CA Top Secret r16
Security Target

ST Version: 1.0
August 18, 2017

3333 Warrenville Road
Suite 800
Lisle, IL 60532

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
304 Sentinel Drive, Suite 100
Annapolis Junction, MD 20701

Table of Contents

1 Security Target Introduction 6
1.1 ST Reference 6
1.1.1 ST Identification 6
1.1.2 Document Organization 6
1.1.3 Terminology 7
1.1.4 Acronyms 8
1.1.5 References 9
1.2 TOE Reference 9
1.3 TOE Overview 9
1.4 TOE Type 13
2 TOE Description 14
2.1 Evaluated Components of the TOE 14
2.2 Components and Applications in the Operational Environment 14
2.3 Excluded from the TOE 15
2.3.1 Not Installed 15
2.3.2 Installed but Requires a Separate License 16
2.3.3 Installed but Not Part of the TSF 16
2.4 Physical Boundary 17
2.5 Logical Boundary 17
2.5.1 Enterprise Security Management 18
2.5.2 Security Audit 18
2.5.3 Communications 18
2.5.4 User Data Protection 19
2.5.5 Identification and Authentication 19
2.5.6 Security Management 19
2.5.7 Protection of the TSF 20
2.5.8 Resource Utilization 20
2.5.9 TOE Access 20
2.5.10 Trusted Path/Channels 21
3 Conformance Claims 22

3.1 CC Version 22
3.2 CC Part 2 Conformance Claims 22
3.3 CC Part 3 Conformance Claims 22
3.4 PP Claims 22
3.5 Package Claims 22
3.6 Package Name Conformant or Package Name Augmented 23
3.7 Conformance Claim Rationale 23
4 Security Problem Definition 24
4.1 Threats 24
4.2 Organizational Security Policies 25
4.3 Assumptions 26
4.3.1 Personnel Assumptions 26
4.3.2 Physical Assumptions 26
4.3.3 Connectivity Assumptions 26
4.4 Security Objectives 27
4.4.1 TOE Security Objectives 27
4.4.2 Security Objectives for the Operational Environment 29
4.4.3 Operational Environment Components Rationale 30
4.5 Security Problem Definition Rationale 30
5 Extended Components Definition 32
5.1 Extended Security Functional Requirements 32
5.2 Extended Security Assurance Requirements 32
6 Security Functional Requirements 33
6.1 Conventions 33
6.2 Security Functional Requirements Summary 33
6.3 Security Functional Requirements 35
6.3.1 Class ESM: Enterprise Security Management 35
6.3.2 Class FAU: Security Audit 36
6.3.3 Class FCO: Communications 38
6.3.4 Class FDP: User Data Protection 39
6.3.5 Class FIA: Identification and Authentication 43

6.3.6 Class FMT: Security Management 44
6.3.7 Class FPT: Protection of the TSF 48
6.3.8 Class FRU: Resource Utilization 49
6.3.9 Class FTA: TOE Access 49
6.3.10 Class FTP: Trusted Path/Channels 49
6.4 Statement of Security Functional Requirements Consistency 50
7 Security Assurance Requirements 51
7.1 Class ADV: Development 51
7.1.1 Basic Functional Specification (ADV_FSP.1) 51
7.2 Class AGD: Guidance Documentation 52
7.2.1 Operational User Guidance (AGD_OPE.1) 52
7.2.2 Preparative Procedures (AGD_PRE.1) 53
7.3 Class ALC: Life Cycle Support 53
7.3.1 Labeling of the TOE (ALC_CMC.1) 53
7.3.2 TOE CM Coverage (ALC_CMS.1) 54
7.4 Class ATE: Tests 54
7.4.1 Independent Testing - Conformance (ATE_IND.1) 54
7.5 Class AVA: Vulnerability Assessment 55
7.5.1 Vulnerability Survey (AVA_VAN.1) 55
8 TOE Summary Specification 56
8.1 Enterprise Security Management 56
8.1.1 [PM]ESM_ACD.1: 56
8.1.2 [PM]ESM_ACT.1: 56
8.1.3 [PM]ESM_ATD.2: 56
8.1.4 [PM]ESM_EAU.2: 57
8.1.5 [AC+PM]ESM_EID.2: 57
8.2 Security Audit 58
8.2.1 [AC+PM]FAU_GEN.1: 58
8.2.2 [AC]FAU_SEL.1: 58
8.2.3 [PM]FAU_SEL_EXT.1: 60
8.2.4 [AC]FAU_STG.1: 60

8.2.5 [AC+PM]FAU_STG_EXT.1: 61
8.3 Communications 61
8.3.1 [AC]FCO_NRR.2: 61
8.4 User Data Protection 62
8.4.1 [AC]FDP_ACC.1(1): 62
8.4.2 [AC]FDP_ACC.1(2): 63
8.4.3 [AC]FDP_ACF.1(1): 63
8.4.4 [AC]FDP_ACF.1(2): 67
8.5 Identification and Authentication 68
8.5.1 [PM]FIA_AFL.1: 68
8.5.2 [PM]FIA_USB.1: 68
8.6 Security Management 69
8.6.1 [PM]FMT_MOF.1: 69
8.6.2 [AC]FMT_MOF.1(1): 70
8.6.3 [AC]FMT_MOF.1(2): 71
8.6.4 [PM]FMT_MOF_EXT.1: 71
8.6.5 [AC]FMT_MSA.1: 71
8.6.6 [AC]FMT_MSA.3: 72
8.6.7 [PM]FMT_MSA_EXT.5: 72
8.6.8 [AC+PM]FMT_SMF.1: 73
8.6.9 [AC+PM]FMT_SMR.1: 75
8.7 Protection of the TSF 75
8.7.1 [AC+PM]FPT_APW_EXT.1: 75
8.7.2 [AC]FPT_FLS_EXT.1: 76
8.7.3 [AC]FPT_RPL.1: 76
8.7.4 [AC+PM]FPT_SKP_EXT.1: 76
8.8 Resource Utilization 76
8.8.1 [AC]FRU_FLT.1: 76
8.9 TOE Access 76
8.9.1 [AC+PM]FTA_TSE.1: 77
8.10 Trusted Path/Channels 77

8.10.1 [AC+PM]FTP_ITC.1: 77
8.10.2 [PM]FTP_TRP.1: 78

Table of Figures

Figure 1-1: TOE Boundary 10
Figure 1-2: ESM PP context for the TOE 12

Table of Tables

Table 1-1: Product Specific Terminology 8
Table 1-3: Acronym Definition 8
Table 2-1: Evaluated Components of the TOE 14
Table 2-2: Evaluated Components of the Operational Environment 15
Table 2-3: Operational Environment System Requirements 17
Table 4-1: Threats 25
Table 4-2: TOE Organizational Security Policies 26
Table 4-3: Personnel Assumptions 26
Table 4-4: Connectivity Assumptions 26
Table 4-5: TOE Objectives 28
Table 4-6: TOE Operational Environment Objectives 29
Table 4-7: Operational Environment Components Rationale 30
Table 6-1: Security Functional Requirements for the TOE 34
Table 6-2: Auditable Events 37
Table 6-3: Access Control SFP 40
Table 6-4: Management Functions 45
Table 6-5: TSF Management Functions by Role 48
Table 8-1: Command Types Summary 64
Table 8-2: Access Control SFP 65
Table 8-3: TSF Management Functions by Activity 74

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.1.1 ST Identification

ST Title: CA Top Secret r16 Security Target
ST Version: 1.0
ST Publication Date: August 18, 2017
ST Author: Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-1.

Term	Definition
ACID	An ACID, or Accessor ID, is a unique character-string identifier that is used to identify a user's security record, organizational segment, administrative role, or logical group.
Administrator	Individuals interacting with Top Secret in a capacity where they are attempting to view or modify the functions or security attributes of Top Secret or of other administrators or users.
Control ACID	An ACID that can be associated with a user to define an administrative role for that user. Also may be associated with an Organizational ACID to define the control ACID's scope of authority.
Dataset	A filesystem object residing on the mainframe system.
Department	An arbitrary organizational unit defined by the TSF to identify operating system objects for policy enforcement.
Division	An arbitrary organizational unit defined by the TSF that contains two or more departments.
Fetch	The act of executing an object on the underlying operating system without reading it.
LPAR	Short for logical partition. One mainframe system can be running multiple instances of z/OS in separate LPARs. Used for redundancy or parallel processing.
Object	Programs, files, configuration settings, and authentication capabilities that exist on z/OS and can be protected by the TOE's access control policy.
Organizational ACID	An ACID that defines an organizational unit (department, division, zone).
Profile ACID	An ACID that can be defined as a subject for access control rules that User ACIDs can be assigned to, allowing User ACIDs to be logically grouped together when defining policies.
Resource	General term for items or functions on the mainframe system other than datasets. Includes but is not limited to TSO accounts, TSO procedures, commands, programs, transactions, and storage areas.
Role	A logical grouping that gives all members the same authorizations. In Top Secret, an administrator's role is assigned by associating them with a control ACID. A user's role is assigned by associating them with one or more profile ACIDs that define access control permissions.
Scratch	The action to delete an object on the underlying operating system.
Security Record	A security record, or secrec, is maintained by the TSF and built into a user's address space at login time. It contains a set of user and profile records copied into a user's address space, including information such as resources that a user can access and what operations they are authorized to perform against these resources.
Subject	A user or a program operating on behalf of a user.
SYSID	A unique identifier for a mainframe system in a given environment.
User	Individuals interacting with Top Secret in a capacity where they are attempting to interact with mainframe resources and Top Secret is adjudicating their actions against its access control policy.
User ACID	A type of ACID used to define user accounts.
Zone	An arbitrary organizational unit defined by the TSF that contains two or more divisions.

Table 1-1: Product Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
AC	Access Control
ACID	Accessor ID
CICS	Customer Information Control System
CLI	Command Line Interface
CPF	Command Propagation Facility
DCA	Department Control Administrator
DSN	Dataset Name
ESM	Enterprise Security Management (note that the acronym 'ESM' also commonly refers to External Security Manager in the context of mainframe security products such as Top Secret)
GSO	Global System Option
ICSF	Integrated Cryptographic Services Facility
JES	Job Entry Subsystem
JCL	Job Control Language
LCF	Limited Command Facility
LDAP	Lightweight Directory Access Protocol
LSCA	Limited Security Control Administrator
MSCA	Master System Control Administrator
NDT	Node Descriptor Table
OS	Operating System
OSP	Organizational Security Policy
PM	Policy Management
PP	Protection Profile
SAF	System Authorization Facility
SCA	(Central) Security Control Administrator
SMF	System Management Facility
SMS	System Managed Storage
SSH	Secure Shell
STC	Started Task
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSO	Time Sharing Option
VCA	Division Control Administrator
ZCA	Zone Control Administrator

Table 1-2: Acronym Definition

1.1.5 References

As of r16 all product guidance for Top Secret can be found at https://docops.ca.com/ca-top-secret-for-z-os/16-0/en. This ST also references the following Common Criteria documentation:

[1] or [AC] Standard Protection Profile for Enterprise Security Management Access Control, version 2.1 (AC PP)
[2] or [PM] Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1 (PM PP)
[3] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[4] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[5] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[6] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004

1.2 TOE Reference

The TOE is CA Top Secret r16.

1.3 TOE Overview

CA Top Secret (also referred to as the TOE) is an Enterprise Security Management product that provides host-based access control to z/OS systems that reside in its Operational Environment. The TOE enforces administrator-configurable rules that control access to mainframe systems and their data, ensuring that resources are protected from unauthorized access. The TOE includes a policy management function that is used to configure a uniform set of access control policies against multiple distinct physical or logical mainframe instances deployed in the enterprise. This is done using the command propagation facility (CPF) method of administration.

The following figure depicts the TOE boundary:

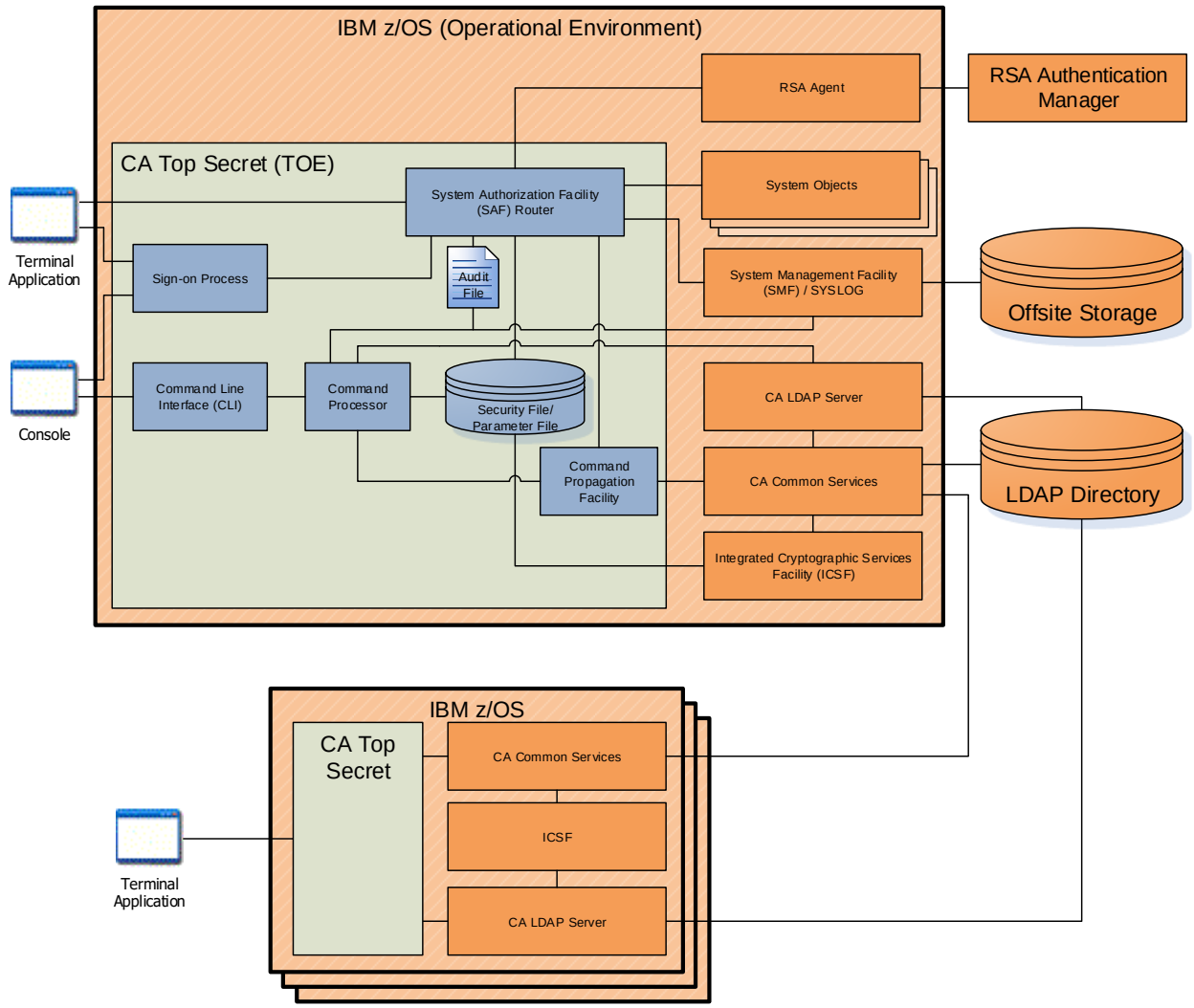

Figure 1-1: TOE Boundary

Note that CA Chorus Software Manager (CSM), which is used to download and install the TOE onto IBM z/OS, is not depicted in this figure. It is only used to acquire the TOE and does not impact the TSF once it has been deployed into its evaluated configuration.

