CA ACF2™ r14 SP1 for z/OS
Security Target

Version 1.1
March 7, 2011

Prepared for:
CA
2400 Cabot Drive
Lisle, IL 60532

Prepared by:
Booz Allen Hamilton
Common Criteria Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090-2950

Table of Contents

List of Figures

List of Tables

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. This ST targets Evaluation Assurance Level 4 (EAL4).

1.1.1 ST Identification

ST Title:	CA ACF2™ r14 SP1 for z/OS
ST Version:	1.1
ST Publication Date:	March 7, 2011
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this ST provides identifying information for CA ACF2™ r14 SP1 for z/OS. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type.

Chapter 2 describes the TOE Description, which includes the physical and logical boundaries, and describes the components and/or applications that are excluded from the evaluated configuration.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the Security Problem Definition as it relates to threats, Operational Security Policies, and Assumptions met by the TOE.

Chapter 5 identifies the Security Objectives of the TOE and of the Operational Environment.

Chapter 6 describes the Extended Security Functional Requirements (SFR) and Security Assurance Requirements (SAR).

Chapter 7 describes the Security Functional Requirements.

Chapter 8 describes the Security Assurance Requirements.

Chapter 9 is the TOE Summary Specification (TSS), a description of the functions provided by CA ACF2 for z/OS r14 to satisfy the SFRs and SARs.

Chapter 10 is the Security Problem Definition Rationale and provides a rationale or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims for the chosen EAL, any deviations from CC Part 2 with regards to SFR dependencies, and a mapping of threats to assumptions, objectives, and SFRs. It also identifies the items used to satisfy the Security Assurance Requirements for the evaluation.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-2: Terminology Definitions. This table is to be used by the reader as a quick reference guide for terminology definitions.

Terminology	Definition
Abort mode	Abort mode indicates that CA ACF2 is in full control of all access requests. Violations result in termination of the request.
Access	Access indicates a User ID's ability to use a resource.
Access Rule	A type of CA ACF2 rule that governs access to data sets.
ACF2 Security Database	Consists of the logonid, rules, and Infostorage database.
ACF2 Logonid Database	The security database that contains the Logonid records.
ACF2 Rules Database	The security database that contains rule records (dataset Access rules only).
ACF2 Infostorage Database	The security database that contains all other CA ACF2 security records.
Administrator	A user with privileges to manage the TOE, TOE data, and other TOE users. These are Security Administrators and Scoped Security Administrators.
Administrative authority	Administrative authority indicates the different classes of authority that are assigned via user attributes. This determines the functions a security administrator can perform.
Attribute	An attribute is a specific authority, privilege, or restriction that is assigned to a User ID.
Authorization	Authorization is how CA ACF2 allows access to a protected resource.
Batch	Batch is a method of processing large amounts of data at one time for jobs too large to perform immediately online.
Customer Information Control System	CICS is a teleprocessing monitor that can be used for a variety of applications. It is a transaction manager designed for rapid, high-volume online processing.
Certificate Name Filtering	CNF allows administrators the ability to associate certificates with users without having to add each certificate to the CA ACF2 security file.
Database	A database is a systemized collection of data stored for immediate access.
Data set	A data set is a group of logically related records stored together and given a unique name.
Default	Default is a value or action the computer system automatically supplies unless an administrator specifies an alternative.
Data Facility Storage Management	The DFSMS Subsystem is a method of storage management.
Entity	An entity is the name of an object as referenced by the system and security.
Field Definition Record	A required user-customized configuration module.
Logon ID	The Logon ID, or LID, is required by a user to gain entry to the TOE. The user must provide a valid logonid that has not been canceled or suspended and has a valid password. Each LID uniquely identified an authorized user.

Information Management System	IBM Information Management System (IMS) is a joint hierarchical database and information management system with extensive transaction processing capabilities.
Integrated Cryptographic Services Facility	ICSF is a component of z/OS and ships with the base product. It is the software component that provides access to the zSeries crypto hardware.
Logonid	A User ID Definition.
Multi-level security	Multi-Level Security (MLS) is a security policy that prevents disclosure and declassification of data based on defined levels of sensitivity of data and levels of clearance of users to that data.
Node	A single instance of the TOE. Synonymous with a Virtual Machine instance on the same machine.
Object	Any resource protected by the TOE.
Passticket	A method of authentication the TOE utilizes which is issued for specific session and cannot be used again once that session has ended. In order to generate a PassTicket, a user's UID string, time of day and session are needed.
Passphrase	A passphrase is a type of password that can exceed eight characters and can contain blanks.
RACROUTE	RACROUTE is a method of requesting information from the TOE. The list of requests are AUDIT, AUTH, CLASS = DATASET, DASDVOL, TAPEVOL, TSOAUTH, others, DEFINE, CLASS = DATASET, DASDVOL, TAPEVOL, DIRAUTH, EXTRACT, FASTAUTH, etc. These requests allow for resource validation, auditing, and data retrieval along with other possible request types. For more information, reference CA ACF2 for z/OS r14 Administrator Guide.
Resource	Any component of the computing or operating system required by a task. For the purposes of data protection, these resources are the objects reside on the system.
Resource Rule	A type of CA ACF2 rules that governs access to resources.
Resource Access Control Facility	RACF is an IBM program product that provides system entry, resource access control, auditing, accountability, and administrative control for the z/OS operating system.
Rule	Rules specify who can access resources and under which conditions resources can be shared.
Scope of authority	Scope of authority indicates what logical units the user has administrative control over.
Security administrator	A security administrator is primarily responsible for implementation and maintenance functions such as defining users, resources, and levels of access. The administrative authority determines what the security administrator can do.
Security file	Security files contain the Security Records that contain all user definitions, resource entitlement controls, and security control options. Generally, this refers to the three CA ACF2 security data bases: The Logonids database, the Rules database, and the Infostorage database.
Security label	Security labels classify users, data, and resources. Standard access rules and permissions still apply, but only after MAC label dominance checks determine that a user can access data and resources based on their security label and the security label of the data or resources the user wants to access.
Security validation algorithm	The Security Validation Algorithm determines whether CA ACF2 can accept or deny users' requests to use a resource.
Source or origin	Source or origin indicates the location of an access request (a terminal or reader).
Supervisor Calls (SVC)	Administrative calls for the TOE that allow for some management action.

	For example, SVCA is used to allow or deny a SAF request.
SYSID	A system identifier; a maximum of four characters may be specified and the value may contain an asterisk (*) for masking.
System Management Facility File	The SMF File is part of the Operational Environment and provided by z/OS for the purpose of event logging.
Time-Sharing Option	TSO enables two or more users to execute their programs at the same time by dividing the machine resources among terminal users.
User ID	The UID is a unique identification used for each accessor of the TOE to identify with when attempting to authorize.
User ID String	The UID string identifies a user to reduce the number of access and resource rules that must be written.
User	A user is the lowest User ID level in the security structure. Generally, a user can sign on via a password and initiate jobs.
Violation	A violation is an unauthorized attempt to access a protected resource.
z/OS UNIX ID	z/OS UNIX User Identifier

Table 1-1: Customer Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation. This is an end user or an administrator.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between an end user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

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

Acronym	Definition
ACF2	CA ACF2
CC	Common Criteria
CICS	Customer Information Control System
CNF	Certificate Name Filtering
CPF	Command Propagation Facility
DAC	Discretionary Access Control
DFSMS	Data Facility Storage Management Subsystem
EAL	Evaluation Assurance Level
FDR	CA ACF2 Field Definition Record
GSO	Global Systems Option
ICSF	Integrated Cryptographic Services Facility
IMS	Information Management System
LDS	LDAP Directory Services

LID	Logon ID
MAC	Mandatory Access Control
MLS	Multi-level Security
MSM	Mainframe Software Manager
MVS	Multiple Virtual Storage
MUSASS	Multiple User Single Address Space System
POE	Port of entry
RACF	Resource Access Control Facility
SAF	System Authorization Facility
SMF	System Management Facility
STC	Started Task Command
SVC	Supervisor Call
SYSID	System Identifier
TMP	Terminal Monitor Program
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSO	Time-sharing option
UID	User Identification String

Table 1-3: Acronym Definitions

1.1.5 References

[1] Common Criteria for Information Technology Security Evaluation, CCMB-2007-09-004, Version 3.1 Revision 3, July 2009.

[2] CA ACF2™ Security for z/OS Administrator Guide r14

[3] CA ACF2™ Security for z/OS Multilevel Security Planning Guide r14

[4] CA ACF2™ Security for z/OS Implementation Planning Guide r14

[5] CA ACF2™ Security for z/OS Auditor Guide r14

[6] CA ACF2™ Security for z/OS Installation Guide r14

[7] CA ACF2™ Security for z/OS Reference Guide r14

[8] CA ACF2™ Security for z/OS Report and Utilities Guide r14

[9] IBM z/OS Version 1 Release 11 Planning for Installation

1.1.6 CC Concepts

The following are CC concepts as used in this document. A Subject is any user of the TOE (user, security administrator, scoped security administrator, applications or process issuing RACROUTE call). An Object (i.e., resource or entity) can be a dataset, volume, command issued by a user, etc. An Operation is any action on a resource. A Security Attribute is information such as User ID, passwords, APPLID, Source etc. that is kept in

the User ID record for the user/administrator. An External Entity is anything outside of the TOE that affects the TOE.

1.2 TOE Reference

1.2.1 TOE Identification

CA ACF2™ r14 SP1 for z/OS

1.3 TOE Overview

CA ACF2 delivers access control software for z/OS operating systems and includes interfaces for CICS, TSO, and IMS.

The TOE allows administrators to control user access to protected resources such as datasets and volumes and their associated data. CA ACF2 controls access to the system and its data and resource through the use of policies and privileges that limit how and when a user or administrator can access the TOE and what they can do once they are authenticated. Additionally, these administrators can be scoped to control what content they have control over. This is performed by placing content within the privileged user's UID string as discussed in Section 9.1.4.7.

The TOE:

- Provides a platform for access control to protected data resources.
- Protects critical data sets and resources so that only the appropriate people have access to them
- Reports on any unauthorized access attempts through the ability to allow users and administrators to read the audit records.
- Integrates with and operates as a policy enforcement mechanism of the z/OS Operating System. CA ACF2 is called by z/OS for all security access control checks made by the operating system. No action is allowed to be performed by users or administrators on the z/OS without first accessing CA ACF2 for an authorization decision.
- Records all policy enforcement decisions made by z/OS and stores them in the SMF File unless otherwise configured for policy enforcement decisions that successfully grant access to not be stored. This configuration is decided during installation.
- Maintains a user database for all users and administrators and their associated security attributes on the z/OS operating system.
- Provides protection against unauthorized destruction, disclosure, or modification of data and resources.

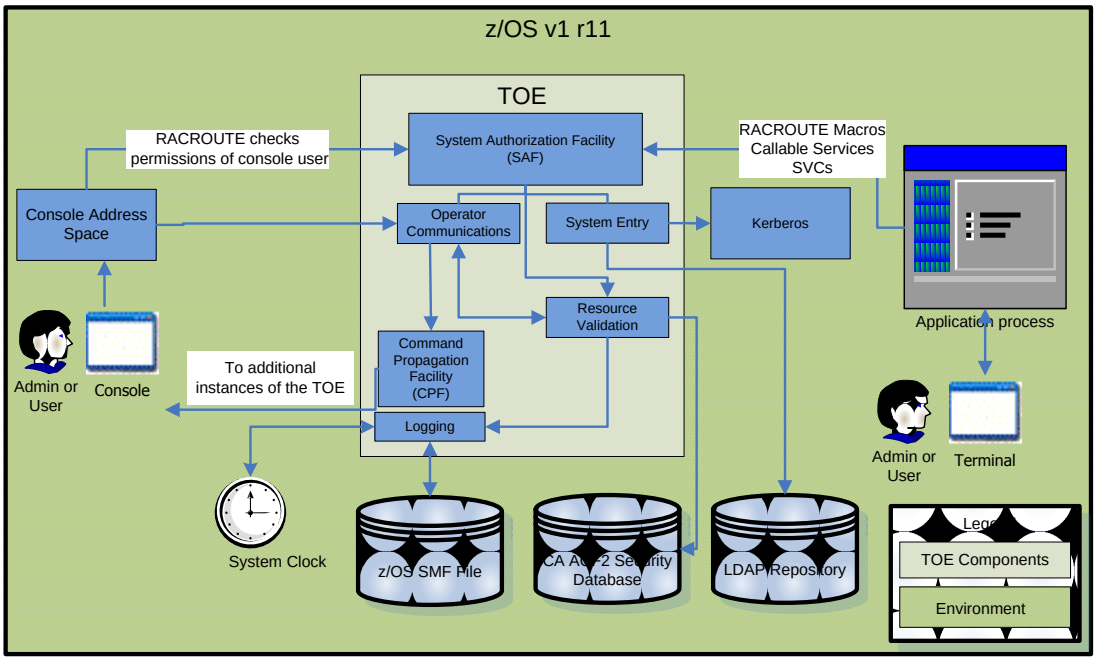

Figure 1-1: TOE Boundary

As illustrated in Figure 1-1, there are two types of users (administrators and users) of the TOE. Users and administrators make calls to the TOE to perform actions on objects protected by the TOE which are located on the z/OS. These calls can be done through the console or through applications running on top of the z/OS operating system. In addition, applications running on top of the z/OS operating system can also make calls to the TOE. Since all calls to the TOE are requests to perform actions on objects located on the z/OS, the TOE is used to restrict all unauthorized access to these objects.

The users and administrators access the TOE through the Console Address Space and/or Application processes. When a user or administrator attempts to communicate through the console to the Console Address Space locally, a SAF RACROUTE request is issued as part of the process of sending their request to the TOE which checks the permissions of the user or administrator to ensure that they are allowed to access the TOE or perform the action on an object. If the user or administrator is attempting to access the TOE remotely, they would communicate through the terminal to the Application process which is used for callable services, RACROUTE macros, and CA ACF2 Supervisor Calls (SVCs).

The components within the TOE include System Authorization Facility (SAF), Command Propagation Facility (CPF), LDAP Directory Services (LDS), and operator communications. Security calls are performed with operator communications. The CA ACF2 SAF component replaces the SAF router that is distributed with z/OS and is used by the TOE to get control of SAF calls so that it can determine how to process the calls.

The CPF facility routes security administration to all or selected virtual machines on the same box, resulting in single-point administration. Changes made to User IDs, passwords, or access levels can be propagated to all nodes to which the user is defined. LDS allows security information to be directly accessible through LDAP compliant directory enabled applications

Figure 1-1 shows a connection from the CPF to additional instances of the TOE. This connection is used to support multiple systems at a hardware level through the use of logical partitions. It can also support multiple systems at a software level through the use of IBM's z/VM running at a first level with one or more guest z/OS images running as guests under control of the z/VM. These additional instances would exist on the same box as the initial instance of the TOE.

The Operational Environment (OE) consists of the following components: z/OS, Console Address Space, Application process (i.e. third-party applications), Kerberos, z/OS SMF File, CA ACF2 Security database, console, and terminal.

The following security classes are enforced by the TOE: Security Auditing, User Data Protection, Identification and Authentication, Security Management, and TOE Access. For an explanation of each of these security classes, see section 1.3.4 Logical Boundary.

1.4 TOE Type

The TOE type for CA ACF2 r14 SP1 for z/OS is System Access Control. System Access Control is defined by CCEVS as "A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. Limiting access to information system resources only to authorized users, programs, processes, or other systems."

2 TOE Description

2.1 Evaluated Components of the TOE

Component	Definition
System Authorization Facility (SAF)	The IBM System Authorization Facility (SAF) provides a system wide interface to CA ACF2. The key component that SAF uses is the CA SAF Router (A component of CA ACF2). All RACROUTE calls are processed through the CA SAF router to CA ACF2. CA ACF2 processes all SAF calls by default. This enables CA ACF2 to manage all of the unique processing needed to provide full security coverage for the z/OS platform. There are 2 components of the CA ACF2 SAF interface: 1. SECTRACE command: This provides a means of tracing and reporting on SAF calls issued 2. CA ACF2 access and resource rules. These provide, for authorization requests, the means by which security policy can be interpreted to determine whether access should be granted or denied.
Facility	The FACILITY class can be used for a wide variety of purposes depending on the products installed on the system. Among other things, the FACILITY class controls the use of catalog, IDCAMS, and DFDSS functions against SMS-managed volumes.
Common Services	Common Services is a set of common components used by a number of CA's Mainframe products. It is free but requires a separate install. CA ACF2 uses several components that assist in the initialization of the TOE (CAIRIM, CALMP, and CAIENF), notifications from the TOE (CAIENF), standard security (CAISSF), and communication (CAICCI).
LDAP Directory Services (LDS)	An LDAP directory provides a method to maintain directory information, such as email accounts, in a central location, for storage, update, retrieval, and exchange. LDAP directories can be utilized as network accessible databases for organization and indexing of network security information. As LDAP is becoming an integral part of most networks, CA ACF2 provides the LDAP Directory Services (LDS) option. LDS is the functionality that allows CA ACF2 to interface with and transmit data to the remote repository. Unlike other products and services that use pull technology on a scheduled basis; this is a

	proactive approach that pushes the change as it occurs, providing a real time update of the changed data.
Operator Communications	CA ACF2 has three primary operator commands. They are START, STOP, and MODIFY. These commands have multiple sub-functions that are controlled by the CA ACF2 and allow for configuration setup, configuration changes and shut down options. Authorization is required to perform that function. In addition there are a number of commands that establish and configure CA SAF tracing. These are also controlled by CA ACF2 and require specific authorization. The CA SAF Sectrace commands are as follows: SECTRACE DELETE, SECTRACE DISABLE, SECTRACE DISPLAY, SECTRACE LOGERR, SECTRACE MODIFY, SECTRACE NOLOGERR, and SECTRACE SET.
Command Propagation Facility (CPF)	Routes security administration to all or selected nodes synchronously or asynchronously, resulting in single-point administration. Changes made to User IDs, passwords, or access levels can be propagated to all nodes to which the user is defined. For example, USER01 is defined to two nodes, with node A (where node is a virtual machine on the same box) as the local node and node B as a second node on the same box. If the user changes the password on node A, CPF automatically propagates the change to node B. Through the use of command function keywords, a user can specify which node receives these commands and how the local node processes them.

