**	**OE.TIME**	**OE.ADMIN**	**OE.BACKUP**	**OE.INSTALL**	**OE.LOCATE**	**OE.OS**
T.AUDIT	X							X					
T.TRANSMIT				X									
T.SYNC					X								
T.UNAUTH		X											
P.GEN_KEYS						X							
P.DES_KEYS							X						
P.MANAGE			X										
P.PROTECT		X											
A.ADMIN									X				
A.BACKUP										X			
A.INSTALL											X		
A.LOCATE												X	
A.MANAGE									X				
A.OS													X
A.TIME								X					

Table 4 Environment to Objective Correspondence

8.1.1.1 T.AUDIT

A user may perform unauthorized actions that go undetected.

This Threat is satisfied by ensuring that:

- O.AUDIT: This objective ensures all security relevant actions are recorded.
- OE.TIME: This objective ensures the IT environment provides a reliable time source for the TOE to provide an accurate timestamp for all audit records.

8.1.1.2 T.TRANSMIT

An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing the unauthorized user to intercept and modify transmitted information.

This Threat is satisfied by ensuring that:

- O.TRANSMIT: This objective ensures TSF data is protected when transmitted between parts of the TOE.

8.1.1.3 T.SYNC

An unauthorized user may cause the data (security administration data and access control permissions) on the ESS and Managed System to become unsynchronized, as a result obsolete access controls, including old authentication data may be exploited.

This Threat is satisfied by ensuring that:

- O.UPDATE: This objective ensures synchronization occurs between ESS and the Managed Systems.

8.1.1.4 T.UNAUTH

An unauthorized user may gain access to and/or modify the TOE data.

This Threat is satisfied by ensuring that:

- O.AUTH: This objective ensures only authorized users gain access to the TOE and its data.

8.1.1.5 P.GEN_KEYS

Cryptographic keys will be generated in accordance with requirements defined by FIPS-140-1.

This Organizational Security Policy is supported by ensuring that:

- OE.GEN_KEYS: This objective ensures the cryptographic keys are generated in accordance with requirements defined by FIPS 140-1. The algorithm is 3DES and key size is 128.

8.1.1.6 P.DES_KEYS

Cryptographic keys will be destroyed in accordance with requirements defined by FIPS-140-1.

This Organizational Security Policy is supported by ensuring that:

- OE.DES_KEYS: This objective ensures the cryptographic keys are destroyed in accordance with requirements defined by FIPS 140-1. The destruction method is zeroization.

8.1.1.7 P.MANAGE

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

This Organizational Security Policy is supported by ensuring that:

- O.MANAGE: The objective ensures the TOE provides the tools/functions that allow the administrator to effectively manage the TOE and its security functions.

8.1.1.8 P.PROTECT

The TOE shall be protected from unauthorized accesses and modification of TOE data and functions

This Organizational Security Policy is supported by ensuring that:

- O.AUTH: This objective ensures only authorized users gain access to the TOE and its data.

8.1.1.9 A.ADMIN

The authorized administrators are competent, not careless, willfully negligent, or hostile and will adhere to the guidance and instructions provided in the TOE documentation. The authorized administrators are also trained for proper TOE operation.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: Authorized administrators are competent, non-hostile, well trained, and follow all administrator guidance.

8.1.1.10 A.BACKUP

The authorized administrator follows the computer system backup and recovery procedures, to enable the computer system and product to be restored to a secure state after a failure of the computer system or product.

This Assumption is satisfied by ensuring that:

- OE.BACKUP: Periodic computer system and product backups are performed by the authorized administrator for recovery of the computer system and product in case of failure.

8.1.1.11 A.INSTALL

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

This Assumption is satisfied by ensuring that:

- OE.INSTALL: The individuals responsible for the TOE must ensure that the TOE and its operating environment is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

8.1.1.12 A.LOCATE

The components of TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

This Assumption is satisfied by ensuring that:

- OE.LOCATE: The individuals responsible for the TOE must ensure that the TOE critical to security policy is protected from physical attack and modification.

8.1.1.13 A.MANAGE

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

This Assumption is satisfied by ensuring that:

- OE.ACCESS: Procedures are established to limit a user’s access to the TOE and to distribute security related responsibilities and privileges among different users.
- OE.PHYS: A comprehensive physical security policy restricting use of and access to the TOE is established and enforced.