As illustrated in Figure 1-1, CA Top Secret is the lone component of the evaluation. CA Top Secret contains several components within the TOE boundary that are synonymous with CA Top Secret as a product. These components provide the ability to enforce access control policies against resources on the z/OS systems that are part of the Operational Environment as well as the ability for administrators to configure these policies. Because the TOE intercepts all commands issued on the mainframe system, both normal system operation and the administrative usage of CA Top Secret are protected by the TOE's policy enforcement mechanism.

The TOE boundary includes the sign-on process, which performs validation of logon credentials and determines if logon requests are authorized based on access control policy. However, the actual interface where a user or administrator will supply their credentials is not considered to be part of the TOE because this will be through an application that provides an interface to z/OS, such as TSO. Therefore, it is the responsibility of the operational environment to display a warning banner since Top Secret does not present an external interface to a human user that is exclusively for its own use. Any attempt to authenticate to the mainframe system will be directed internally by the OS to the Top Secret sign-on process for evaluation by the TSF.

All management activities for the TOE are performed by an administrator using an authorized terminal application. Using CPF, an administrator can issue the same command and have it apply to multiple different physical and/or virtual systems, allowing for single-point enterprise management.

Policy data and user data are stored in the security file which is installed as part of the TOE. To maintain synchronization between distributed systems, user identities are defined in a central LDAP directory in the Operational Environment and are propagated to the TOE via CA LDAP Server, which is a separately installed environmental component running on the mainframe system. CA Top Secret does not have any mechanism to perform active synchronization or reconciliation between the users defined in the security file and in an environmental LDAP server. This sort of functionality is typically expected by an environmental Identity and Credential Management product. The Operational Environment only provides an LDAP interface to the TOE so that remotely-initiated operations against the user ACIDs defined on the mainframe is possible. The TSF does not exercise any independent control over when this interface is executed, nor does it initiate any outbound communications on its own. The TOE also has the ability to support RSA SecurID token authentication when configured to do so. This requires an administrative mapping between user ACIDs and RSA SecurID token identities to be performed. Once configured, the TOE will interface with the RSA Agent that resides on the underlying z/OS platform to perform the token authentication.

The TOE records its audit data to the SMF and SYSLOG facilities that are part of the underlying operating system. These are the log facilities that are used by z/OS and other various applications running on it; there is no separate log data stream that is exclusively used by Top Secret. As part of general mainframe administration best practices, administrators are expected to back up SMF and SYSLOG data to centralized cold storage on a periodic basis. An organization that does this will also ensure that Top Secret log data generated on all the various CPF nodes will be aggregated in a central location so that audit review of activities performed throughout the environment can be performed from a single point.

The TOE can be thought of as a combination of a Policy Management product and a distributed Access Control product, as shown in the following figure:

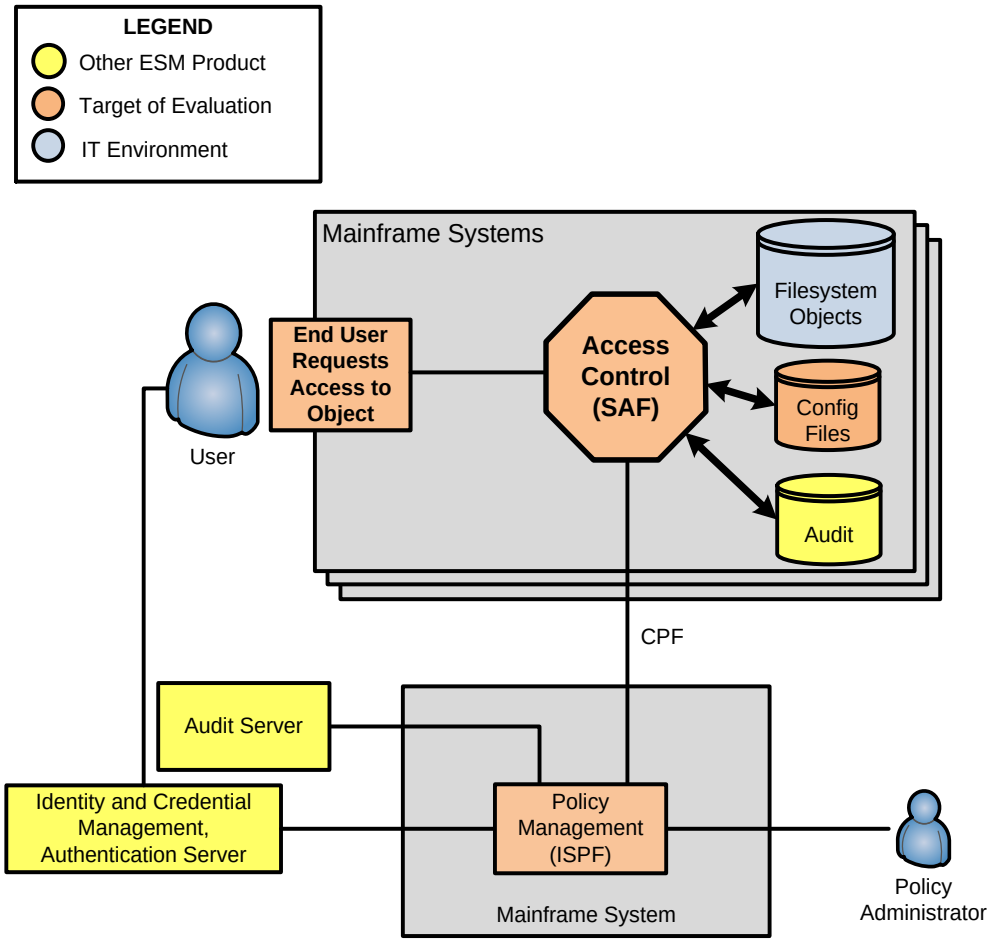

Figure 1-2: ESM PP context for the TOE

Figure 1-2 illustrates the TOE in the context of the Enterprise Security Management Protection Profile suite. Access Control on the managed endpoint can be seen as an Access Control product. The CLI component of the TOE can be seen as a Policy Management capability. The external LDAP directory provides centralized identity definition for mainframe users, and audit data that is written to SMF can be logged to an external source along with the rest of the mainframe audit logs.

Figure 1-2 was derived from the conceptual diagram presented in the AC PP with some minor differences. These differences do not impact the ability of the TOE to claim exact conformance with the AC PP and PM PP. They are as follows:

- Because the TOE claims conformance to both the AC PP and PM PP, the Policy Management component was highlighted as part of the TOE.
- The TSF is not expected to interface with a Secure Configuration Management product.
- The other products with which the TOE interfaces have not currently been evaluated against Enterprise Security Management PPs.

1.4 TOE Type

The TOE type for Top Secret is Enterprise Security Management, specifically Host-Based Access Control and Policy Management. The TOE includes an agent that runs on a mainframe system to provide access control to resources on the mainframe system as well as the capability to administer this agent. Using CPF, management commands issued on one instance of the TOE can be transmitted through the Operational Environment to other systems, allowing for simultaneous administration of multiple systems.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The TOE is limited to CA Top Secret, which at a general level provides both the means to enforce access controls against protected system resources, the interface to define these rules, and the repository in which rule information is stored. The following table describes the TOE components in the evaluated configuration:

Component	Definition
Audit/Tracking File	The Audit/Tracking File records security-related events such as security violations and resource access.
Command Line Interface (CLI)	The CLI provides a mechanism to configure the TOE.
Command Processor	A TOE subsystem that is responsible for receiving administrative commands from different external interfaces and parsing them into a standardized format that the TSF will interpret.
Command Propagation Facility (CPF)	The CPF provides a single-point management capability that allows CA Top Secret commands issued on one system to be propagated to distributed systems or to different logical partitions (LPARs) of the same system.
Parameter File	The parameter file contains all control options that are customizable by an administrator. It is invoked during startup but can be maintained dynamically via the TSS MODIFY command.
Security File	The security file contains all security records for users and resources and is used to define each user's access permissions. When a user logs on to the system, their secrec is built from data in the security file that applies to them.
Sign-on Process	The sign-on process intercepts authentication requests made to the mainframe system which allows the TSF to determine whether the requests are valid.
System Authorization Facility (SAF) Router	The IBM System Authorization Facility (SAF) provides a system wide interface to CA Top Secret. The key component that SAF uses is the CA SAF Router (A component of CA Top Secret). All RACROUTE calls are processed through the CA SAF router to CA Top Secret. CA Top Secret processes all SAF calls by default. This enables CA Top Secret to manage all the unique processing needed to provide full security coverage for the z/OS platform.

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon to function properly:

Component	Definition
CA LDAP Server	In the Operational Environment, an LDAP directory is used to provide a centralized definition for user identities. CA LDAP Server is a z/OS application that is used to translate LDAP communications from an LDAP directory into commands that will synchronize the TOE's users with those defined in LDAP.

Chorus Software Manager (CSM)	CA Chorus Software Manager is a utility that simplifies the acquisition and maintenance of mainframe software. In the evaluated configuration, CSM will be used to install the TOE.
Common Services	CA Common Services is a set of common components used by several CA's mainframe products. It supports the TOE specifically by providing TCP/IP communications services that are used to support remote communications.
Integrated Cryptographic Services Facility (ICSF)	IBM ICSF is the default cryptographic engine provided by z/OS. It supports the TOE by providing services that allow for remote TCP/IP communications to be encrypted using FIPS-validated cryptography. **Note that ICSF is responsible for generation of cryptographic keys used in trusted communications. As per the FIPS 140-2 Security Policy for ICSF (CMVP certificate #2763), the vendor assumes that a minimum of 384 bits of entropy is used to seed the DRBG to perform this function.**
RSA Agent	A z/OS application that brokers authentication attempts that use RSA SecurID token authentication.
RSA Authentication Manager	A service that resides within the organization that maintains a repository of RSA SecurID tokens and can determine if authentication attempts using RSA SecurID are valid.
System Management Facility (SMF)	SMF is a component of IBM z/OS that provides a standardized logging format for z/OS programs. The TOE's audit data is transmitted to the Operational Environment as SMF logs.
Terminal	The terminal is a remote interface used to administer the TOE or operate the mainframe system. A mainframe operator will use a TN3270e class terminal emulator to interact with the mainframe using the terminal.
z/OS	IBM z/OS is the mainframe operating system on which CA Top Secret is installed. The TOE has been tested on z/OS version 2.1 with the IBM SSL Cryptographic Module (CMVP certificate #2829) and IBM ICSF PKCS#11 Cryptographic Module (CMVP certificate #2763).

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

These components are not installed with CA Top Secret and are therefore not included in the TOE boundary. It does not matter if they are installed on the Operational Environment because they are out of scope for the requirements in this evaluation as explained below.

- **EUA** – Extended User Authentication (EUA) can make a requirement for some users to be processed for additional authentication beyond the normal CA Top Secret User ID and password validation, and enables other users to sign on without further user authentication. Including this functionality requires a third-party product, and additional software that is

plugged into a CA Top Secret optional component for use with Tokens / Common Access Cards.

- **Compliance Manager Integration** – Compliance Manager allows Administrators to collect, and report on security relevant activity, and generate alerts requiring action when possible compliance violations occur. It has no security impact on the TOE and is not included in the evaluated configuration of the TOE.
- **CA Top Secret Option for DB2 UDB** – CA Top Secret Option for DB2 UDB is outside the scope of the evaluated configuration because it is used to provide fine-grained access controls to database environments. In the evaluated configuration, the scope of the TOE is limited to the access control functionality that mandated by the AC PP for host-based access control, which does not include databases.
- **DFSMS** – DFSMS is an IBM designation for the DF/HSM, DFDSS, DFSORT, DFRMM, and RACF products when used in a DFSMS system. It is not a necessary component for CA Top Secret because the TOE contains its own security file to perform the same functionality.

By default, none of these components are implemented by Top Secret. Therefore, administrators do not need to take any specific actions to prevent their use.

2.3.2 Installed but Requires a Separate License

No components are installed that require a separate license.

2.3.3 Installed but Not Part of the TSF

These components are installed with CA Top Secret but are not included in the TSF.

- **Group Logon Parameter** – CA Top Secret only validates the use of the GROUP logon parameter if the user specifies a group that is not the default specified in his user ACID. This functionality is not commonly used for the current functions of the product and is only supported for backward compatibility. The functionality provided by this is not used for object access by the TOE.
- **UADS or No UADS (User Attribute Data Set)** – An obsolete feature that is not part of the evaluated configuration. The advantages of bypassing UADS are faster logon processing and eliminating the need to maintain both UADS and the security file.
- **SYSPLEX –** The coupling facility is a feature of z/OS that allows systems in a sysplex environment to communicate and share data with each other. In the evaluated configuration, CPF will be used to communicate with external systems.
- **Non-FAIL Mode of operation** – Top Secret provides a configurable security mode option that affects the global enforcement of access control policy rules. When the product is first installed, the default setting for this mode is QUIET, which means the product acts as if it is not even present on the system. As part of a typical rollout process, administrators will typically escalate the security mode over a period of time once they are certain the access control rules that are being put in place will not adversely affect the behavior of the mainframe system. The TOE is not considered to be in its evaluated configuration until it has

been set into FAIL mode, which is the only mode that will block access attempts that are not permitted by policy.

By default, the excluded functionality is not enabled unless otherwise specified. Therefore, administrators do not need to take any specific actions to prevent their use.

Also, note that the product contains a large amount of functionality that is not directly related to addressing the SFRs that are described in this Security Target. These features may serve a security purpose but they have been excluded from the evaluation because the notion of exact Protection Profile conformance dictates that evaluation claims cannot be made for functionality above and beyond what is specified by the claimed PPs. These functions may be used in the evaluated configuration but the customer should be aware that no security claims are made for any functionality that is not described as being within the scope of the TOE.

2.4 Physical Boundary

The physical boundary of the TOE includes the CA Top Secret software that is installed on the mainframe system. The TOE does not include the hardware or operating systems of the systems on which it is installed. It also does not include the third-party software which is required for the TOE to run. The following table lists the minimum software components that are required to use the TOE:

Component	Requirement
Platform	IBM System z mainframe (zEC12, z114, z196, z9 series, z10 series, z13)
Disk Storage	700 MB or greater
Operating System	IBM z/OS, version 2.1, RSU1506 (Recommended Service Upgrade) or higher
System Components	• INIT/JOB • JES2 • TSO • TCP/IP • VTAM • CA Common Services for z/OS r14.1 or above • CA LDAP Server for z/OS r16
Cryptographic Module	• IBM ICSF • IBM System SSL • IBM Ported Tools for z/OS - OpenSSH

Table 2-3: Operational Environment System Requirements

2.5 Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Enterprise Security Management
2. Security Audit
3. Communications
4. User Data Protection
5. Identification and Authentication
6. Security Management
7. Protection of the TSF

8. Resource Utilization
9. TOE Access
10. Trusted Path/Channels

2.5.1 Enterprise Security Management

The TOE provides enterprise security management through its ability to define and enforce access control policies across distributed systems. The TSF provides the ability to define these policies through its management interface. Policies can be defined to control access to processes, files, system configuration, and use of the authentication function for mainframe systems. Each system has its own policy so a policy is uniquely identified by the name of the system to which it is applied. Individual policy rules can be targeted at one or more remote systems using CPF, whether they are on different LPARs of the same system or they are remote systems connected via TCP/IP.

The TOE relies on its internal security file to identify subjects for access control policy enforcement. The TOE can be connected to an LDAP directory in the Operational Environment so that enterprise users defined in a central location can have their identities replicated across all mainframe systems and LPARs in the enterprise. Subject data can be augmented by attributes that are defined by the TOE and stored within the security file. Administrators of the TOE are also defined using the security file.