Table 2-1: Evaluated Components of the TOE

2.2 Components in the Operational Environment

Component	Definition
z/OS	z/OS is the operating system for IBM's zSeries 900 (z900) line of mainframe servers.
Console Address Space	The MVS console can change global configuration parameters of the TOE via a modify MVS command, since CA ACF2 gets control of the command when it comes into the TOE via operator console communications.
Kerberos	Kerberos for z/OS verifies requests as a trusted

	third-party authentication service. Using conventional shared secret key cryptography, Kerberos confirms the identities of users/administrators, without relying on authentication by the host operating system, without basing trust on host addresses, without necessitating physical security of all hosts on the network, and under the premise that packets traveling along the network can be read, changed, and inserted at will. The TOE calls Kerberos from the Operational Environment to perform these actions.
z/OS SMF File	This is the z/OS's database which is used for the logging of events that occur on the TOE.
CA ACF2 Security Database	Divided into three individual databases: • CA ACF2 Logonids DB – contains logonid records for all users on the system. These records define each system user in terms of general identification, status, privileges, access history, attributes related to TSO, CICS, IMS, and VM, and violation statistics • CA ACF2 Rules DB – contains all data set access rules. These rules describe the conditions (environment) for accessing particular data sets, and determine whether access is permitted or prevented for a user • CA ACF2 Infostorage DB – contains all infostorage records including resource rules, unstructured records, and structured records
Console	This is the local interface used by users/administrators of the TOE to access CA ACF2 through the console address space for management and audit functionality.
Terminal	The remote interface used by users/administrators of the TOE to access CA ACF2 through the Application Process.
Application Process	This includes all third party application processes which TOE users and administrators perform actions on which are monitored by the TOE for authentication, authorization, and in some instances management of objects through the TOE.

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 CA ACF2™ r14 SP1 for z/OS but are not included in the evaluated configuration. They provide no added security related functionality. 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 ACF2™ r14 SP1 for z/OS 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 ACF2 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 ACF2 optional component for use with Tokens / Common Access Cards.
- **ELM Integration** - Enterprise Log Manager (ELM) allows Administrators to collect, normalize, aggregate, 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 Compliance Manager for z/OS Integration** – CA Compliance Manager for z/OS 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 ACF2™ Option for DB2 UDB** – CA ACF2 Option for DB2 UDB is outside the scope of the evaluated configuration because it has no security impact on the TOE and is excluded from the evaluated configuration.
- **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 ACF2 because the TOE contains its own databases to perform the same functionality.

2.3.2 Installed but Requires a Separate License

There are no components installed with CA ACF2™ r14 SP1 for z/OS that require a separate license.

2.3.3 Installed But Not Part of the TSF

These components are installed with CA ACF2™ r14 SP1 for z/OS, but are not included in the TSF.

- **Group** – CA ACF2 only validates the use of the GROUP parameter if the user specifies a group that is not the default specified in his User ID record. This functionality is not commonly used for the current functions of the TOE, and is only supported by the TOE for backward compatibility. The functionality provided by Group is not used for object access by the TOE.
- **UADS or No UADS (User Attribute Data Set)** – Obsolete and can be shut off. 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 User ID database.
- **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. It allows multiple systems to share one security file. Security in a sysplex environment is based on:
    - The communication function or Cross System Coupling Facility (XCF) that provides a way for each system in the sysplex to send messages or signals to all other systems.
    - The data sharing function or Cross System Extended Services (XES) that provides the ability for systems in the sysplex to share common data that would normally be obtained from a database. This function saves system resources by reducing I/O to the database.
- **Security Modes –** The following security modes are not security enforcing and are therefore not included in the evaluated configuration:
    - Rule Mode – Lets the TOE validate rules for different data sets in different modes while the site is migrating to full security. CA ACF2 checks for a $MODE statement in the rule set when it validates an access request. If there is no $MODE statement in the rule set or if no rule set exists, the system-wide mode specified determines how access rules are processed.
    - Quiet Mode – Accesses are not validated or logged. Logonid, source, and other validations still take place. A site can use this mode until they have written basic access rules for the system to reduce the number of access violations logged.
    - Log Mode - Logs access violations, but allows access. A user can use this mode after they have written basic access rules to generate access violation reports and determine what access rules still need to be written.

- Warn Mode – Logs access violations and issues appropriate warning messages to the users, but allows accesses. Warn mode may be used during rollout of security to alert users of the need to modify security entitlements to grant them appropriate access.

- **CA Mainframe Software Manager (MSM)** – The CA MSM is a utility used by the TOE that allows for the initial acquisition of CA ACF2. This utility is part of the operational environment and provides no security enforcing functionality for the TOE once it has been acquired.

2.4 Physical Boundary

The TOE includes the CA ACF2 components:

- Operator Communications
- System Authorization Facility (SAF)
- Command Propagation Facility (CPF)
- Common Services
- LDAP Directory Services (LDS)
- FACILITY class

The following table illustrates the minimum requirements needed to install CA ACF2 on a z/OS system.

Requirement	Description
An Operating System	z/OS V1R9 or later
A TSO/E Session	A TSO/E Session on the IPLed system must be established using a locally-attached or network-attached terminal
Proper Security	In order to install the z/OS UNIX files, the following is required: • The user ID must be a superuser (UID=0) or have read access to the BPX.SUPERUSER resource in the SAF FACILITY class. • The user ID must have read access to FACILITY class resources BPX.FILEATTR.APF, BPX.FILEATTR.PROGCTL, and BPX.FILEATTR.SHARELIB (or BPX.FILEATTR.* if a user chooses to use a generic name for these resources). The commands to define these FACILITY class resources are in SYS1.SAMPLIB member BPXISEC1. • Group IDs uucpg and TTY, and user ID uucp, must be defined in the security database. These IDs must contain OMVS segments with a GID value for each group and a UID value for the user ID. (For ease of use and manageability, define the names in uppercase.)

OMVS Address Space Active	For ServerPac only (not SystemPac), an activated OMVS address space with z/OS UNIX kernel services operating in full function mode is required.
SMS Active	The Storage Management Subsystem (SMS) must be active to allocate z/OS UNIX file systems (HFS or zFS) and PDSE data sets, whether they are SMS-managed or non-SMS-managed. Also, the use of z/OS UNIX file systems (HFS or zFS) is supported only when SMS is active in at least a null configuration, even when the file systems are not SMS-managed. Do either of the following: • To allocate non-SMS-managed z/OS UNIX file systems (HFS or zFS) and PDSE data sets, a user must activate SMS on the driving system in at least a null configuration. A user must also activate SMS on the target system. • To allocate SMS-managed z/OS UNIX file systems (HFS or zFS) and PDSE data sets, A user must activate SMS on the driving system in at least a minimal configuration. Then a user must define a storage group, create SMS-managed volumes, and write, translate, and activate a storage class ACS routine that allows the allocation of z/OS UNIX file systems (HFS or zFS) and PDSE data sets with the names in the ALLOCDS job. A user must also activate SMS on the target system.
DFSORT	msys for Setup job XMLGNR8 requires DFSORT or an equivalent sort program on the system on which the XMLGNR8 job is run.
Language Environment Requirements	The CustomPac Installation Dialog uses the Language Environment run-time library, SCEERUN. If SCEERUN is not in the link list on the driving system, a user must edit the ServerPac installation jobs to add it to the JOBLIB or STEPLIB DD statements.
CustomPac Installation Dialog	If installing a ServerPac or dump-by-data-set SystemPac for the first time, a user will need to install the CustomPac Installation Dialog on the driving system. See *ServerPac: Using the Installation Dialog* or *SystemPac: CustomPac Dialog Reference* for instructions. For subsequent orders a user will not need to reinstall the dialog. IBM ships dialog updates with each order. A user can check the PSP bucket for possible updates to the CustomPac Installation Dialog. For ServerPac, the upgrade is ZOSV1R11 and the subset is SERVERPAC. For SystemPac dump-by-data-set orders, the upgrade is CUSTOMPAC and the subset is SYSPAC/DBD.
Proper Level for Service	In order for a user to install service on the target system that they are building, a user's driving system must minimally meet the driving system requirements for CBPDO Wave 1 and must have the current (latest) levels of the program management binder, SMP/E, and HLASM.
SMP/E ++JAR Support	If the ServerPac order contains any product that uses the ++JAR support introduced in SMP/E V3R2 (which is the SMP/E in z/OS V1R5), the driving system requires IBM SDK for z/OS, Java 2 Technology Edition, V1 (5655-I56) at SDK 1.4 or later. z/OS itself does not use the ++JAR support.
zFS Configured Properly	If using a zFS for installation, then a user must be sure that the zFS has been installed and configured, as described in *z/OS Distributed File Service zSeries File System Administration*.
Internet Delivery Requirements	If intending to receive the ServerPac or SystemPac dump-by-data-set order by way of the Internet, a user will need the following:

	• SMP/E PTF UO00678 (APAR IO07810) if SMP/E level is V3R4 (which is in z/OS V1R7, V1R8, and V1R9). v ICSF configured and active so that it can calculate SHA-1 hash values in order to verify the integrity of data being transmitted. If ICSF is not configured and active, SMP/E calculates the SHA-1 hash values using an SMP/E Java application class, provided that IBM SDK for z/OS, Java 2 Technology Edition, V1 (5655-I56) or later is installed. IBM recommends the ICSF method because it is likely to perform better than the SMP/E method. (To find out how to configure and activate ICSF, see *z/OS Cryptographic Services ICSF System Programmer's Guide*. For the required SMP/E setup, see *SMP/E User's Guide*.) • A download file system. The order is provided in a compressed format and is saved in a download file system. The size of this file system can be approximately twice the compressed size of the order to accommodate the order and workspace to process it. • Firewall configuration. If the enterprise requires specific commands to allow the download of the order using FTP through a local firewall, a user must identify these commands for later use in the CustomPac Installation Dialog, which manages the download of the order. • Proper dialog level. If a user is using a CustomPac Installation Dialog whose Package Version is less than 17.00.00, he/she must migrate the dialog to this level or later. The user can determine if he/she has the correct dialog level by looking for the text "This dialog supports electronic delivery." at the bottom of panel CPPPPOLI. If the dialog is not at the minimum level, follow the migration scenarios and steps described in *ServerPac: Using the Installation Dialog*.
Additional Internet Delivery Requirements for Intermediate Download	If planning to download the ServerPac or SystemPac dump-by-data-set order to a workstation and from there to z/OS, a user will need the following in addition to the requirements listed in item 13 on page 56: • Download Director. This is a Java applet used to transfer IBM software to workstation. For Download Director requirements, see http://inetsd01.boulder.ibm.com/dldirector/faq.html. • The ServerPac or SystemPac dump-by-data-set order accessible to the host. To make the order (files) accessible to z/OS, can do either of the following: o Configure the workstation as an FTP server. After downloading the order to the workstation, the dialogs used to install a ServerPac or SystemPac dump-by-data-set order can point to a network location (in this case, workstation) to access the order. Consult the documentation for the workstation operating system to determine if this FTP capability is provided or if it has to install additional software. Commercial, shareware, and freeware applications are available to provide this support. This option requires the use of ICSF. o Use network drives that are mounted to z/OS. The mounting can be accomplished using the NFS base element, server message block (SMB) support provided by the Distributed File Service base element,

		or the Distributed FileManager component of the DFSMSdfp base element. The package is received from the file system defined as the SMPNTS. For information about NFS, see *z/OS Network File System Guide and Reference*. For information about configuring Distributed File Service SMB support, see *z/OS Distributed File Service Customization*. For information about using the Distributed FileManager, see *z/OS DFSMS DFM Guide and Reference*. ○ CD write capability. If specified that 100% electronic delivery is required, there might be CD images associated with the order. The images are delivered in ISO9660 format and are packaged in zip files (with an extension of .zip). These files require the workstation to have CD write capability and might have to acquire software to support this capability.

Table 2-3: Minimum requirements for installation of CA ACF2 r14 SP1 for z/OS

Note: For more information on the hardware requirements for z/OS, see the z/OS v1 r11 Planning for Installation Guide.

Note: The TOE is a single hardware base that can contain multiple nodes. This is discussed for the Command Propagation Facility (CPF) which allows for the updating of information such as a user password from node A to node B. More information can be found in Section 9.1.3.3.2 regarding the virtual machines.

The evaluated configuration includes the following:

- CA ACF2™ r14 SP1 running on z/OS v1.11.

2.5 Logical Boundary

The logical boundary of the TOE is described in the terms of the security functionalities that the TOE provides to the systems that utilize this product for information flow control.

The logical boundary of the TOE will be broken down into five security classes: Security Audit, Identification and Authentication, Security Management, User Data Protection, and TOE Access. Listed below are the security functions with a listing of the capabilities associated with them:

2.5.1 Security Audit

The TOE creates and maintains audit records for all security-relevant events on objects which it protects, such as system entry, data access, and resource access. The TOE writes information in the audit records depending on the event that generated that audit record. Some of the information that is included in the audit record is the user's identifier and the object identifier that the user attempted to access.

CA ACF2 uses the System Management Facility (SMF) File to record all security-relevant events. These records are secured from accidental disclosure or destruction by the access control (DAC and MAC policies) protection mechanisms of the TOE. CA ACF2 provides authorized users and administrators with the ability to produce reports on a wide range of events. For example, the ACFRPTPW report provides an audit trail of system entry events. A variety of parameters can be set to customize the reports to display the violations by a particular type or by a group of users.

2.5.2 Identification & Authentication

CA ACF2 validates authentication for both the OS and TOE. It controls how, when, and which resources a user or administrator can access. CA ACF2 requires that each user and administrator have a valid User ID and authenticate utilizing the necessary mechanism (i.e. password verification, passphrase verification, digital certificate verification, passticket verification, Kerberos authentication on Operational Environment) before entering the system. The TOE also tracks user and administrator failed authentication attempts and if they surpass the threshold for failed authentication attempts the TOE will suspend the user or administrator account from being able to authenticate to the TOE.

By default, CA ACF2 requires that all User IDs are password protected. The security administrator which created the user or administrator assigns the first password. The user or administrator associated with the User ID will then change the password immediately or later when it expires. The TOE will also enforce the user or administrator to create a password which meets a password policy. The additional authentication mechanisms are set to none by default and require an administrator to configure the authentication applications to utilize these mechanisms. The TOE will enforce the use of these authentication mechanisms when a user or administrator has been configured to use one of the additional mechanisms. In addition to the enforcement of a password policy, when passphrases are used the TOE requires a user or administrator to create a passphrase which meets a passphrase policy.

2.5.3 Security Management

The TOE maintains three roles: security administrators, scoped security administrator, and users. Administrators manage the TOE and its users/administrators; whereas a user's primary ability is to manage their own password and resources as well as those that are scoped to them. These users/administrators can access the TOE locally through the Console Address Space or remotely through the Application Process. Along with the roles, privileges exist that affect what functions a user or administrator may perform or what a user or administrator can access. These privileges are AUDIT, SECURITY, LEADER, CONSULT, and ACCOUNT.

The SECURITY, ACCOUNT, and AUDIT privileges are the most commonly used in reference to being assigned to the users and administrators. An administrator has the SECURITY privilege assigned to their User ID record. This privilege will allow the administrator to perform management actions and view audit records within their scope. Any administrator with ACCOUNT administrative authority can create

users/administrators. On the other hand, either a user or administrator can have the AUDIT privilege defined in their User ID record. This allows the user or administrator to display any audit record, and are considered to be an auditor.

2.5.4 User Data Protection

CA ACF2 determines whether an individual user or administrator can be permitted access to a resource. Users and administrators cannot perform any action on a CA ACF2 controlled system unless they can first be identified and are then authorized access by CA ACF2. Therefore, CA ACF2 is protecting the resources of the computer system.

CA ACF2 performs two main methods of access control, one being mandatory access control (MAC) and the other being discretionary access control (DAC).

MAC imposes a security policy based on security labels. Security labels classify users, data, and resources. Standard access rules of z/OS and permissions still apply as well as those configured by CA ACF2 regarding passwords and other authentication methods, but only after MAC label dominance checks determine that a user can access data and resources based on their security label and the security label of the data or resources the user wants to access.

DAC security policy manages the controlled sharing of data and resources using rules. Depending on an implementation option, a Security Administrator, Scoped Security Administrator, or the user which is the rule owner can write rules to permit operations on that resource. If a user or administrator tries to access data without permission, the system creates a violation audit record and denies access.