- OE.MANAGE: The product, its users and environment will follow and comply with all physical, procedural and personnel site security policies.

8.1.1.14 A.OS

It is assumed that the underlying operating system and associated DBMS will provide capabilities and be configured appropriately to protect TSF data and functions (logically as well as physically).

This Assumption is satisfied by ensuring that:

- OE.OS: Those that mange the under lying operating system must ensure that it is correctly installed and protected from unauthorized access.

8.1.1.15 A.TIME

The operating environment will provide a reliable system time.

This Assumption is satisfied by ensuring that:

- OE.TIME: The IT environment must provide a reliable time source for the TOE.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that the following table, **Table 5 Objective to Requirement Correspondence** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUDIT	**O.AUTH**	**O.MANAGE**	**O.TRANSMIT**	**O.UPDATE**	**OE.GEN_KEYS**	**OE.DES_KEYS**	**OE.TIME**
FAU_GEN.1	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_SAR.3	X							
FCS_CKM.1						X		
FCS_CKM.4							X	
FCS_COP.1				X				
FDP_ACC.2		X						
FDP_ACF.1		X						
FIA_ATD.1		X						
FIA_UAU.2		X						
FIA_UID.2		X						
FMT_MSA.1			X					
FMT_MSA.3			X					
FMT_MTD.1			X					
FMT_SMF.1			X					
FMT_SMR.1		X						
FPT_ITT.1				X				

	O.AUDIT	O.AUTH	O.MANAGE	O.TRANSMI	O.UPDATE	OE.GEN_KE	OE.DES_KE	OE.TIME
FPT_ITT.3				X				
FPT_TRC.1					X			
FPT_STM.1								X

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TOE shall generate audit records of the security relevant actions of the users of the TOE to ensure that users are held accountable for their actions on the TOE. The TSF must present this information in a readable and searchable format to authorized administrators and ensure that only authorized administrators are able to access this information.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The security-related events that are auditable and the contents of the audit records ensures that the user that caused the event is identified.
- FAU_SAR.1: The audit records are presented in a readable format so the authorized administrator can read all audit records.
- FAU_SAR.2: Read access of the audit records is restricted to those users who have been granted explicit read access.
- FAU_SAR.3: Audit records can be sorted and searched based on various fields within the audit record.

8.2.1.2 O.AUTH

The TOE must ensure that only authorized users gain access to the TOE and its resources by uniquely identifying and authenticating all users before granting access to the TOE and its resources.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2: The TOE uses the ESS access control SFP to grant user access to the objects managed by the TOE.
- FDP_ACF.1: Access to the objects is based on the subject's and object's security attributes.
- FIA_ATD.1: Define the unique attributes that are associated with individual users.
- FIA_UAU.2: The TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user
- FIA_UID.2: The TOE requires each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

8.2.1.3 O.MANAGE

The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1: The ability to modify security attributes is restricted to the authorized administrator.
- FMT_MSA.3: The authorized administrators can specify alternative values to override the default restrictive values.
- FMT_MTD.1: The ability to manage the ESS and Managed System data is restricted to the authorized administrator.

- FMT_SMF.1: The authorized administrator is provided with the capability to manage audit data and manage the ESS access control SFP.
- FMT_SMR.1: The TOE maintains the administrator role.

8.2.1.4 O.UPDATE

The TOE must ensure synchronization occurs between ESS and the Managed Systems.

This TOE Security Objective is satisfied by ensuring that:

- FPT_TRC.1: The TOE ensures the consistency of TSF data (security administration data and access control permissions) that is replicated between the ESS and the Managed Systems.

8.2.1.5 O.TRANSMIT

The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1: The operation of data encryption and decryption is performed in accordance with FIPS-140-1.
- FPT_ITT.1: The TOE will protect data from disclosure and modification when it is transmitted between separate parts of the TOE ensuring the proper synchronization of the databases.
- FPT_ITT.3: The TOE will detect any modifications of data transmitted during the automatic update process and will abort the transaction and issue an audit record if any data integrity errors are found.