To administer the TOE, administrators will log in to the mainframe like a normal user. This can either be with ACID and password (or password phrase), or RSA SecurID token authentication can be used. Once in the system, the permissions defined for them will determine the administrative commands they are authorized to execute.

2.5.2 Security Audit

The TOE generates SMF records of auditable events such as enforcement of access control rules and execution of configuration changes that are written to the SMF journal in the Operational Environment. The operating system's SYSLOG facility will also log information about the operation of the Top Secret application. The TOE also has the ability to log to a local Audit/Tracking file that is created, maintained, and protected by the TSF. Audit data shows the administrative activities performed on the TOE as well as the TSF's enforcement of access control policies against objects on the mainframe system. The SMF and SYSLOG records are protected by the TSF but these facilities are native z/OS components and part of the Operational Environment. An administrator can configure the types of events for which logs are generated.

Audit data can be backed up to a virtual direct-access storage device (DASD) in the Operational Environment. Virtualized DASDs are encrypted using native z/OS encryption, which protects any off-site storage of audit data. Transmission of audit data to the Operational Environment will occur within the local system so there is no applicable trusted channel used to protect this data.

2.5.3 Communications

The TOE provides feedback to administrators when changes to policy rules are attempted. The TOE returns the SYSID of the target system along with the success or failure of the attempted change. The CPF journal file maintained by Top Secret records the CPF activities performed and their results.

2.5.4 User Data Protection

The TOE performs host-based access control against endpoint systems. Access control policies can protect processes, files, system configuration, and use of the authentication function from various actions on z/OS systems. Policies can be applied to users and groups on endpoint systems. The TSF controls access based on subject identity based on subjects that are defined internally to the mainframe. Subject data is encapsulated as a secrec, which the TSF maintains and uses to make access control decisions. The access that is allowed to users is based on rules. If no rule exists to control access to a resource of a class type, a default level of protection defined for the class type is applied. Once a rule has been created for that resource, the resource is "protected" at which point its access control becomes deny-by-default unless authorized otherwise by a rule.

Certain attributes can be applied to users that allow the user to bypass rule checking for different types of activities and automatically grant or deny permission to perform these activities. In the evaluated configuration, the only bypasses that have been claimed are the NORESCHK, NOVOLCHK, NODSNCHK, NOSUBCHK, NOLCFCHK, and SUSPEND user attributes.

By default, the TSF includes a set of rules to control access to itself so that untrusted users cannot tamper with security-relevant data or affect the operation of the TOE.

2.5.5 Identification and Authentication

Administrative identity data and privileges are stored in the files protected by the TOE on the local mainframe system. This data can be synchronized to an LDAP directory in the Operational Environment so that user identities are defined uniformly throughout an enterprise. Both users and administrators are associated with their applicable security attributes at login time through the creation of the secrec. Because of this, permissions are bound to the user or administrator when logging in, so any changes to their permissions will not take effect until the next time they log in.

The TOE also provides the ability to limit the likelihood of a brute force authentication attack by limiting the number of failed authentication attempts that are allowed before an account is locked out.

2.5.6 Security Management

Administrative privileges on the TOE are based on authorizations and scoping. The TOE defines the concepts of department, division, and zone to create a classification hierarchy for all objects in the system. Administrators can then be assigned control over one or more departments, divisions, and/or zones to be able to manage users or objects within that scope of control. Authorizations are associated with statically defined attributes that are associated with the administrator's account. A Policy Administrator as defined by the PM PP is any administrator with sufficient privileges to manage some aspect of the TSF. This allows different administrators to configure the security posture of the TSF as well as its access control policy rules.

The TOE includes the DEFPROT protection rule that enforces restrictive default values by putting the TSF into a deny-by-default posture for all access attempts made against resource class elements that have the DEFPROT rule associated with them.

The Node Descriptor Table (NDT) in the security file defines authorized and active senders of CPF commands, so remote management can only be initiated by authorized and compatible instances of Top Secret. Distributed components trust one another by shared secret.

Changes to the TOE's security file that are initiated by an LDAP directory are converted from LDAP communications to equivalent management commands that are recognized by the TOE. Any changes initiated from LDAP are therefore subject to authorization before being implemented.

The TOE's policy engine prevents the definition of ambiguous policies by defining a strict order of precedence for which rules are enforced first. For example, deny rules always take precedence over allow rules for the same subject and rules that apply to a specific subject always take precedence over rules that apply to a group that the subject belongs to.

2.5.7 Protection of the TSF

If a system is managed remotely, an active network connection to the management point is not needed for the policy to be enforced so a disruption in communications will not compromise access control policy enforcement. This is because policies are transmitted to remote systems and consumed there so the actual policy enforcement and policy decision point is always the system on where an access attempt is being performed.

If an error occurs that causes the TOE to be shut down, new users will be unable to log in. Existing users will continue to have security enforced upon them because their ability to interact with the Operational Environment is derived from the secrec that already exists in their address space.

Systems receiving management commands remotely via CPF will protect themselves from replayed policy data using TLS to secure remote TCP/IP communications. Replay attempts will be rejected as invalid or unauthorized commands.

No mechanism is provided by the TSF to allow access to administrator credential data or protected key data. Administrator credentials are not stored in plaintext and storage of key data is the responsibility of the cryptographic module in the Operational Environment.

2.5.8 Resource Utilization

If the TOE is being used to manage a system remotely via CPF and the destination node cannot be reached, the commands are queued in a file managed by Common Services and buffered until communications are re-established, at which point they are transmitted in their original order.

2.5.9 TOE Access

The TOE's access control policy enforcement engine is able to controls access to the mainframe system's authentication function based on date, time, and/or source of the attempt. A user that is flagged as being suspended is also blocked by the TSF from authenticating to the mainframe. LDAP is only used to define identity data that is then synchronized with the TOE's security file and is not used for authentication; the TSF is in full control of the authentication function.

2.5.10 Trusted Path/Channels

The TOE relies on the Operational Environment to protect authentication and administration data transferred to the mainframe in the course of remote management and between distributed systems via CPF. The Operational Environment includes several cryptographic components that are used to facilitate trusted communications as follows:

- IBM Integrated Cryptographic Services Facility (ICSF): provides PKCS#11 services for cryptographic primitives that have been approved by the Cryptographic Algorithm Validation Program (CAVP).
- IBM System SSL: provides cryptographic services that are used to secure TCP/IP communications using TLS as well as implement the TLS protocol. These services, except for random number generation, have been approved by the CAVP. In the evaluated configuration, System SSL is configured to invoke ICSF's deterministic random bit generator (DRBG) so that it is only using CAVP-approved services to perform key generation and key exchange.
- IBM Ported Tools for z/OS – OpenSSH: provides functionality to implement the SSH protocol. In the evaluated configuration, this component is configured to invoke ICSF to perform all cryptographic services related to the establishment and use of SSH.

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) are Part 2 extended to include all applicable NIAP and International interpretations through August 18, 2017.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through August 18, 2017.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

- Standard Protection Profile for Enterprise Security Management Access Control, version 2.1
- Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1

The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE:

- TD0042
- TD0055
- TD0066
- TD0079

3.5 Package Claims

The TOE claims exact conformance to NIAP-approved Protection Profiles.

The TOE claims following architectural variations and/or optional SFRs that are defined in the appendices of the claimed PPs:

- AC PP
  - Host-Based Access Control (Appendix C.1.1)
  - Optional Host-Based Access Control Capability – Protection from System Administrators (Appendix C.1.2)
  - Conditional Enforcement of Session Establishment (Appendix C.4)
- PM PP
  - Subject Attribute Definition (Appendix C.1.2)
  - Authentication Failure Handling (Appendix C.7.1)
  - TOE Session Establishment (Appendix C.7.2)

This does not violate the notion of exact conformance because the PPs specifically indicate these as allowable variations and options and provide both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

Also, note that the FTA_TAB.1 claim has been omitted from the SFRs defined by the PM PP because the TSF does not provide its own authentication interface that is distinct from what is provided by its underlying operating system. This is an acceptable omission as per NIAP Technical Decision TD0055.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are consistent with the Protection Profile claims.

3.7 Conformance Claim Rationale

The AC PP states the following: “The purpose of an Access Control product is to enforce access control policies.”

The PM PP states the following: “A TOE that conforms to this PP may be able to define policies that control access to any of a wide variety of resources.”

The TOE provides the ability to both define and enforce access control policies. These access control policies enforce access to the resources that are defined for Host-Based Access Control in the AC PP. Additionally, the TOE includes a mechanism to distribute defined access control policies to remote systems. Therefore, the conformance claims to AC PP and PM PP are appropriate. The SFRs that were chosen from these PPs include all required SFRs and a subset of optional SFRs defined as such by the PPs. Therefore, the conformance claim of exact conformance is appropriate.

4 Security Problem Definition

Listed below are the applicable threats, organizational security policies, assumptions, and security objectives that are defined for the evaluation of the TOE. Since the TOE claims conformance to multiple Protection Profiles, the security problem definition has been condensed into a single section to more thoroughly describe the expectations of the TOE and the Operational Environment. The Security Target uses the following conventions to describe the security problem definition:

- In some cases, the same name is used to identify two items with different wordings. When an item whose definition is overloaded is referenced, it will be identified with its PP reference preceding its name (e.g. [AC]T.UNAUTH as opposed to [PM]T.UNAUTH).
- If the item's wording is identical in both claimed PPs, it will be referenced by its name only.
- All references to "Access Control product" and "Policy Management product" are considered to refer to the parts of the TOE that are responsible for these capabilities. Since the TOE claims both PPs, these references are to parts of itself rather than to two distinct products.

4.1 Threats

This section identifies the threats against the TOE as well as the threats that the TOE is deployed into the Operational Environment to mitigate. These threats have been taken from the AC PP and PM PP. The following table combines the threats defined in these PPs and indicates the PP(s) from which they were taken:

PP	Threat	Threat Definition
[PM]	T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
[PM]	T.CONTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
[AC]	T.DISABLE	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
[AC] [PM]	T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
[AC]	T.FALSIFY	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
[AC]	T.FORGE	A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
[PM]		A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
[AC] [PM]	T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
[AC]	T.NOROUTE	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
[AC]	T.OFLOWS	A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
[AC]	T.UNAUTH	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.
[PM]		A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
[PM]	T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
[PM]	T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

Table 4-1: Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the AC PP and PM PP. The following table combines the policies defined in these PPs and indicates the PP(s) from which they were taken:

PP	Policy Name	Policy Definition
[PM]	P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
[AC]	P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

Table 4-2: TOE Organizational Security Policies

Note that while the TSF does not provide the ability to display a configurable warning banner, the organization can still configure the mainframe operating system to display a configurable warning banner prior to any access to the system, which includes the TSF. Therefore, it is expected that the intent of this organizational security policy can still be satisfied by the Operational Environment of the TOE in its evaluated configuration.

4.3 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the AC PP and PM PP. The tables listed in the following subsections list the assumptions defined in these PPs and indicates the PP(s) from which they were taken.

For those assumptions that were defined in the PPs as optional and are claimed as part of the security problem definition for the TOE, the suffix "(optional)" has been added.

4.3.1 Personnel Assumptions

PP	Assumption	Assumption Definition
[AC]	A.INSTALL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.
[PM]	A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

Table 4-3: Personnel Assumptions

4.3.2 Physical Assumptions

No physical assumptions have been defined for the TOE.

4.3.3 Connectivity Assumptions

PP	Assumption	Assumption Definition
[AC] [PM]	A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
[AC] [PM]	A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
[AC]	A.POLICY	The TOE will receive policy data from the Operational Environment.
[AC] [PM]	A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.
[AC] [PM]	A.USERID	The TOE will receive identity data from the Operational Environment.

Table 4-4: Connectivity Assumptions

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

This section identifies the security objectives of the TOE. These objectives have been taken from the AC PP and PM PP. The following table combines the objectives defined in these PPs and indicates the PP(s) from which they were taken:

PP	TOE Objective	TOE Objective Definition
[PM]	O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
[PM]	O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
[PM]	O.AUTH	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
[PM]	O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
[AC]	O.DATAPROT	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
[PM]	O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
[AC]	O.INTEGRITY	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
[PM]		The TOE will contain the ability to assert the integrity of policy data.
[AC]	O.MAINTAIN	The TOE will be capable of maintaining policy enforcement if disconnected from the Policy Management product.
[PM]	O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
[AC]	O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.
[AC]	O.MONITOR	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).
[AC]	O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
[PM]	O.POLICY	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.
[AC]	O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
[PM]		
[PM]	O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
[AC]	O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.
[PM]		The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

Table 4-5: TOE Objectives

Note the following in the above table:

- In some cases, the same name is used to identify two objectives with different wordings. When an objective whose definition is overloaded is referenced, it will be identified with its PP reference preceding its name (i.e. [AC]O.SELFID).
- All references to "Access Control product" and "Policy Management product" are considered to refer to the parts of the TOE that are responsible for these capabilities. Since the TOE claims both PPs, the references are to itself rather than to two distinct products.
- The O.BANNER objective is not claimed because the display of the warning banner is under control of the Operational Environment and not the TSF. An administrator will access the TOE by logging in to the mainframe system with an account that has appropriate privileges to do so. There is no separate authentication method to access the TOE once the administrator has logged on to the mainframe so the operating system is responsible for the display and maintenance of a warning banner. As per NIAP Technical Decision TD0055, this was modified to be an environmental objective (which is shown as OE.BANNER in section 4.4.2 below).

4.4.2 Security Objectives for the Operational Environment

The TOE's operating environment must satisfy the following objectives:

PP	Environmental Objective	Environmental Objective Definition
[PM]	OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
[PM]	OE.BANNER	The Operational Environment will display an advisory warning regarding use of the TOE.
[AC] [PM]	OE.CRYPTO (optional)	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.
[AC] [PM]	OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
[AC]	OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce.
[PM]	OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
[PM]	OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
[PM]	OE.ROBUST (optional)	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
[AC] [PM]	OE.SYSTIME (optional)	The Operational Environment will provide reliable time data to the TOE.
[AC]	OE.USERID	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.
[PM]		The Operational Environment shall be able to identify a user requesting access to the TOE.

Table 4-6: TOE Operational Environment Objectives

Note the following in the above table:

- In some cases, the same name is used to identify two objectives with different wordings. When an objective whose definition is overloaded is referenced, it will be identified with its PP reference preceding its name (i.e. [AC]OE.USERID).
- If the objective's wording is identical in both claimed PPs, it will be referenced by its name only.
- All references to "Access Control product" and "Policy Management product" are considered to refer to the parts of the TOE that are responsible for these capabilities. Since the TOE claims both PPs, the references are to itself rather than to two distinct products.

4.4.3 Operational Environment Components Rationale

The following table summarizes how the Operational Environment components and applications are expected to satisfy the Operational Environment objectives in the evaluated configuration. Some Operational Environment objectives are in fact satisfied by the TSF. The reason for this is that the TOE claims conformance to multiple Protection Profiles and each Protection Profile assumes that anything covered by another Protection Profile is part of the Operational Environment.

PP	Environmental Objective	Satisfied by
[PM]	OE.ADMIN	N/A – this objective is satisfied by a personnel assumption
[AC]	OE.CRYPTO	ICSF
[PM]	OE.CRYPTO	ICSF
[AC] [PM]	OE.INSTALL	N/A – this objective is satisfied by a personnel assumption
[AC]	OE.POLICY	The TSF
[PM]	OE.PERSON	N/A – this objective is satisfied by a personnel assumption
[PM]	OE.PROTECT	The TSF
[AC] [PM]	OE.SYSTIME (optional)	Mainframe system clock
[AC] [PM]	OE.USERID	z/OS

Table 4-7: Operational Environment Components Rationale

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives which are defined in this ST represent the combination of the assumptions, threats, OSPs, and objectives that are specified in the two Protection Profiles to which the ST and TOE claim exact conformance. The associated mappings of assumptions to environmental objectives, SFRs to TOE objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profiles.