When CA ACF2 locates the rule set, it interprets the rules to locate one that matches the environment that currently exists. If no rule matches the environment, CA ACF2 denies access to the resource. On the other hand, after CA ACF2 locates a rule that matches the current environment, it compares the access request against privileges, User ID (and UID) and scope of the user/administrator as specified in that rule. In accordance with what the rule specifies for these permissions, CA ACF2:

- Grants the access and does not audit the event
- Grants the access and writes an informational audit entry
- Prevents the access and writes a “violation attempt” audit entry

2.5.5 TOE Access

CA ACF2 is capable of denying access to users and administrators based on the following conditions:

1. They have been suspended
2. They fail to enter a correct User ID/authentication credential
3. They request to authenticate when a policy denies their access. Policies can be based on time/date of entry, source or entry, and/or APPLID used for entry.

2.6 Logical Boundary of the Operational Environment

2.6.1 Cryptographic Support

The TOE makes calls to z/OS's ICSF module to perform encryption on data that is utilized by the TOE for its operation. In addition, CA ACF2 calls the CMAC routine (key derivation routine) which hashes the password and User ID into 16-bytes. This string of bytes will then be sent to ICSF and the operational environment to perform encryption/decryption. Additionally, CA ACF2 makes calls to z/OS' ICSF module to perform encryption on data that is maintained within x.509 Digital Certificates.

2.6.2 Time Stamps

The TOE relies on the underlying OS for reliable time. The TOE functions such as audit logging rely on reliable time stamps that are produced by z/OS.

2.6.3 Audit Storage

The TOE relies on the underlying OS for storage of audit data. The TOE creates audit records on events which it stores on the z/OS SMF file.

3 Conformance Claims

3.1 CC Version

This ST is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2007-09-004, Version 3.1 Revision 3, July 2009.

3.2 CC Part 2 Conformant

This ST and Target of Evaluation (TOE) is Part 2 conformant for EAL4 to include all applicable NIAP and International interpretations through 7 March 2011.

3.3 CC Part 3 Conformant plus flaw remediation

This ST and Target of Evaluation (TOE) is Part 3 conformant plus flaw remediation for EAL4 to include all applicable NIAP and International interpretations through 7 March 2011.

3.4 PP Claims

This ST does not claim Protection Profile (PP) conformance.

3.5 Package Claims

This TOE claims a package for EAL 4.

3.6 Package Name Conformant or Package Name Augmented

This ST and Target of Evaluation (TOE) is conformant to EAL package claims augmented with ALC_FLR.1 and ASE_TSS.2**.**

3.7 Conformance Claim Rationale

There is no Conformance Claim rationale for this ST.

4 Security Problem Definition

4.1 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated. The following are threats addressed by the TOE.

T.ACCESS	Unauthorized users or administrators could gain access to objects protected by the TOE that they are not authorized to access.
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded; thus masking a user's action.
T.MASK	Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.

4.2 Organizational Security Policies

There are no Organizational Security Policies that apply to the TOE.

4.3 Secure Usage Assumptions

The specific conditions listed in this section are assumed to exist in the environment in which the TOE is deployed. These assumptions are necessary as a result of practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

4.3.1 Personnel Assumptions

A.ADMIN	One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
A.PATCHES	Administrators exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.

A.NOEVIL Administrators of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.

4.3.2 Connectivity Assumptions

There are no connectivity assumptions for this ST.

4.3.3 Physical Assumptions

A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

5 Security Objectives

5.1 Security Objectives for the TOE

The following security objectives are to be satisfied by the TOE.

O.ACCESS The TOE will provide measures to authorize users and administrators to access objects protected by the TOE once they have been authenticated. User and administrator authorization is based on access rights configured by the authorized administrators of the TOE.

O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users and administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.

O.AUTH The TOE will provide measures to uniquely identify all users and administrators. The TOE will authenticate the claimed identity prior to granting a user or administrator access to the objects protected by the TOE.

O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, objects, and security information relative to the TOE.

O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.

O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's and an administrator's logical access to the TOE and to explicitly deny access to specific users and administrators when appropriate.

5.1.1 Security Objectives for the operational environment of the TOE

The following security objectives for the Operational Environment of the TOE must be satisfied in order for the TOE to fulfill its security objectives.

OE.ADMIN One or more authorized administrators will be assigned to configure the Operational Environment, and install,

	configure, and manage the TOE and the security of the information it contains.
OE.EAVESDROPPING	The Operational Environment will encrypt TSF data when called by the TOE to prevent malicious users from gaining unauthorized access to TOE data.
OE.NOEVIL	All administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.
OE.LOCATE	The TOE will be located within controlled access facilities that will prevent unauthorized physical access.
OE.SYSTIME	The operating environment will provide reliable system time.

6 Extended Security Functional Requirements

6.1 Extended Security Functional Requirements for the TOE

There are no extended Security Functional Requirements for this ST.

6.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

7 Security Functional Requirements

7.1 Security Functional Requirements for the TOE

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

Security Function	Security Functional Components
Security Audit	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User identity association
	FAU_SAR.1(1) Audit Review
	FAU_SAR.1(2) Audit Review
	FAU_SAR.2 Selectable audit review
	FAU_SEL.1 Selective audit
User Data Protection	FDP_ACC.2(1) Complete access control
	FDP_ACC.2(2) Complete access control
	FDP_ACF.1(1) Security attribute based access control
	FDP_ACF.1(2) Security attribute based access control
Identification and Authentication	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_SOS.1(1) Verification of Secrets
	FIA_SOS.1(2) Verification of Secrets
	FIA_UAU.2 User authentication before any action
	FIA_UAU.4 Single-use authentication mechanisms
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UID.2 User identification before any action
	FIA_USB.1 User-subject binding
Security Management	FMT_MOF.1(1) Management of Security Functions Behavior
	FMT_MOF.1(2) Management of Security Functions Behavior
	FMT_MOF.1(3) Management of Security Functions Behavior
	FMT_MOF.1(4) Management of Security Functions Behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

Security Function	Security Functional Components
TOE Access	FTA_TSE.1 TOE session establishment

Table 7-1: Security Functional Requirements for the TOE

7.1.1 Class FAU: Security Audit

7.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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

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

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

c) [***all auditable events between subjects and resources and those from Modules as specified in Table 7-2 below.***].

Module	Event Type
ACFRPTNV (Environment Report)	- CA ACF2 startup - CA ACF2 shutdown - CA ACF2 console MODIFY commands
ACFRPTDA (DIRAUTH loggings)	- DIRAUTH call failures (invalid parm list) - DIRAUTH call failures (insufficient information to validate the access) - DIRAUTH call completed successfully (but resulted in deny access based on MLS controls)
ACFRPTCR (TSO Command Statistics Log)	- Log of Commands
ACFRPTDS (Data Set/Program Event Log)	- Data set Loggings - Data set access violations - Data set access trace requests - Program use loggings and violations - MLS Seclabel audit
ACFRPTEL (Infostorage Update Log)	- Updates to ENTRY records, Resource rule sets, GSO records, CA ACF2 for DB2 Resource rule sets and records, and other types of Infostorage records
ACFRPTJL (Restricted Logonid Job Log)	- Accesses by Logonids having RESTRICT attribute
ACFRPTLL (Logonid Modification Log)	- Maintenance of Logonid records (via ACF command) - Signon activity updates to Logonid records

	(i.e. access count updates, time/date last-used updates, password changes as appropriate, etc.)
ACFRPTOM (UNIX System Services Report)	- Loggings of z/OS UNIX (fka UNIX System Services, or USS) events
ACFRPTPW (Invalid Password/Authority Log)	Log unsuccessful access attempts and reason for failure, i.e.: - Password violation - Invalid submission path - Out of shift (LOGSHIFT) accesses
ACFRPTRL (Rule ID Modification Log)	- Update activity to the RULES database
ACFRPTRV (Resource Event Log)	- Resource loggings - Resource violations - MLS Seclabel Audit - Trace requests
ACFRPTSG (CA Statistics Report)	Statistics for: - Coupling Facility - Cache facility - Command Propagation Facility (CPF) - SAF RACROUTE requests - z/OS UNIX System Services
ACFRPTST (SAF Trace Report)	- SAF traces

Table 7-2: Audited Events by Module

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***CPUID, Jobname (if applicable), Source (if applicable)***].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: *All audit records are SMF type 230 records by default. This value can be modified by altering the ACFFDR @SMF definition.*

Application Note: *Auditable events are all events that a user or administrator (or an application on behalf of the user/administrator) generates, as well as events from the system that do not have the parameter log=nofail on the RACROUTE request. Only applications or systems can specify the log=nofail*

parameter. Refer to Section 9.1.1.2 in the TSS for further information.

7.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

Application Note: *The use of the word user in this requirement applies to both users and administrators, as defined in Table 1-1.*

7.1.1.3 FAU_SAR.1 (1) Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 (1) The TSF shall provide [***authorized users and administrators with the AUDIT privilege***] with the capability to read [***all audit information collected by FAU_GEN.1***] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

Application Note: *All audit records are SMF type 230 records by default. This value can be modified by altering the ACFFDR @SMF definition.*

Application Note: *An administrator is defined as such by having the SECURITY or other appropriate privilege. See Section 9.1.4 for more information on the privileges included in the evaluated configuration.*

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

7.1.1.4 FAU_SAR.1 (2) Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 (2) The TSF shall provide [***authorized administrators with the SECURITY or other appropriate privilege***] with the capability to read [***all audit information collected by FAU_GEN.1 within their scope***] from the audit records.

FAU_SAR.1.2 (2) The TSF shall provide the audit records in a manner suitable for the user with the security privilege to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: *All audit records are SMF type 230 records.*

Application Note: *An administrator is defined as such by having the SECURITY or other appropriate privilege. See Section 9.1.4 for more information on the privileges included in the evaluated configuration.*

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

7.1.1.5 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

7.1.1.6 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:
a) [**resource access failures and successes**]

b) ***[none]***

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note: *By default, CA ACF2 audits all resource access attempts. It is selectable whether or not any successes are audited. In the evaluated configuration, the TOE is configured to audit both failures and successes.*

7.1.2 Class FDP: User Data Protection

7.1.2.1 FDP_ACC.2 (1) Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

FDP_ACC.2.1 (1) The TSF shall enforce the [***Discretionary Access Control***] on [***users and objects***] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 (1) The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

Application Note: *A user can refer to a user or administrator, an application issuing a RACROUTE call, a terminal command, or a console command. An object can be a data set, volume, command issued, etc.*

Application Note: *If the TOE does not leverage the use of Security Labels on users and objects, the Discretionary Access Control policy is used to enforce access controls for users who are authenticating to the TOE.*

7.1.2.2 FDP_ACC.2 (2) Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

FDP_ACC.2.1 (2) The TSF shall enforce the [***Mandatory Access Control Policy***] on [***users and objects***] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 (2) The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

Application Note: A user can refer to a user or administrator, an application issuing a RACROUTE call, a terminal command, or a console command. An object can be a data set, volume, command issued, etc.

Application Note: CA ACF2 allowing or disallowing an operation actually refers to telling z/OS that the operation should be allowed or disallowed. When z/OS is correctly configured, it will abide by this decision.

Application Note: The following table lists all operations allowed by TOE users:

AccessLevel (DAC)	DIRAUTHLevel (MAC)
Read	Read
Create	Read
Write	Write
Control	ReadWrite
Update	ReadWrite
Scratch	ReadWrite
Fetch	ReadWrite
Alter	ReadWrite

Table 7-3: User Performed Operations on the TOE

Application Note: CA ACF2 leverages RACF commands to perform some of the above operations. The name of the operation has changed in CA ACF2 including ALTER which is now ALLOC, CONTROL which is now WRITE, and UPDATE which is now WRITE.

Application Note: The following list of classes is included in the evaluated configuration:

Interface	Resource Classes	
Base CA ACF2 products	DATASET	PROGRAM
	OPERCMDS	SECLABEL
	TSOAUTH	UNIXPRIV
	FACILITY	
CA ACF2 CICS Interface	None, issues CA ACF2 SVC calls using type codes (CFC for files, CKC for transactions, and CPC for programs)	
CA ACF2 IMS Interface	None, issues CA ACF2 SVC calls for type codes only (ITR for transactions, ICM for commands, and IPS for PSBs)	

Table 7-4: Resource Classes Included in the Evaluated Configuration

Application Note: *CA ACF2 allowing or disallowing an operation actually refers to telling z/OS that the operation should be allowed or disallowed. When z/OS is correctly configured, it will abide by this decision.*

7.1.2.3 FDP_ACF.1 (1) Security Attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 (1) The TSF shall enforce the [***Discretionary Access Control policy***] to objects based on the following: [***all operations between users and objects based upon the security attributes defined in Table 7-6, as well as resource class name and entity name***]

Application Note: *A user can refer to a user or administrator, an application issuing a RACROUTE call, a terminal command, or a console command. An object can be a data set, volume, command issued, etc.*

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: [***the TOE will permit the requested operation to the protected object (i.e. entity) if the user has a User ID or UID String which authorizes the operation on the object. Access to resources maintained by the TOE can be controlled by the following privileges:***

- ***ACCOUNT – Change, Create, Delete, and Display resources***
- ***AUDIT – Display all Records***
- ***CONSULT – Display certain fields***
- ***LEADER – Display and change certain fields***
- ***SECURITY - Display and Change resource***

- ***USER - Display and change certain fields in own record***
- ***READALL - Read and execute all data sets at the site***
- ***REFRESH - Issue modify ACF2 REFRESH commands***
- ***OPERATOR - Issue operator commands in TSO***

In addition, if any of the following access restrictions are defined, they must be true:

- ***the Source where the request was initiated must be allowed,***
- ***the APPLID of the application where the request was initiated must be allowed,***
- ***the Time/Date when the request was initiated must be allowed,***
- ***the additional vendor defined fields must allow the request,***
- ***the resource class name of the object must allow the request,***
- ***the entity name of the object must allow the request,***
- ***and the request is within the scope of the user***].

Application Note: *If the value of Source, APPLID, Time/Date, and any additional vendor defined fields are not present in the rule for the object, then no comparison is done for those attributes.*

Application Note: *A user can refer to a user or administrator, an application issuing a RACROUTE call, a terminal command, or a console command. An object can be a data set, volume, command issued, etc.*

Application Note: *See Section 9.1.4 for more information on the privileges included in the evaluated configuration.*

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

a) If the ownership matches the subject, then any operation is allowed by that subject.

b) If the object is data set and the prefix matches the data set high level qualifier, then any operation is allowed by that subject for a specified data set

c) If the subject is APF authorized

d) If the subject is a MUSASS
e) If the subject has the security attribute of SECURITY
f) If the subject has the security attribute of NON-CNCL
g) If Unix UID is 0 (root)].

FDP_ACF.1.4 (1) The TSF shall explicitly deny access of subjects to objects based on the [***restriction that a user with the SECURITY privilege but no ACCOUNT privilege cannot insert or delete any logonid records.***].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

7.1.2.4 FDP_ACF.1 (2) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(2) The TSF shall enforce the [***Mandatory Access Control***] to objects based on the following: [***all operations between users and objects based upon the security attributes ACCESSLevel, Type, Object Security Label, and Subject Security label***].

Application Note: *A user can refer to a user or administrator, an application issuing a RACROUTE call, a terminal command, or a console command. An object can be a data set, volume, command issued, etc.*

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 type of access is based on the values of Type and ACCESSLevel, as defined below***:

ACCESSLevel	Type=MAC	Type=EQUALMAC	Type=RVRSMAC
Read	User Dominates	Equivalence	Resource Dominates
Read/Write	Equivalence	Equivalence	Equivalence
Write	Resource Dominates	Equivalence	User Dominates

Table 7-5: Security Functional Requirements for the TOE

a) For Equivalence - if the security label on subject and object match, allow access

b) For User Dominates - if security label on subject dominates object, allow access

c) ***For Resource Dominates - if security label on the object dominates the user, allow access***].

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

FDP_ACF.1.4 (2) The TSF shall explicitly deny access of subjects to objects based on the [***if the object has a security label and the subject does not***].

Application Note: *If the subject has a label and the object does not, access is allowed.*

Application Note: *Subjects are users or applications running on behalf of users, objects are entities grouped as resources. Type is a global access variable that determines what type of access control model to implement. (See table below in section 6.1.3.2) Objects are called entities in the TOE. The TOE reads the subject and object label establishes dominance and will allow access based on the AccessLevel requested, and access control model type.*

7.1.3 Class FIA: Identification & Authentication

7.1.3.1 FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within 0-255***] unsuccessful authentication attempts occur related to [***all user and administrator login attempts***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**surpassed**], the TSF shall [***suspend the user's or administrator's User ID***].