8.2.1.6 OE.GEN_KEYS

Cryptographic keys will be generated in accordance with requirements defined by FIPS-140-1.

This IT Environment Security Objective is satisfied by ensuring that

- FCS_CKM.1: Cryptographic keys that control access to encrypted data are generated in accordance with an algorithm and key size that meets the FIPS 140-1 Level 1, Section 4.8.1 Key Generation.

8.2.1.7 OE.DES_KEYS

Cryptographic keys will be destroyed in accordance with requirements defined by FIPS-140-1.

This IT Environment Security Objective is satisfied by ensuring that

- FCS_CKM.4: Cryptographic keys are destroyed in accordance with the zeroization destruction method that meets the FIPS 140-1 Level 1, Section 4.8.5 Key Destruction.

8.2.1.8 OE.TIME

The IT environment shall provide a reliable time source for the TOE to provide an accurate timestamp for all audit records.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_STM.1: The IT environment provide a reliable timestamp for the use of the TOE.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package. The EAL chosen is based on the statement of the security environment (assumptions, threats and organizational policy) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL2) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is conscientious, non-hostile, and well trained (A.ADMIN and A.MANAGE). The TOE is physically protected (OE.LOCATE), properly and securely configured (OE.INSTALL), and is periodically backed up (OE.BACKUP). Given these aspects, a TOE based on good commercial development practices is sufficient. EAL 2 is an appropriate level of assurance for the TOE described in this ST. As such, it is believed that EAL 2 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Strength of Functions Rationale

The claimed TOE minimum strength of function is SOF-basic. This strength of function level was selected because it generally corresponds with the claimed assurance level of EAL 2.

The TOE includes security functional requirements that have a specific strength of function metrics or a mechanism of a probabilistic or permutational nature. Of those requirements; FCS_CKM.1 and FCS_COP.1 are cryptographic mechanisms, which is outside the scope of the evaluation.

The password mechanism is of a probabilistic or permutational nature. The password mechanism is used in the Identification and Authentication security function to authenticate user identity. The relevant security functional requirement is FIA_UAU.2. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis included in BMC Vulnerability Analysis

8.5 Requirement Dependency Rationale

The following table identifies each security functional and assurance requirement in this ST. The table enumerates the dependencies of each requirement as specified in the CC and then identifies the requirement in this ST that satisfies each of those dependencies. Note that in some cases a dependency is satisfied by a hierarchically (as defined in the CC) greater requirement component (identified in **bold**) or an IT Environment requirement (identified in *italics*).

ST Requirement	CC Dependencies	ST Dependencies Met
FAU_GEN.1	FPT_STM.1	*FPT_STM.1*
FAU_SAR.1	FAU_GEN.1	*FAU_GEN.1*
FAU_SAR.2	FAU_SAR.1	*FAU_SAR.1*
FAU_SAR.3	FAU_SAR.1	*FAU_SAR.1*
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4 and FMT_MSA.2	FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FCS_CKM.1] and FMT_MSA.2	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1] and FCS_CKM.4 and FMT_MSA.2	FCS_CKM.1 and FCS_CKM.4
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	**FDP_ACC.2** and FMT_MSA.3
FIA_ATD.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.1
FIA_UID.2	None	None
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and **FDP_ACC.2**
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	None	None
FPT_ITT.3	FPT_ITT.1	FPT_ITT.1
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1
FPT_STM.1	None	None

Table 6 Requirement Dependencies

The security functional requirement FMT_MSA.2 is concerned with ensuring that only secure values are accepted for security attributes. For this ST, this requirement only applies by the generation of the cryptographic key pair. The keys are automatically generated, therefore there are no secure values that must be presented. Thus, the requirement is not applicable.

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	**Cryptographic support**	**User data protection**	**Identification and authentication**	**Security management**	**Protection of the TSF**
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FCS_COP.1		X				
FDP_ACC.2			X			
FDP_ACF.1			X			
FIA_ATD.1				X		
FIA_UAU.2				X		
FIA_UID.2				X		
FMT_MSA.1					X	
FMT_MSA.3					X	
FMT_MTD.1					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_ITT.1						X
FPT_ITT.3						X
FPT_TRC.1						X

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.