The set of assumptions and objectives have been defined based on the optional SFRs that have and have not been claimed. This definition was performed according to the instructions presented in the security problem definition rationale for the claimed PPs.

Because the TOE consists of both Access Control and Policy Management components, all references to these components in the security problem definition are understood to refer to the TSF and not the

Operational Environment. Since the SFRs that provide the assumed capabilities are part of the TSF, the accuracy of these objectives will be verified by testing.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PPs to which the ST and TOE claim conformance. These extended components are formally defined in the PPs that require their usage.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration —to be performed on functional requirements. This ST will highlight the four operations in a manner which is consistent with the claimed PPs, specifically:

- Assignment: allows the specification of an identified parameter. Indicated with **bold text** inside square brackets.
- Refinement: allows the addition of details. Indicated with *italicized text*.
- Selection: allows the specification of one or more elements from a list. Indicated with <u>underlined text</u> inside square brackets.
- Iteration: allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used. However, when an operation is completed by the PP author such that the ST author did not have discretion to modify it, the square brackets are preserved to indicate that an operation was made but the text formatting was not performed to show that the operation was taken directly from a claimed PP rather than completed by the ST author.

In addition to this, the fact that the TOE claims conformance to multiple PPs means that there are numerous SFRs with non-unique names. Rather than altering the SFR names, the following conventions have been defined:

- For SFRs that are only defined in one of the claimed PPs: the SFR name is prefaced with a reference to the PP from which it was taken in square brackets; i.e. **[AC]**FCO_NRR.2.1.
- For SFRs that are identical in both of the claimed PPs: the SFR name is prefaced with the text "AC+PM" in bold square brackets; i.e. **[AC+PM]**FAU_GEN.1.1.
- For SFRs that have the same name but different definitions in each of the claimed PPs: in addition to having the SFR name prefaced with "AC+PM" in bold square brackets, markers are placed in bold square brackets that identify the parts of the SFR which belong to each PP. For example, the list of auditable events specified in **[AC+PM]**FAU_GEN.1.1 will have some entries prefaced with **[AC]**, some entries prefaced with **[PM]**, and still others prefaced with **[AC+PM]**.

These conventions have been defined to unambiguously identify the SFRs that are from the claimed PPs so that the claim of exact conformance can be confirmed and so that duplicate functional claims are not re-iterated unnecessarily.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Enterprise Security Management	**[PM]**ESM_ACD.1	Access Control Policy Definition
	[PM]ESM_ACT.1	Access Control Policy Transmission
	[PM]ESM_ATD.2	Subject Attribute Definition

Class Name	Component Identification	Component Name
	[PM]ESM_EAU.2	Reliance on Enterprise Authentication
	[AC+PM]ESM_EID.2	Reliance on Enterprise Identification
Security Audit	**[AC+PM]**FAU_GEN.1	Audit Data Generation
	[AC]FAU_SEL.1	Selective Audit
	[PM]FAU_SEL_EXT.1	External Selective Audit
	[AC]FAU_STG.1	Protected Audit Trail Storage (Local Storage)
	[AC+PM]FAU_STG_EXT.1	External Audit Trail Storage
Communications	**[AC]**FCO_NRR.2	Enforced Proof of Receipt
User Data Protection	**[AC]**FDP_ACC.1(1)	Access Control Policy
	[AC]FDP_ACC.1(2)	
	[AC]FDP_ACF.1(1)	Access Control Functions
	[AC]FDP_ACF.1(2)	
Identification and Authentication	**[PM]**FIA_AFL.1	Authentication Failure Handling
	[PM]FIA_USB.1	User-Subject Binding
Security Management	**[PM]**FMT_MOF.1	Management of Functions Behavior
	[AC]FMT_MOF.1(1)	
	[AC]FMT_MOF.1(2)	
	[PM]FMT_MOF_EXT.1	External Management of Functions Behavior
	[AC]FMT_MSA.1	Management of Security Attributes
	[AC]FMT_MSA.3	Static Attribute Initialization
	[PM]FMT_MSA_EXT.5	Consistent Security Attributes
	[AC+PM]FMT_SMF.1	Specification of Management Functions
	[AC+PM]FMT_SMR.1	Security Roles
Protection of the TSF	**[AC+PM]**FPT_APW_EXT.1	Protection of Stored Credentials
	[AC]FPT_FLS_EXT.1	Failure of Communications
	[AC]FPT_RPL.1	Replay Detection
	[AC+PM]FPT_SKP_EXT.1	Protection of Secret Key Parameters
Resource Utilization	**[AC]**FRU_FLT.1	Degraded Fault Tolerance
TOE Access	**[AC+PM]**FTA_TSE.1	TOE Session Establishment
Trusted Path /Channels	**[AC+PM]**FTP_ITC.1	Inter-TSF Trusted Channel
	[PM]FTP_TRP.1	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class ESM: Enterprise Security Management

6.3.1.1 [PM]ESM_ACD.1 Access Control Policy Definition

[PM]ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

[PM]ESM_ACD.1.2 Access control policies defined by the TSF shall be capable of containing the following:

- Subjects: [**z/OS mainframe users, started tasks**]; and
- Objects: [**programs, files, host configuration, authentication function on mainframe systems**]; and
- Operations: [**ability to create, read, modify, execute, delete, terminate, or change permissions of objects, ability to use authentication function on mainframe systems**]; and
- Attributes: [**subject identity and organizational membership that is defined on the mainframe system, time data that is defined by the mainframe system**]

Application Note: *Organizational membership includes zone, division, and/or department membership.*

[PM]ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

6.3.1.2 [PM]ESM_ACT.1 Access Control Policy Transmission

[PM]ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: [immediately following creation of a new or updated policy, at a periodic interval].

6.3.1.3 [PM]ESM_ATD.2 Subject Attribute Definition

[PM]ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [**user ACID, profile ACID, department, bypass attributes, AUDIT attribute, FACILITY attribute, violation count, SUSPEND attribute**].

[PM]ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

6.3.1.4 [PM]ESM_EAU.2 Reliance on Enterprise Authentication

[PM]ESM_EAU.2.1 The TSF shall rely on [[**z/OS authentication mediated by the TSF, RSA SecurID token authentication mediated by the TSF**]] for subject authentication.

[PM]ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.3.1.5 [AC+PM]ESM_EID.2 Reliance on Enterprise Identification

[AC+PM]ESM_EID.2.1 The TSF shall rely on [[**TOE Security File**],[**z/OS**]] for subject identification.

[AC+PM]ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.3.2 Class FAU: Security Audit

6.3.2.1 [AC+PM]FAU_GEN.1 Audit Data Generation

[AC+PM]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; and

b) All auditable events identified in Table *6-2* for the [not specified] level of audit; and

c) [**no other auditable events**].

Component	Event	Additional Information
[PM]ESM_ACD.1	Creation or modification of policy	Unique policy identifier
[PM]ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy
[PM]ESM_ATD.2	Association of attributes with subjects	None
[PM]ESM_EAU.2	All use of the authentication mechanism	None
[AC]FAU_SEL.1	All modifications to audit configuration	None
[PM]FAU_SEL_EXT.1	All modifications to audit configuration	None
[AC+PM]FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
[AC]FCO_NRR.2	The invocation of the non-repudiation service	Identification of the information, the destination, and a copy of the evidence provided
[AC]FDP_ACC.1	Any changes to the enforced policy or policies	Identification of Policy Management product making the change
[AC]FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	Subject identity, object identity, requested operation
[PM]FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions	Action taken when threshold is reached

	taken when the threshold is reached, and any actions taken to restore the normal state	
[PM]FIA_USB.1	Successful and unsuccessful binding of user attributes to a subject	None
[AC]FMT_MOF.1	All modifications to TSF behavior	None
[AC]FMT_MSA.3	All modifications of the initial values of security attributes	Attribute modified, modified value
[AC+PM]FMT_SMF.1	Use of the management functions	Management function performed
[AC+PM]FMT_SMR.1	Modifications of the members of the management roles	None
[AC]FPT_FLS_EXT.1	Failure of communication between the TOE and Policy Management product	Identity of the Policy Management product, reason for the failure
[AC]FPT_RPL.1	Detection of replay	Action to be taken based on the specific actions
[AC+PM]FTA_TSE.1	Denial of session establishment	None
[AC+PM]FTP_ITC.1	All use of the trusted channel functions	Identity of the initiator and target of the trusted channel
[PM]FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with trusted path functions, if available

Table 6-2: Auditable Events

[AC+PM]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 (if applicable), 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, [**the information in Table 6-2**].

6.3.2.2 [AC]FAU_SEL.1 Selective Audit

[AC]FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [subject identity, object identity]; and

b) [**authorization result**]

6.3.2.3 [PM]FAU_SEL_EXT.1 External Selective Audit

[PM]FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by [an ESM Access Control product] from the set of all auditable

events based on the following attributes:

a) [subject identity, object identity]; and

b) [**authorization result**]

6.3.2.4 [AC]FAU_STG.1 Protected Audit Trail Storage (Local Storage)

[AC]FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

[AC]FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3.2.5 [AC+PM]FAU_STG_EXT.1 External Audit Trail Storage

[AC+PM]FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [**SMF, SYSLOG, and TOE-internal storage**].

Application Note: *As stated in the claimed PPs, examples of external IT entities could be an Audit Server ESM component on an external machine, an evaluated operating system sharing the platform with the TOE, or a centralized logging component. Transmission to multiple sources is permitted.*

In the case of this evaluation, the TSF is transmitting its audit data to log streams that are maintained by the local operating system(s) on which the TOE is installed. Since the TOE's audit data is transmitted to log facilities that are used by the entire OS, remote storage and centralization of audit data is performed as part of administering the OS.

[AC+PM]FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

[AC+PM]FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.3.3 Class FCO: Communications

6.3.3.1 [AC]FCO_NRR.2 Enforced Proof of Receipt

[AC]FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received [policies] at all times.

[AC]FCO_NRR.2.2 The TSF shall be able to relate the [**SYSID**] of the recipient of the information, and the [**command data**] of the information to which the evidence applies.

[AC]FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to [originator] given [

- **the ruleset change is immediately attempted and feedback of its success or failure is displayed to the administrator initiating the change**
- **if CPF is configured for synchronous communications, the TSF does not interactively allow for the execution of additional commands until a command has successfully executed on all target nodes**
- **if CPF is configured for asynchronous communications, the TSF will queue any commands that are not unsuccessfully sent to a remote node and attempt to retransmit them every 30 seconds**].

6.3.4 Class FDP: User Data Protection

6.3.4.1 [AC]FDP_ACC.1(1) Access Control Policy

[AC]FDP_ACC.1.1(1) The TSF shall enforce the [access control Security Function Policy (SFP)] on [

- subjects: subset of users from an organizational data store, [**started tasks**]; and
- objects: programs, files, host configuration, authentication function, [**no additional objects**]; and
- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, ability to use authentication function, [**no additional operations**]]

6.3.4.2 [AC]FDP_ACC.1(2) Access Control Policy

[AC]FDP_ACC.1.1(2) The TSF shall enforce the [self-protection Security Function Policy (SFP)] on [

- subjects: subset of users from an organizational data store, [**no additional subjects**]; and
- objects: programs, files, and configuration values that comprise or contain TOE data, [**no additional objects**]; and
- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, [**no**

additional operations]]

6.3.4.3 [AC]FDP_ACF.1(1) Access Control Functions

[AC]FDP_ACF.1.1(1) The TSF shall enforce the [access control SFP] to objects based on the following: [all operations between subjects and objects defined in Table *6-3* below based upon some set of organizational attributes].

Subject	Object	Operation
Mainframe User or Started Task	Processes	Execute
		Delete
		Terminate
		Change Permissions
	Files	Create
		Read
		Modify
		Delete
		Change Permissions
	Host Configuration	Read
		Modify
		Delete
	Authentication Function	Login

Table 6-3: Access Control SFP

[AC]FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **If no rule exists to govern access to an object, access to that object is determined by the following:**
  - **The ALL record defines objects that are globally accessible regardless of ACID.**
  - **If a rule does not exist to control access to an object, access is permitted by default. Once a rule has been defined to control access to an object, it is considered to be "protected" and access is denied by default.**
  - **The DEFPROT rule can be applied to treat all objects of a certain type as protected.**
  - **The TSF's operational mode defines how access violations are handled.**
- **The object must be accessed during a date or time that**

is authorized by the applicable rule(s).

- **The object must be accessed using a facility interface that the user is authorized to use.**
- **Access to an object can only be granted to a user ACID who owns the object or who has the same organizational ACID as the owner or one that is hierarchically higher.**
- **Masking values can be used to have rules apply simultaneously to multiple subjects and/or objects.**
- **A collection of rules can be defined in a profile ACID which can be assigned to multiple users.**
- **The requested access type must be authorized by access level.**
    - **Access levels include read, create, write, control, update, scratch, fetch, execute, all, and none.**
    - **If write access is allowed, read and fetch access are also implicitly allowed.**
    - **If create access is allowed, read access is also implicitly allowed.**
- **Conflicting rules take precedence over one another based on the following hierarchy:**
    - **Rules that apply to the subject's user ACID are checked first, followed by rules that apply to any assigned profile ACIDs, followed by rules where the subject is the ALL record.**
    - **Profile ACID rules are checked in a strict order that can be defined by an authorized administrator.**
    - **The global OVERRIDE setting does not check profile ACID rules if the subject has at least one user ACID rule defined for it.**
    - **The global MERGE/ALLOVER setting does not check the ALL record rules if the subject has at least one user ACID or profile ACID rule defined for it.**
    - **The global MERGE/ALLMERGE setting does not return a rule result until all applicable rules have been checked.**

- **Within a collection of dataset rules, priority is given to rule(s) that most specifically identify the dataset.**
- **A SOURCE entry on an ACID takes priority over PERMIT rules for terminal access.**
- **If any rule has the AUDIT attribute set for it, access to the object protected by that rule is audited, regardless of whether or not that particular rule is the one that is used to determine whether the access is allowed.**
- **If two rules of the same specificity apply to an operation, the more permissive rule takes precedence unless the rule evaluates to ACCESS(NONE) or ACTION(DENY)**].

[AC]FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

- **NORESCHK allows an ACID to bypass all resource checking except for data sets and volumes.**
- **NOVOLCHK allows an ACID to bypass all volume checking.**
- **NODSNCHK allows an ACID to bypass dataset checking.**
- **NOSUBCHK allows an ACID to bypass job submission security checking.**
- **NOLCFCHK allows an ACID to bypass limited command facility (LCF) checking**].

[AC]FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**a user whose ACID is suspended cannot access the authentication function regardless of other authorizations**].

6.3.4.4 [AC]FDP_ACF.1(2) Access Control Functions

[AC]FDP_ACF.1.1(2) The TSF shall enforce the [self-protection SFP] to objects based on the following: all operations between subjects and objects based upon some set of organizational attributes.

[AC]FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the TOE will not permit requested operations against

objects that are defined to be protected unless the acting subject is the individual that was responsible for the TOE's installation and initial configuration].

[AC]FDP_ACF.1.3(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

[AC]FDP_ACF.1.4(2) The TSF shall explicitly define access of subjects to objects based on the following additional rules: [none].

6.3.5 Class FIA: Identification and Authentication

6.3.5.1 [PM]FIA_AFL.1 Authentication Failure Handling

[PM]FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [**1-254**]] unsuccessful authentication attempts occur related to [**authentication to the mainframe system**].

[PM]FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [**lock the account until an administrator manually unlocks the account or changes the password**].