Dependencies: FIA_UAU.1 Timing of authentication

Application Note: *See the CA ACF2 Administrator Guide, MAXTRY options of GSO PSWD Record.*

7.1.3.2 FIA_ATD.1 Security Attributes

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**see Table 7-6 below]**

Role	Attribute	Specific Attribute Definition
User and Scoped Security Administrator	User ID	Unique identifier per user/administrator
	Password	User definable password.
	Passphrase	User definable passphrase
	Authentication Data	Defines what type of authentication method is used per application (Kerberos pass ticket, passphrase, password, and certificate). This also stores statistics on password and access histories.
	Security Label	Security labels classify users, data, and resources (MAC only).
	Proxy Records	The LDAPBIND PROXY USER profile record contains the information needed to connect to the LDAP server, including: BINDDN, BINDPW, LDAPHOST, DOMAINDN, LOCALREG, and ENABLE/DISABLE
	Source	How a user or administrator accesses the TOE (Terminal, facility)
	APPLID	Application IDs of the applications which the user can perform requests from.
	Time/Date	Times/DaysOfWeek user is allowed to log on to TOE.
	CERTDATA	Identifies the X.509 digital certificate(s) associated with the user/administrator
	Privilege	Each privilege applies a set of abilities to a User ID and allows the individual to perform actions related to that privilege as long as it is within their scope.
	Suspend	Indicates whether the User ID is suspended, and the date this action was taken.
Security Administrator	User ID	Unique identifier per administrator
	Password	User definable password
	Passphrase	User definable passphrase
	Privilege	Each privilege applies a set of abilities to a User ID and allows the individual to perform actions related to that privilege as long as it is within their scope.
	Authentication Data	Defines what type of authentication method is used per application (Kerberos, pass ticket, passphrase, password, certificate)

Table 7-6: CA ACF2 Generated User Security Attributes

Attribute	Specific Attribute
BINDDN	The distinguished name to use when authenticating to the LDAP server.
BINDPW	The password to use when authenticating to the LDAP server.
LDAPHOST	The LDAP server URL and port.
DOMAINDN	The distinguished name of an EIM domain.
LOCALREG	The name of the local registry.
ENABLE/DISABLE	Specifies whether or not new connections may be established with the specified EIM domain.

Table 7-7: Proxy Record Fields

Dependencies: No dependencies.

7.1.3.3 FIA_SOS.1 (1) Verification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1 (1) The TSF shall provide a mechanism to verify that secrets meet [

a) A password must always be set

b) a configured minimum length of characters

c) a minimum configurable number of numeric characters

d) a minimum configurable number of uppercase letters

e) a minimum configurable number of lowercase letters

f) a minimum configurable number of special letters as defined in the PSWDPLST list

g) a configured limit of repeating characters

h) restrict the password to disallow restricted password prefixes (RESWORD) if the GSO PSWD option PSWDRSV is set

i) Prevent a user from specifying a new password that contains his 8 byte username or first four bytes of his username

j) Expiration date of password is a configurable number of days

k) A requirement to disallow the new password of a user/administrator to match the previous configured number of passwords].

Dependencies: No dependencies.

Application Note: *The PSWDPLST list is a list of defined special characters.*

Application Note: *The composition for this requirement is administrator-defined and is not hard-coded into the system. Guidance can be found in the CA ACF2 Administrator Guide to perform the configuration required to achieve the expected password policy.*

7.1.3.4 FIA_SOS.1 (2) Verification of Secrets

Hierarchical to: No other components

FIA_SOS.1.1 (2) The TSF shall provide a mechanism to verify that secrets meet [

a) Minimum passphrase length is of a configurable number of characters

b) Expiration date of passphrase is configurable number of days

c) New passphrases cannot match a configured number of a user/administrator's previous passphrases].

Dependencies: No dependencies

Application Note: *The composition for this requirement is administrator-defined and is not hard-coded into the system. Guidance can be found in the CA ACF2 Administrator Guide to perform the configuration required to achieve the expected password policy.*

7.1.3.5 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

7.1.3.6 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [***passticket authentication***].

Dependencies: No dependencies.

Application Note: *Passtickets are issued for a specific session and cannot be used again once that session has ended.*

7.1.3.7 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components

FIA_UAU.5.1 The TSF shall provide [***passwords, passtickets, Kerberos, digital certificates, or passphrases***] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***application from which the user is requesting system entry***].

Dependencies: No dependencies

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

Application Note: *The authentication method required for user/administrator authentication depends on the application from which they are accessing the TOE. The only time the authentication method is selectable by the user/administrator is if the application allows passwords or passphrases.*

7.1.3.8 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.

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

Dependencies: No dependencies.

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

7.1.3.9 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [***see Table 7-6***].

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: [

1. The TOE will create the user's UID string

2. The TOE will create the user's security environment (ACUCB, ACEE, and ACMCB)].

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: [***none***].

Dependencies: FIA_ATD.1 User attribute definition.

Application Note: *The use of the word user in this requirement applies to both users and administrators.*

7.1.4 Class FMT: Security Management

7.1.4.1 FMT_MOF.1 (1) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 (1) The TSF shall restrict the ability to [**determine the behavior of, modify the behavior of**] the functions [***See Table 7-8***] to [***the Security Administrator***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Function.

Operation	Administrative Functions
Define	Subject security attributes
Change	Subject security attributes
Manage	User identities
Manage	Authentication data by an administrator
Control	Authentication data that users are allowed to manage
Manage	Authentication data associated with user
Manage	Password policies
Manage	Threshold for unsuccessful authentication attempts
Manage	Actions to be taken in the event of authentication failure
Manage	Attributes used to make explicit access or denial based decisions
Manage	Audit events

Table 7-8: CA ACF2 List of Security Management Functions

7.1.4.2 FMT_MOF.1 (2) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 (2) The TSF shall restrict the ability to [**determine the behavior of, modify the behavior of**] the functions [***Table functions listed in Table 7-8 according to scope]*** to [***the Scope Security Administrator***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Function.

7.1.4.3 FMT_MOF.1 (3) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 (3) The TSF shall restrict the ability to [**determine the behavior of, modify the behavior of**] the functions [***self passwords and passphrases***] to [***users***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Function.

7.1.4.4 FMT_MOF.1 (4) Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 (4) The TSF shall restrict the ability to [**determine the behavior of, modify the behavior of**] the functions [***UID string]*** to [***the user that is the owner of the object***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Function.

7.1.4.5 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [***the Mandatory Access Control and Discretionary Access Control policies***] to restrict the ability to [**modify, delete,** [***manage, add, control, change***]] the security attributes [***defined in Table 7-6***] to [***Security Administrators or Scoped Security Administrators within their scope***].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions.

7.1.4.6 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

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

FMT_MSA.3.2 The TSF shall allow the [***Security Administrators or Scoped Security Administrators within their scope***] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

7.1.4.7 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***see Table 7-8***].

Dependencies: No dependencies.

Application Note: *If the Command Propagation Facility (CPF) is enabled, the security functions listed in Table 7-8 can be performed and simultaneously pushed to all additional instances of the TOE.*

7.1.4.8 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [***security administrator, scoped security administrator, and user***].

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

Dependencies: FIA_UID.1 Timing of identification.

7.1.5 Class FTA: TOE Access

7.1.5.1 FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on: [

1. The user's or administrator's status is suspended
2. A policy which limits user or administrator access based on
a. Time/Date
b. Source (IP address, POE)
c. APPLID (application user or administrator is trying to authenticate by)

].

Dependencies: No dependencies.

7.2 Operations Defined

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation. All of the components in this ST are taken directly from Part 2 of the CC except the ones noted with "_EXT" in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, selection, and refinement to be performed on functional requirements. These operations are defined in Common Criteria, Part 1 as:

7.2.1 Assignments Made

An assignment allows the specification of parameters and is specified by the ST author in [***italicized bold text***].

7.2.2 Iterations Made

An iteration allows a component to be used more than once with varying operations and is identified with the iteration number within parentheses after the short family name, e.g. FAU_GEN.1 (1), FAU_GEN.1 (2).

7.2.3 Selections Made

A selection allows the specification of one or more items from a list and is specified by the ST author in [**bold text**].

7.2.4 Refinements Made

A refinement allows the addition of details and is identified with "Refinement:" right after the short name. ~~The old text is shown with a strikethrough~~ and ***the new text is specified by italicized bold and underlined text***.

8 Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL4 augmented with ALC_FLR.1 and ASE_TSS.2.

8.1 Security Architecture

8.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D: The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D: The developer shall design and implement the TSF so that it is able to protect itself from tampering by un-trusted active entities.

ADV_ARC.1.3D: The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C: The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C: The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C: The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C: The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C: The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.1.2 Functional Specification with Complete Summary (ADV_FSP.4)

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

8.1.3 Implementation Representation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation. Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence. Evaluator action elements:

ADV_IMP.1.1E The evaluator *shall confirm* that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

8.1.4 Architectural Design (ADV_TDS.3)

ADV_TDS.3.1D	The developer shall provide the design of the TOE.
ADV_TDS.3.2D	The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.3.1C	The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.3.2C	The design shall describe the TSF in terms of modules.
ADV_TDS.3.3C	The design shall identify all subsystems of the TSF.
ADV_TDS.3.4C	The design shall provide a description of each subsystem of the TSF.
ADV_TDS.3.5C	The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.3.6C	The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
ADV_TDS.3.7C	The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.
ADV_TDS.3.8C	The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.
ADV_TDS.3.9C	The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
ADV_TDS.3.10C	The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.
ADV_TDS.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.3.2E	The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

8.2 Guidance Documents

8.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

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.

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

8.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

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.

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.

8.3 Lifecycle Support

8.3.1 Authorization Controls (ALC_CMC.4)

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labeled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.3.2 CM Scope (ALC_CMS.4)

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.3.3 Delivery Procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

8.3.4 Identification of Security Measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

8.3.5 Flaw reporting procedures (ALC_FLR.1)

ALC_FLR.1.1D The developer shall document flaw remediation procedures addressed to TOE developers. Content and presentation elements:

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. Evaluator action elements:

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

8.3.6 Life-cycle Definition (ALC_LCD.1)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

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

8.3.7 Tools and techniques (ALC_TAT.1)

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

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

8.4 Security Target Evaluation

8.4.1 Conformance Claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

8.4.2 Extended Components Definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

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

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

8.4.3 ST Introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

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

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

8.4.4 Security Objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.4.5 Security Requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.4.6 Security Problem Definition (ASE_SPD.1)

ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

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

8.4.7 TOE Summary Specification (ASE_TSS.2)

ASE_TSS.2.1D The developer shall provide a TOE summary specification.

ASE_TSS.2.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.2.2C The TOE summary specification shall describe how the TOE protects itself against interference and logical tampering.

ASE_TSS.2.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

ASE_TSS.2.3C The TOE summary specification shall describe how the TOE protects itself against bypass.

8.5 Tests

8.5.1 Analysis of Coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.5.2 Basic Design (ATE_DPT.2)

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.5.3 Functional Tests (ATE_FUN.1)

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

ATE_FUN.1.2D The developer shall provide test documentation

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

8.5.4 Independent Testing (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

8.6 Vulnerability Assessment

8.6.1 Vulnerability Analysis (AVA_VAN.3)

AVA_VAN.3.1D The developer shall provide the TOE for testing.

AVA_VAN.3.1C The TOE shall be suitable for testing.

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.
AVA_VAN.3.4E	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 Enhanced-Basic attack potential.

9 TOE Summary Specification

9.1 TOE Security Functions

The following sections identify the security functions of the TOE. They include Security Audit, Identification and Authentication, User Data Protection, Security Management, and TOE Access.

9.1.1 Security Audit

CA ACF2 collects security and system audit information and consolidates the information in the z/OS SMF File and the CA ACF2 security database. Administrators with the appropriate privilege and scope are able to use the audit information for monitoring, alerting, and reporting of information regarding user activity.

CA ACF2 provides numerous reports for different events that can occur while the TOE is running. For instance, any attempted violation CA ACF2 detects appears on a report. In addition, standard reports display each update to any of the CA ACF2 Security Databases. Thus, any addition, change, or deletion of any of CA ACF2 user, rule, or control information is visible to a person reviewing these reports as long as it is within the scope of that user/administrator to do so. Records produced from the database and SMF records provide information presented in the various CA ACF2 reports. CA ACF2 also records events such as the startup and shutdown of the TOE. Numerous other reports are available to record occurrences or produce audit trails of authorized activities. A user can produce each type of report independently of the others. The reports are further explained in Section 9.1.1.2.

The file records regarding start-up address the initialization of the TOE and its components and the success/failure of this event. The information is recorded and as previously stated stamped with the time and date. The shutdown file records address the shutdown of the TOE and its components. These records are also stamped with a date and time and whether it was a successful shutdown. These events can be viewed with the ACFRPTNV report generator which produces logging of each START (S ACF2), MODIFY (F ACF2), and STOP (P ACF2) of the TOE.

An administrator with the AUDIT privilege can be scoped to only certain rules, User ID records, and infostorage records. The READALL privilege which is defined in the User ID record can be set to allow a user with this privilege to be able to read and execute all data sets at the site, regardless of the access rules. CA ACF2 continues to enforce the existing rules for any other type of access.

In addition to the default information that is audited by the TOE (startup/shutdown of the TOE and all events between subjects and objects), the TOE allows selectable auditing to be performed by those administrators with sufficient privilege and scope. For instance, an administrator is capable of auditing certain types of access for a particular security label. This is done by designating the access types in the Seclabel Profile Data Record (e.g. READ, CONTROL, CREATE, WRITE, UPDATE, ALTER, FETCH, SCRATCH) followed by rebuilding the security classifications table with the command, "F ACF2,

MLS", for the changes to take effect. Security label auditing can then be activated by turning on the global option, MLSECAUD, in the CONTROL (GSO) MLSOPTS record. However, no security label auditing will be performed unless the MLSECAUD option is set and MLS is active on the system, even if access types have been specified for security labels defined in the system. The MLS Seclabel Audit process will create SMF records, from which the reports from Section 9.1.1.2 can be generated to display the audit information for a specified security label.

CA ACF2 is also capable of creating audit records for violations, traces, and logging. These record types can be accessed through ACFRPTRV.

9.1.1.1 AUDIT Privilege

An administrator or user with the AUDIT privilege defined in their User ID record can display User ID records, access and resource rules, and infostorage records. An auditor can issue the ACF SHOW subcommands that display CA ACF2 system control options, but an auditor cannot modify any of these components of the CA ACF2 system. Additionally, an auditor cannot update or delete User ID records or access any resources other than those authorized through rules and scope. The AUDIT privilege also gives users search and read access to directories in HFS. An administrator with the SECURITY privilege is also capable of displaying audit information as long as it is within their scope.

9.1.1.2 CA ACF2 Reports

CA ACF2 provides numerous reports to allow users/administrators of the TOE. These reports are listed below.

- ACFRPTXR - This report was created for auditors, security administrators, and management to identify which users could access which data sets and resources.
- ACFRPTIX - This report identifies all changes to the access rules affecting any specified high-level index (or pattern) over any period of time (assuming the input SMF records are available).
- ACFRPTDA – This report identifies any MLS-generated RACROUTE REQUEST=DIRAUTH calls that have been logged as a result of not successfully passing MLS validation with a return code of 0.
- ACFRPTDS - This report has four parts and includes all data set and volume access requests that were created due to: Logging options, Trace requests, Access violation attempts, and Accesses allowed but journaled.
- ACFRPTRV - This report is in three parts, similar to the first three mentioned for the ACFRPTDS report, but reports on accesses to resources protected through CA ACF2 resource rules and security labels when MLS is active on a system.

- ACFRPTEL - This report displays all changes, additions, or deletions that occurred to any entry records, resource rules, or other records in the CA ACF2 Infostorage Database.
- ACFRPTNV - This report generator produces a report that notes the use of the following commands: START (S ACF2), STOP (P ACF2), and MODIFY (F ACF2). The report shows the date and the time that each command was used.
- ACFRPTPW - This report contains an entry for each attempt to access the system that CA ACF2 denied for any reason. The reason for denial is also identified.
- ACFRPTRX - This report is similar to the Cross-Reference Report produced by ACFRPTXR. This report is sorted by logonid record and matches users with data set and resource rules.
- ACFRPTLL - This report contains an entry for each occurrence of an update to the CA ACF2 Logonid database.
- ACFRPTJL - This report contains an entry for each time a restricted logonid (with an activated RESTRICT attribute) enters the system.
- ACFRPTRL - This report has an entry for each change, addition, or deletion of any access rule record.
- ACFRPTSL - This report enables the flexible selection and display of logonid information.
- ACFRPTCR - This report contains a record for each TSO command or CLIST issued during any TSO session by users with TSO-TRC set in their logonid records, or for all TSO users if the CMDREC bit is set in the GSO OPTS record.

  ACFRPTST - This report provides output from the SECTRACE command, including RACROUTE parameter lists and environmental information.
- ACFRPTOM - This report provides z/OS UNIX/UNIX System Services/OpenEdition system logging, including security label violations when MLS is active on a system.
- Other Report Types include the CA ACF2 report Preprocessor (ACFRPTPP) and recovery program (ACFRECVR).

These reports include selectable audit review based on “types of events.” This allows for SMF reports to be more specific based upon event type as chosen by authorized users.

9.1.1.3 LOG = NOFAIL

The value specifies whether CA ACF2 overrides the LOG parameter on a matching RACROUTE AUTH or FASTAUTH call and treats it as LOG=ASIS. This is a way of logging to SMF a violation that is not normally logged because the RACROUTE AUTH or FASTAUTH call specified LOG=NONE or LOG=NOFAIL or LOG=NOSTAT.

NOFAIL is the default for the TOE. Note that LOG|NOLOG in the CLASMAP does not affect RACROUTE AUTH or FASTAUTH calls that are logged. NOLOG will not prevent loggings.

9.1.2 Identification and Authentication

The TOE requires that each user and administrator have a valid User ID and authenticate with the required mechanism before entering the system. The TOE enforces this for both the OS and the TOE itself.