6.3.5.2 [PM]FIA_USB.1 User-Subject Binding

[PM]FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**secrec**].

[PM]FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**a user's secrec is associated with the user at initial authentication to the system and contains the following fields:**

- **User ACID**
- **Control ACID type**
- **Facilities the user can access**
- **What resources are permitted to the user**
- **What administrative authorities are granted to the user**].

[PM]FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**changes to a user's attributes that would affect their secrec take effect the next time they log on following the change being made unless it is manually refreshed]**.

6.3.6 Class FMT: Security Management

6.3.6.1 [PM]FMT_MOF.1 Management of Functions Behavior

[PM]FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions: [**specified in Table 6-4**] to [**authorized roles with the following conditions:**

- **An administrator cannot grant privileges that they do not possess themselves.**
- **An administrator cannot modify ACIDs at their own level or higher.**
- **An MSCA can perform all administrative functions without restriction.**
- **An SCA can perform every administrative function for the ability to create or modify an SCA or define the scope of an LSCA.**
- **An LSCA has the same permissions as an SCA except that scope checking rules apply. The scope of an LSCA can only be defined by an MSCA.**
- **A ZCA can administer any divisions, departments, VCAs, DCAs, users, or profiles within their zone.**
- **A VCA can administer any departments, DCAs, users, or profiles within their division.**
- **A DCA can administer any users or profiles within their department.**
- **The activities that a DCA, VCA, or ZCA can perform is based on the administrative authorities that are defined for the ACID**].

SFR	Management Activity
[PM]ESM_ACD.1	Creation of policies
[PM]ESM_ACT.1	Transmission of policies
[PM]ESM_ATD.2	Association of attributes with subjects
[PM]ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
[AC+PM]ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
[PM]FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
[PM]FAU_STG_EXT.1	Configuration of external audit storage location
[PM]FIA_AFL.1	Configuration of authentication failure threshold value
	Configuration of actions to take when threshold is reached
	Execution of restoration to normal state following threshold action (if applicable)
[PM]FIA_USB.1	Definition of subject security attributes, modification of subject security attributes
[PM]FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
[PM]FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)
[PM]FMT_SMR.1	Management of the users that belong to a particular role
[PM]FTA_TAB.1	Maintenance of the banner - This is not applicable as per NIAP TD0055 because the banner is maintained by the environmental applications used to access the TOE.
[AC+PM]FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
[PM]FTP_TRP.1	Configuration of actions that require trusted path (if applicable) - This is not applicable because the TOE uses the trusted path that is established by the Operational Environment's cryptographic functionality.

Table 6-4: Management Functions

Application Note: *Administrators with defined control ACIDs can use their user ACIDs to perform tasks on the mainframe unrelated to the administration of the TOE (and the access control SFP will be applied to them for all relevant rules); however, for security purposes it is recommended that if the individual needs to perform other tasks on the mainframe, a separate unprivileged user ACID be created for this purpose.*

6.3.6.2 [AC]FMT_MOF.1(1) Management of Functions Behavior

[AC]FMT_MOF.1.1(1) The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions[: audited events, repository for remote audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage, [**no other functions**]] to

[an authorized and compatible Policy Management product].

Application Note: *The TSF automatically enforces secure behavior for Access Control SFP behavior to enforce in the event of communications outage so this function is not configurable.*

This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA Top Secret, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA Top Secret".

6.3.6.3 [AC]FMT_MOF.1(2) Management of Functions Behavior

[AC]FMT_MOF.1.1(2) The TSF shall restrict the ability to [determine the behavior of] the functions[: policy being implemented by the TSF, [**no other functions**]] to [an authorized and compatible Policy Management product].

Application Note: *This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA Top Secret, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA Top Secret".*

6.3.6.4 [PM]FMT_MOF_EXT.1 External Management of Functions Behavior

[PM]FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the behavior of the functions of Access Control products: audited events, repository for remote audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage, [**no other functions**] to [**the following roles:**

- **Audited events are configurable within a zone, division, or department, or globally configurable by an SCA or MSCA ACID with CONSOLE authorization.**
- **Repository for remote audit storage is globally configurable by an ACID with CONSOLE authorization.**
- **Access Control SFP is globally configurable by an ACID with CONSOLE authorization or on a per-user basis by a ZCA, VCA, or DCA with scope over the user and the ACID authorization.**
- **Policy being implemented by the TSF is configurable within a zone, division, or department by a ZCA, VCA, or DCA with scope over both the subjects and objects to which the policy rules apply.**

- **Access Control SFP behavior to enforce in the event of communications outage is not applicable because the TSF will automatically continue to enforce the latest policy data that it received**].

Application Note: *This SFR was written from the perspective of a Policy Management product being a standalone TOE. For CA Top Secret, "the TSF" and "Access Control products" should both be interpreted as "CA Top Secret".*

6.3.6.5 [AC]FMT_MSA.1 Management of Security Attributes

[AC]FMT_MSA.1.1 The TSF shall enforce the access control SFP to restrict the ability to [change_default, query, modify, delete, [**create**]] the security attributes: access control policies, access control policy attributes, implementation status of access control policies to [an authorized and compatible Policy Management product].

Application Note: *This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA Top Secret, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA Top Secret".*

6.3.6.6 [AC]FMT_MSA.3 Static Attribute Initialization

[AC]FMT_MSA.3.1 The TSF shall enforce the [access control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

[AC]FMT_MSA.3.2 The TSF shall allow the [authorized and compatible Policy Management product] to specify alternative initial values to override the default values when an object or information is created.

Application Note: *This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA Top Secret, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA Top Secret".*

6.3.6.7 [PM]FMT_MSA_EXT.5 Consistent Security Attributes

[PM]FMT_MSA_EXT.5.1 The TSF shall [only permit definition of unambiguous policies].

[PM]FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [[**no action**]].

Application Note: *As defined in the PM PP, this element is vacuously satisfied by virtue of the fact that the TSF does not allow for the definition of ambiguous policies.*

6.3.6.8 [AC+PM]FMT_SMF.1 Security Management Functions

[AC+PM]FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [configuration of audited events, configuration of repository for remote audit storage, configuration of Access Control SFP, querying of policy being implemented by the TSF, management of Access Control SFP behavior to enforce in the event of communications outage, **[management functions defined in Table 6-5**]].

SFR	Management Activity
[PM]ESM_ACD.1	Creation of policies
[PM]ESM_ACT.1	Transmission of policies
[PM]ESM_ATD.2	Association of attributes with subjects
[PM]FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
[PM]FAU_STG_EXT.1	Configuration of external audit storage location
[PM]FIA_AFL.1	Configuration of authentication failure threshold value
	Configuration of actions to take when threshold is reached
	Execution of restoration to normal state following threshold action (if applicable)
[PM]FIA_USB.1	Definition of subject security attributes, modification of subject security attributes
[PM]FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
[PM]FMT_MSA.1	Management of sets of subjects that can interact with security attributes
	Management of rules by which security attributes inherit specified values
[PM]FMT_SMR.1	Management of the users that belong to a particular role

Table 6-5: TSF Management Functions by Role

6.3.6.9 [AC+PM]FMT_SMR.1 Security Management Roles

[AC+PM]FMT_SMR.1.1 The TSF shall maintain the roles [**MSCA, SCA, LSCA, ZCA, VCA, DCA**].

[AC+PM]FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.3.7 Class FPT: Protection of the TSF

6.3.7.1 [AC+PM]FPT_APW_EXT.1 Protection of Stored Credentials

[AC+PM]FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

[AC+PM]FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

6.3.7.2 [AC]FPT_FLS_EXT.1	*Failure of Communications*
[AC]FPT_FLS_EXT.1.1	The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: [enforce the last policy received].

6.3.7.3 [AC]FPT_RPL.1	*Replay Detection*
[AC]FPT_RPL.1.1	The TSF shall detect replay for the following entities: [**CPF commands**].
[AC]FPT_RPL.1.2	The TSF shall perform [**the following action: reject the replayed policy**] when replay is detected.

6.3.7.4 [AC+PM]FPT_SKP_EXT.1	*Protection of Secret Key Parameters*
[AC+PM]FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.8 Class FRU: Resource Utilization

6.3.8.1 [AC]FRU_FLT.1	*Degraded Fault Tolerance*
[AC]FRU_FLT.1.1	The TSF shall ensure the operation of [enforcing the most recent policy] when the following failures occur: [restoration of communications with the Policy Management product after an outage].

6.3.9 Class FTA: TOE Access

6.3.9.1 [AC+PM]FTA_TSE.1	*TOE Session Establishment*
[AC+PM]FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [day, time, [**source, terminal, SYSID, FACILITY, ACID SUSPEND attribute**]].

6.3.10 Class FTP: Trusted Path/Channels

6.3.10.1 [AC+PM]FTP_ITC.1 Inter-TSF Trusted Channel	
[AC+PM]FTP_ITC.1.1	The TSF shall use [TLS] to provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.
[AC+PM]FTP_ITC.1.2	The TSF shall permit [the TSF**]** to initiate communication via the trusted channel.

[AC+PM]FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for transfer of policy data, [**no other functions**].

6.3.10.2 [PM]FTP_TRP.1 Trusted Path

[PM]FTP_TRP.1.1	Refinement: The TSF shall *use* [SSH] *to* provide a *trusted* communication path between itself and remote users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification, disclosure.
[PM]FTP_TRP.1.2	The TSF shall permit [remote users] to initiate communication via the trusted path.
[PM]FTP_TRP.1.3	Refinement: The TSF shall require the use of the trusted path for *initial user authentication, execution of management functions*.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the PPs against which exact conformance is claimed and a subset of the optional SFRs. All hierarchical relationships, dependencies, and unfulfilled dependency rationales in the ST are considered to be identical to those that are defined in the claimed PPs.

Any references to “Access Control product” or “Policy Management product” that appear in the SFRs are considered to apply to the TSF since the TOE claims conformance to both PPs. The TSF implements both capabilities in a single product.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are consistent with those defined in the claimed PPs.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 Developer action elements:

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.1.1.2 Content and presentation elements:

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.1.1.3 Evaluator action elements:

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 SFRs.

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 Developer action elements:

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 Content and presentation elements:

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 Evaluator action elements:

AGD_OPE.1.1E

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

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 Developer action elements:

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 Content and presentation elements:

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.3 Evaluator action elements:

AGD_ PRE.1.1E

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

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life Cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 Developer action elements:

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 Content and presentation elements:

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 Evaluator action elements:

ALC_CMC.1.1E

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

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 Developer action elements:

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 Content and presentation elements:

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 Evaluator action elements:

ALC_CMS.1.1E

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

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 Developer action elements:

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 Content and presentation elements:

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 Evaluator action elements:

ATE_IND.1.1E

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

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 Developer action elements:

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 Content and presentation elements:

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 Evaluator action elements:

AVA_VAN.1.1E

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

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR.

8.1 Enterprise Security Management

8.1.1 [PM]ESM_ACD.1:

Administrators of Top Secret are able to define access control policies by using the command-line interface (CLI) on the mainframe system. These policies can be simultaneously transmitted to one or more remote systems using the Command Propagation Facility (CPF) and processed by separate instances of the TOE running on those systems.

CA Top Secret is an integrated product that provides both Policy Management and Access Control capabilities, so there are no compatibility considerations for the ability to define policies. Every single operation that the Access Control component is capable of controlling is something that can be defined in a policy by the Policy Management component. Therefore, the subjects, objects, and operations against which an Endpoint Agent can control access is the same set of subjects, objects, and operations that can be defined in a policy by the Policy Management component. Information about the subjects, objects, and operations that the TSF can control access to is provided in section 8.4.

Each instance of Top Secret only instantiates a single policy at one time. The policy identifier is synonymous with the unique SYSID value of the mainframe on which Top Secret is installed.

8.1.2 [PM]ESM_ACT.1:

When an administrator enters a command that will affect the behavior of Top Secret's access control mechanism, the changes are immediately propagated to the local security file(s). If Top Secret is being used to administer multiple systems via CPF, the CPF messages are sent to Common Services and transmitted to the other systems. If a remote CPF node is unavailable, the node is periodically checked for availability and the administrative commands are sent once the node is available. Remote TCP/IP communications (as opposed to other partitions on the same local mainframe system) are secured by Common Services using TLS.

8.1.3 [PM]ESM_ATD.2:

Top Secret defines several different accessor IDs, or ACIDs, that can be associated with subjects. User ACIDs are analogous to usernames and uniquely identify users on the mainframe system. Using CA LDAP Server, the mainframe can receive changes that are made to a centralized LDAP repository in the Operational Environment and convert them to equivalent commands that are recognized by the TOE. This allows for an organization to synchronize user account data with other mainframe environments as well as other systems or applications.

One or more users can also be associated with a profile ACID, which allows multiple users with similar responsibilities to have a single set of permissions applied to them. Top Secret also can define organizational ACIDs of zone, division, and/or department. This is a hierarchical relationship where a zone contains one or more divisions and a division contains one or more departments. Zone and division

ACIDs are optional and serve primarily as a construct to group ACIDs and resources together for simplified administration. A user ACID is always directly assigned to a department. This means that they can be granted access to objects that are owned by the department.

ACIDs can be assigned bypass attributes for disaster recovery purposes. These bypass attributes include NORESCHK, NODSNCHK, NOVOLCHK, NOLCFCHK, and NOSUBCHK. Users with any of these attributes assigned to their ACIDs will bypass certain types of checks that would have otherwise been enforced by the access control SFP. Additionally, if the user ACID has the AUDIT attribute set, all activities performed by that user are logged.

In addition to checking whether a user is authorized to access a resource, Top Secret can grant users access to specific facilities within the system. If a user has the SUSPEND attribute, their account is suspended and they are not granted entry regardless of any other authorizations. One way the SUSPEND attribute can be triggered automatically is if the user ACID exceeds the configured violation threshold for failed logon attempts (see **[PM]**FIA_AFL.1). The number of current violations is tracked within the user ACID to determine whether the threshold has been exceeded. The FACILITY attribute defines the specific facilities (e.g. TSO) that the user is allowed to access. Profile ACIDs and the ALL record can also be assigned the FACILITY attribute but not the SUSPEND attribute.

8.1.4 [PM]ESM_EAU.2:

For administrators to access Top Secret, they must be identified and authenticated to the mainframe system on which it is installed. In the evaluated configuration, administrator accounts are defined as users on the mainframe system itself. A user or administrator wishing to access the mainframe will invoke the desired interface (such as TSO) and provide their credentials to it. The authentication request is received by the TOE's sign-on process, which interfaces internally with SAF to determine if the authentication request is valid, both in terms of correct credentials and in terms of whether the TOE's access control policy will grant access to the system based on the user ACID making the request, the interface or application they are attempting to use, and the day/time of the request. This is described in more detail under **[AC+PM]**FTA_TSE.1. When the TOE is configured to use RSA SecurID token authentication, a mapping between ACIDs and SecurID token IDs will be defined within the TSF.

The administrator connects to the mainframe system using a TN3270e terminal emulator and provides their username and password or RSA SecurID token value to the system for validation. If the credentials are valid and the TSF determines that the authentication should be permitted, the administrator is granted access to the mainframe. To determine if an SecurID token value is accurate, the TSF will interface with the environmental RSA Agent based on the RSA SecurID token ID mapped to the ACID requesting access. The RSA Agent will communicate with the central RSA Authentication Manager and return an appropriate response to the TOE. Authentication requests will always be handled internally by the mainframe system against the system's own access control policy and security file. Any change made to an environmental LDAP directory would also need to be propagated to the TOE's security file for it to affect the behavior of the mainframe system. The environmental CA LDAP Server component provides an LDAP interface to the TSF to facilitate this.