Each user/administrator is assigned a unique user identifier called a User ID. The User ID is the key attribute of a User ID record, and allows the TOE to associate the other attributes of the User ID record to the user/administrator upon successful authentication. An administrator will create a User ID record for each user/administrator that is added to the system. The User ID record can contain the following security relevant information: User ID, Password/Passphrase, Authentication Data, Security Label, Proxy Records, Source, APPLID, Vendor Defined Fields, CERTDATA, suspend, and Time/Date (see Table 7-6 for more information). The information contained in each User ID record depends on the type of record (user or administrator) created, and the attributes which the administrator wants to define. For example, all User ID records must have the User ID and the password attributes defined. However, not all User ID records require that the Time/Date attribute to be defined which is used to determine when authentication is allowed. The attributes of a User ID record are utilized by the TOE to perform access control decisions on the users and administrators of the TOE.

Once a User ID record has been created, the user or administrator associated with that User ID can then authenticate to the TOE, and access the system which the TOE protects. A user or administrator can authenticate to the TOE through several different system applications. Each application requires the user or administrator to provide their User ID and authenticate utilizing the required mechanism (i.e. password verification, passphrase verification, digital certificate verification, passticket verification, Kerberos authentication on Operational Environment) which is determined by the application. The application makes the decision on which authentication mechanism is required on a user/administrator by user/administrator basis by utilizing the configured mechanism set by an administrator. Refer to the Sections 9.1.2.1 through 9.1.2.5 for more information on the different authentication mechanisms.

Before authorization to the TOE is complete, the TOE will perform additional authorization checks to determine if the user/administrator can be denied session establishment. Refer to the Section 9.1.5 for more information on denying session establishment. Once a user or administrator has authenticated to the TOE, a session is created for them. The creation of a session involves creating their UID string, and creating their security environment (ACEE, ACUCB/ACMCB) which involves loading their stored information from the CA ACF2 Security Database into memory, along with the UID string. Refer to Section 9.1.2.6 for more information on the UID string. In addition, the TOE allows a user/administrator to specify a security label after

authentication that they have been authorized to use. The chosen security label is also loaded into their security environment. If a security label is not specified, a default security label is used that has been set by an administrator.

Once the session has been created, all requests a user or administrator has on the CA ACF2 system are authorized by the TOE. The TOE performs the authorization by associating the user/administrator's security environment to the application that will perform the request, making the access control decision based on the application and the associated security environment. Because of this, each request is performed on behalf of the user/administrator's identity by an application, and the TOE determines if the user/administrator's identity has the authority to make such a request from that application. Refer to Section 9.1.3 for more information on access control decisions.

9.1.2.1 Password Verification and Password Policy

When a user or administrator authenticates to the TOE utilizing the password mechanism, the user/administrator must provide their password to the TOE to be checked against the stored hashed password. The TOE will then request the ICSF component to hash the password provided, and will then compare the hashed password against the hashed password stored in the User ID record associated with the User ID submitted by the user/administrator. If the hash of the password provided matches the hash of the password stored in the User ID record, this authorization check is successful and further authorization checks can be performed. Refer to Section 9.1.5 for more information on the TOE Access authorization checks. However, if the hashed passwords do not match the user/administrator has failed authentication, and the count for number of failed authentications is increased by one (refer to Section 9.1.2.7 for suspending a user/administrator).

The ability to change passwords and how they can be changed is also controlled by CA ACF2. CA ACF2 requires password protection for all User IDs by default, which requires the password attribute to be defined upon user/administrator creation. Passwords have a maximum length of eight characters, and the TOE has the ability to enforce a configured policy on all passwords before they are updated.

Security Administrators have the capability to configure the TOE's password policy. In the evaluated configuration, the following restrictions will be set by a Security Administrator, and therefore will be the password policy for the TOE:

- A password must always be set
- Have a minimum length of 6 characters
- Have at least one numeric character
- Have at least one uppercase letter

- Have at least one lowercase letter
- Must contain a special character
- Have at least one character selected from the PSWDPLST list
- There cannot be more than 2 repeating characters
- There cannot be more than 1 pair of repeating characters
- The initial characters cannot match one of the entries in the restricted password prefix list (RESWORD) if the GSO PSWD option PSWDRSV is set
- A user cannot specify a new password that contains their 8 byte username or first four bytes of their username
- Passwords will expire after a period of 90 days, requiring a user/administrator to change their own password
- When a password is changed it cannot match any of the previous three passwords used by the user/administrator

9.1.2.2 Passphrase Verification and Passphrase Policy

In addition to a password, a User ID can have an optional password phrase called a passphrase. Passphrases can be used instead of passwords in applications that support them, and can be defined for a User ID in addition to a password. A passphrase can be up to 100 characters long and can include mixed-case letters, numbers, and special characters including blanks.

When a user or administrator authenticates to the TOE utilizing the passphrase mechanism, the user/administrator must provide their passphrase to the TOE to be checked against the stored hashed passphrase. The TOE will then request the ICSF component to hash the passphrase provided, and will then compare the hashed passphrase against the hashed passphrase stored in the User ID record associated with the User ID submitted by the user/administrator. If the hash of the passphrase provided matches the hash of the passphrase stored in the User ID record, this authentication check is successful. Refer to Section 9.1.5 for more information on the TOE Access authentication checks. However, if the hashed passphrases do not match, the user/administrator has failed authentication, and the count for number of failed authentications is increased by one (refer to Section 9.1.2.7 for suspending a user/administrator).

Security Administrators have the capability to configure the TOE's passphrase policy with the PWPHRASE GSO options record. In the evaluated configuration, the following restrictions will be set by a Security Administrators, and therefore will be the passphrase policy for the TOE:

- Must be at least fifteen characters long
- Passphrases will expire after a period of 90 days, requiring a user/administrator to change their own passphrase
- When a passphrase is changed it cannot match any of the previous three passphrases used by the user/administrator

9.1.2.3 PassTicket Generation

To generate a PassTicket, the PassTicket generator algorithm must be used. This algorithm requires specific information as input data:

- The user's USERID
- The application ID, APPLID, for which the PassTicket is being generated
- A time and date stamp
- A security key, which should be known to both the application generating the PassTicket, and the target application which will be using the PassTicket

There are two ways to generate a PassTicket using this cryptographic algorithm.

3. If running on a z/OS system, the RCVTPTGN callable service can be used to generate the PassTicket on the host. The Application must pass RCVTPTGN a USERID and an APPLID; the callable service will then use the current time and date stamp, and extract the necessary profile record from the Infostorage database to obtain the security key. Using all four pieces of information and applying the cryptographic algorithm an 8 byte PassTicket is generated.
4. An administrator can create a program that incorporates the algorithm for any function that generates a PassTicket. This method allows the PassTicket to be generated on a network.

9.1.2.4 PassTicket Verification

A PassTicket is a generated character string that can be used in place of a password, with the following constraints:

- A specific PassTicket may be used for authentication once
- The PassTicket must be used within 10 minutes of being generated

When a user or administrator authenticates to the TOE utilizing the PassTicket mechanism, the user/administrator must provide their PassTicket to the TOE to be checked for authorization. The TOE will then request the ICSF component to decrypt the PassTicket, and the TOE will then evaluate the following combinations of information to determine if the provided PassTicket can be used for authentication:

1. The application name concatenated with the group name and User ID. (Note: Groups are not used in the evaluated configuration)

2. The application name concatenated with the User ID.
3. The application name concatenated with the group name. (Note: Groups are not used in the evaluated configuration)
4. The application name.

The TOE will check each combination until one of them matches the PassTicket's character string or all combinations have been checked. If a matching combination is found the TOE then checks the PassTicket's session key values to determine if they are valid, and if they are this authorization check is successful and further authorization checks can be performed. Refer to Section 9.1.5 for more information on the TOE Access authorization checks. However, if none of the combinations match the PassTicket's character string or if the session key value(s) are not valid, user/administrator has failed authentication, and the count for number of failed authentications is increased by one (refer to Section 9.1.2.7 for suspending a user/administrator).

The TOE will use the PassTicket verification process if configured by an administrator. The TOE also requires the application to generate a PassTicket by calling the z/OS RCVTPTGN callable service. The application must provide the RCVTPTGN callable service with the User ID and the APPLID which will be used for the PassTicket's combination. The callable service will then use the current time and date stamp, and extract the necessary APPLID record from the CA ACF2 Security Database to obtain the security key which the TOE will recognize as being associated with the application. The RCVTPTGN callable service will utilize all four pieces of information and will apply the ICSF cryptographic algorithm to the PassTicket string to generate the 8 byte PassTicket. The administrator can then provide the user/administrator with the 8 byte PassTicket.

9.1.2.5 Certificate Verification

The TOE provides the ability to perform authorization checks based on an X.509 Digital Certificate. Digital certificates provide a means of authentication through the use of public-key cryptography and a trusted third party, known as a Certification Authority. A digital certificate is generated by the Certification Authority and is identified uniquely by its serial number and by the associated distinguished name of the Certification Authority ("issuer's distinguished name").

If a user/administrator accesses z/OS resource, the certificate is presented to CA ACF2. Using the certificate serial number and the issuer's distinguished name, CA ACF2 associates the certificate with a User ID. The TOE then determines if the certificate is valid and if associated user/administrator can authenticate to the TOE with the certificate.

Determining that the certificate is valid means that CA ACF2 can properly parse the certificate and extract various fields from it – it does not mean that CA ACF2 will do other types of validation processing such as verifying signatures. The reason for this is that this type of validation processing is the responsibility of the caller of the underlying SAF initACEE callable service (which CA ACF2 supports). The details of these

restrictions can be found in the IBM z/OS Security Server RACF Callable Services document.

CA ACF2 provides complete functionality to generate, install, and maintain digital certificates, key rings, and digital certificate mappings, including the following:

- Request ICSF to generate the key pair for a digital certificate, and also to sign the generated certificate.
- Create a PKCS #12 certificate package
- Create a PKCS #10 certificate request
- Export a digital certificate or certificate package and private key from CA ACF2 to a z/OS dataset
- Display a certificate that is in a z/OS dataset and determine if it is associated with a CA ACF2 user/administrator
- Display a certificate registered with CA ACF2
- Automatically register a digital certificate with CA ACF2
- Associate a CA ACF2 user/administrator with a digital certificate
- Change, display, and delete information about a digital certificate for a CA ACF2 user/administrator
- Create, change, display, and delete a key ring
- Add and remove a certificate from a key ring
- Assign a CA ACF2 user/administrator to a group of certificates via User ID mapping (as directed by GSO CERTMAP records)
- Assign a CA ACF2 user/administrator to a group of certificates based on filters on the issuer and subject distinguished names, system ID, application ID, or application-defined variables
- Change, delete, and display a CA ACF2 User ID mapping CERTMAP GSO records

9.1.2.6 Associating a User with a Certificate

Certificates are associated to CA ACF2 users and administrators through the use of CERTDATA user Profile records. The CERTDATA segment of the User Profile record identifies an X.509 digital certificate associated with the user/administrator. A user/administrator can have more than one certificate, but a single certificate cannot be used by more than one user/administrator.

The TOE supports key rings for digital certificates. A key ring allows an administrator to associate one or more digital certificates to a particular user/administrator. This feature

allows for multiple certificates for different applications if they require varying attributes or information for authenticating to the application process. These are certificates that can be used by the user/administrator. The application used for authentication can request that CA ACF2 pass back one or more trusted digital certificates based on the key ring value passed to it. The application can ask for a trusted certificate by supplying a certificate label or the subject's distinguished name, or by requesting the default certificate. If the application is authorized to make the request, CA ACF2 passes back a trusted certificate and the application will then typically use this to support subsequent security-related functions such as Secure Sockets Layer (SSL). Normal key ring processing defines a specific certificate to be used for SSL or encryption. The rest of the certificates on the key ring are normally the signing (Certificate Authority) certificates.

9.1.2.7 Kerberos

Kerberos for z/OS verifies requests as a trusted third-party authentication service. When the TOE is configured to use Kerberos, the TOE will call z/OS's Kerberos component from the Operational Environment to perform the initial authentication check for the user/administrator. Using conventional shared secret key cryptography, Kerberos confirms the identity of a user/administrator and makes the authentication check to see if it has been successful. However, if Kerberos determines that the authentication has failed, then the TOE will increase the number of failed authentications by one (refer to Section 9.1.2.7 for suspending a user/administrator).

Kerberos uses electronic tickets to authenticate a user/administrator to a server. A ticket, which is only valid for a single server and a single user/administrator during a certain period of time, is an encrypted message containing the name of the user/administrator and server, the user/administrator's network address, a time stamp, and a session key. Once the user/administrator receives this ticket, they can use it to access the server as many times as desired until the ticket expires. The user/administrator cannot decrypt the ticket but can only present it to the server. Nobody listening in on the network can read or modify the ticket as it passes through the network without detection or invalidation.

9.1.2.8 UID String

The user identification string (UID string) is constructed by CA ACF2 when a user authenticates to the TOE. The UID string's function is to define users and administrators to provide greater flexibility and ease of use in writing authorization rules.

The UID string specifies a 1 to 24 character pseudo field constructed of User ID record fields. CA ACF2 uses the User ID record information stored in the user/administrator's security environment to verify their system access and privileges, and it uses the UID string to verify a user/administrator's access to objects in a more efficient manner. Furthermore, while the session environment identifies a unique user/administrator, the UID string can identify a user/administrator in the rules created for access control.

9.1.2.9 Suspended User

The TOE monitors the number of failed attempts to authenticate to the TOE. Once an administrator configured threshold of failed authentication attempts is surpassed for a

particular User ID, the TOE will suspend that User ID. When a User ID is suspended the TOE will not allow the user/administrator associated with the suspended User ID to authenticate to the TOE. The threshold is configured by an administrator and can be set to a value within zero to 255 failed authentication attempts. Once a user/administrator has been suspended, an administrator must reactivate the suspended User ID to allow them to attempt to authenticate to the TOE again.

9.1.3 User Data Protection

CA ACF2 performs access control based on policies defined by Mandatory Access Control (MAC) and Discretionary Access Control (DAC). These policies are created and modified by security administrators with the appropriate scope. MAC and DAC handle authorization requests by examining their User ID, User ID String (UID), scope, and authority.

CA ACF2 uses rule sets to determine whether or not a user or administrator can be granted access to a given resource. These rule sets are defined by a composition of access and/or resource rules which are compiled by an authorized security administrator. The rule set is then transformed into an object record and stored in the CA ACF2 Security Database. If CA ACF2 needs to consult the rule set(s) to determine whether a service can be performed, the TOE translates the related rule sets and returns a response, allowing or denying the action. In addition to these rule sets, MLS is implemented in CA ACF2, providing an extra layer of security which provides classifications that are applied alongside the rule sets to further enforce access control. For complete information on implementing and auditing MLS on a system using CA ACF2, see the CA ACF2 Multilevel Security Planning Guide.

The two main forms of access control, MAC and DAC, are discussed below in sections 9.1.3.1 and 9.1.3.2.

9.1.3.1 Mandatory Access Control

In CA ACF2, MAC is used to impose security policies based on security labels. Security labels classify users, data, and resources. The label dominance relationship established between a subject's security label and an object's security label controls the requested access. Standard access rules and permissions still apply, but only after MAC label dominance checks determine that a user can access data and resources based on their security label and the security label of the data or resources the user wants to access.

The purpose of MAC is to prevent the system from allowing data with a high sensitivity security label from being disclosed to a user with a lower sensitivity security label. MAC enforces both the "simple security property", which restricts read accesses, and the "confinement property", which restricts write accesses ("write-down" protection). CA ACF2 uses the principle of MAC label dominance to determine how security labels compare in an MLS system, and, based on the comparison, whether MAC access is allowed or denied. In explaining a dominance relationship, the following example is provided.

If there are two security labels, X and Y:

- X dominates Y if:
    - The security level of X is greater than or equal to the level of Y, and
    - X contains at least all categories contained in Y
- X is disjoint from Y if:
    - Neither X nor Y includes all of the categories of the other

In the first rule (X dominates Y, above, both conditions must be true for Label X to dominate Label Y. So, the "and" is important. If the Level of X is less than the Level of Y, then the dominance check has already failed and label X will never dominate Label Y. However, if the Level of X is greater than or equal to the Level of Label Y, then, the categories of Label X and Label Y must be compared to see if all the categories in Label Y are in Label X. If Label X's level is higher than Label Y's, dominance has not yet been established, until the categories are compared. In the second rule (X is disjoint from Y), above, if neither security Label X nor Y includes all the categories of the other, the labels are said to be incomparable or disjoint; neither one dominates.

Note: The term "greater than" is used informally to mean dominates. Although labels cannot be compared in a numerical sense, the concept of "greater than" is a convenient way to think of label dominance.

Label X would dominate Label Y if the security level used by X is greater than or equal to the security level provided by Y and X contains at *least* all the categories contained in Y. If X does not contain all the categories provided in Y, the two resources are disjointed. If the Level of X is less than the Level of Y, then the dominance check has failed and Label X will never dominate Label Y. These levels whether X and Y or Classified, Unclassified, Secret, or Top Secret, are determined by the administrative configuration applied to the TOE by a trusted admin.