8.1.5 [AC+PM]ESM_EID.2:

To manage Top Secret or interact with any protected resources on the mainframe system, users and administrators must log in to the system on which Top Secret is installed by providing their username and password (or password phrase) that are defined within the mainframe system itself. While z/OS provides the mechanism to authenticate to the system, Top Secret will apply relevant access control policy rules to validate the authentication request. When a user is first logged in, Top Secret associates the user with their ACID and queries the security file to determine what objects they can access on the system. The cached user permissions are built into the user's address space as a security record, or secrec. Access requests are then validated against the secrec that identifies the requesting subject through their user ACID. In the case where RSA SecurID token authentication is used, the user will have a SecurID token with a unique ID. This is mapped to the user's ACID within the security file. When a user attempts to authenticate to the TOE using their SecurID token, the correct token ID will be used when querying the RSA Authentication Manager based on this mapping.

Since Top Secret is itself considered to be a system resource just like every other object on the mainframe that is protected by the TSF, there is no distinction between how users and administrators identify themselves.

8.2 Security Audit

8.2.1 [AC+PM]FAU_GEN.1:

Audit data is generated by Top Secret for both administrative activity and for access attempts made against environmental resources that are mediated by Top Secret. The startup and shutdown of Top Secret itself is audited using the z/OS SYSLOG facility. It is not possible to shut off the auditing function separately from the TOE itself, so auditing of startup/shutdown of auditing is synonymous with the startup and shutdown of the TOE. Any change to the set of auditable events is audited to SMF and/or the Top Secret Audit/Tracking file. Regardless of which specific mechanism is used to create the audit record, each audit record contains fields to record date, time, event type, subject identity (if applicable), and outcome information. Listed below are sample audit events for the types of behavior that is audited by the TSF (along with a summary of the actual behavior being audited when it does not clearly correspond to the information in Table 6-2) along with sample audit records for these events.

- Start-up and shutdown of the audit functions (startup and shutdown of the TOE)
  - `N 4040000 XE14  17150 09:20:10.16  00000090 *TSS2001I CA TOP SECRET MSTR INITIALIZATION COMPLETE`
- Creation or modification of policy
  - `05/30/17  10:41:24  XE18  MASTER1  TSS16BAH  STC TSSAUTHZ  *08*-CA  S000003 RESOURCE  TYPE & NAME :  CTL-OPTN  TSS ADD(BAHSCA1) DSN(BAHSCA1.)`
- Transmission of policy to Access Control products (issuance of CPF commands)

```
17150 16:01:28.47 STC00004 00000090  TSS9810I COMMUNICATIONS
ESTABLISHED WITH NODE XE14
17150 163827   TO: XE14       ID: 000000068       ISSUED BY:
STRTE01
17150 163827   TSS PER(CPFUSR2) DSN(SYS1.PARMLIB) TARGET(XE14)
WAIT(N)
```

- Association of attributes with subjects (defining attributes for ACIDs)
  - `RES=TSS CREATE(BAHUR8) NAME('BAH US16A') TYPE(USER) PASS(  ) PHRASE(  &  XE18  MASTER1`
- All use of the authentication mechanism
  - `N 0080000 XE14  17150 10:17:59.05  00000090  TSS7100E 009 J=QAENT01 A=QAENT01 T=A01TD002 F=TSO - INCORRECT PASSWORD`
- All modifications to audit configuration
  - `06/05/17  15:05:37  XE14  STRTE01  TSS16BAH  STC TSSAUTHZ  OK  S000239 RESOURCE  TYPE & NAME :  CTL-OPTN  TSS PER(QAENT01) DSN(SYS1.PARMLIB) ACCESS(UPDATE) ACTION(AUDIT)`
- Invocation of the non-repudiation service (validation of CPF receipt)
  - `17150 165129  TSS9819I COMMAND NOT SENT TO INACTIVE NODE XE14`
- Any changes to the enforced policy or policies
  - (see creation or modification of policy)
- The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state
  - `N 0080000 XE18 17150 11:20:58.14 JOB00049 00000090 TSS7120E Password Violation Threshold Exceeded N 0080000 XE18 17150 11:20:58.14 JOB00049 00000090 TSS7100E 001 J=BAHDE01C A=USER1 T=INTRDR F=BATCH - ACID SUSPENDED N 0020000 XE18 17150 11:20:58.14 JOB00049 00000090 TSS7141E Use of Accessor ID Suspended`
- Successful and unsuccessful binding of user attributes to a subject
  - (See association of attributes with subjects)
- All modifications to TSF behavior (configure how the TSF enforces access control violations)
  - `06/02/17  15:20:54  XE18  BOSDE01  BOSDE01  STC TSSAUTHZ  OK  S000094 RESOURCE TYPE & NAME  CNTL OPT  MODE(FAIL)`
- All modifications of security attributes (configuration of policy data over CPF)
  - `17150 16:01:28.47 STC00004 00000090 TSS9810I COMMUNICATIONS ESTABLISHED WITH NODE XE14 17150 163827 TO: XE14 ID: 000000068 ISSUED BY: STRTE01 17150 163827 TSS PER(CPFUSR2) DSN(SYS1.PARMLIB) TARGET(XE14) WAIT(N) 17150 163827 FR: XE14 ID: 000000068 17150 163827 TSS0300I PERMIT FUNCTION SUCCESSFUL`
- All modifications of the initial values of security attributes (set default access enforcement for rules)
  - `06/02/17  15:18:09  XE18  BOSDE01  BOSDE01  STC TSSAUTHZ  OK  S000094 RESOURCE TYPE & NAME  CNTL OPT  MODE(WARN)`
- Use of the management functions
  - `06/06/17  14:00:54  XE14  BOSDE01  TSS16BAH  STC TSSAUTHZ  OK  S000239 RESOURCE  TYPE & NAME :  CTL-OPTN  TSS REM(BOSDE02) PSUS`

- Modifications of the members of the management roles
  -
```
06/02/17  09:41:06  XE18  MASTER1   TSS16BAH  STC
TSSAUTHZ                      OK          S000094
RESOURCE  TYPE & NAME :   CTL-OPTN  TSS CREATE(SECMSCA) TYPE(SCA)
NAME('SCA CENTRAL ACID') PASS(         )
```
- Failure of communication between the TOE and Policy Management product
  -
```
17150 165129   TO: XE14       ID: 000000072       ISSUED BY:
STRTE01
17150 165129   TSS PER(CPFUSR2) DSN(SYS1.PROCLIB) TARGET(XE14)
WAIT(Y)
17150 165129   TSS9819I COMMAND NOT SENT TO INACTIVE NODE XE14
```
- Denial of session establishment (login failure for reason other than invalid credentials)
  -
```
05/30/17  12:33:53  XE18  BAHUSR3   BAHUSR3   TSO       FAIL  01
IKJEFLC                      *1C*-06  INI          A55TG003
RESOURCE  TYPE & NAME :             NAME=BAH US33A
```

Note that there is no auditable event for "establishment and disestablishment of communications with the audit server" because all audit data is transmitted to the Operational Environment on the underlying local OS. Additionally, auditing related to trusted communications ("detection of replay," "all use of the trusted channel functions," and "all attempted uses of the trusted path functions") is non-applicable because the TSF relies on environmental components to facilitate trusted communications.

8.2.2 [AC]FAU_SEL.1:

The auditable events that are audited by Top Secret's access control functionality are dependent on its configuration. By default, all violations will be logged if logging is enabled. Allowed accesses can be audited on a per-rule basis by including the ACTION(AUDIT) setting on the rule. Additionally, if a user's ACID has the AUDIT attribute set, all activities performed by the user are logged.

8.2.3 [PM]FAU_SEL_EXT.1:

Administrators use Top Secret's management interface to configure the set of auditable events by subject through configuration of the subject's ACID. The auditing for individual rules is controlled through the configuration of those rules.

8.2.4 [AC]FAU_STG.1:

Audit data is stored locally on the mainframe system using SMF, the Audit/Tracking File, and SYSLOG. The amount of storage space allocated to SMF and SYSLOG are defined by z/OS and are not controlled by Top Secret. SMF and SYSLOG are both the common repositories for audit storage on the mainframe so other mainframe applications may be using these facilities in addition to Top Secret. SMF writes to files named SMF.MANx, where "x" typically designates a sequential alphanumeric value. SYSLOG data is typically written to sequential files named SYSLOGxx, beginning with 00. Since these are files that reside on the mainframe system, they are automatically protected by Top Secret and access to them can be granted on a per-rule basis.

If audit data is logged to the Audit/Tracking file, the $$LOG$$ SYSOUT file can be used to track its capacity. Its capacity is limited to one direct access storage data (DASD) volume at most and is defined by an Administrator during initial configuration. The Administrator can also define a secondary file that

doubles the total audit storage capacity. Regardless of whether a backup file is used, the audit data is treated as a wraparound file such that the oldest stored data is overwritten once all storage has been exhausted. The TSSBCKUP utility can be used to archive the file(s) so that its space is not exhausted. This utility calls the IBM IEHMOVE procedure to move the stored DASD to tape.

The following information is provided for informational purposes only to describe the expected behavior of the Operational Environment; it is not within the scope of the TSF. SMF allocates 128MB of space by default but this can be configured to be up to 1GB. SMF also provides a configurable warning threshold to notify an administrator when a certain percentage of the SMF space has been exhausted (between 10 and 90, default is 25). If SMF space becomes completely exhausted, the system can be configured either to continue processing with the loss of SMF data or to enter a re-startable wait state.

8.2.5 [AC+PM]FAU_STG_EXT.1:

All audit data that is recorded on the mainframe system, including for Top Secret, gets written to z/OS via SMF or SYSLOG. SMF and SYSLOG are both environmental components that reside on the local system. These facilities act as generalized audit storage repositories for the OS itself as well as any applications that run on it such as Top Secret. Top Secret does not write its audit data to a specialized repository that is exclusively for its own use. Instead, Top Secret writes its audit data to the generalized logging facilities that are provided by the OS. Therefore, any offsite backup/storage of audit data is a function initiated on the z/OS system and is not handled by Top Secret. For example, a job can be written to back up the SYSLOG data stored on the JES spool to a permanent storage location on the local OS using the IASXWR00 program to extract the data and the IEBGENER program to write it to a data set. An organization is expected to perform regular backups of this log data to a centralized cold storage or warm storage location as part of general z/OS administrative duties. The Top Secret Audit/Tracking file can also optionally be used as an additional method of audit storage. This file stores duplicates of the SMF data and is protected by the TSF as part of its self-protection SFP.

SMF type 80 records are used for logs of security-related activities and incidents that occur on the system. SMF and SYSLOG data can be stored on a virtual direct-access storage device (DASD) in the Operational Environment. Virtualized DASDs are encrypted using native z/OS encryption, which protects any off-site storage of audit data. Transmission of audit data to the Operational Environment will occur within the local system so the trusted channel used to protect this data as it goes outside the TOE boundary is provided by inter-process communication and not a secure network protocol. The Top Secret Audit/Tracking file can also be stored on DASD and is backed up using the TSSBCKUP procedure or TSSARCHI JCL.

Any offsite backup/storage of audit data is a function initiated on the z/OS system and is not handled by Top Secret. For example, the SYSLGSVW job can be used to copy the weekly SYSLOG data to tape and empty its local contents.

8.3 Communications

8.3.1 [AC]FCO_NRR.2:

In addition to administration for the local system, Top Secret provides the ability to simultaneously configure multiple systems using the Command Propagation Facility (CPF). The Node Definition Table

(NDT) record maintained by Top Secret defines remote CPF nodes and whether they are authorized to issue commands to and/or receive commands from the system where the NDT record is located. External communications are facilitated by CAICCI, which is a part of the environmental CA Common Services component.

The TSF can be configured to handle CPF in either synchronous or asynchronous mode using the WAIT and keyword. If the TSF is configured to be in synchronous mode (WAIT(YES)), a CPF command that is issued interactively will prevent additional interactive commands from being entered until the initial command has been processed on all target nodes. This is used to prevent identically-configured systems from potentially becoming desynchronized. If the TSF is configured to be in asynchronous mode (WAIT(NO)), a command will be executed locally and on any remote nodes that are available. Any commands that are not successfully transmitted to a remote node are queued by CAICCI and will retry the transmission every 30 seconds until the node becomes available, at which point all missed commands are transmitted in order. While this is occurring, additional commands can be executed on the nodes that are available. Regardless of the CPF mode, the remote node will return a receipt of the success or failure of the executed command as soon as the command is received by the remote node and processing of it is attempted.

All commands issued via CPF are first issued to the local system and if the command fails locally, they will not be transmitted via CPF. Remote systems are uniquely identified by SYSID. The CPF journal identifies, for each command that is processed by a remote node, the SYSID value of the node and the command that was issued, which identifies any changes made to the policy rules. This provides a record of what commands were processed by remote CPF nodes and serves as a receipt for the transaction.

An administrator can check the general status of CPF at any time using the 'STATUS(CPF)' command.

8.4 User Data Protection

8.4.1 [AC]FDP_ACC.1(1):

CA Top Secret is deployed to control access to a variety of objects on one or more z/OS mainframe systems in the Operational Environment. The access control policy that is enforced by the TSF is made up of a collection of access control rules. These rules define the subject-object-operation combinations that are mediated by Top Secret.

Rules are issued by an administrator using the TSS PERMIT command. The general structure of the TSS PERMIT command is to define an ACID (subject), target resource (object), and permitted access levels (operations). The subject can either be a user ACID or a profile ACID. Since multiple user ACIDs can be attached to a single profile ACID, profiles can effectively serve as groups of users for the purposes of administration. Resources include system objects such as datasets, programs, and operator commands. Operations include read, create, write, control, update, scratch, fetch, execute, all, and none.

Table 8-2 defines the full list of behavior in the evaluated configuration as it corresponds to what is required by the AC PP for host-based access control. Masking can be used to allow for wildcards for objects. For each rule, the ACTION(AUDIT) attribute can be set to audit all activities mediated by the rule. If this attribute is not set, only instances where the rule rejects an access attempt will be audited. Other attributes such as time of day restrictions can optionally be added to the rule to place conditional restrictions on when or how it is applied.

When a user logs in to the mainframe, Top Secret examines their ACID, any profile ACIDs they are attached to, any organizational ACIDs they belong to, their authorized facilities, and any bypass attributes that are associated with them and creates a security record, or secrec, that defines all the user's authorizations and is stored in their address space on the system. Any access requests made by the user will be checked against their secrec to determine if the requests should be authorized.

8.4.2 [AC]FDP_ACC.1(2):

The purpose of Top Secret is to prevent unauthorized system access. This assumes that users on the mainframe are not trusted. Therefore, they may attempt to circumvent access control policy enforcement by terminating Top Secret, altering its behavior, or preventing it from loading on system startup.

By default, Top Secret protects the objects that it is comprised of so that untrusted subjects do not have the ability to modify its functionality. ACIDs must either be an MSCA or SCA control ACID or have specifically-assigned privileges to manage the TSF (see section 8.6.8).

Top Secret considers the following objects to be components of itself and therefore protected against unauthorized access by an out-of-the-box access control policy:

- Security File (both primary and backup)
- Audit File
- Recovery File
- All FACILITY entries (required for logon)
- All datasets that comprise Top Secret
- All administrative 'TSS' commands

For each of these objects, only the MSCA can access them by default. Other dataset objects that are relevant to the TSF such as the Parameter File are automatically protected when the TSF is configured in FAIL mode.

8.4.3 [AC]FDP_ACF.1(1):

The access control SFP controls access to different operations depending on the type of object being accessed. The Top Secret command syntax defines different instructions for writing rules against different types of objects. Table 8-1 provides a summary of the types of objects that are used to define the access control SFP as specified in the AC PP.

Object/Rule Type	Summary
ACID	Accessor ID. In the context of an object, can refer to user ACIDs, profile ACIDs, control ACIDs, or organizational ACIDs. Top Secret has the ability to grant one ACID the authority to submit a job on behalf of a second ACID, inheriting the permissions of that ACID when doing so.
DATASET	Defines one or more filesystem objects.
FACILITY	In Top Secret, the term FACILITY is analogous to application name. Users can be allowed or denied system entry based on the application they are using to request access to the system.
IBMFAC	Short for IBM Facility. Represents native z/OS callable services such as RAUDITX, SERVER, and RDCEKEY that are used to interact with

	system facilities such as SMF. Note that the term 'facility' is used differently between Top Secret and z/OS.
JESJOBS	Job Entry Subsystem (JES) is an interface to z/OS that receives jobs, schedules them for processing, and controls their output. Top Secret can restrict the ability of users to submit jobs on the system.
LCF	Limited Command Facility (LCF) provides the ability to define either a whitelist or blacklist for mainframe system commands to apply to a particular user.
OPERCMDS	Defines one or more operator commands, or the ability to manipulate system configuration.
PROGRAM	Defines one or more programs that access control restrictions can be placed upon.
RESOURCE	General term for rules that control access to system objects other than datasets.
SOURCE	Defines unallowable source of origin for a particular ACID's attempts to access the system.
TERMINAL	Defines allowable source of origin for a particular ACID's attempts to access the system.

Table 8-1: Command Types Summary

Table 8-2 below provides a mapping of the command types listed above to the access control SFP that is defined by the AC PP for host-based access control. This SFP can be enforced against users manually accessing system resources either directly or through jobs submitted that execute on their behalf. Started tasks, which are initialized and then execute in their own address space without user intervention, are associated with ACIDs and can also have the access control SFP applied to their system usage through this association.

Subject	Object	Operation	Command Type
Mainframe User or Started Task	Processes	Execute	DATASET JESJOBS LCF RESOURCE (PROGRAM) RESOURCE (ACID) VOLUME
		Delete	DATASET VOLUME
		Terminate	RESOURCE (OPERCMDS)
		Change Permissions	DATASET RESOURCE (PROGRAM) VOLUME
	Files	Create	DATASET VOLUME
		Read	
		Modify	
		Delete	
		Change Permissions	
	Host Configuration	Read	DATASET LCF RESOURCE (OPERCMDS) RESOURCE (IBMFAC) VOLUME
		Modify	
		Delete	
	Authentication Function	Login	ACID FACILITY SOURCE TERMINAL

Table 8-2: Access Control SFP

In general, system activity is processed by the CA SAF router where Top Secret determines whether any rules apply to the activity. Once Top Secret has processed the request, the activity is either blocked or routed to the operating system where it can be completed. By default, actions against objects for which no rule exists will be allowed. Once at least one rule is defined that applies to a given object, Top Secret considers it to be a "protected" resource and only allows access that is explicitly defined by a rule. A DEFPROT (default protection) rule can be written to treat all objects of a certain type as protected so that a restrictive deny-by-default posture can be enforced. Rules can also be written where the subject is the ALL record, which applies a global set of default permissions to an object regardless of the ACID requesting access to it.

Top Secret has several different operational modes that define how the TSF will respond in the event an access request is not permitted by the defined access control rules. In the evaluated configuration, only FAIL mode is permitted. In this mode, the TSF will enforce the defined access control policy to prevent unauthorized activities on the system.

The TSF defines the following additional concepts for rule enforcement:

- DAYS, TIMES, FOR, UNTIL, CALENDAR, and TIMEREC parameters can be used to govern when an ACID can log in to the system. Collectively, these can be used to define allowed days or dates, one or more sets of allowed time intervals within a given day, and a finite lifespan for the access.
- The TIME parameter of a rule can optionally be defined to have it apply only during a time range.
- An ACID must be requesting access to the system using an application (FACILITY) that they are authorized to be using.
- Rules can contain masking values or wildcards that can group objects together.
- A rule defines all authorized operations for a given subject-object pairing. The set of operations includes read, create, write, control, update, scratch, fetch, execute, all, and none.
    - If an ACID is granted write access to a resource, both read and fetch access are implicitly granted.
    - If an ACID is granted write access to a resource, both read and fetch access are implicitly granted.
    - If an ACID is granted create access to a resource, read access is implicitly granted.
- Objects can be owned by user ACIDs or by organizational ACIDs. Objects owned by organizational ACIDs effectively "belong to" that part of the organization. If an object is owned by a user ACID, the user has full access to it. If an object is owned by an organizational ACID, the user must belong to the same department or division as the object's owner to even be eligible for having access granted to it. In other words, if an object is owned by a zone ACID, ONLY user ACIDs of the same zone (or of a department/division within the zone) can access the object, and only if a TSS PERMIT rule grants access to them.

Note that in all cases above, "an ACID" can refer either to an individual user ACID, a profile ACID that a user is assigned to, or the ALL record.

Top Secret's rule processing engine determines all rules that apply to a requested operation and applies a rule selection algorithm to determine the most applicable rule in the event of a conflict. Listed below are the potential rule conflicts and how the selection algorithm is handled:

Record ordering: When checking for authorizations, those that apply to the user ACID are checked first, followed by the assigned profile ACIDs, followed by the ALL record. The profile ACIDs associated with a user have their precedence defined in a strict order. When configuring the user ACID, the administrator can specify the order in which the profile ACIDs should apply. Depending on how Top Secret is configured, the selection algorithm may return the first match or it may return the best match. The AUTH control option determines how the record ordering is applied, as described below:

- **OVERRIDE (default setting):** The TOE checks each ACID record one by one. As soon as a PERMIT rule is found, it is evaluated against the request and a decision is returned.
- **MERGE/ALLOVER (or simply MERGE):** The TOE checks the user ACID record along with every applicable profile ACID record and returns a decision based on the best match. If no PERMIT rule is found in any profile ACID record, it checks the ALL record.
- **MERGE/ALLMERGE:** The TOE checks the user ACID record. If no PERMIT rule is found, it merges every profile ACID record along with the ALL record and returns a decision based on the best match.

For example, if a user wishes to update a dataset that their user ACID only has READ access to, but they are assigned a profile ACID that gives them UPDATE access to the same dataset, a setting of OVERRIDE would prohibit this since the rule selection algorithm returns the privilege level of READ. If the same request was made with the MERGE control option applied, the request would be authorized because both the user and profile authorizations are checked before returning a decision. Similarly, if the ALL record defines a privilege level of UPDATE for a dataset and a user's profile ACIDs only give the user READ access, a setting of MERGE will cause the update attempt to be rejected while a setting of MERGE/ALLMERGE would incorporate the ALL record before making an access control decision and would authorize the requested update as a result.

Object name: The Top Secret security validation algorithm processes object names in order from most specific to least specific. For example, a specific dataset name is the most specific type of object (e.g. "EXAMPLE.DATASET"), followed by a dataset name that uses masking characters (e.g. "EXAMPLE.DATA*"), followed by the high-level qualifier used to identify the dataset (e.g. "EXAMPLE"). Note that if the ownership of an object is defined by its exact name, masking characters cannot be used in access rules that apply to it.

Source of origin restriction: If an ACID has a valid SOURCE entry defined and a PERMIT rule defines a different TERMINAL that the ACID is authorized to use that is not present in the SOURCE entry, the SOURCE entry takes priority and the access will be rejected.

Auditing: If any applicable rule has the AUDIT attribute set, the access will be audited, regardless of whether any other applicable rules have this attribute set.

Order of operations: If two rules with the same level of specificity apply to an operation, the more permissive rule takes precedence unless the rule evaluates to ACCESS(NONE) or ACTION(DENY)

There are several exceptions to the standard rule processing engine, as follows:

- ACIDs can be assigned bypass attributes to grant unconditional access to different types of objects on the system, listed below. Bypass attributes are not recommended for normal operation and should primarily be used for troubleshooting purposes.
    - NORESCHK – bypass all rules EXCEPT for DATASET and VOLUME.
    - NOVOLCHK – bypasses all rules of type VOLUME. Does not bypass DATASET rules unless NODSNCHK is also applied.
    - NODSNCHK – bypasses all rules of type DATASET.
    - NOSUBCHK – bypasses all rules of type JESJOBS.
    - NOLCFCHK – bypasses all rules of type LCF.
- Regardless of whether the user is requesting access at a valid time and using a valid facility to interact with the system, if their ACID has the SUSPEND attribute, their access will be denied.

8.4.4 [AC]FDP_ACF.1(2):

Top Secret enforces the self-protection SFP on itself. This SFP is the deny-by-default policy that is implemented for dataset and resource access. This ensures that an untrusted user cannot bypass enforcement of the access control SFP by modifying or terminating the Top Secret software. This includes Top Secret itself as well as the files it uses to define subject, rule, configuration, and audit data. Section 8.4.2 describes the components that are part of the TSF and are therefore protected by default.

This ensures that the software cannot be removed except by the MSCA account that is used to install and set up the TOE.

If for whatever reason Top Secret shuts down, no new users can log on because it operates in a fail-secure posture. Existing users will continue to have security enforced because their secrecs were built at login time and exist in their own address spaces. Access control enforcement remains the same as if Top Secret were active except that access to OPERCMDS are unconditionally denied because there is no ability to determine their ownership if Top Secret is not running. The security file is further protected against tampering by automatically making a daily backup of itself. Top Secret defines a recovery process by which the backup security file is converted to be the primary and the recovery file is used to reconcile any differences between the two. Finally, Top Secret provides a timer task that does a periodic integrity check by comparing the compiled Top Secret code to what is running in the address space where it was originally loaded. By default, this occurs every 30 seconds. If the check fails, Top Secret will generate a notification of this so that an administrator can review and determine what remedial action, if any, is appropriate.

8.5 Identification and Authentication

8.5.1 [PM]FIA_AFL.1:

Top Secret defines a configuration value, PTHRESH, which defines the maximum number of failed login attempts that a user or administrator can make before their account is suspended. A single cumulative value for failed login attempts is maintained for both password and password phrase credentials. The number of consecutive attempts is maintained within the user ACID. Once the account is suspended in this manner, it is locked out until an administrator manually resets the user ACID either by manually changing the password for the locked-out account or by issuing a TSS REMOVE command on the SUSPEND attribute of the user's ACID. By default, the PTHRESH value is set to 4, but can be configured to be any number between 0 and 254. When it is set to zero, unlimited failed login attempts are permitted.

8.5.2 [PM]FIA_USB.1:

When an administrator first logs on to the mainframe system, Top Secret collects all their privileges on the system and builds them into a security record, or secrec. Administrators and users both access the system in the same manner and the term "administrators" is being used to distinguish end users from those individuals who have the authority to manage Top Secret. Administrators have control ACIDs (and potentially administrative privilege attributes) defined for them whereas users do not. In general, it is a recommended security practice that separate ACIDs be defined for the same individual to manage Top Secret and to perform work on the mainframe, but Top Secret does not enforce this separation of duties.

Specifically, Top Secret will control access to its management functions by examining the control ACID assigned to the administrator and any privilege attributes defined for their user ACID. These are combined to determine the full set of authorizations that administrators must configure Top Secret, its subjects, and its access control enforcement. These authorizations are then placed into the administrator's secrec. The secrec also defines the administrator's permissions to access the system as a user if they perform activities other than administration of Top Secret. This includes the facilities that they can use to

access the system and the resources they have access to (including the types of operations that are authorized as part of this access).

A secrec is created at login time and remains persistent in the administrator's address space until they log out of the system or it is manually rebuilt by issuing a TSS REFRESH command.

This behavior is not affected by the presence of an LDAP directory in the Operational Environment. The environmental CA LDAP Server component will propagate any LDAP changes to the security file and the TOE will use the data stored within the mainframe to associate users with subjects.

8.6 Security Management

8.6.1 [PM]FMT_MOF.1:

The TSF provides for the ability to perform internal management functions. Fundamentally, these functions typically involve the manipulation of the security file. Top Secret defines its management privileges by scope and by authorized permissions. Administrative roles are arranged in a strict hierarchy such that an administrator can only modify administrators of a lower hierarchical role. The following are the administrative roles in hierarchical order from top to bottom:

- The MSCA is the root administrator and has full authority over the entire TSF. The MSCA has the ability to create SCAs. There can be only one MSCA.
- An SCA is a super administrator who has every privilege that the MSCA has except the ability to create or modify LSCAs and other SCAs.
- An LSCA is a scoped administrator who can be assigned scope over multiple zones, divisions, and/or departments. It is functionally similar to a ZCA that can have the ability to administer more than a single zone.
- The ZCA, VCA, and DCA are scoped administrators that have the authority to perform management functions within their own zones, divisions, and departments, respectively. A zone is made up of one or more divisions and a division is made up of one or more departments.

The LSCA, ZCA, VCA, and DCA control ACIDs primarily define the scope of what those administrators are capable of administering. The only abilities granted to these ACIDs by default is the ability to create organizational ACIDs within their own hierarchy, such as a ZCA having the ability to define new divisions within their zone. To perform specific administrative functions, the control ACID also requires administrative authorities to be defined for it. Most administrative authorities are restricted to the scope of the administrator (e.g. a ZCA granted the ability to create user ACIDs can only attach those ACIDs to departments within his or her own zone) but those that affect the global configuration of Top Secret are not. Administrative authorities that are relevant to the operation of the TSF as described in the claimed Protection Profiles are broken up into general groups, summarized in the list below:

- ACID: Defines the extent to which a control ACID can create or modify user and profile ACIDs within their scope.
- DATA: Defines the fields of an ACID's secrec that the administrator is authorized to query.
- FACILITY: Defines the facilities that an administrator is authorized to grant ACIDs the use of.

- MISC1: Defines additional ACID capabilities that an administrator is authorized to manage that aren't described in the ACID group such as whether administrators can revoke the SUSPEND status of an ACID.
- MISC2: Defines the ability of an administrator to perform special facility-oriented administration such as whether they can configure CICS or TSO UADS fields for ACIDs within their scope and whether they can issue TSS commands targeting remote nodes using CPF.
- MISC8: Defines the ability of an administrator to query (but not modify) a variety of global tables as well as the ability to administer the passwords of ACIDs within their scope.
- MISC9: The MISC9 keyword deals with higher level administrative authority such as the ability to manipulate the ALL record for a resource class and the ability to administer the CONSOLE attribute.
- RESOURCE: Defines the permissions that are granted to administer resource access, such as the operations that an administrator is permitted to grant access to in TSS PERMIT rules.
- SCOPE: Used only to define the zones, divisions, and/or departments that an LSCA has scope over.

Note that an administrator can only grant authorities to other administrators that they themselves already possess. For a list of the specific administrative authorities that belong to each group, refer to the CA Top Secret User Guide.

The environmental CA LDAP Server product can be used to translate LDAP queries on user data into equivalent commands that are recognized by CA Top Secret, which are then executed as if a human administrator was issuing them via TSO. The CA LDAP Server component in the Operational Environment must be assigned an ACID that has sufficient privilege to manage user ACIDs so that these LDAP queries can be processed by the TOE.

8.6.2 [AC]FMT_MOF.1(1):

The TSF provides the ability to manage the functions of its access control enforcement mechanism. The following lists the functions defined by the SFR and describes the administrative authority that is needed to manage them:

Audited events ([AC]FAU_SEL.1) – Any administrator who can define access control rules can apply the ACTION(AUDIT) setting to it, allowing for successful access to be audited. An MSCA, SCA, LSCA, or administrator with the ACID(AUDIT) administrative authority can apply the AUDIT attribute to a user ACID within their scope.