There are three types of MAC label dominance checks in CA ACF2 MLS system:

- MAC dominance check
- Reverse MAC dominance check
- Equal MAC dominance check

9.1.3.1.1 Security Labels

When a user logs on to the TOE, he/she may specify a security label to apply to the User ID belonging to him/her. If a security label is not defined by the user/administrator, CA ACF2 provides a default security label for the user. Alternatively, if the user had a previous security label applied in an earlier session, that label is applied. Once CA ACF2 verifies that the user is authorized to use a security label, the security label is maintained

in the user's address space and is used to make access decisions until the user logs off. CA ACF2 ensures that a user cannot alter his security label in any way while logged onto the system.

Important! When MLS is activated, any users who are already logged onto the system and any jobs or started tasks that are currently running will not have security labels nor will they be assigned default security labels by CA ACF2. Therefore, to obtain security labels, users must logoff and re-logon to the system and jobs, and started tasks must be restarted and rerun after MLS is activated.

9.1.3.1.2 MAC Dominance Check

The MAC dominance check requires a user's security label to dominate the resource's label. This is due to the fact that opening a resource for write access implicitly opens the resource for read access. To read or read/write, the subject's label must dominate the object's security label. To write only, the object's security label must dominate the subject's security label.

9.1.3.1.3 Reverse MAC Dominance Check

The reverse MAC dominance check is the opposite of the MAC dominance check. Reverse MAC dominance requires that the resource's security label dominates the user's security label for the requested access to be allowed.

9.1.3.1.4 Equal MAC Dominance Check

If two labels are equal, they dominate each other. Equal MAC dominance checking, which is used for any class that requires two-way communication, requires that the user and resource security labels are the same for the requested access to be allowed.

9.1.3.2 Discretionary Access Control

CA ACF2 uses Discretionary Access Control (DAC) to protect data. CA ACF2 DAC security policy manages the controlled sharing of data and resources using rules. Depending on an implementation option, a security administrator or rule owner can write rules to permit sharing. If a user tries to access data without permission, the system creates a violation record and denies access.

9.1.3.3 Authority

Each security administrator, in addition to their scope, must also be assigned particular types of administrative authorities. These authorities define the security functions that the administrative User IDs can perform for User IDs within their scope. Upper level security administrators can grant administrative authorities to lower level administrators within their scope provided the higher level administrators already possess the appropriate authorities. These upper level security administrators are granted the SECURITY privilege while more scoped administrators possess the ACCOUNT, CONSULT, LEADER, and/or AUDIT privileges. These privileges are described in Section 9.1.4.1.

9.1.3.3.1 Administrator Authorities

Administrative Authority and the scope of that administrator, in all cases, are verified at the sending and target Virtual Machine. This is performed before the command can be successfully executed on the target VM. The authorities are determined based on the administrator's privileges discussed in Section 9.1.4.1 as well as the information stored within his or her User ID String. Based on the information provided from these security attributes, the limitations of the administrator's authority can be determined.

9.1.3.3.2 Command Propagation Facility

In addition to propagating changes, the Command Propagation Facility (CPF) allows administrators to view the contents of the CA ACF2 Security Database via distributed nodes. The viewing is completely secure since the administrators scope is verified at both locations, allowing the administrator to review the security information for which he or she is responsible for at all nodes in the CPF domain.

CPF propagated administration executes on the remote system using the authority and scope of the administrator as defined in the remote system, and not using the authority and scope of the administrator from the originating system. For example, if an administrator who is defined with the SECURITY attribute on one system propagates a CA ACF2 command to a system where that administrator is defined without the SECURITY attribute, then the command is limited to the non-SECURITY authority. It should also be noted in regards to data propagation that user-initiated password changes at system entry that are propagated using CPF cause the user's password to change at each VM where the change is sent.

9.1.3.3.3 LDAP Directory Services

An LDAP directory provides a method to maintain directory information, such as email accounts, in a central location, for storage, update, retrieval, and exchange. LDAP directories can be utilized as network accessible databases for organization and indexing of network security information.

LDS uses the LDAP protocol and native TCP/IP to communicate the changes from the CA ACF2 Security Databases to the remote LDAP repository. Servers enabled with Secure Sockets Layer (SSL) technology protect unauthorized parties from viewing sensitive information during a secure session. Using the XREF mapping record, you configure which LID fields are to be sent to the remote repository and what the remote attribute name is.

When CA ACF2 uses LDS to connect to the remote LDAP directory, it is the client application to the remote LDAP Server. Using the standard LDAP protocol, CA ACF2 formats the add, modify, or delete request and sends it to the remote LDAP Server through native TCP/IP.

9.1.3.4 Security Modes

CA ACF2 for z/OS r14 is capable of using several security modes to assist in access control. However, only Abort mode is included in the evaluated configuration and is the

default mode for the TOE. During Abort mode, the TOE prevents unauthorized access to data, logs violations, and issues a violation message to the user. For more information on the excluded security modes, see Section 2.3.3.

9.1.3.5 Multiple-User, Single Address Space System

In the multiple-user single address space system (MUSASS) environment, the programming system (such as CA Roscoe) carries out all requests to resources on behalf of the user. Consequently, the "owner" of the address space becomes the MUSASS. Thus, CA ACF2 must validate the requests based on the authority of the MUSASS, as opposed to the individual user, unless another user can establish additional communications with CA ACF2. Because only the MUSASS knows which user initiated the request, the MUSASS becomes responsible for assisting CA ACF2 in validating those requests.

For CA ACF2 to process these validation requests, the MUSASS must first build a control block to identify the user. The ACUCB is a large control block and contains information concerning path control; record read error information, a work buffer, and more. The MUSASS environment does not need much of this information. CA ACF2 contains a design feature, the ACMCB, which provides only the minimum information necessary to define each user to CA ACF2 and still permit full CA ACF2 security controls.

In general, a MUSASS interacts with CA ACF2 in three distinct areas. These areas are user sign-on, user resource request validation, and user sign-off.

9.1.3.6 NON-CNCL and APF-Authorized

A user with the NON-CNCL privilege defined in their logonid record has full access to any data set or resource despite any security violations that can occur during the access attempt. These violations are logged by CA ACF2. However, the logonid can access a data set or resource without logging as long as the access is defined by an existing data access or resource rule, or is permitted by virtue of the logonid's PREFIX field. All accesses outside of those normally permitted by the PREFIX or rules are permitted, but logged.

The Supercall facility lets an APF-authorized requester perform database maintenance functions without explicit CA ACF2 authorization. The Supercall facility is available only through the ACFSVC TYPE=A SVC call. To invoke the Supercall, the caller must be APF-authorized or a MUSASS.

9.1.3.7 Object Ownership

The first ownership is done by privilege, whereby one's privilege level allows them to administer entitlement controls (rules) for a protected resource. Since this could allow them to grant themselves access to the protected resource – this conveys an implicit level of ownership.

Next, for data sets, the PREFIX field within the Logonid record by default will be populated with the Logonid value when a Logonid is created. CA ACF2 automatically

regards data set resources beginning with that prefix value as being owned by that Logonid; no security checks are done and access is automatically granted. Additionally, that user also is granted administrative access to the data set access rule(s) matching that prefix value (depending on the CENTRAL setting of the GSO RULEOPTS record).

In an MLS environment, access is strictly controlled by the MLS security controls assigned by the MLS administrator to protected resources and users. MLS security checks are performed first if MLS grants access with standard DAC security checks performed. Ownership checks are performed only at the DAC level, so data ownership would come into play only if MLS controls were not active or MLS controls were active and they granted access to the user. MLS resources are not owned by users via Logonid but by users with appropriate privilege authorities (i.e. SECURITY – scoped or un-scoped).

For ownership transfer, either a change to the PREFIX value or a change to one's privilege levels would be needed.

9.1.3.8 Object Reuse Protection

A z/OS system ensures that no user or program can scavenge data from an object after it has been deleted. Object reuse protection ensures that when a user deletes an object such as a data set, it is physically erased. Without object reuse protection, the storage would be returned to the storage pool without erasure. A user who obtained storage for a new data set could read the storage and find out what the previous user had put in the data set.

Object reuse protection applies not only to data set objects but also to all objects defined in the system, including address spaces, messages, and devices. A CA ACF2 system provides object reuse protection for data sets if the AUTOERAS option of the GSO OPTS record is set. Object reuse protection for other objects is provided automatically by the environmental operating system.

9.1.4 Security Management

The TOE maintains three roles: security administrators, scoped security administrators, and users. Administrators manage the TOE and its users, while a user only interacts directly with the TOE to perform self-management functions such as password changes. Users also perform operations on objects in the operational environment which are protected by the TOE. While a user can be assigned most types of administrative authority, the user's scope is always limited to itself. The only difference between a scoped security administrator and a security administrator is that a scoped security administrator has restrictions applied based on the policies and privileges set regarding that administrator. For instance, a Security Administrator may be capable of performing management options over the entire TOE while a Scoped Security Administrator may be able to perform the same action but only to a particular User ID selection or for a particular set of applications.

Security Administrators on the TOE are capable of adding/modifying/deleting users as well as the security attributes that apply to those users. This can be performed as long as

the administrator performing the action is privileged to do so and it is within their scope or the user him/herself is performing the action on their own attributes.

When the TOE is first installed, the only User ID present is ACFUSER as defined in the database. A security administrator or the individual installing the TOE can then log on to this User ID to define additional users. Once this has been performed, a security administrator can delete the ACFUSER account. The following privileges can perform the following actions against User ID records: SECURITY – Display and Change, ACCOUNT – Change, Create, Delete, and Display, AUDIT – Display all Records, LEADER – Display and change certain fields, CONSULT – Display certain fields, USER – Display and change certain fields in own record.

CA ACF2 also provides options that can force users to change their passwords at specific intervals, force users to change their passwords the first time they log on, and force users to enter their passwords in a protected field. The rule addressing this policy can be set by administrators with the appropriate privilege and scope but by default the interval period in which a password must be changed is every 90 days. The security administrator can also affect other rules applying to the password such as the threshold for wrong attempts. This is controlled by the PASSLMT option (e.g. PASSLMT = 2). If a user or administrator were to exceed this threshold, their account would be suspended and the event would be audited. Additionally, the minimum password length can be set with MINPSWD which in the evaluated configuration is set to 6.

There are two attributes that must be set to allow for certain commands to be executed by a user on the TOE. The REFRESH attribute is required in order to issue modify ACF2 REFRESH commands. The OPERATOR attribute is required in order to issue operator commands in TSO which is a TSO requirement.

In addition to the security administrator, scoped security administrator, and user roles, the TOE provides special privileges which further define what a user/administrator may or may not do when using the TOE. Each privilege applies a set of abilities to a User ID and allows the individual to perform actions related to that privilege as long as it is within their scope. These privileges are listed below.

9.1.4.1 SECURITY Privilege

Users with this attribute are usually the data security administrators for the site. Normally their duties include the maintenance of all access rule and resource rule records, input source entry records, and scope and shift records.

Security administrators can display and change fields of User Id and security control records based on their scope and security privileges. If the security administrator does not have the SCPLIST field defined in their User ID record, then the security administrator can display and change any User ID record field. However, a security administrator cannot create or delete User ID records unless the security administrator's User ID record also has the ACCOUNT privilege level. To display or change a security User ID record, the user must have the SECURITY or ACCOUNT privilege. If the security User ID record is unscoped, the user must also be unscoped. Additionally, a SECURITY user can

be limited by assigning them RULEVLD or RSRCVLD or both which tells CA ACF2 to check existing access rules for this user instead of allowing access simply based on the SECURITY attribute.

An unrestricted security administrator (one with SECURITY and no scope limits) can create, change, list, or delete any rule record or CA ACF2 infostorage record (such as entry records, scope records, and shift definitions). The unrestricted security administrator can also access any resource because, even if a permitting rule does not exist, he has the authority to create or change such a rule. However, CA ACF2 logs and flags any accesses by security administrators that are not specifically authorized through CA ACF2 rules.

A restricted security administrator has the SECURITY attribute but his authority is limited with a scope record. This record is named in the SCPLIST field of the administrator's User ID record. The restricted security administrator has full SECURITY privileges but can apply them only to rules and security records, including User ID records that fall within this scope.

9.1.4.2 AUDIT Privilege

An auditor can display any user ID record, rule record, or security control record. If scoped, the auditor can only display records within the scope. An auditor does not have the authority to update or delete any of these records or to access any resources except those specifically authorized to him with access or resource rules or other privileges. Through scope records, an auditor can be restricted to only certain rules, certain User ID records, and to certain Infostorage records. The READALL privilege (defined in the User ID record) can be set to grant an auditor or any other privileged user the ability to read and execute all data sets at the site, regardless of the access rules. This is similar to the NON-CNCL attribute, but grants only read and execute accesses; CA ACF2 continues to enforce the existing rules for any other type of access.

9.1.4.3 LEADER Privilege

This attribute does not grant any special powers relative to the Rule or Infostorage database. Leaders cannot create or delete User ID records (unless they also have ACCOUNT). Leaders can, however, change or display a limited number of fields in existing User ID records. The fields they have access to can be controlled at the field level at the site, and the User ID records they have access to can be controlled through scope records. Leaders are usually not too powerful and they usually have very limited scopes.

Group leaders are usually scoped. This means that they can only display and change certain fields of User ID records for their group only. They cannot display the User IDs for users in another group. The user must have the SECURITY, ACCOUNT, AUDIT, or LEADER privilege in the User ID record to display or change a group leader User ID record.

9.1.4.4 CONSULT Privilege

This attribute is usually assigned to administrators who assist other users in using the computer system. Usually consultants cannot update anything significant in User ID records but can display some of the less sensitive fields to help answer questions. The site controls which fields consultants can display or alter, and, through scope records, which User ID records consultants can access.

Consultants are usually scoped. This means that they can only display certain fields of User ID records based on their scope. They cannot display the User IDs for users outside their scope. The user must have the SECURITY, ACCOUNT, AUDIT, or CONSULT privilege in the User ID record to display or change a consultant User ID record.

9.1.4.5 ACCOUNT Privilege

Users with this attribute are usually assigned the responsibility to establish, maintain, and delete User ID records. The ACCOUNT attribute grants no privileges relative to the Rule database or the Infostorage database.

Persons with ACCOUNT can also use the various SHOW subcommands. They can also change and display a large number of individual User ID fields (these fields can be defined by the site).

An account manager can display and change any field of the User ID record based on their scope, and can create and delete any records in their scope. If an account manager does not have the SCPLIST field defined in their User ID record, the account manager can display, change, create, and delete any User ID record.

To display or change an account manager User ID record, the user must have the ACCOUNT privilege. If the record is unscoped, the user must also be unscoped. However, an account manager that has only the ACCOUNT privilege cannot change or list the User ID record of a user with the ACCOUNT and SECURITY privileges. CA ACF2 considers a user with both these privileges more powerful than a user with only one of these.

Along with these two default roles, the TOE provides privileges that allow users to have certain administrative functionalities. These are listed below.

9.1.4.6 Defining Default Values

An Administrator of the TOE is capable of defining default values based on policies created/modified by authorized administrators. These default values include the initial user password, default values during installation as well as those that apply to audit files once the TOE has been configured. These values can be changed and are managed only by administrators with the appropriate privilege of SECURITY.

9.1.4.7 Scope

A *scope record* can be used to limit a user's access to the User ID, Rule, and Infostorage databases. Scope records limit the powers of a privileged user. The authority a security

administrator grants depends upon the privilege the user has. For example, adding a scope record to a User ID with the ACCOUNT privilege limits that user's access to those User ID records related to their office, instead of to the entire company.

To establish these limits, a security administrator must create a scope record and make entries in the LID and UID fields related to those User IDs that the user creates. Additionally, the DSN and INF fields can be specified to further scope access to rule and security records. Next, the administrator must enter the name of the scope record in the SCPLIST field of that User ID before any restrictions apply.

9.1.4.7.1 Types of Roles

The Security Administrator is responsible for the scope of authority. The TOE provides several different levels of control based upon privileges. The following table shows the different types of users/privileges and that user type's scope:

Type	Title	Scope
Security Administrator	Security Administrator	A security administrator has the SECURITY privilege defined in the User ID record.
Scope Security Administrator	Account Managers	An account manager has the ACCOUNT privilege defined in the User ID record.
	Auditors	An auditor has the AUDIT privilege defined in the User ID record.
	Group Leaders	A group leader has the LEADER privilege defined in his User ID record.
	Consultants	A consultant is a user who has the CONSULT privilege in his User ID record.
User	All Users	A normal user ID is one that has no special administrative privileges and thus will be unable to update his user ID or any other user ID (other than perhaps his own password if allowed). A normal user would not be able to modify the mandatory access control policy or discretionary access control policy without special privilege or other administrative authority (such as %CHANGE and/or %RCHANGE authority granted to by a rule).

Table 9-1: Security Administrators and Associated Scope of Authority

9.1.5 TOE Access

The TOE performs checks prior to authentication to the TOE to determine if the user/administrator can be denied the ability to establish a session. If a user/administrator is denied session establishment because of a rule, then the user/administrator will not be authenticated to the TOE.

The first instance where session establishment will be denied is based upon the rule that a user/administrator cannot authenticate to the TOE because their User ID has been suspended. The TOE will determine if a user/administrator has been suspended by reviewing their User ID record for the suspend attribute, and determining if it has been set. Refer to Section 9.1.2.7 for additional information on suspending a User ID.

The second instance where session establishment will be denied is based on user/administrator attributes which are defined during the User ID record's creation or modified at a later time by an authorized administrator. The attributes which can be defined are Time/Date, Source, and APPLID.

The Time/Date attribute, when set, will define a scheduled time when the user/administrator can authenticate to the TOE. If the authentication request occurs outside of that schedule, then the user/administrator will be denied session establishment.

The Source attribute, when set, will define what IP addresses the user/administrator can access to TOE from, and the POE (port-of-entry) which are terminal IDs or console IDs which they can access the TOE from. If the Source attribute is set, the user/administrator will only be able to authenticate to the TOE via the IP addresses and POEs which have been set in the attribute. Authentication requests from any Source outside what is defined in the attribute will deny the user/administrator from establishing a session.

Application protection, when activated, controls the applications which a user/administrator can utilize – including authentication to the TOE. If an authentication request occurs for a user that lacks the proper access to that application, the user/administrator will be denied session establishment.

9.2 Self Protection (ADV_ARC.1)

The TOE forces users/administrators to authenticate to it prior to allowing them to take any actions on objects which the TOE protects within the operational environment. This includes the TOE's configuration files and processes. The TOE also forces the users/administrators to authenticate in a manner consistent with administrative defined policies. These policies include the authentication mechanisms that can be utilized and any access restrictions which can be placed against their ability to authenticate. The TOE will also suspend the ability of users/administrators to successfully authenticate to the TOE due to a consecutive number of failed authentication attempts based on User ID. This assists in protecting the TOE from a potential unauthorized user.

Once users/administrators are authenticated, the TOE maintains individual sessions associated with them through the creation of a security environment which is associated with their User ID. Each security environment defines the authorizations which the associated user/administrator has to perform operations on objects. These security environments are protected by the TOE such that the contents of each individual security environment cannot be affected by a process of another user/administrator.

The TOE monitors all requests from subjects within its operational environment, including requests from users/administrators, OS processes, and system processes. The TOE determines which requests will be authorized to be performed. Therefore, the TOE has the ability to monitor actions by subjects external to itself on its own configuration files and processes. The TOE's access control policies only allow those actions which are defined to be actions from a trusted subject.

The TOE also ensures that information critical for the security of subjects is protected via the operational environment's cryptographic mechanisms. The TOE will call the z/OS ICSF module when the TOE determines that security relevant information can be encrypted before being stored in the operational environment or sent outside the TOE's security perimeter.

9.3 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following table.

Security Function	Security Functional Components
Security Audit	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User identity association
	FAU_SAR.1(1) Audit Review
	FAU_SAR.1(2) Audit Review
	FAU_SAR.2 Selectable audit review
	FAU_SEL.1 Selective audit
User Data Protection	FDP_ACC.2(1) Complete access control
	FDP_ACC.2(2) Complete access control
	FDP_ACF.1(1) Security attribute based access control
	FDP_ACF.1(2) Security attribute based access control
Identification and Authentication	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_SOS.1(1) Verification of Secrets
	FIA_SOS.1(2) Verification of Secrets
	FIA_UAU.2 User authentication before any action

Security Function	Security Functional Components
	FIA_UAU.4 Single-use authentication mechanisms
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UID.2 User identification before any action
	FIA_USB.1 User-subject binding
Security Management	FMT_MOF.1(1) Management of Security Functions Behavior
	FMT_MOF.1(2) Management of Security Functions Behavior
	FMT_MOF.1(3) Management of Security Functions Behavior
	FMT_MOF.1(4) Management of Security Functions Behavior
	FMT_MSA.1 Management of security attributes
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
TOE Access	FTA_TSE.1 TOE session establishment

Table 9-2: Security Functional Components

9.3.1 Security Audit

The audit function of the TOE enforces the FAU_GEN.1, FAU_GEN.2, FAU_SAR.1 (1), FAU_SAR.1 (2), and FAU_SAR.2 and FAU_SEL.1 requirements.

CA ACF2 collects security and system audit information. Administrators with proper privileges are able to monitor, alert, and report information about user activity.

The examination of the TSS showed that each of these requirements was successfully mapped to the SFRs listed above the information provided in the INT section of the ST.

The generation of audits (FAU_GEN.1.1) is provided in Section 2.5.1 as well as in the TSS, Section 9.1.1. In addition to the generation of audits, the AUDIT privilege is discussed in section 9.1.1.1 to explain the use of the privilege in order to view the audited information. FAU_GEN.1.2 is then fulfilled in Section 9.1.1.2 with the mapping of information audited in relation to the event that is occurring. Section 2.5.1 of the INT covers this information as well but in less detail. Section 9.1.1.1 also discusses the information that can be audited based on event with the example of start up and shutdown of the TOE.

FAU_SAR.1 (1) and FAU_SAR.1 (2) are covered in the TSS through Sections 9.1.1.1 and 9.1.1.2 in the TSS. These sections discuss the types of reports/logs that are provided in the TOE as well as the AUDIT privilege. These sections demonstrate the use of scoping (the AUDIT privilege) to apply restrictions on auditing. Additionally, Section

9.1.1.2 outlines the various forms of reports that a security administrator with the appropriate privilege can view or generate. Finally, FAU_SEL.1 is covered in Section 9.1.1 with the discussion of CA Earl in the customization of reports in relation to the preferences of the users on the system. It is also covered in Section 9.1.1.3 with the discussion of LOG = NO FAIL. This allows for a security administrator to decide when or when not to audit information in regards to the value specified for the LOG parameter.

9.3.2 User Data Protection

The User Data Protection function of the TOE enforces the FDP_ACC.2 (1), FDP_ACC.2 (2), FDP_ACF.1 (1), and FDP_ACF.1 (2) requirements.

MLS is a security policy in CA ACF2 that provides mandatory access control (MAC). MLS is an optional layer of protection which forces security classifications, called security labels, for virtually all users, data and resources in a system. Additionally, it validates all access based on these labels, regardless of permissions. MLS offers selective protection of data and resources based on a user's organization's individual needs. CA ACF2 lets a user activate MLS and implement security labels for the users, resources, and data that require a higher level of security.

Section 2.5.4 of the INT section discusses the MAC and DAC requirements as discussed in the TSS but in a much more general level of detail.

FDP_ACC.2 (1) and FDP_ACF.1 (1) are the discussion of Discretionary Access Control in regards to users accessing the TOE. The TSS provides information relating to DAC in Section 9.1.3.2 to 9.1.3.4. Section 9.1.3.2 discusses the actual concept behind DAC and how it acts on the TOE.

FDP_ACC.2 (2) and FDP_ACF.1 (2) cover Mandatory Access Control requirements and are discussed in Section 9.1.3.1. Section 9.1.3.1 provides information detailing MAC then goes into further detail in subsections 9.1.3.1.1 to 9.1.3.1.4. In these sections, security labels and the three forms of dominance checks are covered by the TSS to explain how MAC is applied to subjects and objects on the TOE.

Additional sections provided in the TSS for user data protection include Section 9.1.3.3, Authority, and 9.1.3.4, Security Modes. The only security mode used in the evaluated version of the TOE is ABORT. These two sections explain how authority it enforced on the TOE and what the ABORT security mode allows.

9.3.3 Identification and Authentication

The identification and authentication function of the TOE enforces the FIA_AFL.1, FIA_ATD.1, FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UID.2, and FIA_USB.1 requirements.

CA ACF2 uses the User ID record to verify a user's system access and privileges; CA ACF2 uses the UID to verify a user's access to data and resources. Furthermore, while the User ID identifies a unique user, the UID can identify a user or a group of users in CA

ACF2 rules. The User ID record contains the fields that comprise the UID; however, the actual UID does not exist in the User ID record. The UID string is dynamically built at sign-on time.

Section 2.5.2 in the INT section discusses the basic overview of the Identification and Authentication requirements and is covered in more detail in the sections of the TSS discussed below.

Section 9.1.2 discusses the maintenance of attributes for users with the use of the CA ACF2 Security Database. The database is responsible for storing the security attributes which are relevant to all users of the TOE. This information supports the SFR FIA_ATD.1.

FIA_SOS.1 (1) is fulfilled in Section 9.1.2.1 and 9.1.2.3 with the discussion of the password policy and requirements for password defaults. FIA_SOS.1 (2) is then fulfilled in Section 9.1.2.3 with the policies relating to a user's passphrase.

FIA_AFL.1.1 and FIA_AFL.1.2 is fulfilled by Section 9.1.2.6 with the information regarding the suspension of user accounts when too many attempts are made to connect to the TOE with invalid information.

FIA_UID.2, FIA_USB.1, and FIA_UAU.2 are fulfilled in Section 9.1.2 with the discussion of authentication before any action and authentication methods provided by the TOE which are chosen by the application.

Finally, FIA_UAU.4 is fulfilled in Section 9.1.2.7, passticket, and FIA_UAU.5 is fulfilled with Sections 9.1.2.1/2/3/4/5/7/8/9. These sections cover the five methods of authentication that can be used when accessing the TOE. These methods include passwords, passphrases, digital certificates, passtickets, and Kerberos.

9.3.4 Security Management

The security management function of the TOE enforces the FMT_MOF.1 (1), FMT_MOF.1 (2), FMT_MOF.1 (3), FMT_MOF.1 (4), FMT_MSA.1, FMT_SMF.1, and FMT_SMR.1 requirements.

Security management is required to manage the users, groups and the privileges of users. This is supporting identification and authentication as well as access control. Different aspects of security management support each other. For example user and group management supports the management of access control, because the definition of access rights can be simplified by defining access on a group level and assign users that require access to the appropriate groups. Security management also supports auditing because it allows to define the events to be audited based on individual users, individual protected objects, privileges of the users, type of event, and (in LSPP mode) security label.

Section 2.5.3 of the INT discusses a general overview of the Security Management requirements as shown above and is detailed further with the information below that is covered in the TSS. The INT, TSS, and SFRs can all be mapped and interpreted throughout these sections.

The security management requirements outlined by the TOE are covered by the TSS in Section 9.1.4. The main paragraph of this section identifies the division of roles into Security Administrators and Users. These roles can be scoped based on privileges and allow for variations of off the default roles. This applies to FMT_MOF.1 (1), FMT_MOF.1 (2), FMT_MOF.1 (3), and FMT_MOF.1 (4). These SFRs apply to the security administrator, user, and scoped security administrator. FMT_MOF.1 (1) through FMT_MOF.1 (4) are covered by Section 9.1.4 through 9.1.4.5 as well as Section 9.1.4.8. These sections discuss the different Security Privileges and roles that are applied on the TOE and how these roles and privileges can scope a user. Section 9.1.4.7, Scope, also addresses the FMT_MOF.1 requirements by detailing how scope is used to enforce different levels of privileges for users of the TOE.

Following FMT_MOF.1, the requirements for FMT_MSA.1 are covered in the main Section, 9.1.4, where the discussion of the management functions that are performed on the TOE occurs. These functions typically require the SECURITY privilege which is discussed in Section 9.1.4.1.

FMT_SMF.1 is fulfilled again by Section 9.1.4 as well as with Section 9.1.4.7. 9.1.4.8 discusses the types of roles provided to users and what privileges apply to those roles. Section 9.1.4 then discusses the management functions that are included in the SFR in table 7-7 from Section 7.1.4.3.

9.3.5 TOE Access

The TOE access function of the TOE enforce the FTA_TSE.1 requirement.

This requirement is fulfilled by Section 2.5.5 of the INT by discussing the denial of a session based on a user's status or failure to authenticate correctly. Section 9.1.5 discusses the methods in which a user/administrator authenticates to the TOE as well as what instances could cause a user/administrator to be denied access. These instances include: if the User Id has been suspended by an administrator or if the PASSLMT for that User ID was exceeded, if the User ID attempts access outside of its scheduled time, if the User ID attempts access from a source to which it lacks access, or if the User ID attempts access to an application to which it lacks access.

10 Security Problem Definition Rationale

10.1 Security Objectives Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated assumptions and threats.

Assumption	Objective	Rationale
A.ADMIN One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.	OE.ADMIN One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A.ADMIN in order to ensure that authorized administrators install, manage and operate the TOE in a manner that maintains its security objectives.
A.PATCHES Administrators exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.	OE.ADMIN One or more authorized administrators will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A.PATCHES in order to ensure that the authorized administrators properly patches the Operational Environment and the TOE in a manner that maintains the security objectives of the TOE.
A.NOEVIL Administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.	OE.NOEVIL All administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.	OE.NOEVIL maps to A.NOEVIL in order to ensure that there are no careless, willfully negligent, or hostile administrators of the TOE.
A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.	OE.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.	OE.LOCATE maps to A.LOCATE in order to ensure that physical security is provided in the environment where the TOE operates.

Table 10-1: Assumption to Objective Mapping

Threat	Objective	Rationale
T.ACCESS Unauthorized users or administrators could gain access to objects protected by the TOE that they are not authorized to access.	O.ACCESS The TOE will provide measures to authorize users and administrators to access objects protected by the TOE once they have been authenticated. User and administrator authorization is based on access rights configured by the authorized administrators of the TOE.	O.ACCESS (FDP_ACC.2 (1), FDP_ACC.2 (2), FDP_ACF.1 (1), FDP_ACF.1 (2)) addresses T.ACCESS by providing the authorized administrators with the capability to specify access restrictions on the objects protected by the TOE to authorized users and administrators.
	OE. EAVESDROPPING The Operational Environment will encrypt TSF data when called by the TOE to prevent malicious users from gaining unauthorized access to TOE data.	OE.EAVESDROPPING addresses T.ACCESS by ensuring that the underlying Operating System provides the capability to encrypt TSF data used by the TOE.
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.	O.ROBUST_ADMIN_GUIDANCE (ALC_DEL.1, AGD_PRE.1, AGD_OPE.1) helps to mitigate T.ADMIN_ERROR by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner and to provide the administrator with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure.
	O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, objects, and security information relative to the TOE.	O.MANAGE (FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1) addresses T.ADMIN_ERROR by ensuring only authorized administrators can use the provided resources for managing and monitoring user accounts, objects, and security information relative to the TOE.

Threat	Objective	Rationale
T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.ACCESS The TOE will provide measures to authorize users and administrators to access objects protected by the TOE once they have been authenticated. User authorization is based on access rights configured by the authorized administrators of the TOE.	O.ACCESS (FDP_ACC.2 (1), FDP_ACC.2 (2), FDP_ACF.1 (1), FDP_ACF.1 (2)) addresses T.AUDIT_COMPROMISE by providing the authorized administrators with the capability to specify access restrictions on the objects protected by the TOE, which includes audit records.
T.MASK Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.	O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users and administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.	O.AUDIT (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1 (1), FAU_SAR.1 (2), FAU_SAR.2, FAU_SEL.1) addresses T.MASK by providing the authorized users and administrators with tools necessary to monitor user and administrator activity to ensure that misuse of the TOE does not occur.
	OE.SYSTIME The operating environment will provide reliable system time.	OE.SYSTIME helps to mitigate T.MASK by ensuring the accuracy of the tools necessary to monitor user activity as provided via O.AUDIT.
	O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's and an administrator's logical access to the TOE and to explicitly deny access to specific users and administrators when appropriate.	O.ROBUST_TOE_ACCESS (FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UID.2, FTA_TSE.1), addresses T.MASK by controlling the logical access to the TOE and the objects the TOE protects. By constraining how and when authorized users and administrators can access the TOE, and by mandating the type and strength of the authentication scheme, this objective helps mitigate the possibility of an unauthorized user attempting to login and masquerade as an authorized user or administrator. In addition, this objective provides the administrator the means to control the number of failed login attempts a user or administrator can generate before an account is suspended, further reducing the possibility of an unauthorized user gaining access to the TOE.

Threat	Objective	Rationale
	O.AUTH The TOE will provide measures to uniquely identify all users and administrators. The TOE will authenticate the claimed identity prior to granting a user or administrator access the objects protected by the TOE.	O.AUTH (FIA_ATD.1, FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UID.2, FIA_USB.1) addresses T.MASK by providing measures to uniquely identify and authenticate users and administrators to the TOE through multiple authentication methods. In addition, this objective ensures that the strength of user's password or passphrase meets a scheme which ensure that unauthorized users cannot easily impersonate an authorized user or administrator by guessing their password.

Table 10-2: Threat to Objective Mapping

10.2 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the security functional requirement components that address the stated TOE and environment objectives.

Objective	Security Functional Components	Rationale
O.ACCESS The TOE will provide measures to authorize users and administrators to access objects protected by the TOE once they have been authenticated. User and administrator authorization is based on access rights configured by the authorized administrators of the TOE.	FDP_ACC.2(1) Complete access control	FDP_ACC.2 (1) states the TSF shall enforce the Discretionary Access Control Policy on users requesting access to protected objects within the Operational Environment.
	FDP_ACC.2(2) Complete access control	FDP_ACC.2 (2) states the TSF shall enforce the Mandatory Access Control Policy on users requesting access to protected objects within the Operational Environment.
	FDP_ACF.1(1) Security attribute based access control	FDP_ACF.1(1) states the TSF shall enforce the Discretionary Access Control Policy on users requesting access to objects based on the security attributes defined in Table 7-6, as well as, resource class name and entity name
	FDP_ACF.1(2) Security attribute based access control	FDP_ACF.1(2) states the TSF shall enforce the Mandatory Access Control Policy on users requesting access to objects based on AccessLevel, Type, Object Security Label, and Subject Security label.