Repository for remote audit storage ([AC]FAU_STG_EXT.1) – By default, Top Secret writes audit data to the Operational Environment using SMF. An SCA or MSCA can optionally enable the use of the Audit/Tracking file in addition to or instead of SMF.

Access Control SFP ([AC]FDP_ACC.1(1)) – Top Secret can be set into different operational modes that fundamentally alter the behavior of the access control enforcement mechanism against environmental objects. These include DORMANT, WARN, IMPL, and FAIL modes. An SCA or MSCA can determine the mode that Top Secret is configured to operate in on a global level. In the evaluated configuration, the TOE is set into FAIL mode, which is the mode in which access control policy rules will automatically prevent unauthorized actions from being performed.

Administrators with sufficient privileges to create, modify, and/or delete access control rules can affect the access control SFP behavior without taking the TOE out of its evaluated configuration by defining access control rules that grant users permissions to interact with certain objects on the system.

Policy being implemented by the TSF ([AC]FDP_ACF.1) – ACIDs and rules can be managed globally by an MSCA or SCA. An LSCA, ZCA, VCA, or DCA can manage the access control policies within their own respective scopes. The extent to which they can do this depends on the ACID, FACILITY, MISC1, and RESOURCE administrative privileges that they are assigned. Only an MSCA, SCA, or other administrator with MISC9(BYPASS), MISC9(GLOBAL), or MISC1(RDT) authorizations can manage the bypass attributes associated with ACIDs, the ALL record, or the DEFPROT setting for a given resource type, respectively.

Access Control SFP behavior to enforce in the event of communications outage ([AC]FPT_FLS_EXT.1) – By default, Top Secret does not require an active communications channel to a policy origin point to enforce the access control SFP as defined. For example, if a CPF node loses connection to the system where the CPF commands originated, the loss of connectivity will not affect the ability of the node to enforce the rules that it has already received. Therefore, this function is not applicable.

8.6.3 [AC]FMT_MOF.1(2):

Administrators with MSCA or SCA control ACIDs or other administrators who have DATA administrative authorities can see the current policy rules that are implemented by Top Secret by displaying security record data. The Node Descriptor Table (NDT) on both sides of a CPF transaction identifies the authorized senders and receivers of CPF commands for each system. Within an organization, a system will be uniquely identified via SYSID and its authenticity will be validated using shared certificates that are created, managed, and exchanged by ICSF and Common Services in the Operational Environment. The STATUS(CPF) command can also be used by any administrator with MISC9(CONSOLE) authorization to show whether a given remote node is active or inactive.

8.6.4 [PM]FMT_MOF_EXT.1:

The functions a Policy Management component is required to modify for an Access Control component are identical to the set of functions defined in [AC]FMT_MOF.1(1). Refer to section 8.6.2 for the administration functions Top Secret can perform against its access control enforcement capability and the roles that are privileged to administer those functions.

8.6.5 [AC]FMT_MSA.1:

Top Secret can administer access control policies, both on the local system on which it is installed and on remote systems using CPF. This includes the policies themselves and any attributes that are used to govern the enforcement of access control policies such as individual rules and subject attributes.

In all cases, the access control policies being managed are enforced by Top Secret so there are no issues with compatibility since both management and enforcement are done by the same product. Regarding authorizations, the NDT describes authorized senders and receivers of CPF commands. Additionally, an administrator on the local system is given privileges based on their assigned control ACID. If an administrator issues a command using CPF, their authorization on the remote system is determined by

how they are defined by the target system, which may differ from the originating system if the control ACID assignments are not replicated across distributed systems. Additionally, an administrator must have the MISC2(TARGET) authority to issue TSS commands that are targeted to remote nodes using CPF.

8.6.6 [AC]FMT_MSA.3:

By default, Top Secret can enforce restrictive default values for access control enforcement. In the evaluated configuration, Top Secret is to be set in FAIL mode so that access to a protected object is not granted unless a rule specifically allows it. For even more stringent default security, it is possible to set the DEFPROT configuration for a given object type to treat all objects of that type as protected by default. An administrator can override the restrictive default values by writing permissive rules, by specifying a more permissive DEFPROT configuration for particular object types, or by defining ALL record entries that issue global authorization to objects.

8.6.7 [PM]FMT_MSA_EXT.5:

The TOE's policy definition engine does not allow for the definition of ambiguous policies. Based on the way that Top Secret uses policy data to control access to the system, there are several types of potential inconsistencies that could arise, such as:

- A rule that authorizes a subject action and a separate rule that rejects the same action.
- A rule that authorizes a subject action and a separate rule that rejects the action for a profile ACID that the subject is assigned to.
- A rule that authorizes a subject to access an object and a separate rule that prevents the same subject from performing the same action against a group to which that object belongs.
- A rule that authorizes a subject to access an object without logging the access and a separate rule that authorizes the same subject to access the same object with logging.

These inconsistencies are resolved automatically through the precedent rules described in detail in section 8.4.3 and summarized below:

- Rules are processed in order of specificity to the subject, with user ACID rules checked before profile ACID rules, with the ALL record being checked last. Profile ACIDs are checked in an order that is defined by the administrator when assigning them to the user ACID.
- When the AUTH control option of OVERRIDE is set, the first matching rule is what the TSF evaluates.
- When the AUTH control option of MERGE is set, the TSF merges the user and profile ACID rules to find the best fit.
- When the AUTH control option of MERGE/ALLMERGE is set, the TSF merges the user and profile ACID rules as well as the ALL record rule to find the best fit.
- To find the best fit, rules applying to objects are checked in order of most specific to least specific based on any wildcards that are used and on how specifically the resource's location is described in the rule.
- When two rules are equally a good fit, the more permissive rule is applied unless the rule results in an ACCESS(NONE) or ACTION(DENY) decision.
- Only access attempts from authorized sources are allowed, even if access to a specific terminal is granted to the ACID through a PERMIT rule.

- When an applicable rule has the AUDIT attribute set, the access will be audited regardless of whether any other applicable rules also have this attribute set.

When Top Secret builds the secrec for an ACID, the TSF evaluates all rules that will apply to it and defines a single set of authorizations by resolving all conflicting rules based on the above process.

8.6.8 [AC+PM]FMT_SMF.1:

Top Secret provides administrators with the ability to manage all necessary aspects of the TSF where applicable. The following table provides a high-level description of the method by which each of the activities are performed. Refer to section 8.6.1 for an overview of the privileges required to perform these activities.

SFR	Management Activity	Managed By
[PM]ESM_ACD.1	Creation of policies	All record, PERMIT rules, DEFPROT (RDT configuration)
[PM]ESM_ACT.1	Transmission of policies	CPF
[PM]ESM_ATD.2	Association of attributes with subjects	User ACIDs
[PM]ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	User ACIDs
[AC+PM]ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	User ACIDs
[PM]FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	ALL record, PERMIT rules, user ACIDs
[PM]FAU_STG_EXT.1	Configuration of external audit storage location	N/A – external audit storage is the local operating system's SYSLOG and SMF audit logs
[PM]FIA_AFL.1	Configuration of authentication failure threshold value	Control options
	Configuration of actions to take when threshold is reached	N/A – when the threshold is reached, the user ACID is automatically locked until manually reset by an administrator
	Execution of restoration to normal state following threshold action (if applicable)	User ACIDs
[PM]FIA_USB.1	Definition of subject security attributes, modification of subject security attributes	Control ACIDs
[PM]FMT_MOF_EXT.1	Configuration of the behavior of other ESM products	ALL record, PERMIT rules, user ACIDs
[PM]FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)	GSO records
[PM]FMT_SMR.1	Management of the users that belong to a particular role	Control ACIDs
[PM]FTA_TAB.1	Maintenance of the banner	N/A – the Operational Environment is responsible for displaying the banner, which is considered to be appropriate as per NIAP TD0055

[AC+PM]FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	CPF (note that the TOE will always use the trusted channel for CPF communications if the Operational Environment is configured to facilitate this but CPF configuration allows an administrator to specify the remote endpoints for this channel by identifying the SYSIDs that receive CPF commands)
[PM]FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	N/A – the TOE will always use the trusted path for remote administration if the Operational Environment is configured to facilitate this

Table 8-3: TSF Management Functions by Activity

8.6.9 [AC+PM]FMT_SMR.1:

Administrators of Top Secret are defined by their control ACID, which can be any of MSCA, SCA, LSCA, ZCA, VCA, and DCA. These control ACIDs are described in detail in section 8.6.1. However, MSCA and SCA are generally global administrators and LSCA, ZCA, VCA, and DCA are scoped to administer only a certain subset of the mainframe's subjects and objects. These four administrative roles also require specific privileges to be assigned to them to perform certain management functions. The administrative privileges are assigned on a per-user basis and summarized in section 8.6.1 above. An administrator is associated with their assigned role through their control ACID, which defines both their user identification and the specific actions that they can perform within the scope defined by their control ACID. This role is assigned either explicitly on its creation using the TYPE keyword in a TSS CREATE command or through reassignment of the user's ACID by using the TSS MOVE command on it.

When CPF is used, an administrator that is attempting to configure a remote node will inherit the permissions defined for their user ACID on that remote node. This means that regardless of what role an administrator is assigned on the local system where CPF commands originate, the TSF will assign the administrator with a role that is defined for them on the remote node to determine if the CPF commands are authorized.

8.7 Protection of the TSF

8.7.1 [AC+PM]FPT_APW_EXT.1:

Administrator credential data is stored in an obfuscated manner in the security file. The security file is encrypted and protected from unauthorized access by the TOE's self-protection SFP. Password and password phrase data is always encrypted. Historically, Triple-DES was used as the method of encryption, and this is still supported for legacy use. The TOE also supports the use of AES encryption, performed by the Operational Environment. If the PWENC(AES) control option is specified, the TOE will invoke the operating system's software cryptographic module to perform the encryption. The claimed Protection Profiles do not require a specific method of obfuscation for administrative credential data so either of these control options are permitted in the evaluated configuration. Note that it is possible for

batch jobs to store username/password data on the job card. While this data is not stored by the TSF, it could be used to subvert the TOE's access control policy if compromised. It is therefore recommended that use of this be limited to essential situations and that care is taken to ensure that the TSF is configured to prevent unauthorized users from accessing any job cards that store credential data.

8.7.2 [AC]FPT_FLS_EXT.1:

If Top Secret's use is limited to a single mainframe system, there is no situation in which its policy management capability will be unable to communicate with its access control capability since these capabilities each read to and write from identical security files. Since the access control capability relies on stored security file information to enforce the access control SFP, an active external connection is not required for it to continue to function. In the case of CPF, a node that is unable to communicate with the system that transmitted rule data to it will continue enforcing whatever rules it currently has stored until communications with the policy origin point are restored. Once this occurs, any commands that were issued during the outage are released from a queue and transmitted to the node.

8.7.3 [AC]FPT_RPL.1:

Top Secret protects against replayed data using TLS communications between remote systems. This is provided by cryptographic services on the underlying z/OS platform. This ensures that a CPF note will not receive false policy data because an attacker would need to successfully decrypt the packet, modify the data, and re-encrypt the packet. Additionally, the Node Descriptor Table defines authorized and active senders of CPF commands. The administrator who is sending the command over CPF is also defined with a certain set of privileges, so an attacker would be unable to escalate their privileges as part of a replay attack. Any attempted replay will therefore be rejected by the TSF and logged as an invalid or unauthorized command.

8.7.4 [AC+PM]FPT_SKP_EXT.1:

Top Secret does not provide its own cryptography; instead, it relies on the cryptographic components in the Operational Environment for encryption functions. Any keys used to encrypt password data or establish SSH or TLS secure communications are stored within ICSF and not maintained by the TSF.

8.8 Resource Utilization

8.8.1 [AC]FRU_FLT.1:

Top Secret will enforce the consumed access control policy regardless of whether it can communicate with the source of its policy. This is because each instance of Top Secret includes its own access control enforcement mechanism that is identical to each other instance. In a case where CPF is being used to manage a remote node and the remote node loses connectivity to the source of its policy data, there will be no impact on that node's ability to enforce the access control policy rules it already has. Any CPF commands that are issued by the originating node will be queued and it will periodically attempt to contact the remote node. Once connectivity has been restored, the queued CPF commands will be transmitted in their original order to the remote node.

8.9 TOE Access

8.9.1 [AC+PM]FTA_TSE.1:

As part of the requirements for Host-Based Access Control, the TSF is required to allow or deny access to the login function of the system on which its access control functionality resides. In the case of Top Secret, this means that it must control whether a user is permitted to log in to the mainframe system. At minimum, this is for blanket allow/deny access.

In addition to this, the AC PP provides an optional SFR that allows for the definition of conditional access to the login function. The TSF claims this SFR and specifies that conditional access is based on day, time, source, terminal, and/or the SUSPEND attribute of a user's ACID.

PERMIT rules define the terminal(s) that an ACID can access the mainframe from, so any access attempts outside of this are blocked. SOURCE entries associated with the user's ACID also defines allowed terminal IDs and rejects all access requests the user makes outside of this. As stated in section 8.4.3, SOURCE entries take precedence over TERMINAL PERMIT rules. PERMIT rules for terminal access, like all other PERMIT rules, can define allowable days and times outside of which the access is rejected. For more complex time of use restrictions, the FOR/UNTIL rule attribute can be used to establish a lifetime for the access, and the TIMEREC rule attribute can be mapped to a time record that can define multiple time intervals within a single day (as opposed to the TIMES attribute which can only define a single interval).

In addition to this, Top Secret can allow users access to the system using only a particular FACILITY (application) or from a given system (identified by SYSID).

Finally, if a user's ACID is suspended, that user will not be able to gain system entry.

This functionality is enforced by the TSF regardless of whether the user account was initially defined using the mainframe system itself or whether the account was synchronized from an LDAP directory in the Operational Environment. The TOE does not communicate with the LDAP directory to make any decisions regarding user authentication.

8.10 Trusted Path/Channels

8.10.1 [AC+PM]FTP_ITC.1:

Top Secret can communicate with remote systems over TCP/IP for the purposes of executing remote commands using CPF. This connection occurs over a TLS protected channel between the different mainframe systems. TCP/IP communications are facilitated by CA Common Services, which invokes IBM's ICSF and System SSL components to establish trusted communications using TLS. These components use the following CAVP-validated algorithms to establish TLS communications:

ICSF:

- DRBG conformant to NIST SP 800-90B: certificate #1206

System SSL:

- AES conformant to FIPS PUB 197 and NIST SP 800-38A: certificate #4083
- RSA conformant to FIPS PUB 186-4: certificate #2210
- SHS conformant to FIPS PUB 180-4: certificate #3361

- HMAC conformant to FIPS PUB 198-1: certificate #2665

In the evaluated configuration, System SSL is configured to invoke ICSF for DRBG and Diffie-Hellman services since its own random number generator has been deprecated. Top Secret indirectly initiates all communication via the trusted channel by invoking CA Common Services. CA Common Services then interfaces with System SSL and ICSF as needed to secure remote TLS communications.

8.10.2 [PM]FTP_TRP.1:

As a mainframe application, Top Secret does not provide a separate interface for remote access. Administrators will access the mainframe system using a TN3270e terminal emulator. Administrators will use an SSH-capable client to access the mainframe system, which will handle these communications with OpenSSH for z/OS. In the evaluated configuration, OpenSSH for z/OS is configured to invoke ICSF for all cryptographic primitives that require CAVP validation. ICSF uses the following CAVP-validated algorithms to assist in the establishment of SSH communications.

- AES conformant to FIPS PUB 197 and NIST SP 800-38A: certificate #4036
- RSA conformant to FIPS PUB 186-4: certificate #2070
- SHS conformant to FIPS PUB 180-4: certificate #3327
- HMAC conformant to FIPS PUB 198-1: certificate #2633
- DRBG conformant to NIST SP 800-90A: certificate #1206