Objective	Security Functional Components	Rationale
O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users and administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.	FAU_GEN.1 Audit data generation	FAU_GEN.1 states that the TSF shall be able to generate an audit record for the start-up and shutdown of the audit functions and all auditable events between subjects and resources. For each record, the TSF shall record the date/time/type/outcome of the event, the subject identity of the user which caused the event, the system ID, terminal ID, audit reason indicator, authority, mode, resource name, and if applicable the application or program that the user request was initiated from.
	FAU_GEN.2 User identity association	FAU_GEN.2 states the TSF shall be able to associate each auditable event with the identity of the user or administrator that caused the event.
	FAU_SAR.1(1) Audit Review	FAU_SAR.1(1) states the TSF shall provide the authorized users and administrators with the AUDIT privilege with the capability to read all audit records of events collected by FAU_GEN.1.
	FAU_SAR.1(2) Audit Review	FAU_SAR.1(2) states the TSF shall provide the authorized administrators with the SECURITY privilege with the capability to read all audit records of events collected by FAU_GEN.1 that are within their scope.
	FAU_SAR.2 Restricted audit review	FAU_SAR.2 states the TSF shall prohibit all users and administrators read access to the audit records, except those users and administrators that have been granted explicit read-access.
	FAU_SEL.1 Selective audit	FAU_SEL.1 states that the TSF shall be able to select the events to be audited from the set of all auditable events based upon an administrator's selection of the event's object identity, user identity, or permission.
O.AUTH The TOE will provide measures to uniquely identify all users and administrators. The TOE will authenticate the claimed	FIA_ATD.1 User attribute definition	FIA_ATD.1 specifies the security attributes that can be maintained at the level of the user and administrator. This means that the security attributes listed are assigned to and are changed at the level of the

Objective	Security Functional Components	Rationale
identity prior to granting a user or administrator access the objects protected by the TOE.		user and administrator. In other words, changing a security attribute (see Table 7-6) associated with a user or administrator can have no impact on the security attributes of any other user or administrator.
	FIA_SOS.1(1) Verification of Secret	FIA_SOS.1 states that the TSF shall enforce a password scheme that is sufficient to ensure that unauthorized users cannot easily impersonate an authorized user or administrator by guessing their password.
	FIA_SOS.1(2) Verification of Secret	FIA_SOS.1 states that the TSF shall enforce a passphrase scheme that is sufficient to ensure that unauthorized users cannot easily impersonate an authorized user or administrator by guessing their passphrase.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires users and administrators be authenticated before any access to the TOE and objects protected by the TOE is allowed.
	FIA_UAU.4 Single-use authentication mechanisms	FIA_UAU.4 states that the TSF will prevent the reuse of a passticket for an authenticated session, which prevents an unauthorized user performing a replay attack with this authentication data.
	FIA_UAU.5 Multiple authentication mechanisms	FIA_UAU.5 states that the TSF shall provide passwords, passphrases, passtickets, Kerberos, or digital certificates for authentication, and the TSF shall authenticate any user's or administrator's claimed identity according to the application from which the user or administrator is requesting system entry.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires users and administrators be identified before any access to the TOE and objects protected by the TOE is allowed.
	FIA_USB.1 User-Subject Binding	FIA_USB.1 requires the TOE to perform a binding of security attributes associated with users and administrators that are authenticated with the subjects that represent them in the TOE. The TOE will create a user's UID String and security environment (ACUCB, ACEE, ACMCB) during this process.

Objective	Security Functional Components	Rationale
O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, objects, and security information relative to the TOE.	FMT_MOF.1(1) Management of security functions behavior	FMT_MOF.1 (1) states the TSF shall restrict the ability to perform operations specified in Table 7-8 to the Security Administrator.
	FMT_MOF.1(2) Management of security functions behavior	FMT_MOF.1 (2) states the TSF shall restrict the ability to perform operations specified in Table 7-8 to the Scope Security Administrator based on their scope.
	FMT_MOF.1(3) Management of security functions behavior	FMT_MOF.1 (3) states the TSF shall restrict the ability to perform self password and passphrase changes to users.
	FMT_MOF.1(4) Management of security functions behavior	FMT_MOF.1 (4) states the TSF shall restrict the ability to perform management of the UID string to the users that are the owners of the object.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 states the TSF shall enforce the Mandatory Access Control and Discretionary Access Control policies to modify, delete, manage, add, control, or change the user attributes as listed in Table 7-8 to Security Administrators or Scoped Security Administrators within their scope.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 states the TSF shall enforce the Mandatory Access Control and Discretionary Access Control policies to provide restrictive default values for security attributes that are used to enforce the SFP. It allows the Security Administrators or Scoped Security Administrators within their scope to override the default values set for security attributes when creating users or administrators.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 requires that the TOE provide the ability to manage its security functions as defined it Table 7-8.
	FMT_SMR.1 Security Roles	FMT_SMR.1 requires the TOE to provide the ability to maintain the roles Security Administrator, Scoped Security Administrator, and user. In addition, it requires that users and administrators be associated with these roles.
O.ROBUST_ADMIN_GUIDA	ALC_DEL.1 Delivery Procedures	ALC_DEL.1 describes product delivery and a description of all

Objective	Security Functional Components	Rationale
NCE The TOE will provide administrators with the necessary information for secure delivery and management.		procedures used to ensure objectives are not compromised in the delivery process.
	AGD_PRE.1 Preparative Procedures	AGD_PRE.1 documents the procedures necessary and describes the steps required for the secure installation, generation, and start-up of the TOE.
	AGD_OPE.1 Operational user guidance	AGD_OPE.1 describes the proper use of the TOE from a user standpoint.
O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's and an administrator's logical access to the TOE and to explicitly deny access to specific users and administrators when appropriate.	FIA_AFL.1 Authentication Failure Handling	FIA_AFL.1 provides a detection mechanism for unsuccessful authentication attempts by users and administrators. The requirement enables an administrator to set a threshold that prevents unauthorized users from gaining access to an authorized user's or administrator's account by guessing authentication data. Once the threshold is surpassed the TOE will suspend the targeted user's or administrator's User ID until an authorized administrator takes some action (e.g., un-suspends the account). Thus, limiting an unauthorized user's ability to gain unauthorized access to the TOE.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires users and administrators be authenticated before any access to the TOE and objects protected by the TOE is allowed.
	FIA_UAU.4 Single-use authentication mechanisms	FIA_UAU.4 states that the TSF will prevent the reuse of a passticket for an authenticated session, which prevents an unauthorized user performing a replay attack with this authentication data.
	FIA_UAU.5 Multiple authentication mechanisms	FIA_UAU.5 states that the TSF shall provide passwords, passphrases, passtickets, Kerberos, or digital certificates for authentication, and the TSF shall authenticate any user's and administrator's claimed identity according to the application from which the user or administrator is requesting system entry.

Objective	Security Functional Components	Rationale
	FIA_UID.2 User identification before any action	FIA_UID.2 requires a user or administrator be identified before any access to the TOE and objects protected by the TOE is allowed.
	FTA_TSE.1 TOE session establishment	FTA_TSE.1 states that the TOE will deny session establishment if the user or administrator is suspended, or if there is a policy that defines the date/time, source, and APPLID where access is allowed and the user's or administrator's request does not adhere to the policy.

Table 10-3: Security Functional Requirements Rationale

10.3 EAL 4 Justification

The threats that were chosen are consistent with attacker of medium attack potential, therefore EAL4 was chosen for this ST.

10.4 Requirement Dependency Rationale

All Security Functional Requirement component dependencies have been met by the TOE as defined by the CC Part 2 with the exception of FPT_STM.1 and FMT_MTD.1.

FPT_STM.1, Reliable Time Stamps is a dependency of FAU_GEN.1. This dependency is met by the Operational Environment. The underlying Operating System (z/OS) will be available to the TOE for use in determining the timestamp for the audit trail.

FMT_MTD.1, Management of TSF Data is a dependency of FAU_SEL.1. This dependency has not been included because the "Manage Audit Events" function described in FMT_MOF.1(1) addresses the intent of this requirement.

10.5 Assurance Measures

The SARs for this evaluation have been chosen because they are consistent with the package claim of EAL4. Augmentations to this claim include ALC_FLR.1 and ASE_TSS.2. These optional SARs increase the security assurance of the TOE in the following manners:

- ALC_FLR.1 provides assurance that the TOE is updated in a well-defined manner that is consistent with the development security procedures outlined in ALC_DVS.1.

- ASE_TSS.2 maps the TOE Summary Specification to other components of the ST with a greater amount of scrutiny. Since the TSS is the ultimate driver of the functional test cases, this scrutiny provides a higher degree of assurance that functional testing is both accurate and thorough.

The following table identifies the SARs for this ST.

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Design	TOE Design Specification v1.0 Low Level Design Specifications CA ACF2 Systems Programmers Guide IBM z/Architecture Principles of Operation	These documents describe the security architecture of the TOE and its underlying OS.
ADV_FSP.4 Functional Specification with complete summary	Functional Specification v1.0 IBM z/OS Security Server RACF Callable Services IBM z/OS Security Server RACROUTE Macro Reference IBM MVS Initilization and Tuning Reference IBM z/Architecture Principles of Operations CA ACF2 for z/OS Messages Guide CA ACF2 for z/OS IMS Support Guide CA ACF2 for z/OS Command Reference Guide CA ACF2 for z/OS Administrator Guide CA ACF2 for z/OS Systems Programmer Guide CA ACF2 for z/OS CICS Support Guide	These documents describe the external interfaces to the TOE
ADV_IMP.1 Implementation Representation of the TSF	Low Level Design Specifications (annotated)	These documents demonstrate the correspondence between source code and design documentation.
ADV_TDS.3 Architectural Design	TOE Design Specification v1.0 Low Level Design Specifications (folder)	These documents describe the internal design of the TOE.
AGD_OPE.1 Operational User Guidance	CA ACF2™ for z/OS Administrator Guide r14 CA ACF2™ for z/OS Multilevel Security Planning Guide r14 CA ACF2™ for z/OS Implementation Planning Guide r14 CA ACF2™ for z/OS Auditor Guide r14 CA ACF2™ for z/OS Installation Guide r14	These documents provide guidance on how to use CA ACF2

Component	Document(s)	Rationale
	CA ACF2™ for z/OS Reference Guide r14 CA ACF2™ for z/OS Report and Utilities Guide r14 CA ACF2™ for z/OS CICS Support r14 CA ACF2™ for z/OS IMS Support Guide r14 CA ACF2™ for z/OS Command Reference Guide r14 CA ACF2™ for z/OS Systems Programmer Guide r14 IBM z/OS Version 1 Release 11 Planning for Installation	
AGD_PRE.1 Preparative Procedures	CA ACF2 Installation Guide r14 CA ACF2 Implementation Guide r14 CA ACF2 Multi-Level Security Planning Guide r14 IBM Intro to the New Mainframe Security CA Mainframe Software Manager Product Guide r3.1 ACF2 Install Verification ACF2 Install_r14_MSM_01072011.wmv ACF2 Post Install r14.wmv	These documents describe the setup procedures for ACF2 and provide evidence the setup procedures were followed.
ALC_CMC.4 Authorizations Controls	MF CM Plan Development MF CM Plan Documentation 2010 STAR_Data_Sets STAR_Transfer	These documents describe and demonstrate the implementation and documentation configuration management.
ALC_CMS.4 CM Scope	CI list bookshelf ACF2 CI List Clarity ACF2 ACF2 EAL ALC_CMC file list 22 november	These documents demonstrate the CM scope of the TOE.
ALC_DEL.1 Delivery Procedures	ALC_DEL_MF Security_Electronic Delivery and Installation CA Mainframe Software Manager Product Guide r3.1	These documents describe product delivery for CA ACF2
ALC_DVS.1 Identification of Security Measures	MF CM Plan Development MF CM Plan Documentation Site inspection (folder with pictures) 2010.10.12 Onsite Assessment Report 11-Backup_Procedure-GIS-2008Jun09 1619-GRC-Global_Security-Pre-employment_Screening-2008Apr05 1621 – GSAP 3649-Access_Procedure-2007Jun29 5725-GRC-BP-C-RIM-Records_Security_and_Confidentiality_Policy-2008May23	These documents define the vendor's organizational security measures and provide verification that these measures are followed.

Component	Document(s)	Rationale
	5727-GRC-BP-C-RIM-Records_Disposal_Procedure-2008May15 5804-Privileged_Access-2008Jun24 7417-Enterprise_Procedure-Privacy_and_Data_Protection-2007Mar06 7705-Inactive_User_Account_procedure-2007Jun29 77260Server_Security_Procedure-2008Jun24 7978-US_Employee_Handbook-NorthAmerica-USA-2008Jul14 ALC_DVS CA Lisle Office_Building Security ALC_DVS Lisle Information Brochure	
ALC_FLR.1 Basic Flaw Remediation	Mainframe Security Flaw Remediation STAR ticket documentation STAR ticket Techsupp_policy	These documents provide the policies for issuing new releases of the TOE as corrective actions.
ALC_LCD.1 Life-Cycle Definition	5153-Project_360_Reference_Guide-2008Jul25	This document provides the life-cycle definition of the TOE.
ALC_TAT.1 Tools and Techniques	ALC_TAT[1].1 Overview updated 23 november Assembler Reference Summary	These documents describe the tools and techniques used in the development of the TOE.
ASE_CCL.1 Conformance Claims	CA ACF2 for z/OS r14 Security Target v1.1	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	CA ACF2 for z/OS r14 Security Target v1.1	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	CA ACF2 for z/OS r14 Security Target v1.1	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	CA ACF2 for z/OS r14 Security Target v1.1	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Security Requirements	CA ACF2 for z/OS r14 Security Target v1.1	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	CA ACF2 for z/OS r14 Security Target v1.1	This document describes the security problem definition of the Security Target.
ASE_TSS.2 TOE Summary Specification	CA ACF2 for z/OS r14 Security Target v1.1	This document describes the TSS section of the Security Target.

Component	Document(s)	Rationale
ATE_COV.2 Analysis of Coverage	ACFXREF Utility %CHANGE Test Plan BaseOmvs Test Plan Database Recovery Test Plan MLS Test Plan Reports & Utilities Test Plan Scope Test Plan SuperUserGranularity Test Plan CICS Test Plan CPF Test Plan Dataset Access Test Plan HLI Test Plan IMS Test Plan IPL Test Plan Operator Cmds Test Plan Program Pathing Test Plan Resource Test Plan Tso Sys Entry Test Plan CTADU Certificate Test Plan Kerberos Test Plan LDS Test Plan MVUID Test Plan Passticket Test Plan Password Enhancements Test Plan Password Enhancements Continued Password Global Test Plan Password History Test Plan PSWD MIX SIM Test Plan PWPHRASE Test Plan ACF2_Jes2 Tests	These documents demonstrate functional test coverage for the TOE.
ATE_DPT.2 Testing: Security enforcing modules	CA ACF2 Functional Specification CA ACF2 TOE Design Specification CA ACF2 Low Level Design Specifications ACFXREF Utility %CHANGE Test Plan BaseOmvs Test Plan Database Recovery Test Plan MLS Test Plan Reports & Utilities Test Plan Scope Test Plan SuperUserGranularity Test Plan CICS Test Plan CPF Test Plan Dataset Access Test Plan HLI Test Plan IMS Test Plan IPL Test Plan Operator Cmds Test Plan Program Pathing Test Plan Resource Test Plan Tso Sys Entry Test Plan CTADU Certificate Test Plan	These documents demonstrate depth of functional testing.

Component	Document(s)	Rationale
	Kerberos Test Plan LDS Test Plan MVUID Test Plan Passticket Test Plan Password Enhancements Test Plan Password Enhancements Continued Password Global Test Plan Password History Test Plan PSWD MIX SIM Test Plan PWPHRASE Test Plan ACF2_Jes2 Tests	
ATE_FUN.1 Functional Testing	System Configuration (folder) ACFXREF Utility %CHANGE Test Plan BaseOmvs Test Plan Database Recovery Test Plan MLS Test Plan Reports & Utilities Test Plan Scope Test Plan SuperUserGranularity Test Plan CICS Test Plan CPF Test Plan Dataset Access Test Plan HLI Test Plan IMS Test Plan IPL Test Plan Operator Cmds Test Plan Program Pathing Test Plan Resource Test Plan Tso Sys Entry Test Plan CTADU Certificate Test Plan Kerberos Test Plan LDS Test Plan MVUID Test Plan Passticket Test Plan Password Enhancements Test Plan Password Enhancements Continued Password Global Test Plan Password History Test Plan PSWD MIX SIM Test Plan PWPHRASE Test Plan ACF2_Jes2 Tests acf2 r14 beta1 checklist acf2 r14 beta2 checklist	These documents demonstrate the format of functional testing and provide evidence of its completeness
ATE_IND.2 Independent Testing – sample	Booz Allen Hamilton Independent Functional Test Plan ACF2 System Configuration Test Output (folder) Test Recordings (folder)	These documents outline the tests the evaluators executed to verify the correctness of the functional testing as well as the state of the system prior to the testing. They also provide evidence of the data reviewed during independent functional testing to demonstrate that the

Component	Document(s)	Rationale
		tests completed appropriately.
AVA_VAN.3 Focused Vulnerability Testing	Booz Allen Hamilton Vulnerability Test Plan Test Batch Jobs Wireshark Trace Test Output (folder)	These documents outline the vulnerability research performed and the tests which were used in order to attempt to tamper with or bypass the operational TOE. It also contains a record of the specific batch jobs run to complete the testing as well as the system outputs of these test activities.

Table 10-4: Assurance Requirements Evidence